DEVELOPMENT OF INTELLIGENT NETWORK FOR OFFLINE SIGNATURE VERIFICATION USING PIXEL DENSITY, DIRECTIONAL METHOD AND BOTH METHOD TOGETHER

Deepak Tiwari[1] and Bhawana Sharma[2]

[1]DEPARTMENT OF COMPUTER SCIENCE, STUDENT, AMITY UNIVERSITY RAJASTHAN JAIPUR, INDIA
dee769@gmail.com
[2]DEPARTMENT OF COMPUTER SCIENCE, LECT. IN AMITY UNIVERSITY RAJASTHAN JAIPUR, INDIA
bhawana2104@gmail.com

ABSTRACT **-Today signature verification are used in various places for authentication and security purpose .Every signature or signed identified each person physiological or behavioral characteristic. Signature matching is very important in this time because any person can generated another person signature in fraud way. So systems have need for verification of the signature. The signature verification can be done either offline or online signature matching techniques and in this paper we apply offline signature matching technique. Here we propose an intelligent neural network that work on the feature like pixel density method, directional method and mix both method together .and compared both the result and which of the best. Which Accuracy, Performance, FAR, FRR are best.**

KEYWORDS -Neural Network, FRR, FAR, pixel density method, directional method.

I. INTRODUCTION

Signature has been an individual feature for person recognition. Yet nowadays rising number of dealings especially related to financial and business are being authorized via signatures. Signature may be used as a biometrics as every signature is separate. As signature has already used and accepted as an identification of the person who signed in so many systems, it is important to intensely watch the signature before having any execution about the signee. Signature verification is an important research area in the field of personal authentication and security The purpose of the signature verification system is to differentiate between two classes: the original and the forgery, which are related to intra and interpersonal changeability. The variation among signatures of same person is called Intra Personal Variation. The variation between originals and forgeries is called Inter Personal Variation..

Signature verification is so different with the character identification, because signature is often illegible, and it seem it is just an image with some particular curves that represent the writing style of the person. Signature is just a special case of handwriting and often is just a symbol. So it is knowledge and necessary to just deal with a signature as a complete image with special distribution of pixels and representing a particular writing style and not as a collection of letters and words [5].

Approaches to signature verification fall into two categories according to the acquisition of the data: On-line and Off-line.

On-line data records the motion of the stylus (which is also part of the sensor) while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time. Online systems use this information captured during acquisition. These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive [1].

Off-line data is a 2-D image of the signature. Processing Off-line is complex due to the absence of stable dynamic characteristics. Difficulty also lies in the fact that it is hard to segment signature strokes due to highly stylish and unconventional writing styles. The nature and the variety of the writing pen may also affect the nature of the signature obtained. The non-repetitive nature of variation of the signatures, because of age, illness, geographic location and perhaps to some extent the emotional state of the person, accentuates 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 [1][2][3].

We approach the problem in two steps. Initially the scanned signature image is preprocessed to be suitable for extracting features[2]. Then the preprocessed 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.

Signature Recognition*:* Biometric identification by automatically scanning a person’s 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 effect of the above three factors promises such a high degree of purpose that the signer cannot deny he or she has signed.

Handwritten signatures are of different shapes and sizes and the variations in them are so immense that it is difficult for a human being to distinguish a genuine signature from a forged one by having a glance at the signature. There are different types of signatures used in real life. 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

Automated recognition of handwritten signatures became imperative when it was difficult to distinguish genuine signatures from simulated forgeries on the basis of visual assessment. This led to computer recognition of handwritten signatures, which though a bit slow, is more reliable and efficient.

A. *Motivation*

The motivation behind the 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.

There may be a case where the type of verification system used for training differs from classification using network. Though the test sample is of a genuine person, it might not be possible to prove with either of these systems alone.

B. *Research Objectives*

Signature verification is an important research area in the field of personal authentication. The recognition of human handwriting is important concerning about the improvement of the interface between human-beings and computers [1, 8]. If the computer is intelligent enough to understand human handwriting it will provide a more attractive and economic man-computer interface. In this area signature is a special case that provides secure means for authentication, attestation authorization in many high security environment. The objective of the signature verification system is to discriminate between two classes: the original and the forgery, which are related to intra and interpersonal variability [1]. The variation among signatures of same person is called Intra Personal Variation. The variation between originals and forgeries is called Inter Personal Variation.

