IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Signature Recognition and Verification System via Neural Network

Sandhya Katiyar[1], Shubham Agarwal[2], Shubham Kaushal[3], Himanshu Vats[4]

Assistant Professor, Department of Information & Technology, Galgotia's College of Engg and Technology, Greater Noida, India [1]

B.Tech Scholar, Department of Information & Technology, Galgotia's College of Engg and Technology, Greater Noida, India[2,3,4]

Abstract: As every person has a unique signature with its specific behavioural property ,signatures are widely accepted bio-metric for authentication and identification of a person , so it is very much necessary to prove the authenticity of signature itself. A huge increase in forgery cases relative to signatures induced a need of efficient "Signature Verification System". These systems can be online or offline based on type of input taken by the system. This paper represents a brief review on various approaches used in signature verification systems. Before extracting different features from the signature, some pre-processing of the signature is done. In pre-processing, the signature is colour normalized and scaled into a standard format. The algorithm is based on extracting global features like Area, Height, and Width etc. Euclidean Distance model is used while finding match between test signature and signature stored in the database. The algorithm gives good recognition rate. If a query signature is in the acceptance range then it is an authenticated signature else, it is a forged signature.

Keywords: Signature Verification, Forgery Detection, Global Features, Euclidean Distance and Verification Technique, FAR, FRR.

I. INTRODUCTION

Biometric refers to the authentication techniques that rely on physiological characteristics (face, ,iris, and fingerprint) or behavioural traits(signature, voice) for identity verification of individual.It is emerging as a power full trustable alternative to password-based security systems,as known it is nearly impossible to steal or forge biometric properties. Signature is behavioural biometric: it does not depend on physiological properties of the individual, like fingerprint or iris. Signature based authentication systems have gained a very big popularity in today world and everybody considers it best then the other authentication systems.[2][3][5][7]. The system for signature verification should be neither 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) [6].

The false rejection rate (FRR) and the false acceptance rate (FAR) are used as quality performance measures. The FRR is the ratio of the number of genuine test signatures rejected to the total number of genuine test signatures submitted. The FAR is the ratio of the number of forgeries accepted to the total number of forgeries submitted. Many researchers have used combination of different features and classifiers to developed signature recognition systems.

Among various stochastic approaches, HMMs have proven very effective in modelling both dynamic and static signals [5][6][7][8]. Previous HMM based signature recognition systems used unsuitable HMM topology, different number of states for users and weak features for training and classification of signature images [5][8][9][10][11]. These shortcomings need to be corrected to enhance the effectiveness of the systems.

II. TERMINOLOGIES IN SIGNATURE VERIFICATION

A. Type of Forgeries

In signature verification systems, forgeries may be classified into three basic types :

Random Forgery:
In this type of forgery the forger nor has any information about the author's name neither has access to the genuine signature. And thus forger reproduces a random or guessed signature. [2][6]

Simple Forgery:
In this type of forgery the forger has the information about the author's name but doesn't has access to any sample signature of the author. And the forger reproduce the author's signature in his own style.[2][6]

Skilled Forgery:
In this type of forgery, the forger has access to the author's sample signature and thus reproduce it in an efficient way.
The two legal properties of a handwritten signature are briefly stated below:

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

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

• Non-repudiation-the accumulated effect of the above factor promises such a high degree of purpose that the signer cannot deny he or she has signed.[2][6]

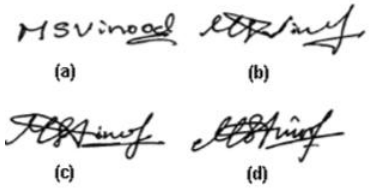

Fig 1. Type of Forgeries a). Random Forgery, b).Unskilled Forgery c).Skilled Forgery d). Original Signature

B. Types of Signature

Generally, handwritten signature verification can be categorized into two kinds-

1.Online Verification

2.Offline Verification.

Online Verification:

It requires an electronic tablet which is connected to the computer to grab the dynamic signature information and a stylus is also needed to sign.[6][7]

Offline Verification:

In this the signature is in static format or on a paper. In online approach we can extract more information about the signature which also includes the dynamic properties of the signature. It can acquire a lot more information about the signature like writing speed, pressure points, strokes, acceleration as well as the static characteristics of signature. It helps to get more accuracy because dynamic properties are very difficult to forge but in this complex hardware is required and user-cooperation is also needed. Digitizer tablets or pressure sensitive pads are used to Scan signature dynamically.

In Offline signature recognition, the signature is available in a static way or from an imaging device so it can only have static characteristics of the signature. The person need not to be present at verification time. So there is some convenience in static signature. Static signature for various situations like document verification, banking transactions etc. can be used. There are limited features available in static signature so very much care is required to get the desired accuracy.[6][7] In this sense signature verification, becomes a typical pattern recognition task knowing that variations in signature pattern are inevitable; the task of signature authentication can be narrowed to drawing the threshold of the range of genuine variation.

