Development of Committee Neural Network for Computer Access Security System

A. Sermet Anagun

Eskişehir Osmangazi University, Industrial Engineering Department,
Bademlik 26030, Eskişehir, Turkey
sanagun@ogu.edu.tr

Abstract. A computer access security system, a reliable way of preventing unauthorized people for accessing, changing or deleting, and stealing the information, needed to be developed and implemented. In the present study, a neural network based system is proposed for computer access security for the issues of preventive security and detection of violation. Two types of data, time intervals between successive keystrokes during password entry through keyboard and voice patterns spoken via a microphone, are considered to deal with a situation of multiple users where each user has a certain password with different length. For each type of data, several multi-layered neural networks are designed and evaluated in terms of recognition accuracy. A committee neural network is formed consisting of six multi-layered neural networks. The committee decision was based on majority voting of the member networks. The committee neural network performance was better than the neural networks trained separately.

1 Introduction

A computer security system should not only be able to identify a person and let him/her access to the system if he/she has a correct security code or deny the access otherwise - *preventive security*, but also be capable of identifying the person whether he/she is indeed the right person - *detection of violations* [1]. To accomplish these goals, a software-based, a hardware-based, or a software and hardware-based security system may be used. In either case, although each person, who is eligible for accessing to the system, has his/her own security code, the code may be found with a trial-error process or stolen from the authorized person by someone else. When this occurs, the attempt made by a person may not be prevented. Due to the drawbacks of the common approaches, a different method in terms of computer access security, which may prevent copying or duplicating the security code issued, should be developed to differentiate an authorized person from the others such that valuable and/or more sensitive information for an organization should be secured.

Several researchers [2-7], in the area of computer access security, have concentrated on user identification based on individual's typing pattern, considered as a special characteristic for each person, using classical pattern recognition techniques, fuzzy algorithms, and neural networks (NNs) as powerful tools for pattern recognition and classification applications. In these studies, time intervals between successive keystrokes while entering a known and long password, an example of software-based

M. Gavrilova et al. (Eds.): ICCSA 2006, LNCS 3982, pp. 11 – 20, 2006.

security system, on a keyboard were considered as an alternative security code to prevent unauthorized person for accessing the system involved and changing some information. Since the same password has been entered by a group of people, this situation may be classified as *multiple users-single password*. In addition, the studies mentioned have focused on preventive security, which basically classifies people into two groups; people who know the correct password and who do not know, without evaluating whether they are indeed authorized.

However, due to the developments in computer technology and the complexity of information systems, which the organizations might have, there may be different situations, which needed to be considered such as *multiple users-multiple passwords*, *single user-single password*, and *single user-multiple passwords*. As discussed in [8], each of these situations may be applied to the computer access security systems considering passwords with different lengths depending on his/her preferences or system's requirements, if applicable. They proposed a multi-layered NN based computer access security system for a situation where *multiple users-multiple passwords* with different lengths. In order to identify users and differentiate valid users from invalid ones (intruder), the NN was trained using a large set of data consisted of keystroke patterns of the participants. During the data collection process proposed, the users were asked to type their own passwords and the other passwords of the remaining participants. The designed system for the *multiple users-multiple passwords* case, has provided approximately 3% error and performed better than a statistical classifier based on Euclidean distance, 13.6%.

On the other hand, the computer access security system should be designed for not only the purpose of preventive security, but also the purpose of detection of violations to make the system more reliable. In the study of [9], a NN based system has been designed and applied to the cases of *multiple users-one password* and *multiple users-multiple passwords* with different lengths for preventive security and detection of violation purposes. Two critical issues, password-dependent identification (the lengths of the passwords different) and password-independent identification (the lengths of the passwords equal) were evaluated in terms of recognition accuracy. It has demonstrated that the users were classified or attempts of an intruder were denied 98.7% of the time.

A multi-layered NN for a computer access security system trained via voice patterns, spoken passwords through a microphone is designed by [1]. It has mentioned that based on their passwords, the users were recognized approximately at a value of 5.5% using the results of the designed of experiments for the NN's parameters and performed better than a statistical classifier. Recently, Anagun [10] proposed a two-stage procedure based on sequentially organized NNs for computer access security system.

