User Identification Based on Handwritten Signatures with Haptic Information

Fawaz A Alsulaiman, Jongeun Cha and Abdulmotaleb El Saddik

Multimedia Communications Research Laboratory (MCR Lab)
School of Information Technology and Engineering (SITE)
University of Ottawa, Ottawa, Canada
fawaz@mcrlab.uottawa, jcha@discover.uottawa.ca,abed@mcrlab.uottawa.ca

Abstract. In this paper we focus our research on user identification rather than user verification by analyzing handwritten signature and haptic information such as pressure. For analysis, a multilayer perception (MLP) neural network is adopted. In order to verify the proposed method, 16 users' signatures were measured with haptic information. We successfully identified users at an average success rate of 81%.

Keywords: Haptics, Identification, Authentication, Biometrics, Neural Networks.

1 Introduction

With the automation of everyday transactions and the increased dependency on computers, the shift of large assets from the traditional form into the digital form requires a similar automation shift in the protection of such assets. In this shift, one important security aspect is authentication. Authentication is the process of validating who you are to whom you claim to be. One commonly used authentication method is textual passwords, where a secret word is selected and presented every time a user must be authenticated. However, passwords can be forgotten, written down, recorded, and shared with friends and family members [1].

In order to avoid these defects, biometrics, which makes use of the personal physiological and behavioral characteristics, is introduced for the purpose of identification or verification. Identification answers the question "who or what is this", while verification verifies who you claim to be. Fingerprints, hand geometry, palm print recognition, face recognition, iris recognition, retina recognition, voice signature, hand written signature recognition, and gait recognition are all different types of biometrics. Some researchers have focused on the haptic characteristics of users, such as force profile when writing a signature, as biometrics information. They have investigated the possibility of haptic authentication. The idea is based on the assumption that every human behaves and touches objects in a unique way.

Most authentication systems verify the user at the beginning when a user logs into a system. However, no further authentication is applied while using the system's assets. Several scenarios can occur (and are not limited to):

1. The user might forget to sign out and then an intruder can abuse such an opportunity.
2. The user might willingly share his/her password with a friend or a family member.
3. An intruder might interfere and impersonate the legitimate user and abuse the legitimate user's privileges.

Keystroke dynamics observes the user's keyboard usage behavior and tries to build a user pattern in order to detect the user's authenticity all the time [2, 3, 5, 6, 7]. The work of analyzing the behavior of user interaction is extended to the mouse as well. Since most users rely on the mouse rather than the keyboard, a user pattern of mouse movements is built to continuously authenticate users [8, 9].

However, in the continuous authentication process, sometimes we need to identify users for forensic purposes. For example, when an intruder attacks a system, he should be identified and the system should be able to provide information about the intruder. In this paper, we propose an identification process based on a handwritten signature and haptic information captured when writing the signature rather than verification. The remainder of this paper is organized as follows: Section 2 discusses related works. Section 3 studies haptics hand signature identification methodology. Section 4 presents the experimental results. Finally, section 5 concludes and discusses future work.

2 Related Works

Observing haptic characteristics for authentication is a new field of research. Orozco et al. [11] examined users' haptic characteristics based on a maze application. They used the Hidden Markov Model (HMM), spectral analysis and time warping and reached probability of verification up to 78.8% with 25% FAR (False Acceptance Rate). Moreover, they reached an identification success rate of 50% using HMM among four users.

Malek et al. [13] use haptics to prevent shoulder surfing attacks on graphical passwords. A shoulder surfing attack is performed by an adversary by watching over a user's shoulder or recording the legitimate user's graphical passwords or textual passwords. The proposed scheme partially prevents shoulder surfing attacks since the attacker can still observe the graphical password but not the forces applied while performing the graphical password. They [14] further enhance such a scheme by using artificial neural networks (ANN) and nearest neighbor (NN). NN allowed for 92% probability of verification (PV), and ANN resulted in PV of 90%.

