

# Keystroke and Eye-Tracking Biometrics for User Identification

Daniel L. Silver and Adam J. Biggs

Intelligent Information Technology Research Laboratory,  
Jodrey School of Computer Science, Acadia University,  
Wolfville, Nova Scotia, Canada B4P 2R6  
[danny.silver@acadiau.ca](mailto:danny.silver@acadiau.ca)  
phone:902-585-1105, fax: 902-585-1067

**Abstract.** Two sources of weak biometric data are investigated for the development of user identification models. A probabilistic neural network model is created from keystroke digraph features extracted from raw typing data. A second model is developed from scan-path features extracted from raw eye-tracking data. A third model is created from a combination of features from the two biometric sources. Experimental results show that models based on keystroke biometric data perform very well, whereas the models involving the eye-tracking data are not as successful but encourage further study.

Keywords: biometric modeling, probabilistic neural networks, eye-tracking, keystroke analysis.

## 1 Introduction

The objective of this research is to develop and compare user models that can accurately identify a user of a computer from keystroke and eye-tracking biometric data [1]. The motivation is to find inexpensive methods to harden conventional computer security methods, such as a username/password pair.

The term *biometrics* refers to a measurable, physical characteristic or personal behavioral trait used to recognize the identity of a person. There are two different classes of biometrics, namely: strong and weak. *Strong biometrics* are biological characteristics that are meant to be unique over an entire population. Fingerprints and DNA patterns are forms of strong biometrics that are often used to identify criminals and victims of crime. *Weak biometrics* are behavioural characteristics that are statistically different among small groups of individuals. Some examples of weak biometrics are facial, gait, voice and handwriting patterns [5].

Using typing or keystroke patterns as a weak biometric was proposed as early as 1980 [2]. Keystroke biometrics requires no additional hardware, so cost is kept low. The technique relies on the habitual typing rhythms that people develop. Features of a user's typing pattern can be extracted using information about adjacent keystrokes called *keystroke digraphs*. For the word 'none' the digraphs would be 'no', 'on', and 'ne'. Each digraph has six associated features determined by the press and release of keys. For example the  $NpOr$  feature would record the time period between the 'n' press,

and the ‘o’ release. Additional features that can be extracted from typing patterns are the number and type of mistakes.

Eye-tracking research reported in the psychology and HCI literature focus on gaze-point data for modeling user attention or pupil dilation to measure cognitive load [8, 7]. There are few papers on the use of eye-tracking biometrics for user identification, however, it has been observed that individuals have different eye *scan paths* [4]. A scan path, defined as the trajectory of eye movement over a visual stimulus, contains a number of fixations and saccades; with the number, duration, order and placement of the fixations and saccades varying among individuals [3]. A *fixation* is when the eye focuses on a particular point and stays there for a period of time, normally between 100ms and 1000ms. A *saccade* is the rapid motion of the eyes between fixation points, with velocities as high as 500 degrees per second [8].

Probabilistic Neural Networks (PNN) are recommended for classification problems and have the advantage of fewer parameters as compared with other types of neural networks [9]. PNNs train quickly because they only require one iteration through the input data and are known to do well on sparse data sets [11]. A PNN has as many outputs as there are possible categories. In the case of user identification, each output category represents a user. After training, each output node generates the expected probability of the associate category, given the input values, with the highest output predicting the classification.

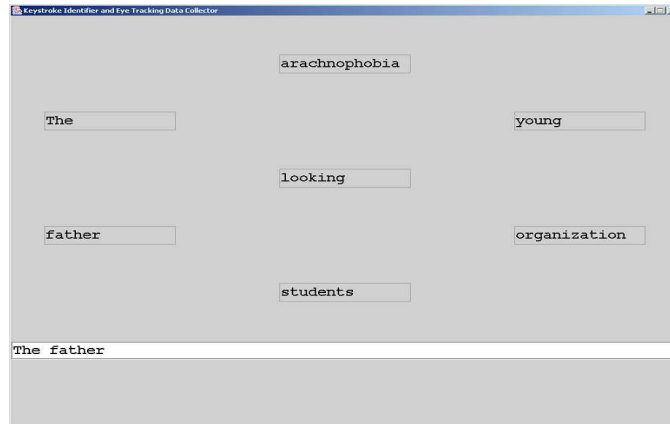
## 2 Biometric Feature Extraction

The following summaries our theory as to the most appropriate eye-tracking and keystroke biometric features for user identification and the methods of data extraction used to obtain these features.

