OFFLINE HANDWRITTEN SIGNATURE VERIFICATION USING NEURAL NETWORK

[1] PALLAVI V. HATKAR, [2] PROF.B.T.SALOKHE

[1] Department of Electronics Engineering, TKIET Warana, India
[2] Department of Electronics Engineering, TKIET Warana, India

ABSTRACT : *The different biometric techniques have been discussed for identification. Such as face reading, fingerprint recognition and retina scanning and these are known as vision based identification. There are non vision based identifications such as signature verification and the voice recognition. Signature verification plays a vital role in the field of the financial, commercial and for the legal matters. Signature by any person considered as the approval for any work so the signature is the preferred authentication. In this paper signature verification is done by means of image processing, geometric feature extraction and by using neural network technique.*

INTRODUCTION

The signature of a person is an important biometric attribute of a human being and is used for authorization purpose. Signature plays an important role in financial, commercial and legal transactions, truly secured authentication. It becomes more and more crucial.[1] A signature by an authorized person is considered to be the "seal of approval" and remains the most preferred means of authentication. [2] Various approaches are possible for signature recognition with a lot of scope of research .The handwritten signature is regarded as the primary means of identifying the signer of a written document based on the implicit assumption that a person's normal signature changes slowly and is very difficult to erase, alter or forge without detection.[3] The handwritten signature is one of the way to authorize transactions and authenticate the human identity compared with other electronic identification methods such as fingerprints scanning, face recognition and retinal vascular pattern screening. [4] It is easier for people to migrate from using the popular pen-and-paper signature to one where the handwritten signature is captured and verified electronically. Signatures are composed of special characters and flourishes and therefore most of the time they can be unreadable. Also intrapersonal variations and interpersonal differences make it necessary to analyze them as complete images and not as letters and words put together. [5]

LITERATURE SURVEY:

B. Herbst. J. Coetzer [2] proposed an on-line/dynamic handwritten signature verification system based on Hidden Markov Models that performs human operators in both accuracy and speed. It uses local signature features sampled from an electronic writing tablet after some novel preprocessing steps, and is a fully automated system in that there are no parameters that need to be manually fine-tuned for different users, it attain best equal error rates of between 2% and 5% for different types of high quality deliberate forgeries, and take a fraction of a second to accept or reject an identity claim on a 700 MHz computer.

JunLin Chen[3] proposed verification system based on video. The signature information is obtained from video of camera which is different from traditional online or offline method. Tracking of the pen tip is done using a particle filter and template
matching method. Classification of unknown signature as genuine or forged is done by considering the distance between the unknown signature and the referenced signature with a threshold. The result shows method can track the nonlinear-moved pen tip exactly, can be used for most common pens. System has more potential capability for signature verification.

Martinez, L.E., Travieso[4] proposed the development of online signature verification system using support vector machine (SVM) and VBTablet 2.0 to verify the input signature by comparing database. This may take place by signing directly on to a digitizing tablet by using stylus which is connected to the universal serial bus (USB) port of computer.. The common verification algorithm is one of the global feature vector machine called support vector machine (SVM). The signature is characterized as pen-strokes consisting x-y coordinates and the data will be stored in the signature database in the form of a txt.file.

Vielhauer.c [5] proposed approach to generating biometric hash values based on statistical features in online signature signals. The output of typical online signature verification systems are threshold-based true-false decisions, based on a comparison between test sample signals and sets of reference signals, this system responds to a signature input with a biometric hash vector, which is calculated based on an individual interval matrix. Especially for applications, which require key management strategies, hash values are of great interest, as keys can be derived directly from the hash value.

All these researches stated that in literature review focus on different methods of signature verification. However these methods are having maximum value of AER (Average Error verification Rate). Hence our focus

is to implement the method which is having minimum value of AER, which is obtained by using Neural Network.

PROPOSED METHODOLOGY:-

1] Objective of the Project:-

The main objective is to present a model in which neural network 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 neural network. In verification stage, on test signatures pre-processing and feature extraction is performed. These extracted features are then applied as input to a trained neural network which will classify it as a genuine or forged signature.

Performance of signature verification method can be calculated by using AER i.e. average error verification rate, where AER is average of False Acceptance Rate (FAR), False Rejection Rate (FRR) of the system.

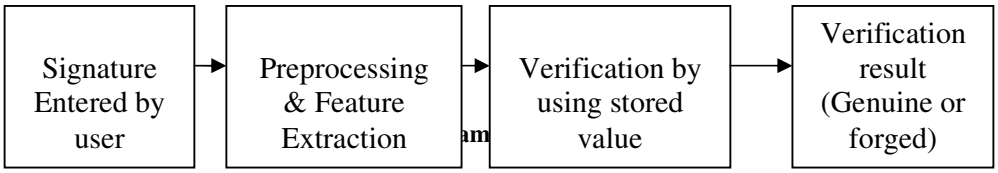
After comparing performance of all four methods

1. Hidden Markov Model (HMM) method achieves an AER of 18.4%.
2. Template matching is having average verification error rate of 18.1%.
3. Support Vector Machines (SVMs) has average verification error rate of 18.0%.
4. Statistical approach has average verification error rate of 17.8%

So to achieve less value of AER Neural network method is used, which is highly suited to modeling global aspects of handwritten signatures.