El Saddik et al. [12] analyzed the relative entropy of different haptic features and introduced the entropic signature that represents the uniqueness of each user's biometrical features. Based on a virtual check application, they calculated the probability of verification (PV) as 50% with 25% FAR and based on a maze application they calculated PV of 95% at 4.5% FAR. They concluded that haptic interfaces are more suited to verification rather than identification. However, we propose a system that is targeting the identification process and argue that the haptic information can be used for identification.

3 Identification of Hand Written Signatures Based on Haptics

3.1 Handwriting Environment

The handwriting environment provides a virtual environment where users can write their signature on a virtual plate as shown in Fig. 1. The users grab and move the end-effector of the haptic device as a pen and its 3-dimensional position is mapped to a cursor in the virtual environment. When the cursor collides against a white rectangular virtual plate, the users can feel the repulsive force based on the penalty-method and red dots are drawn on the collision position. A Phantom OMNI haptic device [4], which can measure 3-dimensional position and orientation of the end-effector, is used as the haptic device.

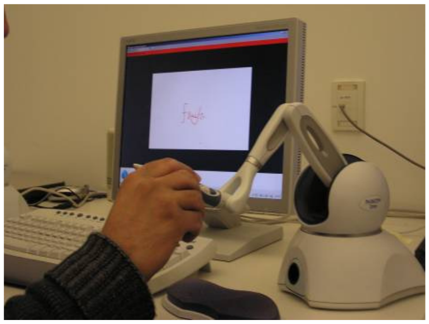
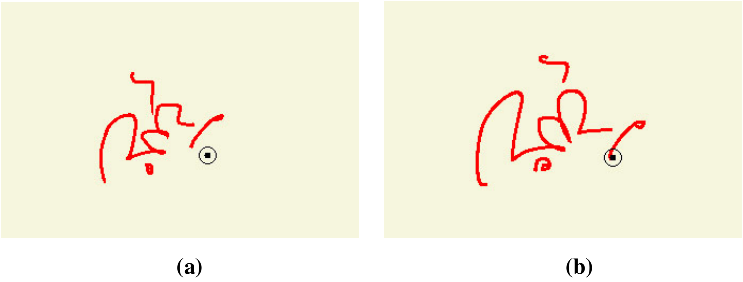


Fig.1. The handwriting environment.

3.2 Feature Extraction and Selection

Many attributes have been incorporated as features in our system. When a user writes his/her signature on a virtual plate, as shown in Fig. 1, the 3-dimensional position (p), force applied (f), velocity (v), angular rotation (a) and timestamp (t) of the virtual pen-tip were measured. A simple element that represents a state in our system can be represented as $s = \{p_x, p_y, p_z, f_x, f_y, f_z, v_x, v_y, v_z, a_x, a_y, a_z, t\}$ where subscript x, y, and z represent spatial dimensions. Fig. 2 shows two handwritten signature trials on the virtual place performed by a user (the 6th user in our experiment described below). Each trial consists of thousands of s elements.



(a) **(b)**

Fig.2. (a) A snapshot shows the 6th user's signature sample. Various haptic properties are not visible but considered in the identification process. The black dot represents the graphical representation of the pen-tip controlled by the haptic device. (b) A snapshot of another sample of the same 6th user's signature. The variation of the positions and scalability compared to (a) is visible.

3.3 User Identification

Identification is the process that answers the question "what is this? Or who is this?" or it is the classification process in a pattern recognition paradigm. In the identification process, we consider the following attributes: position, velocity, force, and angular rotation. Slight variations in some attribute values are acceptable and the system can still identify the right user.

