This is a pre-print. Final version of the paper is published at SPIE conference on Biometric Technology for Human Identification IX, 2012

CUE: Counterfeit-resistant Usable Eye Movement-based Authentication via Oculomotor Plant Characteristics and Complex Eye Movement Patterns

Oleg V. Komogortsev*, Alexey Karpov, Corey D. Holland
Texas State University – San Marcos, 601 University Drive, San Marcos, TX, USA, 78666

ABSTRACT

The widespread use of computers throughout modern society introduces the necessity for usable and counterfeit-resistant authentication methods to ensure secure access to personal resources such as bank accounts, e-mail, and social media. Current authentication methods require tedious memorization of lengthy pass phrases, are often prone to shoulder-surfing, and may be easily replicated (either by counterfeiting parts of the human body or by guessing an authentication token based on readily available information). This paper describes preliminary work toward a counterfeit-resistant usable eye movement-based (CUE) authentication method. CUE does not require any passwords (improving the memorability aspect of the authentication system), and aims to provide high resistance to spoofing and shoulder-surfing by employing the combined biometric capabilities of two behavioral biometric traits: 1) oculomotor plant characteristics (OPC) which represent the internal, non-visible, anatomical structure of the eye; 2) complex eye movement patterns (CEM) which represent the strategies employed by the brain to guide visual attention. Both OPC and CEM are extracted from the eye movement signal provided by an eye tracking system. Preliminary results indicate that the fusion of OPC and CEM traits is capable of providing a 30% reduction in authentication error when compared to the authentication accuracy of individual traits.

Keywords: Biometrics, authentication, eye tracking, eye movements, oculomotor plant, scanpath, brain.

1. INTRODUCTION

Communication between human and computer frequently begins with an authentication request. During this initial phase of interaction, the user supplies the system with verification of his/her identity, often in the form of an alphanumeric password, graphically encoded security phrase, or biometric token (such as an iris or fingerprint scan). In cases where the user is prompted to select the identification key from a sequence of numeric or graphic symbols, there is a danger of accidental or intentional shoulder-surfing, whether performed directly or through the use of hidden recording mediums. Moreover, these problems are exacerbated in multi-user environments, where shared workstation usage and contemporary interaction media often lead to an increased likelihood of both intentional and unintentional shoulder-surfing [1]. Authentication methods requiring memorization of images and symbols have reduced usability, due to the fact that long, sophisticated passwords can be easily forgotten, and short passwords are easy to break. Biometric methods such as iris and fingerprint-based authentication are not completely fraud-proof, as they are based on body characteristics that can be replicated [2-5]. As a result, there is a rising need for usable, shoulder-surfing-resistant, and counterfeit-resistant authentication techniques [1, 6-10].

The proposed CUE authentication can contribute to the resolution of these needs. First, CUE is more usable than password-based techniques due to its biometric nature, requiring no memorization. Second, CUE is shoulder-surfing-resistant, as eye movements and gaze position are hardly observable from the third-person view. Third, CUE is significantly counterfeit-resistant, as it employs the internal, non-visible, anatomical structure of the eye along with the brain's visual attention strategies. The internal, non-visible, anatomical structure of the eye is represented by *Oculomotor Plant Characteristics* (OPC) that include the neuronal control signal and the physical properties of the eye globe's surrounding tissues, ligaments, and extraocular muscles. The brain's visual attention strategies are represented by *Complex Eye Movement* patterns (CEM) that are exhibited in response to specific stimuli. OPC and CEM traits exist only in a living individual, and cannot be easily forged. OPC and CEM-based authentication methods have been investigated previously [11, 12], however, the fusion of OPC and CEM has not been previously considered. Such fusion is

* ok11@txstate.edu; phone 1 512 245-0349; fax 1 512 245-8750; web-page www.cs.txstate.edu/~ok11

particularly attractive because the biometric traits extracted from the OPC and CEM are physiologically different, but may be captured by the same camera sensor. This manuscript provides a unique contribution to the field of biometrics by fusing OPC and CEM traits into a single CUE framework and assessing the resulting advantages of the authentication accuracy; however, this work does not explicitly assess the usability of the CUE framework or its counterfeit resistance potential, these topics will be explored in future work.

