International Conference on Information Engineering, Management and Security
2015 [ICIEMS 2015]

ISBN	978-81-929742-7-9
Website	www.iciems.in
Received	10 - July - 2015
Article ID	ICIEMS048

VOL	01
eMail	iciems@asdf.res.in
Accepted	31- July - 2015
eAID	ICIEMS.2015.048

ONLINE SIGNATURE RECOGNITION USING NEURAL NETWORK

Long CAI[1], Kokula Krishna Hari Kunasekaran[2], Vignesh R[3]
[1]University of Hong Kong, HKSAR, Hong Kong
[2]Techno Forum Research and Development Center, India
[3]Life Member, Association of Scientists, Developers and Faculties, India

ABSTRACT: *Here it discusses about some of the features of signature data and their extraction from the raw data set collected from ATVS signature database. The features include time duration, sign changes of dx/dt and dy/dt, average jerk, number of pen-up pen-down etc. Signature features are pre-processed and brought to a value having same decimal point and trained using back propagation neural network. For signature data of 10 users and accuracy rate of 86% is obtained.*

KEYWORDS: PATTERN RECOGNITION, FALSE ACCEPTANCE RATE, FALSE REJECTION RATE, 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, or they need to be kept secret from others access. Signature is a behavioural biometric. Automatic signature authentication is now getting popular in research areas because of its acceptance in legal and social areas and its widespread use in 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 very easy 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 behavioural biometrics. Physiological biometrics is fingerprint; iris, face recognition etc and behavioural biometrics are signature, voice, hand writing etc. 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

Cite this article as: Long CAI, Kokula Krishna Hari Kunasekaran, Vignesh R. "ONLINE SIGNATURE RECOGNITION USING NEURAL NETWORK." *International Conference on Information Engineering, Management and Security (2015)*: 289-293. Print.

have different shape and size from the authentic signature. Simple forgery may have same semantic meaning like authentic one but overall shape and size may differ. Skilled forgery signatures are the signatures which are given by a person by vigorous practice and a kin observation.

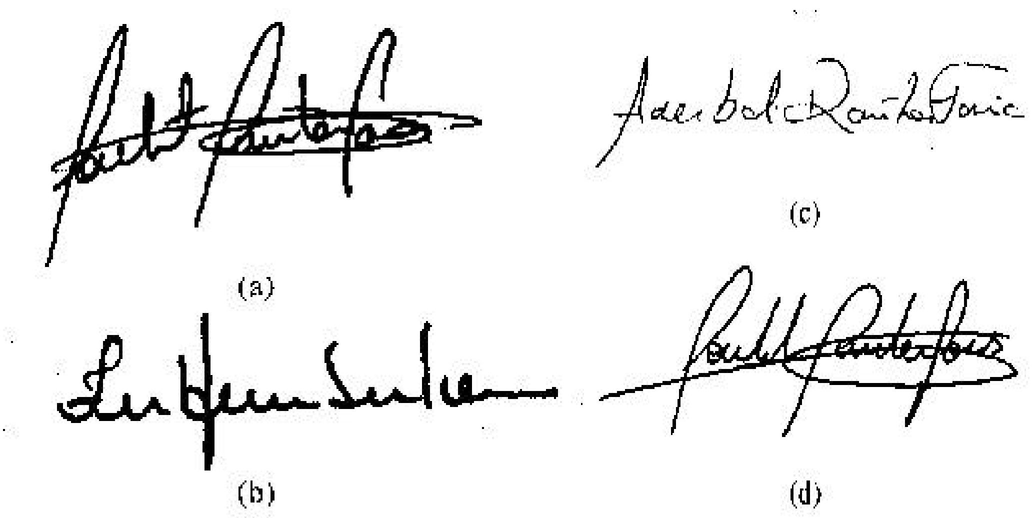


Fig 1: (a) genuine signature; (b) random forgery; (c) simulated simple forgery; (d) simulated skilled forgery

For online signature verification, signature data are generally taken using capacitive tablet or 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 i.e. dynamic and static. According to that features can be classified as dynamic features and static features. Dynamic data can be obtained by electronic tablet or PDA, and static images are obtained either by camera or scanning the photo of the signatures. Dynamic features [1] are functions of time and static features are time independent. Even if a skilled forger produces the same looking signature like the authentic one, but they can't produce the same pressure produced by the authentic one, so it is difficult to forge. The use of pen dynamics over shape of signature would be very useful in forgery detection because dynamic features of a signature are not readily available for 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 [2]. Three signature databases are collected and analysed for a different period of time. Different reasons for inaccuracies are also discussed. Global feature based technique is applied in [4]. 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 [5]. The local function based features are classified with DTW and regional features are classified with HMM. In [7] 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 [8]. Two levels strategy i.e. soft and hard rule are implemented in it.