Through the data analysis, we observed that attributes that have been usually considered independent have some correlation with other attributes, such as the relationship between the attribute f_z to v_x and v_y, or the relationship between attributes p_x, p_y, p_z to a_x, a_y, a_z. Such correlation varies from user to user. This observation leads us to choose a multilayer Perceptron (MLP) neural network (NN) [15, 16] that seeks the level of correlation between attributes to identify each individual user. We applied a supervised learning approach based on a back propagation algorithm with momentum of 0.2 and a learning rate of 0.3. The MLP-NN has 14 input neurons that are connected to hidden layers of 15 neurons and connected to 16 output neurons. Every input neuron is connected to a single attribute while every output neuron is connected to a single class. All analyses were performed with the support of the Weka data mining tool [10].

Each user tried writing the same signature 12 times. The MLP-NN is trained with the first six trials of each user. Therefore, the neural network will contain whole users' templates. The last six trials are purely dedicated to test purposes to verify our assumption of user identification.

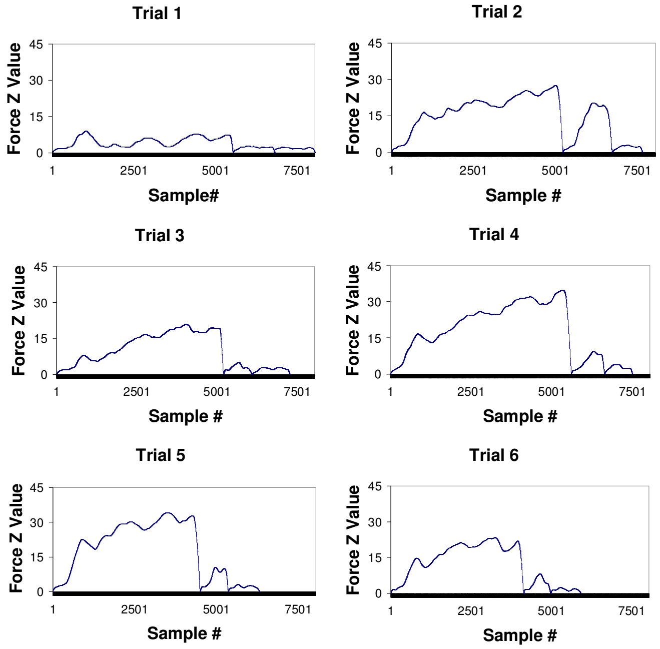


Fig.3. The representation of the first six trials for raw force Z values that forms part of the 6th user's template.

4 Experimental Results

This section presents some experimental results. It discusses the data acquisition and enrollment and reports the identification results.

Data Acquisition

Sixteen users of different ages (25~35), and sexes (2 females, 14 males) have volunteered to participate in the experiment. The experiment setup is illustrated in Fig. 1. Some of the users have never experienced a haptics application before. Therefore, we introduced the touch-enabled environment. We requested from every user to provide twelve handwritten signatures using our system. We do not start the experiment until the user feels comfortable with the environment and after signing at least once without any complications. For users who have experienced haptic devices, we start capturing their signatures from the second trial. Most of the users showed interest in such application. However, we noticed that after a few trials most users felt fatigued.

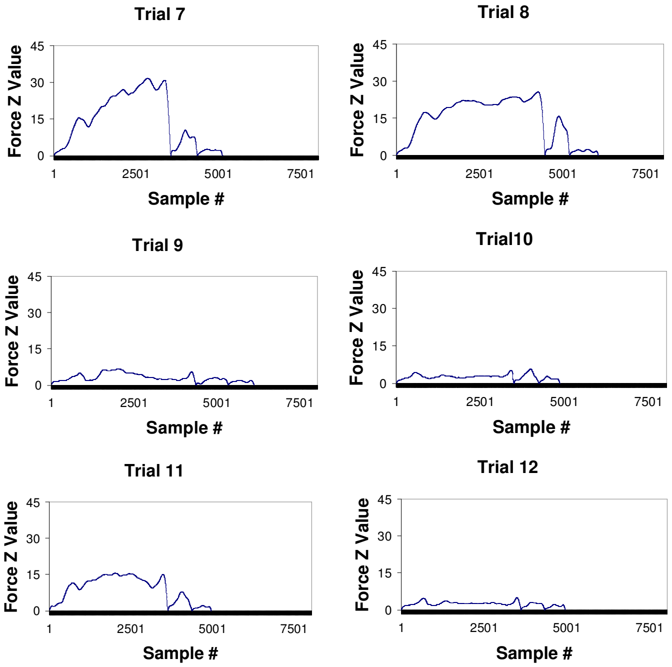


Fig.4. Representation of the 6th user's last six trials based on Force Z values. The last six trials are part of the test process.