2. RELATED WORK

2.1 Passwords

There are several issues related to the use of passwords for authentication. Selection of strong passwords is time consuming, users frequently select passwords that are easy to predict, and re-use passwords across multiple accounts [13]. Easy to remember passwords are easy to break, whereas strong passwords are often difficult to remember [14]. A substantial amount of research has been conducted on the use of graphical passwords in the authentication process, taking into account the human capacity to recall images more easily than text or numbers [8, 15-17]. While graphical passwords are easier to remember, such methods can reveal personal information about the user, may be time consuming, or may offer low accuracy. The CUE technique frees the user from difficult memorization.

2.2 Shoulder-surfing

The possibility of shoulder-surfing reduces the usability of an authentication system, making the user uncomfortable. Research has been conducted on shoulder-surfing resistance, employing an eye gaze-based entry systems [7, 17] or introducing auxiliary tactile input devices during authentication [6, 18]. Eye gaze guided input presents a challenge in multi-user environments (viz. tabletops) where people sit in front of each other, providing an opportunity to estimate user gaze direction [19] and thus reducing the security of such input. The use of auxiliary input devices improves resistance to shoulder-surfing, but can result in longer selection times (30-50% increase) due to additional overhead or confusion [6]. As well, such techniques do not fully protect against intruders correctly guessing the user's password. The CUE technique provides shoulder-surfing-resistant authentication, as visual feedback does not reveal any information about the user.

2.3 Counterfeiting

Advanced biometric methods such fingerprint and iris scans provide a reliable basis for authentication; however, they are generally vulnerable to counterfeiting, and can often be replicated with modern technological advances [2-5] or by removal of the body part necessary for authentication. The CUE technique is void of these challenges because it employs the dynamic characteristics of the oculomotor plant and brain functions which exist only within a living individual. The replication of traits considered in this paper is exceedingly difficult with present and foreseeable methodologies.

2.4 Person Identification via Eye Movements

In the field of human-computer interaction, the human visual system primarily exhibits two major types of eye movement: fixations, in which the eye maintains visual acuity on a stationary object of interest; and saccades, in which the eye rotations rapidly between points of fixation with velocities reaching 700°/s. Sequences of fixations and saccades form scanpaths, which may be interpreted as the brain's visual attention strategy for a given stimulus. Scanpath theory originated from the idea that individuals tend to repeat certain scanpath trajectories during repeated viewings of a given pattern. This phenomenon was first investigated by Noton and Stark [20], who found that the general scanpath displayed by a subject during the first viewing of a pattern was repeated in the initial eye movements of roughly 65% of subsequent viewings. Additional properties of scanpaths which make them promising candidates as a behavioral biometric include: subconscious reproduction, variation by subject, and variation by stimulus.

Previous research in biometric identification via eye movements employed raw eye positional data [21, 22] and a few characteristics related to fixation and saccades [23]. Komogortsev et al. [11] proposed a method of biometric identification based on the anatomical characteristics of the oculomotor plant, using a jumping dot stimulus to facilitate OPC extraction. Holland and Komogortsev [12] investigated eye movement biometrics based on the scanpaths formed during reading. In this work, instead of scanpaths we use a more general term, Complex Eye Movement patterns (CEM), that incorporates the individual and aggregated characteristics belonging to a scanpath, details of which are discussed in Section 3.2. The combination of OPC and CEM biometric traits has not been considered or evaluated in previous research. The current work investigates both under the umbrella of the CUE approach.