The signature authentication can be done by two methods that are verification and recognition. In verification, the features of the test signature are compared with the limited number of stored features of the signature, and need to verify if the signature belongs to that particular person or not. But in recognition we are not known to the output signature, we have to recognize the given signature belongs to the given database or not. In recognition feature matching is done with the entire database.

Online signature verification can be broadly classified into two groups based on their feature extraction: 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 rate (FRR) and false acceptance rate (FAR). False rejection is when the authentic signature is rejected and false acceptance means when a forged signature is accepted to be authentic. When percentage of false rejection rate is equal to the percentage of false acceptance rate 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) [9], 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

Cite this article as: Long CAI, Kokula Krishna Hari Kunasekaran, Vignesh R. "ONLINE SIGNATURE RECOGNITION USING NEURAL NETWORK." *International Conference on Information Engineering, Management and Security (2015)*: 289-293. Print.

for signature verification and recognition using symbolic representation is done in [3]. In [6] a method of string matching or dynamic time warping is done. Local features and stroke based global features are extracted and compared the results by varying the values of absolute and relative speed of the signature. Signature feature vectors are formed in symbolic interval value and test data are inserted to check if it lies within that interval or not. Interval value is set by calculating mean, variance and standard deviation. Writer dependent and feature dependent threshold are set in the database.

- 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.

2. FEATURE EXTRACTION

The database is collected from ATVS signature sub corpus. The database 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.

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 acceleration in y-direction: standard deviation of a_y ; where

Velocity in y-direction v_y= dy/dt

Acceleration in y-direction $a_y = dv_y/dt$

Standard deviation of velocity in y-direction: standard deviation of v_y ; where

Velocity in y-direction v_y= dy/dt

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 v_x= dx/dt

Acceleration in y-direction $a_x = dv_x/dt$

Standard deviation of velocity in x-direction: standard deviation of v_x ; where

Velocity in y-direction v_x= dx/dt

3. METHODOLOGY

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. During 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 base is collected from ATVS signature sub corpus [11]. Database consists of 25 signature data 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 database is divided into three parts for training, validation and testing. For training first 15 signature were extracted, for validation next 5 signature were extracted and for testing also remaining 5 signature were extracted and randomized them. The matching technique used is neural network approach. At first the extracted data are brought to 10th 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.

3.1 Vector matrix form of back propagation algorithm

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

$D^{(s)} = G(v^{(s)})(d_q - x_{out}{}^{(s)})$ for output layer

$D^{(s-1)} = G(v^{(s-1)})W^{(s)T}D^{(s)}$ for all hidden layers

3. The synaptic weights are updated for the network according to

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

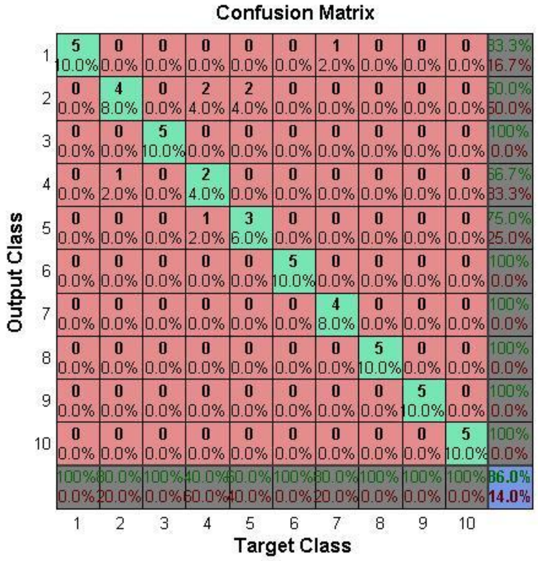
4. Continue steps 1 through 3 until the network reaches the desired mapping accuracy

Cite this article as: Long CAI, Kokula Krishna Hari Kunasekaran, Vignesh R. "ONLINE SIGNATURE RECOGNITION USING NEURAL NETWORK." *International Conference on Information Engineering, Management and Security (2015)*: 289-293. Print.

d_q = desired output
x_{out} = actual output of the neural network
k = iteration number

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. From the confusion matrix in fig2, when genuine signatures were taken the True positive rate found is 86% i.e. false rejection rate (FRR) is 14%. From confusion matrix in fig3, when forgery signatures were taken, the false acceptance rate is 12%.