Error Rates:

The performance of a signature is the evaluation of recognition and verification is done by according to the error representation of a two class pattern recognition problem, the error representations are False Rejected Ratio(FRR)and False Acceptance Ratio(FAR).

The accuracy of the recognition depends upon the ability of the system to increase the inter-variation between signatures of different people while reducing the intra-variation within the signature of the same person. [5][7]

False Rejection Rate(FRR):

The percentage of the identification instance in which false rejection occurs is defined as the False Rejection Rate.[3][8]

False Acceptance Rate:

The false acceptance rate, or FAR, is the measure of thelikelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.[3][7]

Average Error Rate:

It is the average of both Type 1 and Type 2 errors.[3]

Equal Error Rates:

It is the location where FAR and FRR are equal on a ROC or Detection Error Trade-off curve.The value of EER and performance of the system is inversely proportional.[3][7]

III. PROPOSED METHODOLOGY

A. **Data Acquisition**

First signatures are acquired , they can be using black or blue ink pan. they are enclosed in a rectangular box. We try to get at least 10 speciman of each person's signature with maximum possible variations. Then scanning is done and then conversion and then stored in a database.[3][7].

B. **Image Preprocessing**

For improving the accuracy of the later steps like feature extraction and classification pre-processing is a necessary step. and with this computational needs are also reduced.

Following steps are involved in pre processing:

1. **Scanning:** Firstly signature sheet is scanned.
2. **Cropping:** Then signature is separated using crop method form the scanned sheet.
3. **Binarization:** We try to obtain best binary image by using HIT and TRIAL method, RGB image is binarized at threshold value 0.7.
4. **Complement of binary Image:** For computational simplification we obtain the Complement of binary image by changing the background into black and foreground of the image into white.
5. **Noise reduction and Clutter Removal:** Noise like' salt and pepper noise' is removed using Median Filter which was caused during scanning and thus before pre processing unconnected black dots are removed.
6. **Region of Interest:** To obtain region of interest the cropping is done with respect to bounding box of image by calculating first foreground row, first foreground coloum, last foreground row and last foreground coloumn.

DOI 10.17148/IJARCCE.2016.5503

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Phase 1:

Fig2 : Scanned Image

Phase 2:

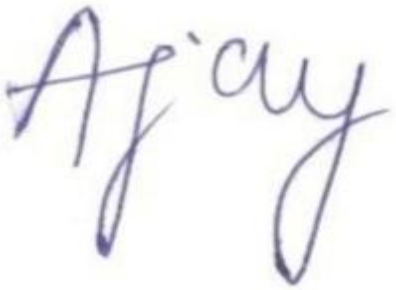

Fig.2 : Separated Signature Sample (RGB)

Phase 3:

Fig. 3 : Binary Image

Phase 4:

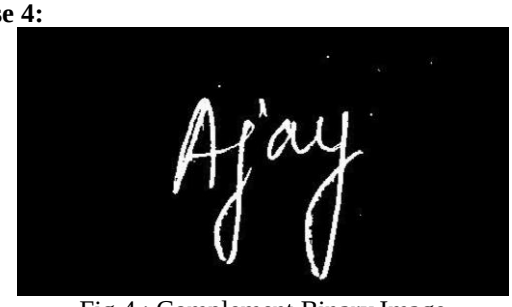

Fig 4 : Complement Binary Image

Phase 5:

Fig 5 : Image After Removal of Noise using Median Filter

Phase 6:

Fig 6 : Region of Interest

C. Feature Extraction :
In this system three types of features are used which are :
1. Grid features
2. Local features
3. Global features.

Overall appearance information of the signature is entertained by the grid information. First the rectangular imag;eis broken down into 96 rectangular segments(12 ? 8), then the area(sum of foreground pixels) is calculated for each segment.

Then the normalization of result is done so that lowest value(for the rectangular with smallest number of black pixels) will be zero and highest value(for the rectangular with highest number of black pixels) equal to one.

Global features contains the properties of the signature like width, height and aspect ratio. These properties are less sensitive to noise. Local features of the image are calculated by partitioning

D. Training the network :
The most crucial part of the system is training a RBFN. From each individual three signatures are used in the training. after that, each input signature is pre-processed

DOI 10.17148/IJARCCE.2016.5503

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

and is given as input to the feature extraction module. After getting all the input signature features input matrices for the training of the first three ANNs are prepared. The classifier will use radial basis function network in this system.

