Offline Signature Verification and Identification Using Angle Feature and Pixel Density Feature And Both Method Together

Rahul Verma, D.S. Rao

Abstract- Today the human signature of a person is used as an identification of person because we are all know that the each person has distinct signature and every signature has its own physiology or behavioral characteristics. So the human signature used as a identification of person in various work like bank checks etc. The fraud person can easily generated the signature instead of unique signer in fraud way so we need a signature identification system. The signature identification can be done either offline or online manner. Here we used the image processing technique for offline signature identification here no dynamic feature are available in offline identification. Neural network is used as a classifier for this system. Here we propose an intelligent neural network that work on the feature like pixel density method, angular method and mix both methods together. And compared these methods and see that which one method is provides the better result and accuracy.

Index Terms-, Angle method, FAR, FRR, Neural Network, Pixel Density.

I. INTRODUCTION

The purpose of our research is to develop a system that automatically classifies handwritten signature images as authentic or fraudulent, with as little misclassifications as possible. At the same time, the processing requirements must be feasible so as to make the adoption of such an automated system economically viable. For human identification, the usage of biometrics is obvious and important in on a daily basis routine. Human signature are used every day for the identification of a person in various work like for processing Bank checks etc., along with the signature it is also required to verify that the signature on the paper is signed by the genuine signer or a forgery signature. So we need a verification system for detecting forgeries signature.

Signature is a behavioral biometric As such one's signature may change over time depending upon his her mood, health, etc. the computerize image is available in offline signature verification so the offline signature verification is important than online signature verification

Broadly speaking, signatures can be classified as,

1. *Simple Signatures:* These are the ones where the person just writes his or her name

2. *Cursive Signatures:* These are the ones that are written in a cursive way

3. *Graphical Signatures:* The signatures can be classified as graphical when cursive signatures depict geometric patterns

The signature verification can be classified into two types, online signature scheme and offline signature schemes:

Online signature schemes the data is received through sensors. The data obtained is usually active data which includes the speed, acceleration, pressure, tip pressure, gradient etc. These data are usually intra-person invariant that is they usually remain constant for a particular person. So this type of signature verification is highly reliable and offers a high degree of accuracy. However the basic shortcoming in this practice is the availability and costs involved in the procurement of highly sensitive instruments used for obtaining and analyzing the data. These constraints limit the usage of online identification. Online identification can easily be extended to various other domains like iris identification, finger print analysis, palm print analysis and retina analysis.

The Offline signature verification systems are based on the use of computer image processing and pattern recognition techniques to solve the different types of problems encountered in pre-processing. Offline analysis schemes involve extraction of passive data, the data which is obtained after the imprint is obtained by various third party hardware like cameras and scanners in a digital format. These methods are usually cost effective; however they lack the basic active information which could have been obtained from other active devices. The static information derived in an off-line signature verification system may be global, structural, geometric or statistical.

Signature Recognition: Biometric identification by automatically scanning a persons signature and matching it electronically against a library of known signature The four legal properties of a handwritten signature are brief stated below

1. *Authentication of the signer:* a handwritten signature allows positive verification of the signer's identity

2. *Acceptance:* the Signature conveys willful intent and acceptance of the terms stated in the document.

3. *Integrity:* the signature establishes the integrity of the signed document, indicating that it has not been altered in any way.

4. *Non-Repudiation:* the accumulated affect of the above three factors promises such a high degree of purpose that the signer cannot deny he or she has signed.

A. *Motive*

The motivation behind our project is the growing need for a full proof signature verification scheme which can guarantee maximum possible security from fake signatures. The idea behind the project is also to ensure that the proposed scheme can provide comparable and if possible better performance than already established offline signature verification schemes. The prospect of minimizing the memory space for storing signature image by the preprocessing extracted feature

Manuscript received on April,2013.

Rahul Verma Computer Science and Engineering Department, Indore Institute of Science and Technology, Indore, India.

Dr. D.S. Rao, Computer Science and Engineering Department, Indore Institute of Science and Technology, Indore, India.

and the training is completed in acquiring less time and provide better accuracy.

The need to make sure that only the right people are authorized to access high-security systems has paved the way for the development of systems for automatic personal authentication.