**Eye-Tracking Features.** Our approach is to extract those features from raw eye-tracking data that preserve the key characteristics of the scan path for each user as they read and type words into a computer system. The field of view for each computer user is divided into four areas: output (where the words are displayed), input (the area where the words are retyped), keyboard (the area below the screen), and other (all the remaining field of view not included in the three previous areas). Figure 1 shows the layout of the collection screen.

We considered five categories of eye-tracking features. *Specific fixations*, considers the 8 most significant (longest duration) fixations extracted from the raw eye-tracking data. The  $x, y$  coordinates and duration are recorded. The *number of fixations* category records the count of fixations in each area of view and over all areas. The features provide information on how a user reads while typing. Better readers tend to have fewer fixations in the input area than poor readers. The *fixation duration* category records the average duration of fixations for each of the four areas and over all areas. Fixation durations help distinguish between fast and slow typists, fast and slow readers, and people that do and do not look down at the keyboard while typing. *Saccade information* provides features of user eye movements between fixations. The average velocity of the eyes during saccades is extracted along with the average duration. The *miscellaneous features* category includes the time it takes to type all the words and the average vertical position of the user’s gaze when looking at the output area.

**Keystroke Features.** The screen used to capture the raw keystroke data is the same as for the eye-tracking data. Commonly typed character sequences guide the choice of keystroke digraphs to be extracted from the raw keystroke data. The common



**Fig. 1.** A screen shot of the data collection program, showing the layout of the screen.

character sequences that are used in our system are “The”, “ing”, “you”, “an”, “er”, “oo”, and “ts”. The average time to press the space bar and the total number of mistakes are also extracted from the raw data.

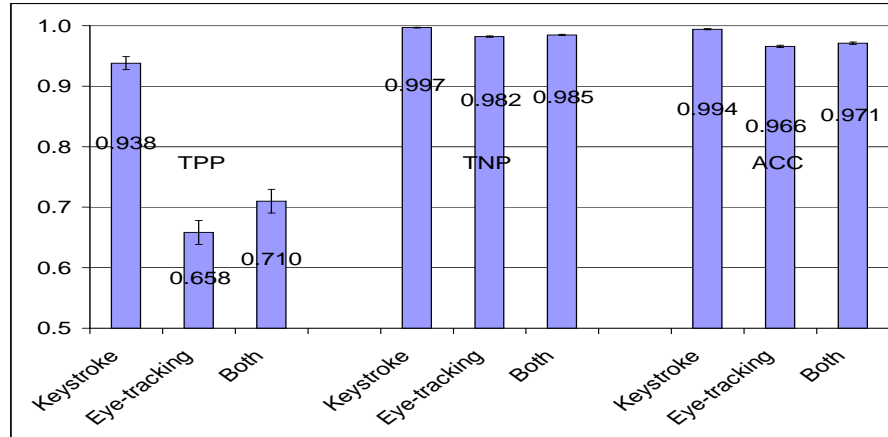
### 3 Experimentation

To test the efficacy of keystroke and eye-tracking biometrics we conducted an experiment that compared user identification models developed from data collected from 21 university students between 20 and 30 years of age.

**Material and Methods.** The biometrics were collected by users interacting with a desktop PC running MS Windows XP with the eye-tracking camera mounted under a 17 inch CRT display screen. The LC Technologies’ Eyegaze System was used capture eye movement [10, 1]. The system uses the video tracking method called *pupil center/corneal reflection* and is capable of 60 samples per second.

A scenario that allowed keystroke and eye-tracking data to be collected at the same time was required. This turned out to be a significant challenge. To obtain the best keystroke data, each user should type the same set of words several times (to decrease the variation in digraphs), but this creates poor eye-tracking data because users tend to memorize aspects of the words and look less at the display. The best eye-tracking data is obtained when users read complex words requiring attention; unfortunately, such words do not facilitate the capture of common key sequences. To overcome this problem, 16 examples of eye-tracking and keystroke biometric data are collected as a user reads and types back different sets of words. Figure 1 shows how the words are spread across the user’s field of view so as to ensure a wide range of eye movement. The first of the sixteen sets of words is displayed on the screen with one word in each of the seven word locations. The user types back the words in any order and then presses “Enter”. Users were limited to using the backspace key to correct mistakes. To focus user attention, if any word is misspelled, the user is required to retype the set of words.