Enrollment

As stated in section 3, in order to form the templates of the signatures with haptic information, the first six signatures for each user were used. One important issue is identifying the attributes and features that should be considered to form the template. Moreover, identifying the number of trials that can be considered sufficient to reach acceptable levels of identification is a field of research.

Identification Results

The rich haptic information such as force, velocity and angular rotation gathered during the creation of the user's handwritten signature and the consistency in the user's behavior motivate us to facilitate such an opportunity not only to verify users but also to identify them. Fig. 3 shows the force z values taken from the first six trials of the 6th user while Fig. 4 illustrates them for the last six trials performed by the same user. After applying the identification methodology described in section 3, we reached an average success rate of 81% on trial seven and 75% in trial eight as illustrated in Fig.5. That is identifying 13 users successfully. We noticed that some users felt fatigued after a few trials and some other users became more familiar with the sense of touch environment, which might have caused changes in the user's behavior in the subsequent trials. This may have affected the average success rate.

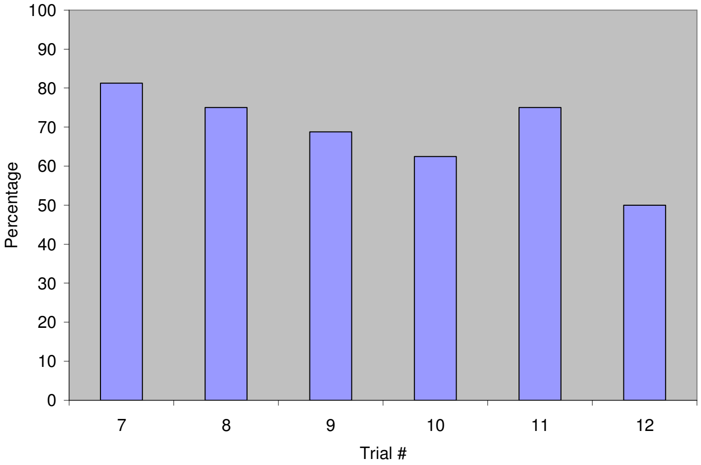


Fig.5. The average success rate of identification for 16 users based on trial number considering using the first six trials in the learning process. The identification rate for the 7th and 8th trials resulted in identification success rate of about 81% and 75% respectively.

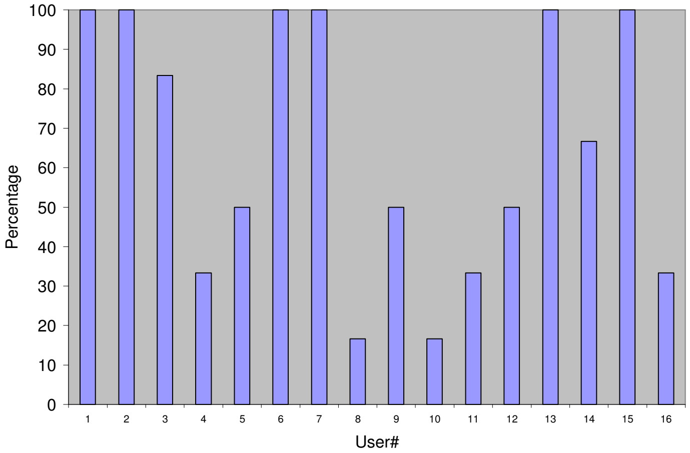


Fig.6. The success rate of identification for 16 users considering the first six trials for learning and the last six trials for test. We can notice that some user has 100% success rate.