B. Offline Signature Verification used in different Areas

The handwritten signature has many purposes and meanings. It can be used to witness intentions (e.g. signing of a contract), to indicate physical presence (e.g. signing in for work), as a seal of approval or authorization and as a stamp of authenticity. Thus, numerous applications for the off-line signature verification are available. Described as follows are a few examples of applications for the system.

1. Financial Institutions

Cheques:

Cheques require our signatures as a form of authentication. Unfortunately, due to the large number of transactions for cheques regularly, it is extremely labor intensive for the banks to examine every single cheque for its signature in great detail to verify its authenticity. This greatly undermines the basic security that consumers expect. Therefore, a potential remedy for this situation is an accurate off-line signature.

Credit Cards:

Another area where off-line signature verification can be put to use is for credit card purchases. With the prolific use of credit cards, the number of transactions per day can be very large, amounting to huge amounts of monetary transactions based merely on signatures without close scrutiny. With a static signature verification system, this can add security to the current system. Furthermore, credit card purchases are becoming digitized One Introduction with the customer just having to sign on an electronic gadget. Unfortunately, this gadget does not check for the authenticity of the customer. It merely acts as a means of obtaining the customers‟ information quickly. However, this gadget can be a stepping-stone for the implementation of a signature verification system since the signatures are captured in the digital form, which makes the identification process more convenient.

II. CHARACTERISTICS OF SIGNATURE

The automatic offline signature verification system, signature must be treating as an image and extracting features from the image. Signature is a special case of handwriting that can be considered as an image. Signatures of a person may be different in shapes and size and it is difficult for a human being to separate a genuine signature from the forged one by only visual analysis of the signatures. Signatures may be simple like a signer writes his name in a simple way, cursive when written in cursive way or graphical that contents some geometric patterns. Before modeling such system some essential characteristics are keep in mind like:

1. *Invariant:* It should not change with the time.
2. *Uniqueness:* It must be unique to the individual.
3. *Inimitable:* Signature may not be produced by other means.
4. *Reducible and comparable:* Capable of being convert in the format that is easy to store or handle and also easily comparable with the others.
5. *Singular:* It must be unique to the individual.
6. *Reliable and Tamper-resistant:* It should be impractical to mask or manipulate.

The various physiological characteristics that satisfy the above requirements are face, hand geometry and the behavioral characteristics that include signature, voice and keystroke pattern.

The various types of forgery include:

***1.** Random Forgeries*

Random forgery is done by a person who doesn’t know the shape and structure of the original signature.fig 1(b) It is produced when the signer knowing the name of the victim and produced signature in his own style. This type of forgery may constitute random pen strokes and is usually easy to detect. For experimental purposes, genuine signatures from writers other than the legitimate owner are commonly used to represent random forgeries. This forgery is easily detected by the visual analysis.

2. Simple Forgeries

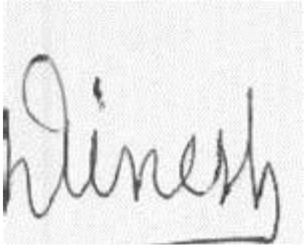
In this type of forgery the person concerned has a vague idea of the actual signature, but is signing without much practice. And It is produced when the signer copy the signature in his own style without having any previous experience. Simple forgeries, the forger’s knowledge is restricted to the name of the signatures owner. Due to the arbitrary nature of signature design, simple forgeries may in some cases bear an alarming resemblance to the writer’s genuine signature. fig 1(c)

3. Skilled Forgeries

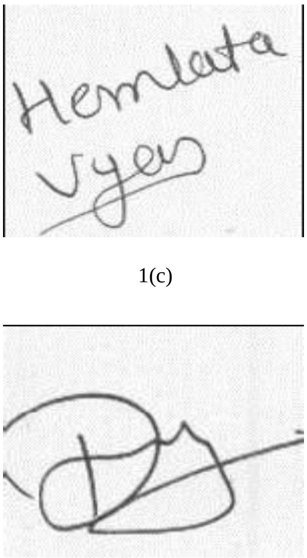
This type of forgery considers appropriate knowledge about the original signature along with ample time for proper practice. Our proposed scheme eliminates random and simple forgeries and also reduces skilled forgery to a great extent. The forger is not only familiar with the writer’s name, but also has access to samples of genuine signatures. Given ample time to practice signature reproduction, he is able to produce so-called skilled forgeries.