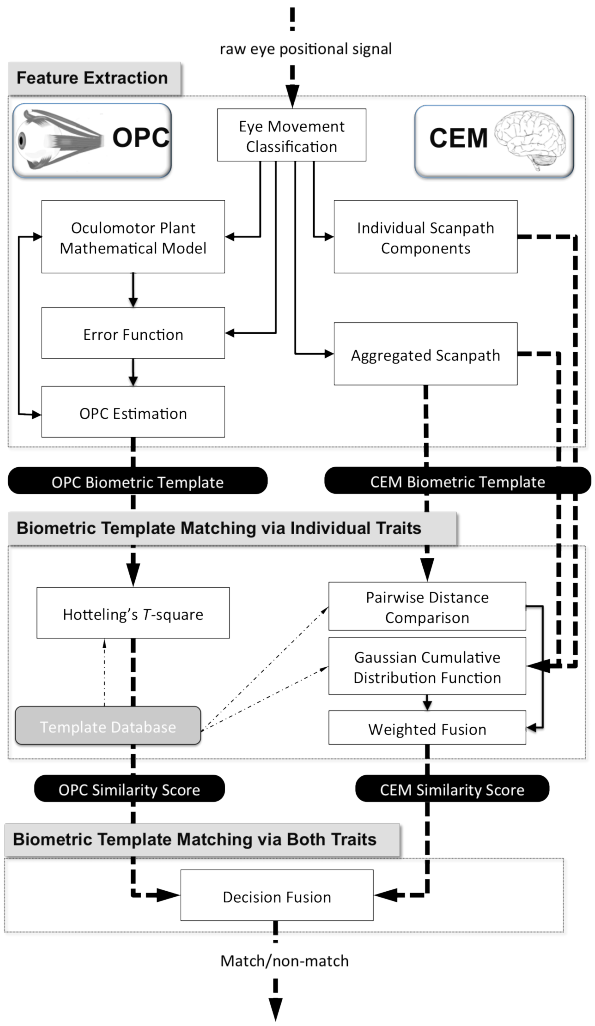

Figure 1. CUE overview.

3. CUE AUTHENTICATION

Figure 1 presents a structural overview of CUE authentication driven by the OPC and CEM biometric modalities.

3.1 Authentication via Oculomotor Plant Characteristics

The left portion of Figure 1 provides an overview of the OPC-based biometrics approach. This section provides a brief description of each module, more detailed descriptions are available in [11].

After the authentication stimulus is presented to the user, the eye tracking system sends the recorded eye movement signal to an *Eye Movement Classification* algorithm, which extracts fixations and saccades from the signal. The extracted saccade trajectories are passed to the *Oculomotor Plant Mathematical Model* which attempts to simulate the supplied trajectories. The error between recorded and simulated trajectories is measured by the *Error Function*, and the magnitude of the resulting error triggers *OPC Estimation* that produces a new set of OPC values with the goal of minimizing error. The OPC values that simulate recorded trajectories with minimal error become the OPC biometric template for a given individual.

The following OPC are included in the biometric template:

- **Length Tension** – *the relationship between the length of an extraocular muscle and the force it is capable of exerting.*

- **Series Elasticity** – *resistive properties of an extraocular muscle while the muscle is innervated by the neuronal control signal.*
- **Passive Viscosity** *of the eye globe.*
- **Agonist Force-Velocity Relationship** – *the relationship between the velocity of agonist muscle extension/contraction and the force it is capable of exerting.*
- **Antagonist Force-Velocity Relationship** – *the force-velocity relationship for the antagonist muscle.*
- **Tension Intercept** – *intercept coefficient in the linear relationship between the force that a muscle applies to the eye and the rotational position of the eye during fixation*.
- **Agonist Tension Slope** – *slope coefficient in the linear relationship between the force that an agonist muscle applies to the eye and the rotational position of the eye during fixation*.
- **Antagonist Tension Slope** – *tension slope coefficient for the antagonist muscle.*
- **Eye Globe's Inertia.**

The template containing these OPC is passed to matching module driven by Hotteling's *T*-square test, producing a matching score between the computed template and the template already stored in the database. Additional OPC discussed in [11] are not part of the considered template; however, their default values are used in saccade trajectory simulation by the oculomotor plant mathematical model.