However, if we consider the success rate per user as illustrated in Fig.6, we can notice that six users is identified with success rate of 100% while the remaining users success rates varies from 83% to 16%.

5 Conclusion and Future Work

In this paper, we have shown that a handwritten signature with haptic information can be used for identification purposes. User identification can be extended to identify a user's handwriting in general, which is very useful in the forensics field. Still, our methodology and most other reviewed methodologies require the user to perform the same task such as solving a simple maze or, in our case, handwriting signatures. This is not applicable for continuous authentication since it is not realistic to ask users to write their signature or to solve a maze all the time. However, this work is the first building block towards reaching a continuous authentication system based on haptic characteristics.

References

1. S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, M. Furlong: Password sharing: implications for security design based on social practice. In Proc. ACM CHI 2007 Conference on Human Factors in Computing Systems 2007. pp. 895-904.
2. R. Joyce, G. Gupta. Identify authentication based on keystroke latencies. Communications of the ACM. Vol.33, Issue.2, 1990. pp. 168-176.
3. F. Monrose, A. Rubin, Authentication via keystroke Dynamics. In Proc 4th ACM Conference of Computer and Communication Security. 1997. pp. 48-56.
4. http://www.sensable.com/haptic-phantom-omni.htm. Site accessed January 2008.
5. F Monrose, M K. Reiter, S Wetzel. Password Hardening based on keystroke dynamics. In Proc. 6th ACM Conference of Computer and Communication Security. 1999. pp.73-82.
6. J. Lee, S. Choi, B. Moon: An evolutionary keystroke authentication based on ellipsoidal hypothesis space. In Proc. 9th annual conference on Genetic and evolutionary computation (GECCO),2007. pp.2090-2097.
7. C. Jiang, S. Shieh, J. Liu. Keystroke statistical learning model for web authentication. In Proc. 2nd ACM symposium on Information, computer and communications security Conference. 2007. pp. 359-361.
8. M. Pusara, C.Brodley. User re-authentication via mouse movements. In Proc. 2004 ACM workshop on Visualization and data mining for computer security. 2004. pp.1-8.
9. H. Gamboa, Ana Fred. An Identity Authentication System based on Human Computer Interaction Behaviour. In Proc. 3rd International Workshop on Pattern Recognition in Information Systems, 2003. pp. 46-55.
10. I. Witten, E. Frank. Data Mining: Practical machine learning tools and techniques. 2nd Edition, Morgan Kaufmann, San Francisco, 2005.
11. M. Orozco, Y. Asfaw, S. Shirmohammadi, A. Adler, A. El Saddik. Haptic-Based Biometrics: A Feasibility Study. In Proc. Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems. 2006. pp. 256-271.
12. A. El Saddik, M. Orozco, Y. Asfaw, S. Shirmohammadi, A. Adler. A Novel Biometric System for Identification and Verification of Haptics Users. IEEE Transaction on Instrumentation and Measurement, Vol.56, No. 3, June 2007.

13.B. Malek, M. Orozco, A. El Saddik, "Novel Shoulder-Surfing Resistant Haptic-based Graphical Password", Proceedings of the Eurohaptics 2006 conference, Paris, France, July 2006.

14. M. Orozco, B. Malek, M. Eid, A. El Saddik, Haptic-Based Sensible Graphical Password. In Proc. Virtual Concept 2006, Playa Del Carmen, Mexico, November 2006.

15. F. Rosenblatt. The perceptron: A probabilistic model for information storage and organization in the brain. Psychological Review, 1958 , Vol.65, pp. 386-408.

16. F. Rosenblatt. Principles of Neurodynamics. Perceptrons and the Theory of Brain Mechanisms. Washington, D.C., Spartan books, 1961.