Our work is concerned with the techniques of off-line signature verification. The static information derived in an off-line signature verification system may be global, structural, geometric or statistical. We concern with offline signature verification which is based on geometric centre and is useful in separating skilled forgeries from the originals. The algorithms used have given improved results as compared to the previously proposed algorithms

C. *.Applications of Off-Line Signature Verification*

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 [7]. 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 daily, it is extremely labour 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

verification system. A practical implementation of the system for a cheque verification application has been built

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. BACKGROUND AND RELATED WORK

A. Introduction

A signature is treated as an image transport a certain pattern of pixel that relate to a specific individual signature verification problem , therefore is concerned with examining and formative whether particular signature truly belongs to a person or not. signature verification is a different pattern recognition problem as two genuine signature of a person are precisely the same the difficulty also sterns from the fact that skilled forgeries follow a genuine pattern unlike fingerprint which vary widely for two different person. signature verification can be divided into two classes, namely, off- and on-line verification.

Off-line or static signatures are scanned from paper documents, where they were written in conventional way. Off-line signature analysis can be carried out with a scanned image of the signature using a standard camera or scanner In off-line verification system, only static features are considered which rely purely on the signature's image but require less hardware.

On-line signature verification methods have proved to be more accurate than off-line methods [11], [13] yet off-line signature verification systems are required when the signatory is not present at the verification stage as may be required for verifying signatures on bank cheques.

As compared to on-line signature verification systems, off-line systems are difficult to design as many desirable characteristics such as the order of strokes, the speed and other dynamic information are not available in the off-line case. The verification process has to wholly rely on the features that can be extracted from the trace of the static sign [2].

III. SIGNATURE CHARACTERISTICS

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 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. So for making 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. There is a growing interest in the area of signature recognition and verification (SRVS) since it is one of the important ways to identify a person.

Recognition is finding the identification of the signature owner. But 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[3].

The various types of forgery include [4] :

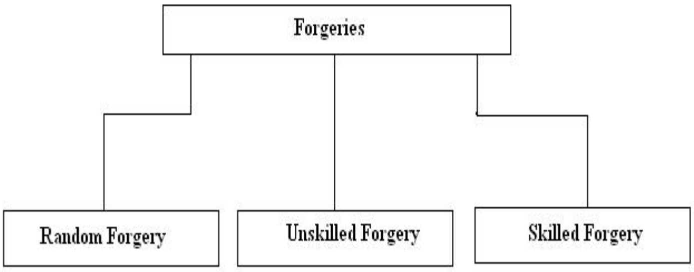


Fig 1 Types of Forgery

1. ***Random forgeries***

Random forgeries encompass any arbitrary attempt at forging a signature, generally without prior knowledge of the owner's name. 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.

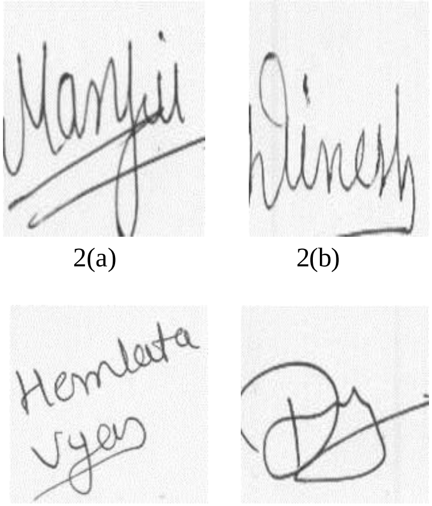
2. *Simple Forgery*

In the case of simple forgeries, the forger's knowledge is restricted to the name of the signature's 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. In such cases, more sophisticated systems, able of detecting subtle stylistic differences, are required in order to distinguish between genuine signatures and forgeries of this type..fig 2(c)

3. *Skilled Forgery*

In some instances, 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.



2(a) 2(b)

2(c) 2(d)

Fig: 2 show (a). Original Signature (b). Random Forgery (c). Simple Forgery (d). Skilled Forgery

IV. PROPOSED APPROACH

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 directional 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. There are three approaches used in this paper for feature extraction. First one is 'The pixel Density method' and the second is 'The Directional Feature Method'.. Also a comparative statement between the simplest pixel density method, Directional Feature method and obviously the proposed mix both method developed so that it may be clear that is it worth to improve the accuracy on the cost of memory and time? and also increase false rejection ratio (FRR).and and decrease false rejection ratio(FAR.).