Here, an intelligent computer access security system using a committee NN consisting of multi-layered NNs trained with a backpropagation learning algorithm is proposed for a situation of *multiple users-multiple passwords*. In order to differentiate authorized person from an intruder, the data composed of time intervals between keystrokes typed via keyboard and voice patterns spoken through a microphone are obtained by means of a data collection systems designed.

2 Data Collection

The time intervals between successive characters occurred, called keystroke dynamics, while entering a password using a keyboard, and finger prints and properties of voice of a person may be considered as person-dependent characteristics. These characteristics, also called special characteristics, may be somehow used in the form of a software-based system for user identification in or to differentiate users of a computer system to secure the information stored. In the present study, two different ways for differentiating a valid user from the others are used to find a better way for a computer access security system in terms of reliability, Based on the selected special characteristics, two types of data are collected from the same group: keystroke dynamics obtained during a password entry via a keyboard and voice patterns recorded as they are being spoken through a microphone.

In order to discuss whether a system mentioned may be applicable to computer access security, a network is formed composed of group of people and passwords with different lengths are assigned to the participants according to their preferences. Afterwards, each participant is asked to enter all of the passwords, using a keyboard and a microphone, respectively, in a random order and four times (arbitrarily between 9 A.M. and 5 P.M.) a day of each week for the period of three months. After the entries completed, both keystroke dynamics and the voice patterns for each user are evaluated and additional entries are made until the necessary number of patterns has been reached statistically. The data for the same passwords belong to the same persons are obtained in a different fashion.

2.1 Keystroke Dynamics

During the password entry process, the users, each of whom has different levels of computer skills, were asked to enter his/her own password and other passwords of the remaining members of the group, which are represented by "*" during the typing process, along with a user identification number in a random order based on a proposed data collection structure. After each entry, a typed phrase via keyboard is displayed on the bottom of the screen followed by a return key.

When the password is typed correctly, the time intervals between successive characters of the password being typed are computed and automatically recorded in a file according to the user and password identification numbers.

During this process, for instance, if the password of ENGINEERING is entered by the first member of the group, the time intervals of (E,N), (N,G), (G,I), (I,N), (N,E), (E,E), (E,R), (R,I), (I,N) and (N,G) would be computed and recorded in a file. Such a file, for each entry, consists of the time intervals of the password typed, user identification number that represents who typed the password, and password identification number that represents which password typed as follows:

$$T_1\ T_2\ T_3\ ...T_N \quad U_1\ U_2\ U_3\ ...U_K \quad P_1\ P_2\ P_3\ \ldots P_J$$

where,

T_i is the i^{th} time interval for the P_j^{th} password typed by the U_k^{th} user, i = 1,2,3,...,N
P_j is the j^{th} password typed by the U_k^{th} user (0 or 1), j = 1,2,3, …,J
U_k is the k^{th} user (0 or 1), k = 1,2,3, …,K

A recorded example pattern for the second password (ENGINEERING) entered via a keyboard by the first user is given as:

22 28 16 11 6 16 11 6 16 17 0 0 0 1 0 0…0 ***0 1 0 …0***

In order to process all the data obtained from the participants within the same NN structure, the time intervals of the shortest password are made equal to the dimension of the longest password by adding a necessary number of zeros.

2.2 Voice Patterns

Many different models have been postulated for quantitatively describing certain factors involved in the speech process. One of the most powerful models of speech behavior is the linear prediction model which has been successfully applied to the related problems in recent years [11].

In speech processing, a phrase is spoken into a microphone, recorded on audio tape as waveform, and then analyzed. The recorded speech waveform has a very complex structure and continually time-varying. The waveforms are analyzed based on frames (shifted windows along with the speech sequence). As the frames dynamically move through time, considering speech is dynamic and information-bearing process, transient features of the signal may be captured [12]. In order to capture the features of the signal, linear-invariant models over short intervals of time for describing important speech events should be implemented.