2] Methodologies of Implementation:-

- **Block Diagram**



Multiple signature of person is stored in database. For probabilistic purpose 1000 signature of person are taken. From the database every signature is retrieved by using MATLAB .The method consists of image prepossessing, geometric feature extraction, neural network training with extracted features and verification. Features are extracted like centre of mass, Normalized area of signature, aspect Ratio, tri surface, six fold surface feature. A verification stage includes applying the extracted features of test

signature to a trained neural network which will classify it as a genuine or forged. All features are further stored in database the stage is called as training stage. Image which will have to verify is tested against all stored feature the stage is called as testing stage.

A Training stage consist of four major steps

1.Retrieval of a signature image from a database , 2. Image pre-processing , 3. Feature extraction , 4.Neural network training

A testing stage consists of five major steps ,1.Retrieval of a signature to be tested from a database, 2. Image pre-processing , 3. Feature extraction , 4. Application of extracted features to a trained neural network , 5. Checking output generated from a neural network

- **Flow chart**

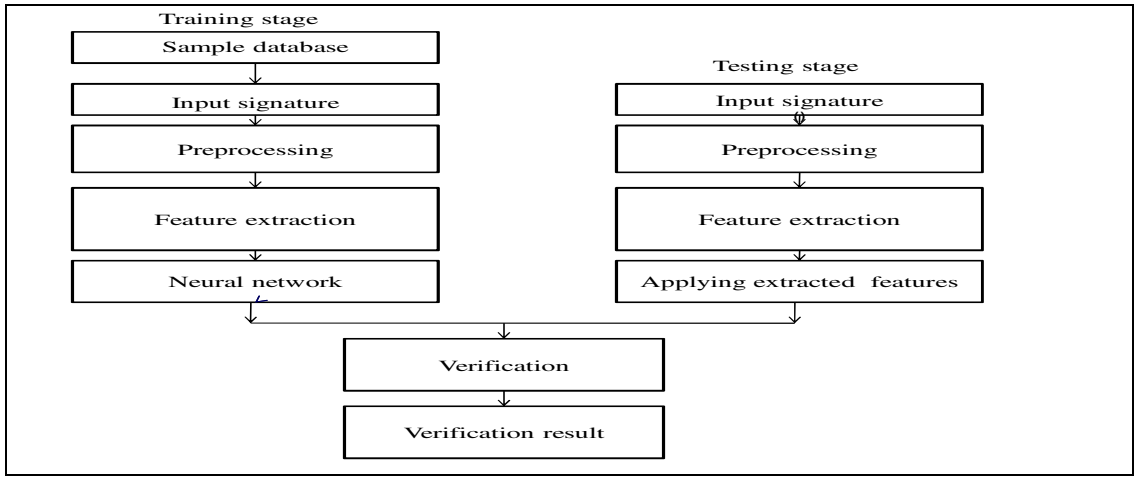


Fig 2: Flow chart

Fig. 3 shows one of the original signature image taken from a database. The different steps applied for its verification are as follows

Fig 3.Signature image from the database

- **Algorithm**

Input: signature from a database Output: verified signature classified as genuine or forged
1. Retrieval of signature image from a database.
2. Pre-processing the signatures.
3. Converting image to binary.
4. Image resizing.
5. Thinning.
6. Finding bounding box of the signature.
7. Feature extraction
8. Maximum horizontal and vertical histogram
9. Centre of mass
10. Normalized area of signature
11. Aspect ratio
12. The tri surface feature
13. The six fold surface feature
14. Transition feature
15. Creation of feature vector by combining extracted features.
16. Normalizing a feature vector.
17. Training a neural network with a normalized feature vector.
18. Steps 1 to 17 are repeated for testing signatures.
19. Applying normalized feature vector of test signature to trained neural network.
20. Using a result generated by the output neuron of the neural network declaring a signature as a genuine or forged.

- **Pre-processing**

The pre processing step is applied both in training and testing phases. Signatures are scanned in gray. The purpose in this phase is to make signature standard and ready for feature extraction. The pre-processing stage improves quality of the image and makes it suitable for feature extraction. The prepossessing stage includes

- Converting image to binary

A gray scale signature image is converted to binary to make feature extraction simpler.

- Image resizing

The signatures obtained from signatory are in different sizes so, to bring them in standard size, resizing is performed, which will bring the signatures to standard size.

- Thinning

Thinning makes the extracted features invariant to image characteristics like quality of pen and paper. Thinning means reducing binary objects or shapes to strokes that are single pixel wide.