In this used major module:

1. *Database Management.* This module handle the process of data acquisition and the maintenance of the signature image and learn feature for each identification number
2. *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. The signature samples are then scanned and then fix in the proper box size. Some typical signatures along with forgery are as shown in Fig. 3.

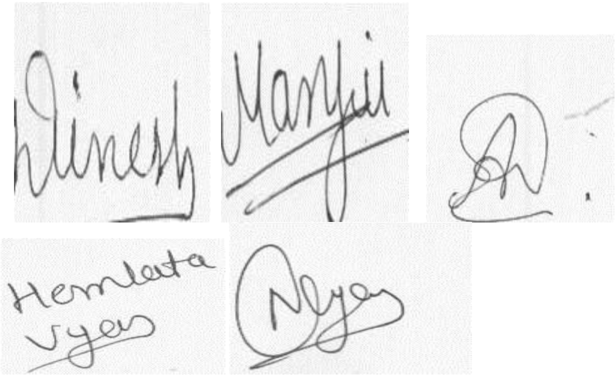


Fig 3 show collection of database

3. *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.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 pixel density of the signature and the directional feature of the signature.

A. *Pixel Density [1]*

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 Fig. 5.

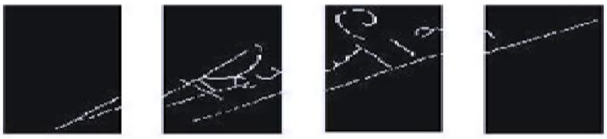


Fig5 Show in the pixel partition in equal segments

B. *Directional Feature [2]*

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 database for training the neural network and also for classification. The process of angle calculation is shown in fig 6,7,8,9,10.

Fig 6 show in Rotation of signature

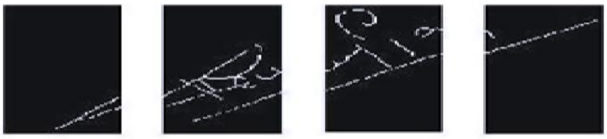


Fig 7Show in divide in equal segments

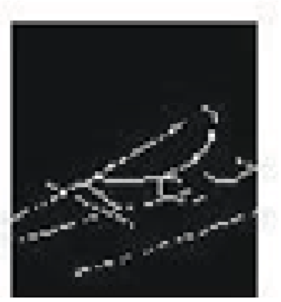


Fig 8 Each partition show a fixed window

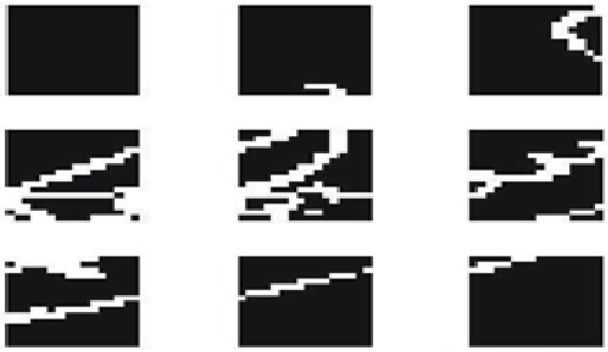


Fig9 Each box these into partition 3 rows and 3colums

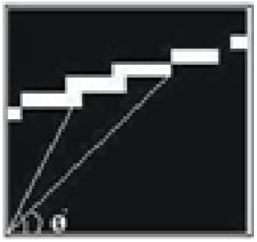


Fig10 Finding angel of white pixels and calculate mean value

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. After that the signature is extracted from the available image and the signature image is again resized. 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. 11

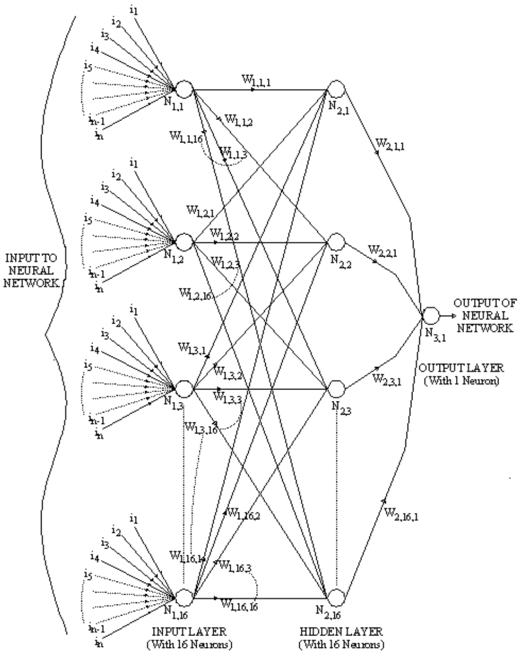


Fig. 11. Proposed Network.