Skilled forgeries are undoubtedly the most difficult to detect, especially by untrained humans. As the production of a skilled forgery involves both planning and effort, similar effort is required to enforce sufficient countermeasures - typically a sophisticated automatic signature verification system.fig 1(d)

1(a)



1(b)



1(c)

1(d)

Fig:1 show (a). Original Signature (b). Random Forgery (c). Simple Forgery (d). Skilled Forgery

III. PROPOSED SYSTEM

There are three approaches used in this paper for feature extraction. First one is ‘The Angular method’ and the second is ‘The Energy density Method’. We used preprocessing algorithm because database extracted from the contour obviously will acquire more memory as compared to the preprocessed image. Also the proposed angular and pixel density method is developed the signature verification system which improved the accuracy and memory and time taken by training. And also increase false rejection ratio (FRR).and decrease false rejection ratio (FAR.).

Signature is a special arrangement of symbols, characters, etc., and may be simple, cursive or geometric. Generally the static feature *i.e.*, the image of the signature is available for the verification and authentication of a genuine person because it is not possible everywhere to capture the dynamic feature. So here we propose a system that works on the static features. The static features that consider of the signature for modeling an offline verification system are an Angular feature in the combination of the pixel density feature which extract locally and the feed forward back propagation neural network use as a classifier. Aspect ratio is also included as a global feature in pixel density method.

In this used major module:

1. *Data Acquisition* The data for the offline signature verification system may be acquire from various ways like by optical pad ,scanner etc. here for making the data base we collect the samples of signature written on the white paper by using the black/ blue pen.

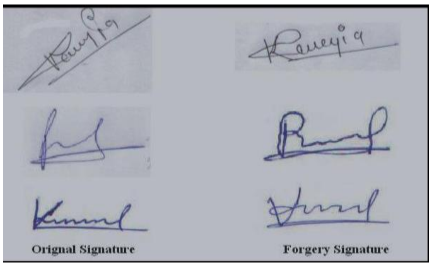
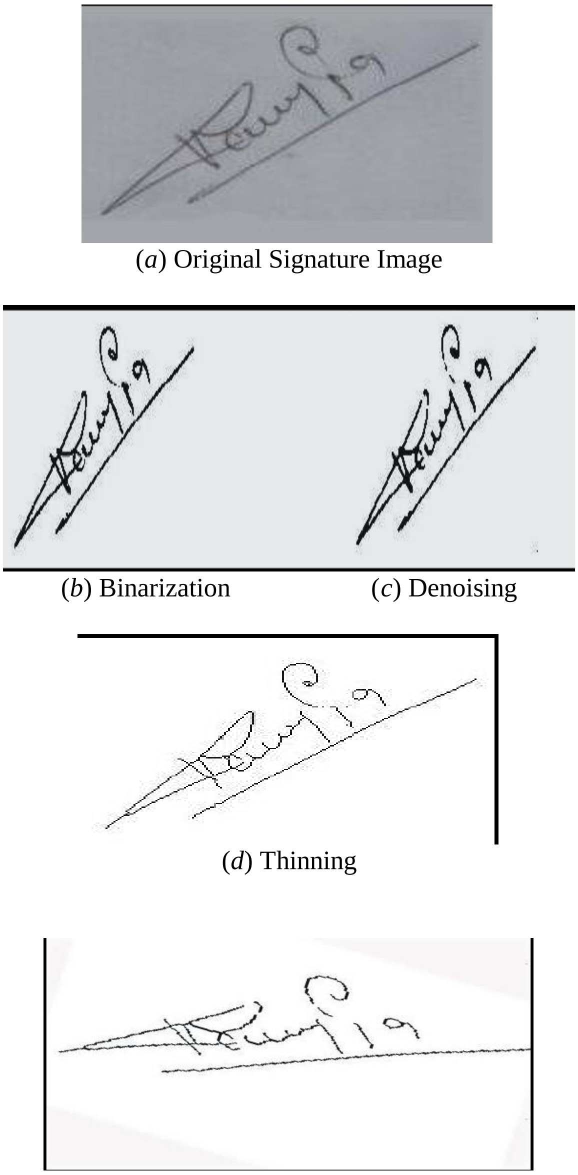


Fig 2 show collection of database

2. *Preprocessing* Before processing the image for feature extracting some preprocessing algorithm are applied on the scanned image like Binarization, Denoising, Thinning algorithm because thin image required less storage memory as compared to original image also skew removal .Shown in Fig. 3



(*a*) Original Signature Image

(*b*) Binarization (*c*) Denoising

(*d*) Thinning

(*e*) Skew Removal

3. Feature Extraction

It is the important part were we decide which portion or part or characteristics are extracted those are useful for our system and on which the designed system give optimum result. For the proposed system the features which are extracted are The Energy density of the signature and The Angle feature of the signature.