There are two well-known and widely used linear prediction models; the autocorrelation and the covariance methods. The autocorrelation method is always guaranteed to produce a stable linear prediction model [11]. The solution of the model is referred to as the autocorrelation method of determining the linear prediction coefficients (LPCs) or parameters [13]. The LPCs have been shown to retain a considerable degree of naturalness from the original speech. Thus, linear prediction models have been applied to speaker identification and verification.

During the password entry process, users are asked to speak the passwords clearly through a microphone and voice patterns of the passwords sampled at 8 bit and 16 kHz are recorded and digitized using WaveStudio. The recorded voice patterns are then transformed to LPCs using the autocorrelation method by means of Matlab to represent each voice pattern as frames or Hamming windows consisting of a certain number of data points and to reduce the dimension of each pattern. After transformation, the voice patterns are represented as follows:

$$X_1\ X_2\ X_3\ .....X_M \quad U_1\ U_2\ U_3\ \ldots U_K \quad P_1\ P_2\ P_3\ \ldots P_J$$

where,

X_i is the i^{th} linear prediction coefficient of an Hamming window corresponding to the P_j^{th} password spoken by the U_k^{th} user, i = 1,2,3,...,M
P_j is the j^{th} password spoken by the U_k^{th} user (0 or 1), j = 1,2,3, …,J
U_k is the k^{th} user (0 or 1), k = 1,2,3, …,K

The recorded voice pattern for the second password (ENGINEERING) spoken through a microphone by the first user is depicted in Fig. 1.

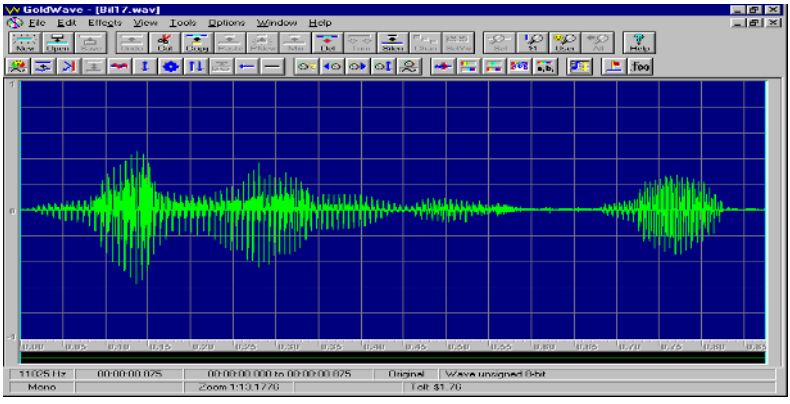

Fig. 1. Voice pattern for the password of ENGINEERING

3 Neural Network Architecture

It has been shown that a layered NN provides more potential alternatives than traditional pattern recognition techniques [1,8,14-15]. A pattern recognition technique, defined as a classification model, is concerned with performing feature extraction, learning the transparent mapping and classifying patterns [16]. For the task of pattern recognition using layered NNs, inputs correspond to features, connections between layers correspond to mapping, and outputs correspond to pattern classes. In addition, a layered NN may contain one or more hidden layers, which represent the domain knowledge and help to perform feature extraction. On the other hand, when a signal, a voice pattern, is represented in the frequency domain, as discussed in [17], signal-processing techniques can be used to determine the basic characteristics of the physical system involved. However, if a large number of examples can be obtained, NNs can be applied to eventually carry out the desired information or signal processing operation using these examples recorded either time or frequency domain [18]. Therefore, instead of signal processing techniques, the NN approach is mostly preferred for recognition and classification purposes.

In this study, two NNs, one for each type of data, are designed consisting of three layers; input, hidden, and output. Each layer is connected to the upper layer, inter-layer connections, via weights, randomly generated real values. A sigmoid function is used to determine the new activation values of the neurons in the hidden and output layers, respectively. Based on the results of the study of [19], the backpropagation algorithm is selected for training the designed NNs.