The proposed ANN scheme uses a multi layer feed forward network employing a back propagation learning algorithm with 4 Neurons in input layer and 1 Neuron in output layer. One hidden layer is present with 40 Neurons. The transfer function used for all the three layers are Hyperbolic Tangent Sigmoid (tansig). Total 4 inputs is given to this neural network[2].

VI. RESULTS:

For the proposed neural network based signature verification system the results are calculated on the basis of False Rejection Ratio (FRR), False Acceptance Ratio (FAR) and on the basis of Time.

TABLE I 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.) (Directional 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

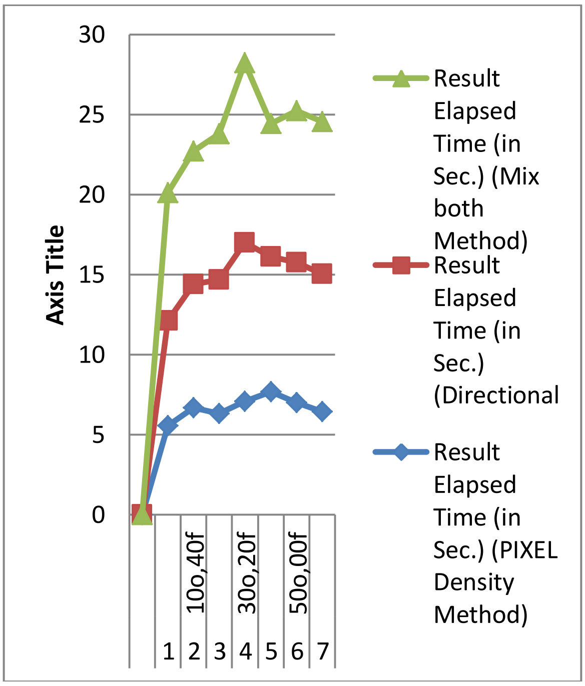


Fig: 12 show the time result of three methods

TABLE II: COMPARISON ON THE BASIS OF ACCURACY

SR NO.	No. of Taining Samples (50% Genuine + 50% Forgery)	Result		
		Accuracy (in%) (Energy Density Method)	Accuracy (in%) (Directional feature only)	Accuracy (in%) (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 III: COMPARISON ON THE BASIS OF FAR

SR NO.	No. of Taining Samples (50% Genuine + 50% Forgery)	Result		
		FAR (in%) (Energy Density Method)	FAR (in%) (Directional feature only)	FAR (in%) (Mix both Method)
1	00o,50f	44	42	17
2	10o,40f	43	46	14
3	20o,30f	46	48	4
4	30o,20f	33	30	0
5	40o,10f	32	28	0
6	50o,00f	28	27	0
7	50o,50f	26	25	0