The raw data files are parsed and the extracted biometric features are written along with the associated user ID to a text file. Two parameters are required to extract the



**Fig. 2.** Results of the experiments showing the mean TPP, TNP and Accuracy (95% conf. intervals) for the three user identification models over the 21 users studied.

fixation data: the length of a minimum fixation (set to 85 milliseconds, or 5 eye-tracking samples) and the maximum gaze-point deviation (set to 12 pixels). The gaze-point deviation is how many pixels a gaze-point can vary from the current fixation position and still be considered at the same fixation.

The NeuroShell 2 neural network package from Ward Systems Group is used to create the PNN user identification models [11]. NeuroShell 2 imports the biometric data file and generates random sets of training, test and production examples that contain equal number of examples for each user (8 for training, 3 for validation and 5 for test). Twenty models were created for each of the three comparative biometrics (keystroke, eye-tracking and combination of keystroke and eye-tracking) from random mixes of the user data.

**Results.** Figure 2 summarizes the mean true positive (TPP) and true negative (TNN) proportions as well as the mean accuracy (ACC) over the 20 models developed for the 21 users. The analysis focuses on the TPP because it is the most important comparative statistic. The keystroke biometric models are successful with a mean TPP of .9381, however the eye-tracking biometric models and combination models are less successful at .6583 and .7099, respectively. The difference between the keystroke biometric models and the eye-tracking models is statistically significant based on a hypothesis T-test ( $p=0.0018$ ). In fact, the worst performance by the keystroke biometric based model over all users was a TPP of 0.75. Although the models developed from eye-tracking biometric features failed to be as successful, the mean TPP result of .6583 is an improvement over the .4372 result obtained in earlier research [1]. This suggests that further enhancements to the method might be possible.

## 4 Conclusion and Future Work

The experimental results of the user identification models based on keystroke biometrics support the findings of Peacock (TPP of .92) [6] and Biggs (TPP of .8564) [1]. We

conclude that keystroke biometrics are a viable method of identification for a small population of users ( $n \leq 30$ ). The method could be adapted to act as an extra layer of security for user name and password authentication.

The less satisfactory results of the models involving eye-tracking biometrics indicate that more characteristic biometric features need to be developed. Existing features might be combined so as to reduce input dimensionality while at the same time adding prior knowledge of the problem domain. We intend to conduct a series of studies to determine those eye-tracking features that are most unique to individual users and less susceptible to noise. Because of the improved results over that reported in [1], we suspect a system that uses a larger field of view would ensure a wider variance in eye-tracking features among users. Finally, images could be used to collect better scan path data without the user being distracted by typing. We have considered this approach and are investigating eye-tracking features that are invariant for a user over different images.

**Acknowledgement:** This research has been funded by a Canadian NSERC grant and by equipment contributions from LC Technologies, of Fairfax, VA.

## References

1. Adam Biggs. Keystroke and eye-tracking biometrics for user identification, 2003. Honours thesis. Acadia University, Wolfville, Nova Scotia.
2. R. Stockton Gaines, William Lisowski, S. James Press, and Norman Shapiro. Authentication by keystroke timing: Some preliminary results. *Rand Report R-256-NSF*, 1980.
3. Albrecht Werner Inhoff, Robin Morris, and John Calabrese. Eye movements in skilled transcription typing. *Bulletin of the Psychonomic Society*, 24(2):113–114, 1986.
4. Benjamin Law, M. Stalla Atkins, A. E. Kirkpatrick, and Alan J. Lomax. Eye gaze patterns differentiate novice and experts in a virtual laparoscopic surgery training environment. *Proceedings of the Eye Tracking Research and Applications Symposium, San Antonio, Texas*, pages 41–48, 2004.
5. Simon Liu and Mark Silverman. A practical guide to biometric security technology. *IEEE Computer Society, IT Profession - Security*, 2000.
6. Alen Peacock, Xian Ke, and Matthew Wilkerson. Typing patterns: A key to user identification. *IEEE Security and Privacy*, 2(5), 2004.
7. Ralph Radach and George W. McConkie. Determinants of fixations positions in words during reading. 1998.
8. Keith Rayner. Eye movements in reading and information processing: 20 years of research. *Psychological Bulletin*, 124(3):372–422, 1998.
9. Donald F. Specht. Probabilistic neural networks. *Neural Networks*, 3(1):41–48, 1990.
10. LC Technologies. The eyegaze development system: A tool for eyetracking applications. 2000. LC Technologies Inc, Fairfax, VA.
11. Steve Ward. Neuroshell 2 release 4.0 users manual, 2000. Ward Systems Group, Inc., Frederick, MD.