(*a*) *Pixel Density*

Energy density is defined as the total energy present in each segment which is used as a local feature. In this method the image is divided in various segments and energy Density of each segment [14] is calculated by counting the total number of once i.e., total no of white pixels in a segments. In the proposed system the signature image is segmented in to the 4 equal parts and calculating the number of ones in each of them. Also we are considering the Aspect ratio which is used as a global feature but here we normalize it for all segments. Aspect ratio is the ratio of Height (maximum vertical distance) to length (maximum horizontal distance) of the signature. We have calculated it after skew removal. Thus, we have a feature vector of size 1*4 for a single signature image and it is used as a final database in an energy density method. For 100 signature image we have feature vector of size 100*4. This final database is fed to the neural network to perform the desired function *i.e.* training or classification as shown in Fig4.

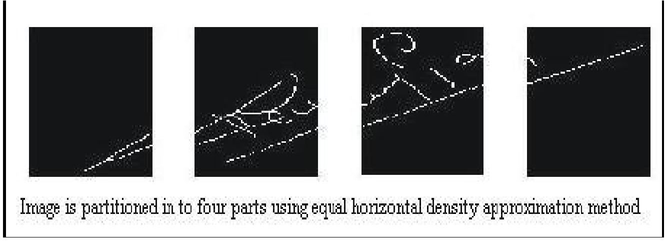


Image is partitioned in to four parts using equal horizontal density approximation method

(b)*Directional feature*

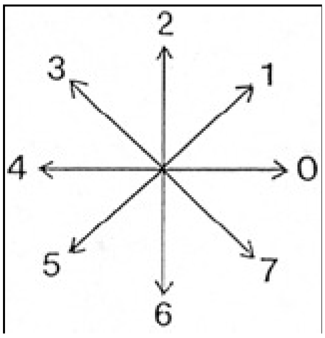


Fig. 3. 8 Connectivity of a Pixel

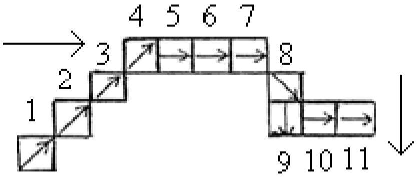


Fig. 3. Direction Changes in a Part of a Signature

Chain-code is based on the direction of the connecting pixels. Each pixel is observed for next connected pixel and their direction changes mapped by giving a numerical value to every possible direction. There are generally 8 connectivity is taken into consideration as shown in the Fig. 2. But in this paper we have used 4 connectivity i.e. 0, 1, 2 & 3. As another 4 directions i.e. 4, 5, 6 & 7 are simply the negation of 0, 1, 2 & 3 directions. To obtain chain-code top left corner is considered as origin and scanning is done left to right, top to bottom (refer Fig. 3). Each pixel has observed separately and direction vector for that pixel is noted down. This process is carried out until the last pixel has scanned. Now, the frequency of occurrence in a particular direction is calculated for each segment and the histogram for each segment is used it to train the neural network.

(*b*) *Angle Feature*

In this method first the Pre-processing image is resized and partitioned into four portion or cell using the equal horizontal method after that each partition(cell) are divided in to 3 row and 3 column of equal size so we have total nine sub cell of each cell. After that consider the sub cell one by one and calculate the angle of each with pixels by considering the bottom left corner after that calculate the mean value of the angles this process is repeat for all the sub cells. Once the value of angles for each sub cell is found then calculating the mean value from that to determine the value of angle for that cell or partition. This process is repeat for the reaming three partitions, so at the end we have the angle vector of size 1*4. This is given as an input to the neural network. For example the data base used consist 100 signature samples. For one sample we have angle vector of size 1*4 so for all 100 sample we have feature vector of size 100 *4 which is used as a final data base for training the neural network and also for classification. The process of angle calculation is shown in Figs. 5, 6, 7, 8 and 9.