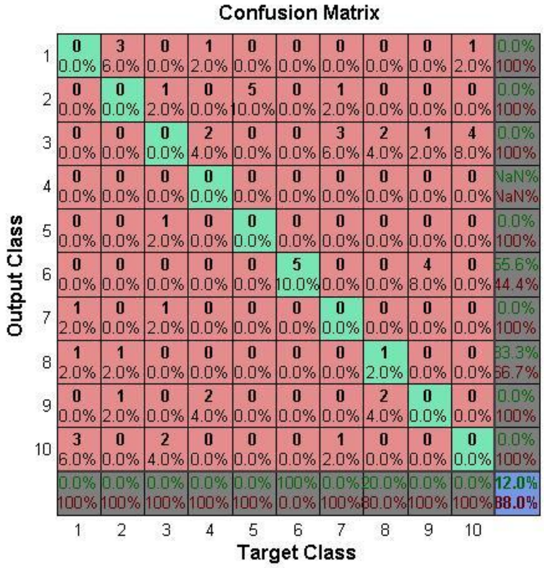
Confusion Matrix

Output Class

	1	2	3	4	5	6	7	8	9	10	
1	5 10.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	1 2.0%	0 0.0%	0 0.0%	0 0.0%	83.3% 16.7%
2	0 0.0%	4 8.0%	0 0.0%	2 4.0%	2 4.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	50.0% 50.0%
3	0 0.0%	0 0.0%	5 10.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
4	0 0.0%	1 2.0%	0 0.0%	2 4.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	66.7% 33.3%
5	0 0.0%	0 0.0%	0 0.0%	1 2.0%	3 6.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	75.0% 25.0%
6	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	5 10.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
7	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	4 8.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
8	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	5 10.0%	0 0.0%	0 0.0%	100% 0.0%
9	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	5 10.0%	0 0.0%	100% 0.0%
10	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	5 10.0%	100% 0.0%
	100% 0.0%	80.0% 20.0%	100% 0.0%	40.0% 60.0%	60.0% 40.0%	100% 0.0%	80.0% 20.0%	100% 0.0%	100% 0.0%	100% 0.0%	86.0% 14.0%

Target Class

Fig2: confusion matrix for genuine signature data of 10 users



Confusion Matrix

Output Class

	1	2	3	4	5	6	7	8	9	10	
1	0 0.0%	3 6.0%	0 0.0%	1 2.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	1 2.0%	0.0% 100%
2	0 0.0%	0 0.0%	1 2.0%	0 0.0%	5 10.0%	0 0.0%	1 2.0%	0 0.0%	0 0.0%	0 0.0%	0.0% 100%
3	0 0.0%	0 0.0%	0 0.0%	2 4.0%	0 0.0%	0 0.0%	3 6.0%	2 4.0%	1 2.0%	4 8.0%	0.0% 100%
4	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	NaN% NaN%
5	0 0.0%	0 0.0%	1 2.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0.0% 100%
6	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	5 10.0%	0 0.0%	0 0.0%	4 8.0%	0 0.0%	55.6% 44.4%
7	1 2.0%	0 0.0%	1 2.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0.0% 100%
8	1 2.0%	1 2.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	1 2.0%	0 0.0%	0 0.0%	33.3% 66.7%
9	0 0.0%	1 2.0%	0 0.0%	2 4.0%	0 0.0%	0 0.0%	0 0.0%	2 4.0%	0 0.0%	0 0.0%	0.0% 100%
10	3 6.0%	0 0.0%	2 4.0%	0 0.0%	0 0.0%	0 0.0%	1 2.0%	0 0.0%	0 0.0%	0 0.0%	0.0% 100%
	0.0% 100%	0.0% 100%	0.0% 100%	0.0% 100%	0.0% 100%	100% 0.0%	0.0% 100%	20.0% 80.0%	0.0% 100%	0.0% 100%	12.0% 88.0%

Target Class

Fig3: confusion matrix for forgery signature data of 10 users

Cite this article as: Long CAI, Kokula Krishna Hari Kunasekaran, Vignesh R. “ONLINE SIGNATURE RECOGNITION USING NEURAL NETWORK.” *International Conference on Information Engineering, Management and Security (2015)*: 289-293. Print.

From the confusion plot the accuracy of the system can be calculated by
Accuracy = (100 – (FAR + FRR)/2) %
The accuracy rate of the system is 86 %

5. CONCLUSION

The main objective of this work is to construct a signature recognition system 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 of 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 are 80. Initial learning rate parameter is 1 and learning rate scheduled at 300. These parameters give a false acceptance rate of 12% and a false rejection rate of 14%. And accuracy rate when calculated gives an accuracy rate of 87%.

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.

REFERENCES

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

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

[3] D.S. Guru and H.N. Prakash “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.

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

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

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

[7] Q.-Z. Wu, S.-Y. Lee, and I.-C. Jou, “On-Line Signature Verification Based on Logarithmic Spectrum,” Pattern Recognition, vol. 31, no. 12, pp. 1865-1871, 1998.

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

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

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

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

Cite this article as: Long CAI, Kokula Krishna Hari Kunasekaran, Vignesh R. “ONLINE SIGNATURE RECOGNITION USING NEURAL NETWORK.” *International Conference on Information Engineering, Management and Security (2015)*: 289-293. Print.