International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 4, July - August 2015 **ISSN 2278-6856**

Online Signature Recognition using Neural Network

Babita Pegu[1], Aditya Bihar Kandali[2]

[1]Jorhat engineering college, Dibrugarh university
Jorhat 785007, India

[2]Jorhat engineering college, Dibrugarh university
Jorhat 785007, India

Abstract

In this work a new method of signature recognition with neural network is proposed. The features are extracted from two raw databases of ATVS signature database: one consisting of 25 signature samples of 350 persons and other 46 signatures of 25 persons. The features include 9 features computed by D.S. Guru and H.N. Prakash and proposed features are no of pen downs, magnitude of average velocity, magnitude of average acceleration and length to height ratio. Signature features are pre-processed with a scaling method and brought to a value having same decimal point. A feed forward neural network is trained using back propagation learning method. With each features removed, an accuracy rate is calculated to check the feature which will be better for signature verification. Accuracy of recognition up to 98% and 89% are obtained using signature samples of 10 persons from each database respectively.

Keywords: signature recognition, neural network, back propagation, confusion matrix.

1. INTRODUCTION

Authentication of user is becoming very important to do business transactions, accessing data and for security purpose. Many different techniques are applying for authentication purpose. User IDs and passwords, PIN codes, ATM card, PAN card are many different ways which are common today, but the problem of such systems are that, they need remembering different PINs or passwords, carry such items and they need to be kept secret from others. Signature is a behavioral biometric. Automatic signature authentication is now becoming popular in research areas because of its acceptance in legal and social areas and its widespread use for authentication purpose.

Since signature for different individuals vary with the variation of individuals, so it is a very robust biometric to authenticate a user. Signature verification is a very difficult pattern recognition problem. Since intra class variations occur, even experts get difficulty to recognize the forgery signature. And also it is not very difficult to forge a signature. Signature is believed to be a reflex action which produces its dynamic properties unconsciously.

Biometrics can be broadly divided into physiological and behavioral biometrics. Some examples of physiological biometrics are fingerprint, iris and face; and behavioral biometrics is signature, voice and hand writing. Authentication of signature is done by detecting forgeries. Forgeries can be divided into random forgery, simple simulated forgery and simulated skilled forgery. Fig1 shows an example of forgery signatures. Random forgeries are produced randomly without any information about the name and person for whom signature is produced. Random forgery are generated when forger do not have any available access to the signature. They may have different shape and size from the authentic signature. Simple simulated forgery may have same semantic meaning like authentic one but overall shape and size may differ. Skilled simulated forgery signatures are the signatures which are given by a large number of practices.

Figure 1: (a) genuine signature; (b) random forgery; (c) simulated simple forgery; (d) simulated skilled forgery [11]

For online signature verification, signature data are generally taken using capacitive tablet or personal data assistance (PDA) which gives the x-y coordinate, pressure readings etc. From these raw data different features can be

computed. Signature authentication problem can be solved by two ways: dynamic and static, which needs computation of dynamic and static features respectively. Dynamic measurement of signature features can be obtained by electronic tablet or PDA; static features can be computed from images obtained either by camera or scanning the photo of the signatures. Dynamic features [9] are functions of time and static features are time independent. Even if a skilled forger produces the same looking signature like the authentic one, they cannot easily learn to produce the same pressure produced by the authentic one. Hence dynamic features help to detect forgery. The use of pen dynamics over shape of signature would be more useful in forgery detection because dynamic features of a signature are not readily available to forger as in the shape of offline signature.

Handwritten signatures can be represented by multiple modals i.e. global and local, shape based and time based. Local shape based signature and their advantages are discussed in [8]. Three signature databases are collected and analyzed for a different period of time. Different reasons for inaccuracies are also discussed. Global feature based technique is applied in [2]. Three global features i.e. projection moment, upper envelope based characteristics and lower envelope based characteristic are used and then multiple neural network is applied for the classification purpose. To remove noise they have applied median filter. A fusion of local and regional features is discussed in [1]. The local function based features are classified with dynamic time warping (DTW) and regional features are classified with hidden markov model (HMM). In [10] signature verification based on logarithmic spectrum is done. Principle components of the logarithmic spectrum are compared with the reference signature and similarity value is calculated between the enrolled and reference signature. A stroke based method for shape and dynamics of signature is discussed in [3]. Two level strategies using soft and hard rule are implemented in it.