3.2 Authentication via Complex Eye Movement Patterns

3.2.1 Structural overview

The right portion of Figure 1 provides an overview of the CEM-based biometrics approach. This section provides a brief description of each module, more detailed descriptions are available in [12].

The raw *Eye Movement Data* produced during a recording is supplied to the *Eye Movement Classification* module. The fixations and saccades forming complex eye movement patterns are processed by two modules: the *Aggregated Scanpath Characteristics* module and the *Individual Scanpath Components* module. Both modules operate with characteristics that are representative of the brain's visual attention strategies. Individual characteristics processed by each module are discussed next.

Individual Scanpath Components include:

- **Fixation Count** – *number of detected fixations.*
- **Average Fixation Duration** – *sum of the duration of all fixations detected, divided by fixation count.*
- **Average Vectorial Saccade Amplitude** – *sum of vectorial saccade amplitudes, divided by the total number of saccades, where the vectorial amplitude of a saccade is defined as the Euclidean norm of the horizontal and vertical amplitudes.*
- **Average Horizontal Saccade Amplitude** – *average amplitude of the horizontal component of saccadic movement.*
- **Average Vertical Saccade Amplitude** – *average amplitude of the vertical component of saccadic movement.*
- **Average Vectorial Saccade Velocity** – *sum of vectorial saccade velocities, divided by the total number of saccades, where the vectorial velocity of a saccade is defined as the Euclidean norm of the horizontal and vertical velocities.*
- **Average Vectorial Saccade Peak Velocity** – *sum of vectorial saccade peak velocities, divided by the total number of saccades.*
- **Velocity Waveform Indicator (Q)** – *the relationship between the duration it takes to reach saccadic peak velocity to the total saccade duration.*
- **Amplitude-Duration Relationship** – *the relationship between the amplitude of a saccade and its duration.*
- **Main Sequence Relationship** – *the relationship between the amplitude of a saccade and its peak velocity.*

Aggregated Scanpath Characteristics include:

- **Scanpath Length** – *total amplitude of all detected saccades.*
- **Scanpath Area** – *area of the convex hull formed by fixation points.*

- **Regions of Interest** – *total number of spatially unique regions identified by applying a spatial mean shift clustering algorithm to the sequence of fixations that define a scanpath.*
- **Inflection Count** – *number of directional shifts in the scanpath.*
- **Fixation Distance** – *aggregated representation of the scanpath defined by fixation points and their coordinates.*

Characteristics obtained by the Aggregated Scanpath Characteristics and Individual Scanpath Components describe the CEM related biometric template.

When two CEM-based biometric templates are compared, all characteristics except Fixation Distance are compared via a Gaussian cumulative distribution function (CDF) that generates a similarity score with value 1 indicating a match and value 0 indicating a non-match. Fixation Distance characteristics are compared via a pairwise distance comparison between the positional centroids of fixations. The total difference is normalized to produce a similarity score with the value indicated above.

The *Weighted Fusion* module produces a combined similarity score via a weighted average of similarity scores produced by each individual metric. Weights for individual metrics are produced empirically. The resulting similarity score is employed for biometric verification, or serves as an input to the *Information Fusion* module combining OPC and CEM biometrics.

3.3 Information Fusion

The similarity scores provided by OPC and CEM are considered for the final match/non-match decisions based on the following information fusion approaches.

3.3.1. Logical OR, AND

The logical fusion method employs individual decisions from the OPC and CEM modalities in the form of 1 (match) or 0 (non-match) to produce the final match/non-match decision via logical OR (or AND) operations. Using the logical OR method, at least one modality must indicate a match for the final match decision. Using the logical AND method, both modalities must indicate a match for the final match decision.