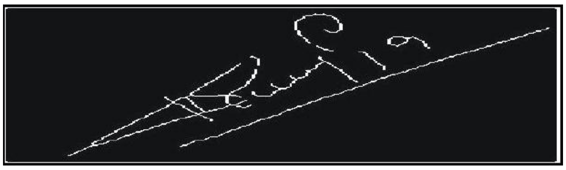


Fig.4. Pre-Processed Signature Image.

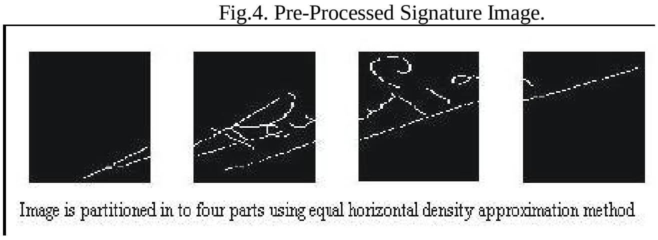


Image is partitioned in to four parts using equal horizontal density approximation method

Fig.5

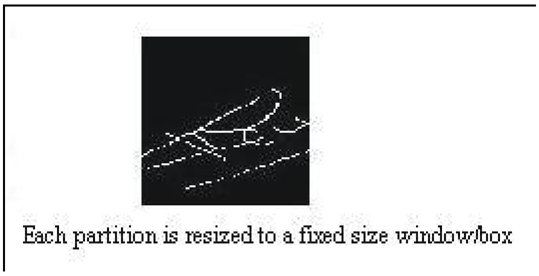


Fig.6

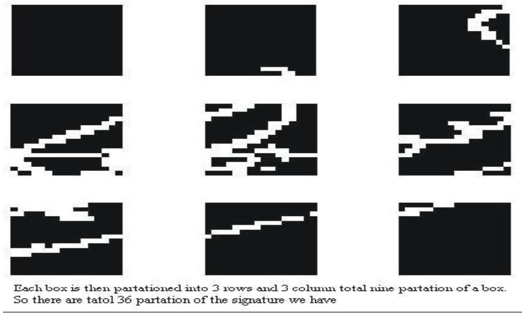

Each box is then partationed into 3 rows and 3 column total nine partation of a box.
So there are tatol 36 partation of the signature we have

Fig.7

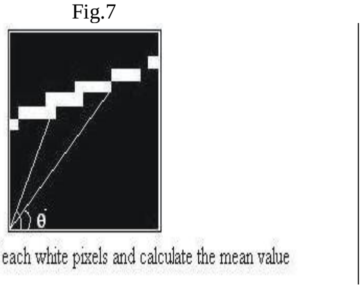

θ
Finding the angle of each white pixels and calculate the mean value

Fig.8

IV. PROCESS OF OFFLINE SIGNATURE VERIFICATION

In the verification stage, a signature to be tested is preprocessed and feature extraction is performed on pre processed test signature image as explained in 2.2 to obtain feature vector of size 60. After normalizing a feature vector it is fed to the trained neural network which will classify a signature as a genuine or forged.

Algorithm

Below gives algorithm for the offline signature verification system in which neural network is used for verifying the authenticity of signatures.
Input: signature from a database
Output: verified signature classified as genuine or forged.
1. Retrieval of signature image from database.
2. Preprocessing the signatures.
   2.1 Converting image to binary.
   2.2 Image resizing.
   2.3 Thinning.
   2.4 Finding bounding box of the signature.
3. Feature extraction
   3.1 Extracting features using angle.
   3.2 Extracting features using pixel density.
4. Creation of feature vector by combining extracted features Obtained from horizontal and vertical splitting.
5. Normalizing a feature vector.
6. Training a neural network with normalized feature vector.
7. Steps 1 to 5 are repeated for testing signatures.
8. Applying normalized feature vector of test signature to Trained neural network.
9. Using result generated by the output neuron of the neural network declaring signature as genuine or forged.

V.IMPLEMENTATION

This part is subdivided divided into two phases first one is the network design and the second one is the classification using network. During the network design phase the neural network is prepared and trained for doing the classification using network work with optimum accuracy and during the classification using network phase the proposed system takes the signature (signature image) and check whether the image given to the input is a genuine or the forged one by comparing with the database. The system can be broadly categorized on the basis of method used for pre-processing and feature extraction from the image database and final input given to the neural network.