The signature authentication is done in two types of problems: signature verification and signature recognition. In verification, the features of the test signature are compared with a few number of stored features of the signature of the claimed person, and need to verify if the signature belongs to that particular person or not. But in recognition the features of the test signature are compared with a few no of stored features of a no of persons and we have to recognize whether the test signature belongs to the one of the enrolled persons and identify the person.

Online signature verification can be broadly classified into two groups based on their feature extraction method: parametric approach and function based approach. In parametric approach a set of parameters (e.g. Speed, displacement, position, pen up pen down, wavelet transform etc.) extracted can be used as a feature to form a signature pattern, and those feature patterns can be used as reference and test signature to examine the authentication of the signature. In function based approach the features are the function of time (e.g. velocity, acceleration, pressure, direction of pen movement etc.). Online signatures are characterized as a time function.

In any verification task there are two types of error involved i.e. false rejection and false acceptance. False rejection occurs when the authentic signature is rejected and false acceptance occurs when a forged signature is accepted to be authentic. When percentage of false rejection rate (FRR) is equal to the percentage of false acceptance rate (FAR) we call it equal error rate. Equal error rate is the measure of the performance of a biometric system. Average error rate is the average of FAR and FRR. The authenticity of test signature is evaluated by matching it with that of reference signature. There are many techniques available for matching e.g. dynamic time warping (DTW) [7], hidden Markov model (HMM), support vector machine (SVM) and neural network (NN). When functions are considered, the matching technique must take into account the variation of duration of signature. A method of similarity measure for signature verification and recognition using symbolic representation is done in [5]. Here the following are discussed:

- Dynamic time warping technique is generally used for function based parameter. But the time complexity of DTW is more of the order of (O^2).
- HMM performs stochastic matching using probability distribution of the features. They can compute both similarity and variability of the pattern. But they require a large dataset to train and are complex.
- Support vector machine classifies one class of data from the other by finding the hyper plane that maximizes the separation between classes. SVM have algorithmic complexity, and requires large storage for large scale task
- Neural network have ability of generalization. They can be used to detect nonlinear equations for dependent and independent variables. They can train large amount of database. Easily implemented in parallel architecture.

In [6] a method of string matching or dynamic time warping is done. Here local features and stroke based global features are extracted and the results are compared, by varying the values of absolute and relative speed of the signature. Then signature feature vectors are formed in symbolic interval value and test data are inserted to check if it lies within that interval or not. After that interval value is set by calculating mean, variance and standard deviation. Finally writer dependent and feature dependent threshold are set in the database

2. FEATURE EXTRACTION

From ATVS signature sub corpus, two sets of database are collected. First database contains 25 genuine signature samples for each user. In the second database each users have 46 samples each. The databases contains raw data values of the signature i.e. x-coordinate, y-coordinate, time stamp, pen up pen down and pressure signal. From these data the features are extracted. Initially from these raw data 33 features were computed. For training in neural network feature selection is done manually where

some features, which give better results were kept. Features are introduced as:

Total duration of signature:

It is the time taken to complete a signature. It can be calculated as the difference between the last time stamp and the first time stamp.

Number of pen ups:

The number of times pen is removed from the pad/paper.

Sign changes of dx/dt and dy/dt:

dx/dt and dy/dt may be positive or negative value. So when it changes the value from positive to negative or negative to positive it is counted.

Average jerk:

Jerk is change in acceleration with respect to time. Average jerk is the mean of the jerk.

Standard deviation of velocity in y-direction:

Standard deviation of v_y ;

Where, velocity in y-direction: $\mathbf{v_y = dy/dt}$ **(1)**

Standard deviation of acceleration in y-direction:

Standard deviation of a_y ;

Where, acceleration in y-direction: $\mathbf{a_y = dv_y/dt}$ **(2)**

Number of local maxima in x direction:

Local maxima can be calculated from change in x with respect to time.

Standard deviation of acceleration in x-direction: standard deviation of a_x ; where

Velocity in y-direction: $\mathbf{v_x = dx/dt}$

Acceleration in y-direction: $\mathbf{a_x = dv_x/dt}$ **(3)**

Standard deviation of velocity in x-direction:

Standard deviation of v_x ; where

Velocity in y-direction: $\mathbf{v_x = dx/dt}$ **(4)**

Length to width ratio:

It is the ratio of length of the signature to the width of the signature i.e. ratio of number of sample point covered by the signature in x-coordinate to number of sample point covered by the signature in y-coordinate.