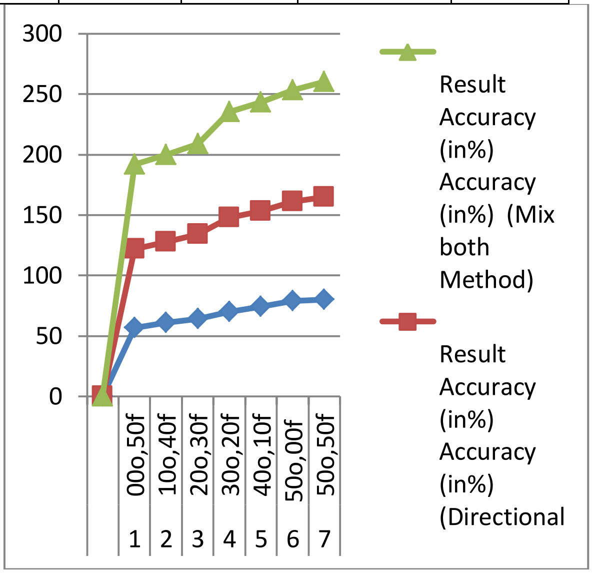


Fig: 13 show the accuracy result of three methods

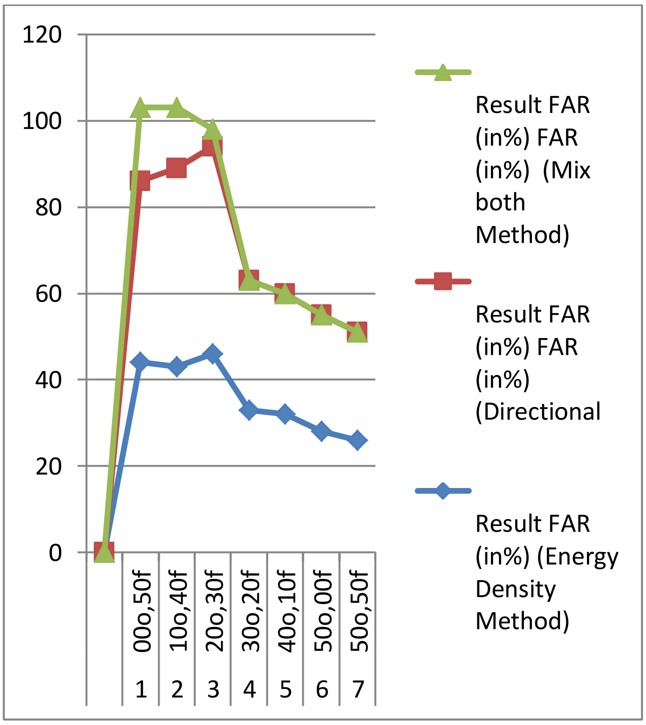


Fig: 14 comparison of FAR

SR NO.	No. of Taining Samples (50% Genuine + 50% Forgery)	Result		
		FRR (in%) (Energy Density Method)	FRR (in%) (Directional feature only)	FRR (in%) (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	3

TABLE IV: COMPARISON ON THE BASIS OF FRR

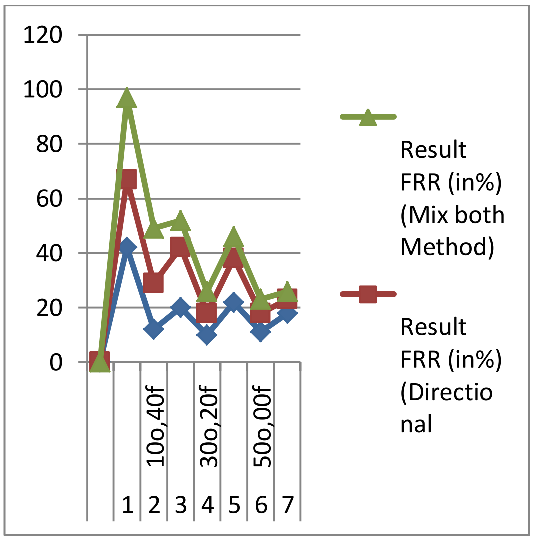


Fig: 15comparison of FRR

VII. CONCLUSION

It is observed from the analysis of the result tables that the directional feature based method of feature extraction for the design of off-line signature verification gives better result than that of pixel density method in terms of accuracy i.e. better FRR and FAR but at the cost of time , the time required for the proposed method is greater than that of basic density method. and I use a both of method together which are better than both or density method . Although time required for network design is slightly greater in case of this proposed method but the accuracy and FAR are satisfactory, and that extra time can be supportable

ACKNOWLEDGEMENTS

We are very thankful to the Miss BHAWANA SHARMA (Department of Computer Science,),,. leturer in Amity University Rajasthan Jaipur, India for their constant support and motivation.

REFERENCES

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

[2] Deepthi Uppalapati, "Integration of Offline and Online Signature Verification systems," Department of

Computer Science and Engineering, I.I.T., Kanpur, July 2007.

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

[4] *Rahul Sharma and Manish Shrivastav"* An Offline Signature Verification System Using Neural Network Basedon Angle Feature and Energy Density*"Department of Electronics and Communication, TIT Bhopal, (MP)*

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