3.3.2. MIN, MAX

The MIN (or MAX) fusion method makes use of the smallest (or largest) similarity score generated by the OPM and CEM modalities, and employs a threshold to arrive at the final decision (if the resulting value is larger than the threshold, a match is indicated, otherwise it is considered a non-match).

3.3.3. Weighted summation

The weighted summation method is performed via the formula $p = \alpha \bullet A + (1 - \alpha) \bullet B$. Here p is the resulting score, A and B stands for scores derived from the OPC and CEM modalities, and $0 \leq \alpha \leq 1$ is the weight. The resulting score, p, is compared with a threshold value, and if p is greater than the threshold a match is indicated, with a non-match indicated otherwise.

4. METHODOLOGY

4.1 Apparatus

Eye movement data was recorded using the EyeLink 1000 eye tracker, with a sampling frequency of 1000 Hz [24]. Stimuli were presented on a 30-inch flat screen monitor positioned at a distance of 685 millimeters from the subject, with screen dimensions of 640 × 400 millimeters, and screen resolution of 2560 × 1600 pixels. A chin rest was employed to ensure stability in the collected data.

4.2 Participants & Data Quality

Eye movement data is collected for a total of 32 subjects (26 males / 6 females), ages 18 – 40 with an average age of 23 (SD = 5.4). Mean positional accuracy of the recordings averaged between all calibration points was 0.74° (SD = 0.54°). 29 of the subjects performed 4 recordings each, and 3 of the subjects performed 2 recordings each, generating a total of 122 unique eye movement records.

4.3 Visual Stimulus & Recordings

Visual stimuli were selected to invoke eye movements which facilitate the extraction of biometric templates and to avoid compromising system security if seen by a shoulder-surfer. Based on these requirements, random text excerpts were extracted from Lewis Carroll's "The Hunting of the Snark" and presented to participants. This poem was chosen for its difficult and nonsensical content, forcing participants to progress slowly and carefully through the text.

For each recording, text excerpts were chosen to require roughly 1 minute to complete and participants were given 1 minute to read. Participants were given a different excerpt for each recording session, and excerpts were selected to ensure the difficulty of the material was consistent, line lengths were consistent, and that learning effects did not impact subsequent readings.

The first two recordings for each subject were conducted during the same session, with a 20 minute break between recordings, and the second two recordings were performed a week later, again with a 20 minute break between recordings.

The recordings are publically available as the Dataset III in the Eye Movement Biometric Database (EMBD) v1 [25].

4.4 Performance Evaluation

The performance of biometric authentication methods is evaluated via the false acceptance rate (FAR) and false rejection rate (FRR) metrics. FAR represents the percentage of imposter records accepted as authentic users and FRR indicates the amount of authentic user records rejected from the system. To simplify the presentation of results, half total error rate (HTER) is reported, which is defined as the averaged combination of FAR and FRR.

The performance of CUE and its components is calculated across all possible combinations of eye movement records. For example, considering 3 eye movement records (A, B, and C) produced by unique subjects, similarity scores are produced for the combinations: A + B, A + C, B + C. For 122 eye movement records, this results in 7381 combinations that are employed for acceptance and rejection tests for both methods.

OPC biometrics considered only the horizontal component of recorded saccades with amplitude greater than 1° and duration over 4 milliseconds, discarding micro saccades and noisy saccadic events. As a result, the average horizontal amplitude was 3.42° (SD = 3.25) prior to filtering and 3.79° (SD=3.26) after filtering. The average magnitude of vertical components prior to filtering was quite small (M=1.2° SD=3.16), therefore vertical components were not considered for OPC derivation due to the high signal/noise ratio of the vertical component of movement.

5. RESULTS

Table I presents authentication accuracy and Figure 2 provides the corresponding Receiver Operating Characteristic (ROC) curves.

Table I. Authentication results for each biometric modality, including similarity thresholds that produced the minimum HTER for each method.