Number of pen downs:

Number of times pen touches the pad/paper to complete a signature.

Average magnitude of velocity:

Velocity at every sample points changes. Average velocity is the mean of the velocities at every sample point.

Average magnitude of acceleration:

Acceleration also changes at every sample points. Therefore average acceleration is the mean of the acceleration at every sample points.

3. METHODOLOGY

The main motive of this work is to find some features suitable for signature verification and to check the performance of the neural network with those features. Here we have used neural network back-propagation algorithm for training a network. In neural network approach, the main procedure to implement is: first of all the features need to be extracted and then the network is to be trained to learn the relationship between the pattern and its class. After training, validation of the network is to be checked by few features to see if the network is giving a satisfactory result or not. After validation, the network is to be tested using features which are completely unknown for the network, to see the performance of the network. Data bases are collected from ATVS signature sub corpus [4]. The reason of using two dataset is to test the generalization capability of the network. Generally it is easy for the network to generalize more with more sample data. In second database sample data is more so it should give more accurate result. Now, first database i.e. dataset I consists of 25 signature data for each individual. Second dataset i.e. dataset II consist of 46 signature sample for each individual. From the raw data set consisting of information of x coordinate, y coordinate, time stamps, pressure and pen up and pen down, features were extracted. Then the databases are divided into three parts for training, validation and testing. From dataset I, 15 signatures were extracted for training, for validation next 5 signatures were extracted and for testing also remaining 5 signatures were extracted. From dataset II, 30 signatures were extracted for training, for validation next 8 signatures were extracted and for testing remaining 8 signatures were extracted. After division of data, they are randomized. The matching technique used is neural network approach. At first the extracted data are brought to 10^{th} decimal point. Then the data is normalized so that the pattern values are between 0 and 1. During training weights are updated to minimize the difference between the desired output and the actual output i.e. error. The fixed weights after training can be used for the task in pattern recognition and classification. The neural network structure used have three layers: one input layer, one hidden layer and one output layer. Activation provides the measure of confidence of corresponding decision of the classifier. Commonly used activation functions are sigmoid functions. The activation function used here is log sigmoid function (logsig). It gives the activation label between 0 and 1. If activation is 1 it means confidence is high and if it is 0 means confidence is zero.

A. Vector matrix form of back propagation algorithm

- An input pattern is presented and calculated the outputs of the network at all the internal layers
- For each of the layers, the sensitivity vector is calculated according to

$$\mathbf{D^{(s)} = G(v^{(s)})(d_q - x_{out}^{(s)})} \quad \text{for output layer} \quad (5)$$

$$\mathbf{D^{(s-1)} = G(v^{(s-1)})W^{(s)T}D^{(s)}} \quad \text{for all hidden layers} \quad (6)$$

The synaptic weights are updated for the network according to

$$\mathbf{W^{(s))}(k+1) = W^{(s)}(k) + \alpha^{(s)}D^{(s)}x_{out}^{(s-1)T}} \quad (7)$$

- Continue steps 1 through 3 until the network reaches the desired mapping accuracy

Where,

$D^{(s)}$ = sensitivity vector of layer of particular layer s

$G(v^{(s)}) = diag[g(v_1^{(s)}), g(v_2^{(s)}), \ldots\ldots g(v_{ns}^{(s)})]$

$g(v)$ = derivative of activation function v

d_q = desired output vector

x_{out} = actual output vector of the neural network

$W^{(s)}$ = weight vector for layer s

k = iteration number

$\alpha^{(s)}$ = learning rate parameter associated with the particular layer s

4. RESULT

Neural network is a generalization tool. The reason why the neural network approach is chosen among the number of other classification method is that, neural network is easy to use and can solve complex problems with ease. From this work it is realized that, when variation of data is more, neural network finds it difficult to generalize. That is why normalization of database is important. When introduced pre-processing of data by converting them to 10^{th} decimal point or same decimal point value the generalization becomes more and classification error decreases. Confusion matrix is a table which helps the visualization of the performance of supervised machine learning. The diagonal boxes in the table from left (up) to right (down) gives the true positive classification. And other boxes show the true negative classification. Fig 2 is showing the confusion matrix of genuine signatures of first dataset. The data consist of 15 genuine signatures of 10 users. From this confusion matrix, the true positive rate found is 98% i.e. false rejection rate (FRR) is 2%. Fig3 shows the confusion matrix of forgery signatures of first dataset. The data consist of 5 forgery signatures of 10 users. From this confusion matrix, when forgery signatures were taken, the false acceptance rate is 8%.