Training a neural network includes setting many tuneable parameters like-

- The type of radial function to be used in the hidden units.
- The distance type.
- The centre of the radial functions (location of the hidden units).
- The spread or radius of the radial functions.
- As for the hidden units, Gaussian function is often used as the radial function and Euclidean
- distance as the distance type. In this case, the output of the i-th hidden unit with centre μi and spread σi is given as follows:

$$\phi_i(\mathrm{x}) = \phi(\|\mathrm{x}-\mu_i\|;\sigma_i) = e^{(-\frac{\|\mathrm{x}-\mu_i\|^2}{2\sigma_i^2})}, \forall i$$

E. Training the network :

After the employment of new signature, its features are extracted and they are fed to match with those already stored in the database. Then if the features are matched then it is classified as genuine otherwise forge.

Table 1

Sr.	Feature		Extracted Value
1	Number of pixels		536
2	Width of picture (in pixels)		144
3	Height of picture (in pixels)		136
4	Maximum Horizontal Projections		11
5	Maximum Vertical Projections		15
6	Dominant Angle-normalized		0.775
7	Baseline Shift (in pixels)		51
8	Trisurface Area1		0.126638
9	Trisurface	Area2	0.287474
10	Trisurface	Area3	0.048674

PROPOSED MODEL:

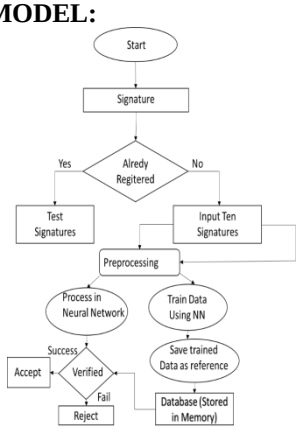

Fig.7: Signature Recognition and Verification System

IV. LITERATURE SURVEY

An individual's signature contains characteristics that it is not always consistent. It changes to a certain extent each time an individual do it.. Offline signature verification is one of most challenging and widely acceptable area of pattern recognition. Being a behavioural biometric trait which can be imitated, the researcher faces a challenge in designing such a system to counter intrapersonal and inter personal variations. Several such researches and previous works are summarized below. **Shashi Kumar D R, K B Raja, R. K Chhotaray, SabyasachiPattanaik** 4 [6] introduced Off-line Signature Verification. Based on Fusion of Grid and Global Features Using Neural Networks. Fusion of global and grid features are used to generate powerful feature set and neural networks are used as classifier. FAR achieved was 4.16% where as FRR was 7.51%. **L.Basavaraj and R.D Sudhaker Samuel** introduced offline signature verification technique based on four speed stroke angle. It extracts dynamic features of static signature image. It is based on the idea that intensity is directly proportional to the speed of the stroke. This method achieved FAR of 13.78% and FRR of 14.25%. **Mohammed A. Abdala& Noor Ayad Yousif** proposed a system based on two neural networks classifier and three powerful features sets(global, texture and grid features).It consists of three stages: the first is pre processing stage, second is feature extraction stage and the last is neuralnetwork (classifiers) stage which consists of two classifiers, the first classifier consists of three Back Propagation Neural Network and the second classifier consists of two Radial Basis Function Neural Network.

V. CONCLUSION

The FAR of the resultant system is 3.2 % and FRR is 2.2%. The ERR of the system shows the accuracy where ROC curve will tell whether FAR and FRR are close to Y-Axis or not. So the resultant ERR of the system is 0.12%. This system is more accurate when Contour Method and SVM.Generally the failure to recognize/verify a signature was due to poor image quality and high similarity between 2 signatures. Recognition and verification ability of the system can be increased by using additional features in the input data set. This study aims to reduce to a minimum the cases of forgery in business transactions

REFERENCES

[1]. Ammar M. ―Performance of parametric and reference pattern based on features in static signature verification: a comparative study‖. In Proceedings of 10th International Conference on Pattern Recognition vol.1 (1990), IEEE Computer Society Press, pp. 646-648

[2]. Ammar, M., Yosheda, Y., Fukumura, T. ―Off-line pre processing and verification of signature.‖ Int. J. Pattern Recognition Arti. Intell. 2,pp. 589-902

[3]. Fierrez-aguilar, J., Alonso-hermira, N., Moreno-marquez, G., Ortega-garcia, J. ―An off-line signature verification system based on fusion of local and global information.‖ In ECCV Workshop BioAW (2004), pp. 295-306.

[4]. Gonzalez, R. C., Woods, R. E. Digital Image Processing. Addison-Wesley Longman Publishing Co., Inc., Boston, USA, 2001.

[5]. J.P. Drouhard, R. Sabourin, M. Godbout, ―Evaluation of a Training Method and of Various Rejection Criteria for a Neural Network Classifier Used for Off-Line Signature Verification,‖ IEEE Int'l Conf. Neural Networks, Orlando, Fla., June 26-July 2, pp. 294-4,299, 1994.

