Signature Based Authentication

Anna Boyko, Georgiy Rozorynov

Abstract - **In this paper the decision of the problem of user authentication via Handwritten Signature Verification (HSV) are given.**

Keywords - **Signature, authentication, neural network.**

I. INTRODUCTION

To solve both the problems of password based authentication (relatively easy to compromise, easy to forget) and biometric authentication (expensive, intrusive, and disastrous if compromised), we attempt to solve the problem of user authentication via HSV [1]. The hardware necessary for HSV is inexpensive and already widely deployed in (e.g. credit card machines in stores, tablet PCs)

The problem consists of verifying a user's identity based on her signature by requiring the user to enter a signature and comparing the signature to a set of previously entered signatures. The system should have a very low false acceptance rate and a pessimistic false rejection rate. Our basic approach to solving the HSV problem uses online back-propagation. Both local and global features of the input signatures are used to train an Artificial Neaural Netowrk (ANN) to authenticate the user.

II. MAIN BODY

Initial input to the system consists of a set of valid signatures by the user in question. The system uses the user's signatures to learn to verify future signatures by the user. The initial output consists of a network that is saved to use for future authentication. Input to the system consists of a (user signature, login identity) pair. The login identity is entered manually or chosen from a list of users on the system. The user signature is entered using a pen or a mouse device, and is recorded as a set of points on a grid, along with temporal data recording the pen's movement during the signature. Output produced by the system is in the form of a Boolean answer signifying whether or not the user has been authenticated based on his signature and login identity.

A Multi-layer layer neural network trained with back propagation with momentum and bias was used to classify the authentication attempt of a user as being valid or invalid. Input to the network is a user signature codified as a real numbers. The output of the ANN is 2 real numbers in the range 0.0 to 1.0 with a threshold function applied to determine the authentication status of the user. The neural network is initially trained against a set of n valid signatures given by the user when he or she is first introduced to the system as well as a set of m invalid signatures. Before each signature is inputted to the ANN for training, a Gaussian noise is applied to the data to increase the robustness of the trained network.

The back-propagation algorithm works as follows:

1. The input data is presented to the network as a set of real numbers. The input is propagated to the output as standard feed forward network network. At each node, the output of the node is the sum of the inputs to that node multiplied by a weight for that input and passed through a biased sigmoid squashing function. The squashing function is computed as follows:

$$\sigma(X,\eta)=\left[1+\exp(-x+\eta)\right]^{-1}. \quad (1)$$

The inputs to a non-input node are the outputs of the previous layer of nodes.

2. After the output is computed, the errors at each node are calculated.

3. The weights in the network are updated.

4. Finally, the biases for the output and hidden nodes are updated.

The input to the network consists of a set of features extracted from the user's signature. The features used were a combination of both global features and features specific to the particular signature.

To train the network, 5-10 user signatures are used as positive examples and 1-2 signatures from 10-15 other users are used as negative examples.

To test the performance of different network configurations, a network was trained on 6 randomly selected signatures from each user. 15 randomly selected signatures from 15 other unique participants were used as negative examples. The network was then tested on 3 of the user's signatures that were not used in the training phase. The process was repeated 5 times for each user (each time selecting a different subset), and results were gathered.

The above experiment was repeated with fast Fourier transformations and Derivatives. Both were tested with and without noise generation. Other features of the network were tested by experimentation but were not carried to completion since performance trends such as convergence and prediction accuracy were easy to identify empirically.

III. CONCLUSION

Our results indicate that the back-propagation algorithm was able to converge on more than 90% of user data and achieved a pessimistic False Rejection Rate of around 30% and a low False Acceptance Rate of 2%. We conclude that the solution presented is successful in solving the Handwritten Signature Authentication Problem.

We have found that a combination of global and local features yields the best error rates. We have also found that adding noise to the input before training makes the resulting system more robust. Transforming the input before training yields much lower error, but is more sensitive. Most importantly, we have presented system can vary in security depending on the situation.

REFERENCES

[1] Gupta, G. A. Review of Dynamic Handwritten Signature Verification. / G. Gupta, A. McCabe – Oxford, New York: Clarendon Press, 1998. – 256 p.

Anna Boyko, Georgiy Rozorynov – National Technical University of Ukraine “Kiev Polytechnic Institute”, Peremogy av., 37, Kiev, 02056, UKRAINE,
E-mail:rozor46@mail.ru