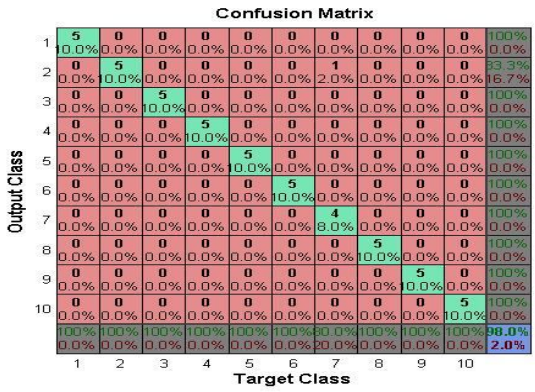

Figure 2: confusion matrix for genuine signature data of 10 users

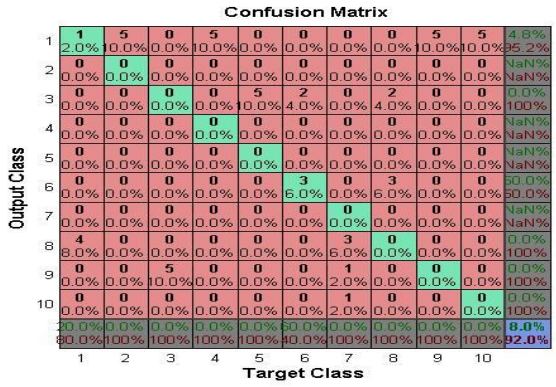

Figure 3: confusion matrix for forgery signature data of 10 users

From the confusion plot the accuracy of the system can be calculated by:

Accuracy = (100 – (FAR + FRR)/2) % **(8)**

The accuracy rate of the system is 95 %

Table 1 show the result obtained from dataset I using all the features extracted. And table 2 shows the result obtained from dataset I and dataset II using all the features extracted and also from removal of one or more features. Table2 gives the comparison of the accuracy of result with 9 and 13 features respectively for different number of classes (users).

From the table3 it is clear that features i.e. Average jerk, Standard deviation of acceleration in y direction, Standard deviation of acceleration in x direction, Standard deviation of velocity in x direction and average acceleration are not very suitable in case of dataset I. And in case of dataset II Time duration of signature and Average acceleration are not suitable. From the final accuracy result it is found that, result of dataset with more sample number gives more accurate result, which reflects the generalization capability of neural network. From table 3 it is observed that when features i.e. length to width ratio, number of pen downs, average magnitude of velocity and average magnitude of accelerations are added with previous 9 features, the network gives a better accuracy. It can also be observed that as the number of classes increases the accuracy decreases in both the cases. It implies that the features mentioned are not very good when database with more number of classes are taken.

5. CONCLUSION

The main objective of this work is to construct a signature recognition system using some feature values so that to get a maximum accuracy label. To do this, some features were extracted and formed pattern from them. The features acts as an input pattern to the neural network and corresponding targets are constructed. In neural network, the patterns are trained according to the target, where weights are updated to get a minimum error. When a stopping condition is reached the iteration stops. In neural network training, many times trial and error is done to get satisfactory neural network architecture. Parameters like hidden nodes in a neural network, initial learning rate parameter, learning rate schedule are needed to be adjusted again and again. Neural network architecture is dependent on these parameters. In this work the nodes in the hidden layers for the first dataset is 60 and second Dataset is 80. Initial learning rate parameter is 1 and learning rate scheduled at 300. These parameters give a false acceptance rate of 8% and a false rejection rate of 2%. And accuracy rate when calculated gives an accuracy rate of 95% for the dataset I. And for the dataset II an accuracy of 89% is obtained using the same parameter. When experiment is performed taking different number of classes, it is found that with increase in the number of classes the accuracy is decreasing. It is because of the fact that, the features considered in the experiment are not very suitable for database with large number of classes.

Since neural network has a generalization capability, once trained its weight need not be changed again. In testing it gives the result from the trained architecture itself. The main drawback of neural network training is that, for larger dataset it is very difficult to adjust the parameters by trial and error method. And the time consumption is more.