During the network design phase the data base is first prepared gathered which consist of 50 genuine and 50 forged signature of an individual person. (i.e. 1000 Signature Samples) and digitized using scanner and perform the preprocessing techniques like Binarization which produce binary image i.e. to convert colored (if any) image in black& white (i.e. in 0 or 1) format, Noise removal or Filtering using median filter, Thinning by Morphological operations (in MATLAB). Skew removal is carried out by the concept of trigonometry. Then the pre-processed image is used for features extraction as stated above. The features that are extracted are the angle feature and the energy density feature (as a local feature) also aspect ratio as a global feature. Once the features are extracted the data base is fed to the neural network for network design and classification using network.

A. Neural Network

any neural network the output layer consists of a single neuron that gives the degree of confidence of the genuineness of the signature presented to the net. The degree of confidence range from 0 to 1. With '0' meaning absolutely confident of the signature being forged and '1' meaning absolutely confident of it being genuine. The proposed architecture of back propagation feed forward neural network is as shown in Fig. 10

The proposed ANN scheme uses a multi layer feed forward network employing a back propagation learning algorithm.

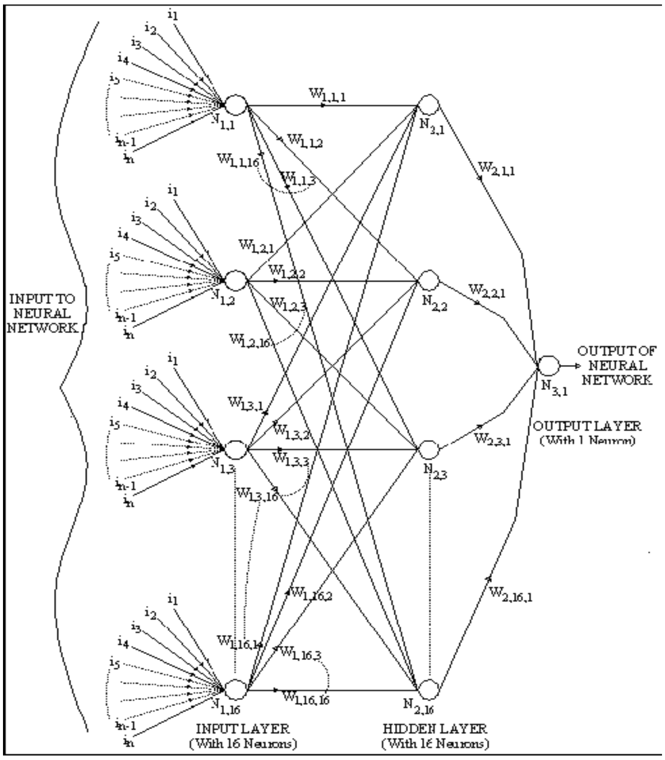


Fig. 10. Proposed Network.

VI. RESULT AND COMPARISON

Now during classification or verification phase the performance is calculated on the basis of FRR, FAR and on the basis of time and also the result obtained from the proposed technique (Angle feature with pixel density) is compared with basic Angle Feature Method or With Basic Pixel Density Method as shown in Table 1-4.

TABLE 1: COMPARISON ON THE BASIS OF TIME REQUIRED FOR TRAINING

SR No.	**No. of Taining Samples (50% Genuine + 50% Forgery)**	**Result**		
		Elapsed Time (in Sec.) (PIXEL Density Method)	**Elapsed Time (in Sec.) (Angle feature only)**	**Elapsed Time (in Sec.) (Mix both Method)**
1	*00o,50f*	*5.561*	6.562	8.001
2	*10o,40f*	*6.673*	7.73	8.32
3	*20o,30f*	*6.328*	*8.331*	*9.124*

4	*30o,20f*	*7.065*	*9.948*	11.22
5	*40o,10f*	*7.680*	*8.439*	8.330
6	*50o,00f*	*6.987*	*8.782*	9.458
7	*50o,50f*	*6.452*	*8.574*	9.532

TABLE 2: COMPARISON ON THE BASIS OF ACCURACY

SR No.	**No. of Taining Samples (50% Genuine + 50% Forgery)**	**Result**		
		Accuracy (in Sec.) (PIXEL Density Method)	**Accuracy (in Sec.) (Angle feature only)**	**Accuracy (in Sec.) (Mix both Method)**
1	*00o,50f*	*57*	65	70
2	*10o,40f*	*61*	67	72
3	*20o,30f*	*64*	*70*	75
4	*30o,20f*	*70*	*78*	87
5	*40o,10f*	*74*	*79*	90
6	*50o,00f*	*79*	*82*	92
7	*50o,50f*	*80*	*85*	95