The number of neurons in the multi-layered NN architecture is varied depending on the data. The input layer is composed of 8-13 neurons, represented time intervals between successive keystrokes obtained from the passwords entered and 75-100, represented LPCs obtained from the transformation process for the passwords spoken. The number of neurons representing the user and typed/spoken password in the output layer are also varied depending on the experiments.

As indicated in [20], more neurons in the hidden layer reduce total error in training; however, fewer neurons increase the network performance in terms of

generalization, meaning that the ability to correlate a pattern with previously used patterns. For that reason, the number of neurons in the hidden layer, which yields to extract features between the input and the corresponding output pattern, are varied depending on the experiments to improve the network performance in regards to generalization. For the keystroke dynamics, the hidden neurons are varied in the range of (4-10), for the voice patterns, in the range of (30-50), respectively. The learning rate is assigned to 0.05, and momentum term to 0.3 based on designed experiments conducted by [1].

4 Experimental Results and Discussion

In regard to the computer access security system, several experiments are designed to investigate the overall performance for the system concerned. Each password is assigned to each user only based on his/her preferences. Then, the data consists of either time intervals or LPCs belong to a specific password selected by a user are introduced to a NN to initiate a *multiple users-multiple passwords* situation. This experiment is performed for both *preventive security* and *detection of violation* purposes. Since each user has a certain password to access to a part of or complete system, this situation may be considered as password-dependent recognition. The experiments are discussed in different sections and the results obtained are compared as follows.

4.1 Keystroke Dynamics Used

The collected data from password entry process were normalized time intervals based on the fraction of the largest element in the data set before presenting them to the NN. The data consisted of time intervals belong to a specific password selected by a user were introduced to a NN, which had N input and (K+J) output neurons.

The multi-layered NNs were trained using the proper data prepared for each of the experiments. In testing phase, the patterns which were not included in the training set, were fed to the designed NNs and the performance of the each NN was evaluated according to the correct/wrong classifications (Type I error). Time intervals obtained from an unauthorized person for the system involved and not included in training data were also tested to verify whether the person may be considered as an intruder (Type II error).

An overall recognition accuracy of 98.8% was obtained for training phase, and Type I and Type II errors were about 2.2% and 4.6%, respectively, in testing, since both user identification number and the pattern code of the entered password were examined simultaneously at each query. The results concluded that when the user identification number and a password for that user were questioned simultaneously, a better performance in computer access security system might be obtained.

4.2 LPCs Used

The same experiment was also conducted using LPCs in terms of preventive security and detection of violation. A three-layer NN was designed with the architectures of M input and K output neurons for the first experiment, M input and (K+J) output neurons for the second experiment, respectively. The designed NN was trained using the

normalized LPCs obtained by transforming the voice patterns. The training was maintained until a predetermined margin value was reached, then the performance of the NN was evaluated according to the Type I error. An overall recognition accuracy of 97.4% was obtained for training phase, and Type I and Type II errors were increased to 5.5% and 10.7%, respectively, in testing. Regarding with the results, the performance of this experiment was significantly lower than the previous one due to the drawbacks of the sampling procedure being used to record the voice patterns. In other words, if a security system were designed based on voice patterns, an intruder would be identified as valid user approximately 11% of the time. On the other hand, the system designed based on the keystroke patterns could not provide 100% accuracy as well.

According to the results, it has also observed that the users were easily and successfully identified and/or classified into proper groups when the sequence and placement of the characters appeared in the passwords are compatible in terms of vowel-consonant and distance between them, and the pronunciation of the passwords are appropriate in terms of linguistics.

4.3 Keystroke Dynamics and LPCs Used

Based on the results of the NNs consisted of different hidden neurons, the best three structures in terms of recognition accuracy are selected to configure a committee NN. A committee NN is then formed by recruiting six neural networks trained with different types of data into a decision-making process. The committee NN provides a reliable technique especially for speech based speaker verification when compared to a single network [21]. Addition, as mentioned in [22], a committee approach to classification is known to produce generally improved results, provided that error rates are less than 50% for each member of the committee.