Table 2: comparison of accuracy of neural network with 9 features and 13 features

No of persons taken	Accuracy with 9 features	Accuracy with 13 features
10	85	98
25	80	89
50	50	49.2
100	36	40.4
200	25.5	27.2
350	16.5714	19.02

Table 1: result showing the accuracy of network using

features	True acceptance rate (%)	False rejection rate (%)	False acceptance rate (%)	Accuracy (%)
All the features mentioned	98	2	8	95

Table 3: result showing the accuracy of network for dataset I and dataset II

Feature/features removed	True acceptance rate (%) Using dataset I	True acceptance rate (%) Using dataset II
- - - - - - (using all features)	74	
Time duration of signature	72.5	75.2
Number of pen ups	70.5	70.4
Sign changes of dx/dt and dy/dt	73.5	72.8
Average jerk	79	63.2
Standard deviation of acceleration in y direction	76.5	69.6
Standard deviation of velocity in y direction	65.5	72
No of local maxima	62	66.4
Standard deviation of acceleration in x direction	76	63.2
Standard deviation of velocity in x direction	74	69.6
Length to height ratio	65	77.6
No of pen down	70	67.2
Average velocity	70	78.2
Average acceleration	74	- - - -
Average jerk, Standard deviation of acceleration in y direction	86	- - - -
Average jerk, Standard deviation of acceleration in y direction, Standard deviation of acceleration in x direction	87.5	- - - -
Average jerk, Standard deviation of acceleration in y direction, Standard deviation of acceleration in x direction, Standard deviation of velocity in x direction, average acceleration	89	- - - -
Time duration of signature, Average acceleration	- - - -	73.6
Time duration of signature, Average acceleration	- - - -	80

References

[1] Aguilar, J.F, Krawczyk S., Garcia, J.O. and Jain, A.K., "Fusion of Local and Regional Approaches for On-Line Signature Verification," Proc. Int'l Workshop Biometric Recognition System, pp. 188-196, 2005.

[2] Bajaj, R. and Chaudhary, S., "Signature Verification Using Multiple Neural Classifiers," Pattern Recognition, vol. 30, pp. 1-87, 1997.

[3] Bovino, L., Impdevo, S., Pirlo, G. and Sarcinella, L. , "Multiexpert Verification of Hand-Written Signature," Proc. Int'l Conf. Document Analysis and Recognition, pp. 932-936, 2003.

[4] DESCRIPTION OF ATVS-SSig DB,National Laboratory of Pattern Recognition (NLPR),Institute of Automation, Chinese Academy of Sciences(CASIA)

[5] Guru, D.S. and Prakash, H.N., "Online Signature Verification and Recognition: An Approach Based on Symbolic Representation". IEEE transactions on pattern analysis and machine intelligence, vol. 31, no. 6, June 2009.

[6] Jain, A.K., Griess, F., and Colonnel, S., "On-Line Signature Verification," Pattern Recognition, vol. 35, pp. 2963-2972, 2002.

[7] Marcos, F.-Z., "On-Line Signature Recognition Based on VQDTW," Pattern Recognition, vol. 40, no. 3, pp. 981-992, 2007.

[8] Nalwa, V.S., "Automatic On-Line Signature Verification," Proc. Third Asian Conf. Computer Vision, vol. 1, pp. 10-15, 1997.

[9] Nelson, W and Kishon, E "Use of Dynamic Features for Signature Verification," Proc. IEEE Int'l Conf. Systems, Man and Cybernetics, vol. 1, pp. 201-205, 1991.

[10] Wu, Q.-Z., Lee, S.-Y., and Jou, I.-C., "On-Line Signature Verification Based on Logarithmic Spectrum," Pattern Recognition, vol. 31, no. 12, pp. 1865-1871,

[11] E.J.R. Justino, F. Bortolazzi, and R. Sabourin, "A Comparison of SVM and HMM Classifiers in the Off-Line Signature Verifications," Pattern Recognition Letters, vol. 26, no. 9, pp. 1377-1385, 2005

AUTHOR

Babita pegu received the B.E. degree in Instrumentation Engineering from Jorhat Engineering College in 2013. She is persuing her M.E. in Jorhat Engineering college from 2013. Her current interest area include pattern recognition, signal processing and intelligent control