Method Name	Thresholds	FAR	FRR	HTER
CUE = OPC	$p_{CUE} = 0.1$	30%	24%	27%
CUE = CEM	$p_{CUE} = 0.5$	26%	28%	27%
CUE = (OPC) OR (CEM)	$p_{OPC} = 0.8$ $p_S = 0.6$	22%	24%	23%
CUE = (OPC) AND (CEM)	$p_{OPC} = 0.1$ $p_S = 0.2$	25%	26%	25.5%
CUE = MIN(OPC, CEM)	$p_{CUE} = 0.1$	30%	24%	27%
CUE = MAX(OPC, CEM)	$p_{CUE} = 0.6$	25%	20%	22.5%
CUE = w_1•OPC+ w_2•CEM	$p_{CUE} = 0.4$	20%	18%	19%
CUE = 0.5•(OPC) +0.5•(CEM)	$p_{CUE} = 0.4$	17%	22%	19.5%

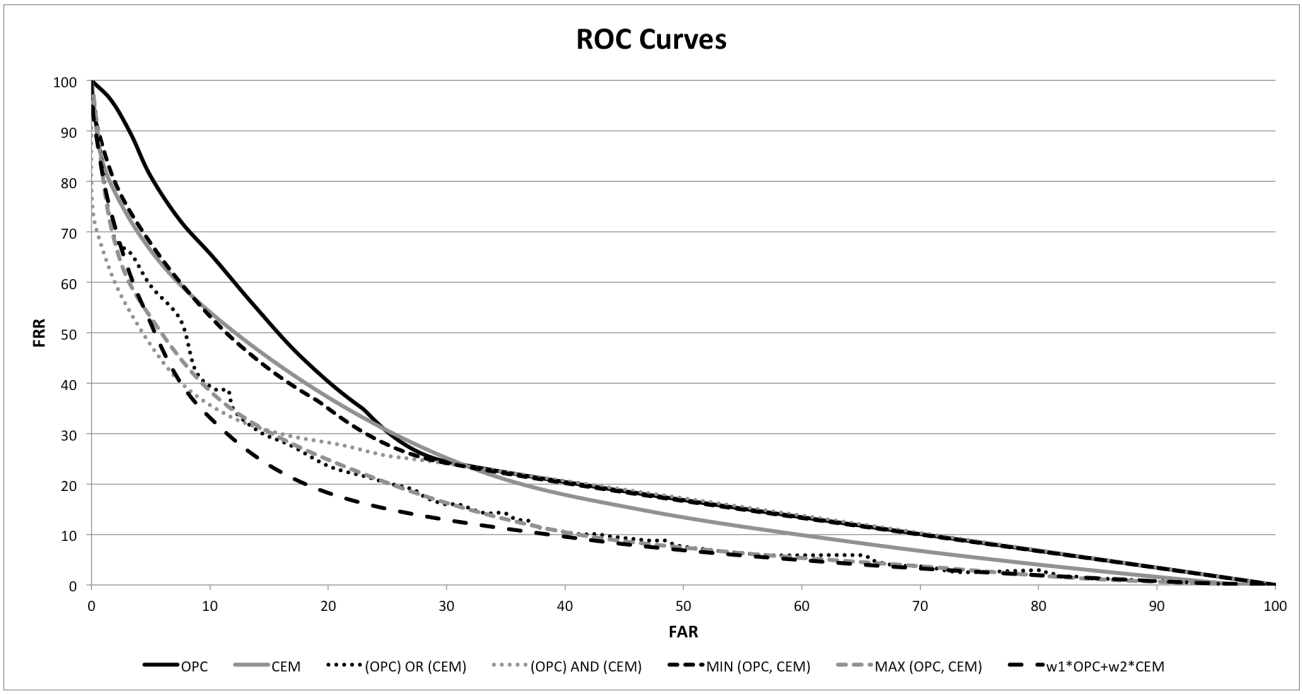

Figure 2. ROC curves for CUE, driven by various authentication methods.