In order to improve the reliability of the system concerned, a committee NN is design to be able to differentiate an authorized person from an intruder. The LPCs extracted from the speech signal and keystroke dynamics are fed to the committee NN. The decision is based on a simple majority opinion of the member networks. That is, the user may be allowed to access to the information stored if he/she is recognized by at least four out of six NNs (i.e. two of three NNs of each group producing the same results or making unanimous decision for the each attempt) as the same person. Otherwise, the attempt for the user would be rejected; thus, the information stored may be secured. The block diagram of the committee NN is shown in Fig. 2.

Both keystroke dynamics and LPCs type data obtained from the participants are used to examine the performance of the committee NN. Approximately 1.7% of the attempts are rejected by the committee NN (Type I error) due to the conflicting results obtained from the NNs trained with different types of data, although the person is authorized.

On the other hand, a tremendous reduction in the error value, approximately 4.2%, is obtained for the attempts of an intruder. That is, when special characteristics of the participants are evaluated based on a majority voting, the risk of accepting an attempt for a person although he/she is not authorized (Type II error) may be reduced. This concluded that, the committee NN had the ability to improve the reliability of the system as far as security is concerned.

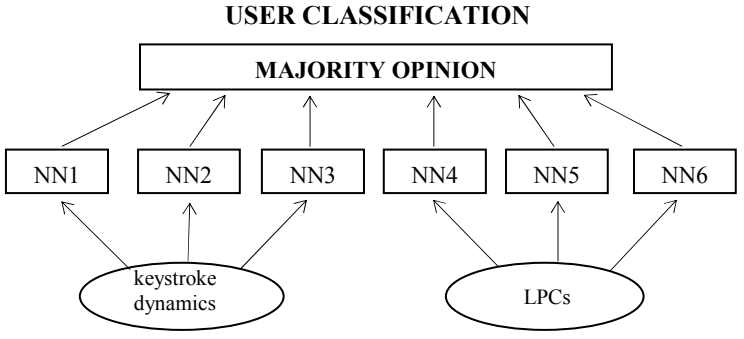

Fig. 2. Architecture of the committee NN. The first three networks are the best NNs trained with keystroke dynamics, whereas the last three networks are the best NNs trained with LPCs in terms of recognition accuracy.

5 Conclusion

In the present study, time intervals between successive keystrokes and voice patterns, which may be considered special characteristics of the users, are used to differentiate users, prevent unauthorized person to access the system, and try to detect the intruders by means of NNs. The experimental results showed that the NN trained using time intervals of a specific password along with the user identification number provided better performance.

It has observed that the data structure had a major effect on the performance of the network designed. The sequence and placement of the characters appeared in the passwords in terms of vowel-consonant and distance between them, and the pronunciation of the passwords in terms of linguistics are revealed to be considered for such a system.

Even if the voice patterns are considered as special characteristics for human beings, the NN trained by means of those patterns could not provide higher accuracy as expected. The voice pattern may be sampled at different parameters, although it increases the number of data points for each record and the training time of the neural network. The linear prediction model used in the study may be modified to produce Hamming windows consisting of more voice data to precisely capture the features of the signals. In order to improve overall performance of the system designed, a committee NN with majority voting was developed for computer access security system in the case of *multiple users-multiple passwords*. Based on the results, it has been observed that the committee NN was able to differentiate attempts made by the authorized person from an intruder with the accuracy of 98.3%, whereas 95.8% of the attempts made by an intruder were declined by the committee NN.

Other issues, such as seeking better security code alternatives (e.g. fingerprints, handwritten signatures, smart cards, and images) to differentiate users more precisely, investigating distinct NN architectures in terms of the number of neurons/layers, types of connections and the cases of *single user-single password*, *multiple users-single password*, and *single user-multiple passwords* to be able to implement this approach in an on-line mode are still available for further investigation.