- Bounding box of the signature

In the signature image, construct a rectangle encompassing the signature. This reduces the area of the signature to be used for further processing and saves time.

- **Feature Extraction**

The features that are extracted are used to create a feature vector. Features are extracted as follows

- Maximum horizontal and vertical histogram

Horizontal histogram is calculated by going through each row of the signature image and counting number of black pixels. A row with maximum number of black pixels is recorded as maximum horizontal histogram.

- Center of mass

Split the signature image in two equal parts and find center of mass for individual parts.

- Normalized area of signature

It is the ratio of area of signature image to the area of signature enclosed in a bounding box. Area of a signature is the number of pixels comprising it.

$$\text{Normalised Area} = \frac{\text{Signature Area}}{\text{Area enclosed in a bounding box}}$$

- Aspect Ratio

It is the ratio of width of signature image to the height of the image. This is done because width or height of person's signature may vary but its ratio remains approximately equal.

$$\text{Aspect Ratio} = \frac{\text{Width of signature in a bounding box}}{\text{Height of signature in a bounding box}}$$

- Tri surface feature

Two different signatures may have same area .so to increase the accuracy of the features three surface feature has been used. In this, a signature is divided into three equal parts and area for each part is calculated.

- The six fold surface feature

Divide a signature in three equal parts and find bounding box for each part. Then calculate centre of mass for each part. Draw a horizontal line passing through centre of mass of each part and calculate area of signature above and below centre of mass within a bounding box. This provides six features.

3] Implementation Tools

The main reasons for the widespread usage of neural networks in recognition are their power and ease of use. Among different types of neural network Probabilistic Neural Network (PNN) is used for signature verification. A probabilistic neural network (PNN) is a classifier which Map any input pattern to a number of classifications & it can be forced into a more general function approximator. PNN is an implementation of a statistical algorithm called kernel discriminant analysis in which the operations are organized into a multilayered feed forward network with different layers.

COMPARISON WITH OTHER METHODS

Comparison with above mentioned method can be done by calculating AER value

AER (Average Error verification Rate)

AER is average of False Acceptance Rate (FAR), False Rejection Rate (FRR) of the system. False Acceptance Rate (FAR), False Rejection Rate (FRR) and Correct Classification Rate (CCR) are the three parameters used for measuring performance of system. The genuine and forged signature samples used for training neural network is applied in the testing phase to check whether neural network classifies it correctly as genuine or forged.

$$\text{FAR} = \frac{\text{Number of forgeries accepted}}{\text{Number of forgeries tested}} * 100$$

$$\text{FRR} = \frac{\text{Number of origionals rejected}}{\text{Number of origionals tested}} * 100$$

$$\text{CCR} = \frac{\text{Number of samples correctly recognised}}{\text{Number of samples tested}} * 100$$

RESULT AND DISCUSSION

For training and testing of the system many signatures are used. The results provided in this research used a total of 1000 signatures. Those 1000 signatures are comprised of 100 sets (i.e. from 100 different people) and, for each person there are 5 samples of genuine signatures and5 samples of forgeries. To train the system, a subset of this database was taken comprising of 5 genuine samples taken from each of the 100 different individuals and 5 forgeries made by different person for one signature. The features extracted from 5 genuine signatures and 5 forged signatures for each person were used to train a neural network. After applying a feature vector of test signature if the output neuron generates value close to +1 test signature is declared as genuine or if it generates value close to -1 it is declared as forged. The Accuracy of system is 86.25%

REFERENCES

1. R. Plamondon and S.N. Srihari, "Online and Offline Handwriting Recognition: A Comprehensive Survey", IEEE Tran. on Pattern Analysis and Machine Intelligence, vol.22 no.1, pp.63-84, Jan.2000

2. B. Herbst. J. Coetzer. and J. Preez, "Online Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model," EURASIP.Journal on Applied Signal Processing, vol. 4, pp. 559–571, 2004.

3. JunLin chen; wen, jing; "Video-Based Signature Verification by Tracking Pen Tip Using Particle Filter Combined with Template Matching" IEEE Conference 2009 , vol. 1 PP. 83 - 88

4. 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

5. Vielhauer.c, Mayerhoper.A "Biometric hash based on statistical features of online signatures" IEEE Conference 2002, vol. 1 PP. 123 - 126

6. Prashanth CR,KB Raja,KR Venugopal, LM Patnaik,"Standard Scores Correlation based Offline signature verification system", International Conference on advances in computing, control and telecommunication Technologies 2009
7. M. Blumenstein. S. Armand. and Muthukkumarasamy, "Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural based Classification," International Joint Conference on Neural Networks, 2006.
8. Prasad A.G. Amaresh V.M. "An offline signature verification system"
9. Ramachandra A. C ,Jyoti shrinivas Rao"Robust Offline signature verification based on global features" IEEE International Advance Computing Conference ,2009.
10. Ashwini Pansare, Shalini Bhatia "Handwritten Signature Verification using Neural Network" International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 1– No.2, January 2012