Table 3: COMPARISON ON THE BASIS OF FAR

SR No.	**No. of Taining Samples (50% Genuine + 50% Forgery)**	**Result**		
		FAR (in Sec.) (PIXEL Density Method)	**FAR (in Sec.) (Angle feature only)**	**FAR (in Sec.) (Mix both Method)**
1	*00o,50f*	*44*	42	17
2	*10o,40f*	*43*	46	14
3	*20o,30f*	46	48	04
4	*30o,20f*	33	30	00
5	*40o,10f*	32	28	00
6	*50o,00f*	28	27	00
7	*50o,50f*	26	25	00

TABLE 4: COMPARISON ON BASIS OF FRR

SR No.	**No. of Training Samples (50% Genuine + 50% Forgery)**	**Result**		
		FRR (in Sec.) (PIXEL Density Method)	**FRR (in Sec.) (Angle feature only)**	**FRR (in Sec.) (Mix both Method)**
1	*00o,50f*	*42*	25	30
2	*10o,40f*	*12*	17	20
3	*20o,30f*	20	22	10
4	*30o,20f*	10	8	8
5	*40o,10f*	22	16	8
6	*50o,00f*	11	7	5
7	*50o,50f*	18	5	00

VII. CONCLUSION

The proposed method can be used as a effective signature verification system. The proposed method was successfully made the offline signature verification with improve the efficiency and accuracy and easily can detected the skilled forgeries. It uses a compact and memory efficient storage of feature points which reduces memory overhead. And from the analysis of the above result tables we found that the feature extraction method angle feature method give the better improved efficiency and accuracy and provides better FAR and FRR and taking little extra time from the Pixel density method. And when we use both method together that it can gives better accuracy among the angle and Pixel density and it also improved the FRR and FAR and takes extra time for training.

ACKNOWLEDGEMENT

We are very thankful to the DEAN Dr. D.S. RAO Indore Institute Of Technology, and all faculty members of IIST, Indore for their constant support an motivation.

REFERENCES

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

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

[3] Deepthi Uppalapati, "Integration of Offline and Online Signature Verification systems," Department of Computer Science and Engineering, I.I.T., Kanpur, July 2007.

[4] Debasish Jena1, Banshidhar Majhi2, Saroj Kumar Panigrahy3, Sanjay Kumar Jena4" Improved Offline Signature Verification Scheme Using Feature Point Extraction Method"orisa ,india.

[5] Prabit Kumar Mishra Mukti Ranjan Sahoo " Offline Signature Verification Scheme" national institute of technology, rourkela.

[6] R. Abbas, "Back propagation Neural Network Prototype for off line signature verification", thesis Submitted to RMIT, (2003).

[7] L. Ravi Kumar, A.Sudhir Babu "Genuine and Forged Offline Signature Verification Using Back Propagation Neural Networks" International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1618-1624.

[8] Ashwini Pansare, Shalini Bhatia "Off-line Signature Verification Using Neural Network" International Journal of Scientific & Engineering Research, Volume 3, Issue 2, February-2012 1 ISSN 2229-5518.

[9] Minal Tomar and Pratibha Singh "A Directional Feature with Energy based Offline Signature Verification Network" International Journal on Soft Computing (IJSC), Vol.2, No.1, February 2011.

[10] Ismail A. Ismail , Mohamed A. Ramadan "An Efficient Off-line Signature Identification Method Based On Fourier Descriptor and Chain Codes" International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010.

[11] S. Pinge, H. Kekre, " Signature Identification using Neural Networks", Proceedings of National Conference on Image Processing (2005) (NCIP 2005), Organized by TSEC, Mumbai, pp 31-39.

[12] M. Blumenstein and B. Verma, "An artificial neural network based segmentation algorithm for off-line handwriting recognition".

[13] Rahul Sharma , manish shrivastav "an offline singnature verification using neural network based on angle and energy density"i*nternational Journal on Emerging Technologies* **2**(2): 84-89(2011)

[14] Jamal Fathi and Abuhasna, "Signature recognition using conjugate gradient neural network".