References

1. Anagun, A.S.: An Artificial Neural Network Approach for a Computer Access Security System Based on the Characteristics of the Users. Endüstri Mühendisliği. 10 (1999) 3-11
2. Hussein, B.R., McLaren, R., Bleha, S.A.: An Application of Fuzzy Algorithms in a Computer Access Security System. Pattern Recognition Letters. 9 (1989) 39-43
3. Bleha, S.A., Slivinsky, C., Hussein, B.: Computer-Access Security Systems Using Keystroke Dynamics. IEEE Transactions on Pattern Analysis and Machine Intelligence. 12 (1990) 1217-1222
4. Bleha, S.A., Obaidat, M.S.: Dimensionality Reduction and Feature Extraction Application In Identifying Computer Users. IEEE Transactions on Systems, Man, and Cybernetics. 21 (1991) 452-456
5. Obaidat, M.S., Macchairolo, D.T., Bleha, S.A.: An Intelligent Neural Network System for Identifying Computer Users. ASME Intelligent Engineering Systems through Artificial Neural Networks. Ed. Dagli *et al*., 1 (1991) 953-959
6. Bleha, S.A., Obaidat, M.S.: Computer Users Verification Using the Perceptron Algorithm. IEEE Transactions on Systems, Man, and Cybernetics. 23 (1993) 900-902
7. Obaidat, M.S,. Macchairolo, D.T.: An On-Line Neural Network System For Computer Access Security. IEEE Transactions on Industrial Electronics. 40 (1993) 235-242
8. Anagun, A.S., Cin, I.: An Alternative Way for Computer Access Security: Password Entry Patterns. Proceedings of the 18th National Conference on Operations Research and Industrial Engineering, Istanbul, Turkey. (1996) 17-20
9. Anagun, A.S., Cin, I.: A Neural Network Based Computer Access Security System for Multiple Users. Computers and Industrial Engineering. 35 (1998) 351-354
10. Anagun, A.S.: Designing a Neural Network Based Computer Access Security System: Keystroke Dynamics and/or Voice Patterns. International Journal of Smart Engineering Design. 4 (2002) 125-132
11. Markel, J.D., Gray Jr., A.H.: Linear Prediction of Speech. Springer-Verlag, New York (1982)
12. Deller Jr., J.R., Proakis, J.G., Hansen, J.H.L.: Discrete-Time Processing of Speech Signals. Macmillian Publishing Co., New York (1993)
13. Rabiner, L.R., Schafer, R.W.: Digital Processing of Speech Signals. Prentice-Hall, Englewood Cliffs (1978)
14. Burr, D.J.: Experiments on Neural Net Recognition of Spoken and Written Text. IEEE Transactions on Acoustics, Speech, and Signal Processing. 36 (1988) 1162-1168
15. Huang, W., Lippmann, R.: Comparisons between Neural Networks and Conventional Classifiers. Proceedings of the 1st International Conference on Neural Networks, (1987) 485-494
16. Pao, Y.H.: Adaptive Pattern Recognition and Neural Networks. Addison-Wesley, Reading (1989)
17. Freeman, J.A., Skapura, D.M.: Neural Networks: Algorithms, Applications, and Programming Techniques. Addison-Wesley Publishing Co., Reading (1991)
18. Soucek, B.: Neural and Concurrent Real-Time Systems - The Sixth Generation. John Wiley-Sons., New York (1989)
19. Anagun, A.S.: A Multilayered Neural Network Based Computer Access Security System: Effects of Training Algorithms. Lecture Series on Computer and Computational Sciences. 4B (2005) 1604-1607

20. Klimasauskas, C.C.: Applying Neural Networks, Part III: Training a Neural Network. PC AI. (1991) 20-24
21. Reddy, N.P., Buch, O.A.: Speaker Verification Using Committee Neural Networks. Computer Methods and Programs in Biomedicine. 72 (2003) 109-115
22. Jerebko, A.K., Malley, J.D., Franaszek, M., Summers, R.M.: Multiple Neural Network Classification Scheme for Detection of Colonic Polyps in CT Colonography Data Set. Academic Radiology. 10 (2003) 254-160