[6]. E.R. Brocklehurst, ―Computer Methods of Signature Verification,‖ J. Forensic Science Society, pp. 445457,1985.

[7]. Y. Qi, B. R. Hunt, ―Signature verification using global and grid features,‖ Pattern Recognition, 27(12), pp.1621–1629, 1994.

[8]. M. Ammar, ―Progress in verification of skillfully simulated handwritten signatures,‖ International Journal of Pattern Recognition and Artificial Intelligence, 5(1–2):337–351, 1991.

[9]. R. Sabourin, G. Genest, F.J. Prˆeteux, ―Off-Line Signature Verification by Local Granulometric Size Distributions,‖IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 19, No. 9, pp. 976-988, 1997.

[10]. S.N. Srihari, A. Xu, M.K. Kalera, ―Learning strategies and classification methods for off-line signature verification,‖Proc. of the 7th Int. Workshop on Frontiers in handwriting recognition (IWHR) , pp. 161–166, 2004.

[11]. C. Allgrove, M. C. Fairhurst, ―Majority Voting for Improved Signature Verification,‖ IEE Colloquium on Visual Biometrics, (Ref No. 2000/018), pp. 911-914, 2000.

[12]. N.A. Murshed, F. Bortolozzi, R. Sabourin, ―Off-Line Signature Verification, Without a Priori Knowledge of Class w2. A New Approach, ‖Proc. Third IAPR Conf. Document Analysis and Recognition, pp. 191-196, Aug. 14-16, Montr´eal, Canada, pp. 191-196, 1995.

[13]. 13] F. Nouboud, R. Plamondon, ―Global Parameters and Curves for Off-Line Signature Verification,‖ Proc. Int'l Workshop on Frontiers in Handwriting Recognition, Taiwan, pp. 145-155, 1994.

[14]. J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[15]. S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.

[16]. M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.

[17]. R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

[18]. R. Sabourin, R. Plamondon, G. Lorette, ―Off-Line Identification with Handwritten Signature Images: Survey and Perspectives,‖Structured Document Image Analysis. New York: Springer-Verlag, pp. 219-234, 1992.

[19]. S. Lee, J.C. Pan, ―Off-line tracing and representation of signatures,‖ IEEE Transactions on Systems, Man and Cybernetics, Vol. 22, pp. 755–771, 1992.

[20]. J. Coetzer, B. M. Herbst, J. A. du Preez, "Offline Signature Verification Using the Discrete Radom Transform and a Hidden Markov Model" , EURASIP Journal on Applied Signal Processing 2004:4, 559–571 2004,Hindawi Publishing Corporation.

[21]. J Edson, R. Justino, A. El Yacoubi, F. Bortolozzi and R. Sabourin, "An off-line Signature Verification SystemUsing HMM and Graphometric features", DAS 2000, pp. 211-222, Dec.2000.

[22]. J Edson, R. Justino, F. Bortolozzi and R. Sabourin, "An offline signature verification using HMM for Random, Simple and Skilled Forgeries", Sixth International Conference on Document Analysis and Recognition, pp. 1031-1034, Sept.2001.

[23]. J Edson, R. Justino, F. Bortolozzi and R. Sabourin, "The Inter personal and Intrapersonal Variability Influences on Off-line Signature Verification Using HMM", Proc. XV Brazilian Symp. Computer Graphics and Image Processing, 2002, pp. 197-202,Oct.2002. [21] J. K. Solanki, "Image Processing using fast orthogonal transform", PhD Thesis Submitted to IIT Mumbai, 1978, pp. 30, 31

[24]. J. Hasna, "Signature Recognition Using Conjugate Gradient Neural Networks", IEEE transactions on engineering, computing and technology, Vol. 14, august 2006, ISSN 1305-5313

[25]. E. Justino, F. Bortolozzi and R. Sabourin. 2001. "Off-line signature verification using HMM for random, simple and skilled forgeries", Proceedings of Sixth International Conference on Document Analysis and Recognition, Vol. 1, pp. 1031-1034.

[26]. E. Justino, F. Bortolozzi and R. Sabourin. 2005. "Comparison of SVM and HMM classifiers in the off-line signature verification", Pattern Recognition Letters, pp. 13771385.

[27]. E. Justino, A. Yacoubi, R. Sabourin and F. Bortolozzi. 2000."An off-line signature verification system using HMM and graphometric features", Proc. of the 4th International Workshop on Document Analysis Systems, pp. 211-222.

[28]. M. Banshider, R .Y Santhosh and B .D Prasanna. 2006. "Novel features for off-line signature verification" International Journal of Computers, Communications &Control ,Vol. 1 , No. 1, pp. 17-24.