The results indicate that OPC biometrics can be performed successfully for a reading task, where the amplitude of saccadic eye movements is relatively small. The HTER of 27% is slightly lower than the HTER of 31% previously achieved by Komogortsev et al. using a jumping dot stimulus [11].

Both OPC and CEM performed with similar accuracy, providing an HTER of 27%. Fusion methods improved the achievable accuracy, providing an HTER of 19% for the best performing weighted addition (where $w_1 = 0.45$ and $w_2 = 0.55$). These results indicate an approximately 30% reduction in authentication error. In a case in which the weights of both OPC and CEM modalities are equal, the CUE is able to achieve the HTER of 19.5%.

6. DISCUSSION

6.1 Recording Equipment & Stimuli

The CUE authentication technique was conducted on very accurate eye tracking equipment with a very high sampling frequency, and participant head position was maintained through the use of a chin rest to avoid potential accuracy issues. Additional research is required to understand the tradeoffs between authentication accuracy and eye tracking specifications such as sampling frequency, positional accuracy, and freedom of head movements.

As well, the current work employed a text-based stimulus for extracting OPC and CEM characteristics. Different types of stimuli may produce different authentication results.

6.2 Stability of the OPC and CEM Traits

Biometric templates were collected within a one week interval that provides extremely limited insight in terms of the stability of considered traits over a longer time span and the impact of such factors as stress, fatigue, aging, and illness. Additional research must be conducted to explore the long-term stability of CUE authentication.

7. CONCLUSIONS

This work illustrates the feasibility of a counterfeit-resistant usable eye movement-based (CUE) authentication method that combines information from two behavioral biometric traits: oculomotor plant characteristics (OPC) and complex eye movement patterns (CEM). The results demonstrate that the combined approach is capable of increasing authentication accuracy by up to 30% when performance is compared to each individual trait. Among considered fusion methods, the weighted summation method provided the highest authentication accuracy.

It should be pointed out that in its current form, CUE may be employed only as a soft biometric approach due to the relatively high achievable half total error rate (HTER) of 19%. It is possible to hypothesize that CUE may function as part of a more general Ocular Biometrics approach, in which additional traits such as iris and periocular information are included to provide higher authentication accuracy. Such a multi-modal Ocular Biometrics approach is particular attractive, as it requires only one camera sensor to obtain information from all ocular traits.

Additionally, our results indicate that OPC performance during a reading task (HTER = 27%) is comparable to its performance during the presentation of jumping dot stimulus (HTER = 31%), indicating that OPC biometrics may be effective for a variety of stimuli.

Future research will be directed toward: the incorporation of CUE into a unified multi-modal Ocular Biometrics framework; evaluation of CUE's usability and counterfeit resistance; construction of a larger eye movement database; and improvement of the individual performance of OPC and CEM components.

8. ACKNOWLEDGEMENTS

This work is partially funded by Texas State University – San Marcos and a grant from the National Institute of Standards #60NANB10D213.

9. REFERENCES

[1] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson, and P. Olivier, "Multi-touch authentication on tabletops," presented at the Proceedings of the 28th international conference on Human factors in computing systems, Atlanta, Georgia, USA, 2010.

[2] J. M. Williams, "Biometrics or ... biohazards?," presented at the Proceedings of the 2002 workshop on New security paradigms, Virginia Beach, Virginia, 2002.

[3] A. Jain, L. Hong, and Y. Kulkarni, "A Multimodal Biometric System Using Fingerprint, Face, and Speech," in *Proceedings of the International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, 1999, pp. 182-187.

[4] J. G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Trans. Pattern Anal. Mach. Intell.,* vol. 15, pp. 1148-1161, 1993.

[5] L. Wiskott, "Face recognition by elastic bunch graph matching," 1997, pp. 129-129. http://doi.ieeecomputersociety.org/10.1109/ICIP.1997.647401

[6] A. D. Luca, E. v. Zezschwitz, and H. Humann, "Vibrapass: secure authentication based on shared lies," presented at the Proceedings of the 27th international conference on Human factors in computing systems, Boston, MA, USA, 2009.

[7] A. D. Luca, R. Weiss, H. Humann, and X. An, "Eyepass - eye-stroke authentication for public terminals," presented at the CHI '08 extended abstracts on Human factors in computing systems, Florence, Italy, 2008.

[8] T. S. Tullis and D. P. Tedesco, "Using personal photos as pictorial passwords," presented at the CHI '05 extended abstracts on Human factors in computing systems, Portland, OR, USA, 2005.

[9] L. Coventry, A. D. Angeli, and G. Johnson, "Usability and biometric verification at the ATM interface," presented at the Proceedings of the SIGCHI conference on Human factors in computing systems, Ft. Lauderdale, Florida, USA, 2003.

[10] O. V. Komogortsev, U. K. S. Jayarathna, C. R. Aragon, and M. Mechehoul, "Biometric Identification via an Oculomotor Plant Mathematical Model," in *Proceedings of the ACM Eye Tracking Research & Applications Symposium (ETRA)*, Austin, TX, 2010, pp. 1-4.

[11] O. V. Komogortsev, A. Karpov, L. Price, and C. Aragon, "Biometric Authentication via Oculomotor Plant Characteristic," in *IEEE/IARP International Conference on Biometrics (ICB)*, 2012, pp. 1-8.

[12] C. Holland and O. V. Komogortsev, "Biometric Identification via Eye Movement Scanpaths in Reading," IEEE International Joint Conference on Biometrics (IJCB), 2011, pp. 1-8.
[13] D. Florencio and C. Herley, "A large-scale study of web password habits," presented at the Proceedings of the 16th international conference on World Wide Web, Banff, Alberta, Canada, 2007.
[14] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'Weakest Link' -- a Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal,* vol. 19, pp. 122-131, 2001.
[15] E. Stobert, "Usability and strength in click-based graphical passwords," presented at the Proceedings of the 28th of the international conference extended abstracts on Human factors in computing systems, Atlanta, Georgia, USA, 2010.
[16] W. Moncur and G. Leplatre, "Pictures at the ATM: exploring the usability of multiple graphical passwords," presented at the Proceedings of the SIGCHI conference on Human factors in computing systems, San Jose, California, USA, 2007.
[17] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords," presented at the Proceedings of the 28th international conference on Human factors in computing systems, Atlanta, Georgia, USA, 2010.
[18] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: authentication usable in front of prying eyes," presented at the Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, Florence, Italy, 2008.
[19] A. Duchowski, *Eye Tracking Methodology: Theory and Practice*, 2nd ed.: Springer, 2007.
[20] D. Noton and L. Stark, "Scanpaths in Eye Movements during Pattern Perception," *Science,* vol. 171, pp. 308-311, January 22, 1971 1971.
[21] P. Kasprowski and J. Ober, "Eye Movements in Biometrics," presented at the Proceedings of the European Conference on Computer Vision (ECCV), 2004.
[22] P. Kasprowski, "Human identification using eye movements," Ph.D., Faculty of Automatic Control, Electronics and Computer Science, Silesian University of Technology, Gliwice, 2004.
[23] L. S. Daniel and J. B. Adam, "Keystroke and Eye-Tracking Biometrics for User Identification," in *Proceedings of the International Conference on Artificial Intelligence (ICAI)*, 2006, pp. 344-348. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.88.4306
[24] EyeLink. (2010). *EyeLink II*. Available: http://www.sr-research.com/EL_1000.html
[25] O. V. Komogortsev. (2011). *Eye Movement Biometric Database v1*. Available: http://www.cs.txstate.edu/~ok11/embd_v1.html