AN ANALYSIS OF EYE MOVEMENT BASED AUTHENTICATION SYSTEMS

Yun Zhang*1,2
1School of Computer Science
Northwestern Polytechnical University, Xi’an, Shaanxi, China

Zheru Chi†2
2Centre for Multimedia Signal Processing
Department of Electronic and Information Engineering
The Hong Kong Polytechnic University
Hong Kong, China

Dagan Feng‡2,3
3School of Information Technologies
The University of Sydney
Sydney, Australia

ABSTRACT

No matter how sophisticated an authentication system has been devised, human is often considered as the weakest link in the security chain. Security problems can stem from bad interactions between humans and systems. Eye movement is a natural interaction modality. The application of eye tracking technology in authentication offers a promising and feasible solution to the tradeoff between the usability and the security of an authentication system. This paper presents a comprehensive study on existing Eye Movement Based Authentication (EMBA) methodologies and systems, and briefly outlines the technical and methodological aspects of EMBA systems. We decompose the EMBA technique into three fundamental aspects: (1) eye movement input modality, (2) eye movement interaction mechanism, and (3) eye movement pattern recognition. The features and functions of the EMBA modules are further analyzed. Emphasis is given on the interrelationship among the modules and their general impacts on the formation and function of the EMBA framework. The paper attempts to provide a systemic treatment on the state of the art technology and also to outline some potential future development directions in eye movement based interaction and security systems.

Keywords: Eye Tracking; Authentication; Human Computer Interaction; Fixations; Saccades.

INTRODUCTION

Eye tracking technology is very promising as an alternation or an auxiliary channel to human-computer interaction (HCI). Applications of eye movements to real time user interfaces can be divided into two categories: (1) using eye movements as a directly control tool, such as a non-touchable mouse pointer for the disabled [1, 2], and (2) analyzing eye movements to obtain the user’s intention and then to facilitate the interaction environment, such as interactive graphical displays [3, 4] and interface usability measurements [5, 6]. The two areas utilized the eyes’ behavioral features and attentional features, respectively.

The authentication system, as a specific application of eye movement based interaction, happens to be an ideal combination of the two features. First of all, from the perspective of interaction modality, eye tracking device is highly resistant to shoulder surfing which is done either by simply looking over a victim’s shoulder, or using technical devices like binoculars or miniature cameras to get the personal identification number (PIN) [7]. Secondly, from the perspective of system usability, eye tracking based interaction is different from the traditional alpha-number schemes. New authentication mechanism, such as a graphical password system is more fitting for the human innate memory capability [8-11]. Last but not least, from the perspective of system security, eye movement is also a unique biometric trait which is determined by both conscious and subconscious viewing behaviors. Such information can be combined with other channels to enhance the validity of identification.

In light of the significance of eye tracking techniques to security system, this paper aims to establish a framework of Eye Movement Based Authentication (EMBA) system and to briefly outline the technical and methodological aspects of each EMBA systems modules. By the comprehensive cases studies of present six EMBA systems, we try to provide a valuable reference and boost further research of such brand new areas.

EYE MOVEMENT BASED AUTHENTICATION FRAMEWORK AND TECHNICAL MODULES

The general structure of an eye movement based authentication system is different from that of a conventional authentication system [12]. In spite of its different applications, an EMBA system in general consists of the following three main modules:

I. Eye movement input modality
   - Fixation based interaction
   - Saccades based interaction

II. Eye movement interaction mechanism
   - Alphabetic password mechanism
   - Graphical password mechanism

III. Eye movement pattern recognition/identification
   - Knowledge based identification
   - Biometrics based identification

Figure 1. EMBA system framework and technical Modules.

A. Eye movement input modality

The input module is the first step and the most principal component to be considered. In other words, what kind of
features from eye movements you choose will determine the whole design of the system.

Fixation based interaction shows the static characteristics of the human vision system, which is the eye movement to stabilize the retina over a stationary object of Area of Interest (AOI). Sometimes, it can also be defined as the total duration and the average location of a series of fixations within an AOI [13]. Fixation based interaction, or sometimes called “gaze-based interaction” [2], has long been the predominant techniques in eye movement based HCI as a real-time input medium. The user’s fixations are extracted and utilized as a pointing device, like a mouse. By fixating his eye for a certain period of time (dwell time), the user can activate the particular command (or input).

Saccades based interaction is kind of dynamic characteristics, which are the discrete movements that quickly change the orientation of the eyes, thereby translating the image of the object of interest from an eccentric retinal location to the fovea. Saccades based interaction is a recently emerged technique [14]. Unlike the fixation based interaction, the saccades based interaction utilizes the dynamic features of eye movements to transmit the user’s personal information or command. A typical example of such dynamic features is scan path, which is an eye movement pattern composed of series of saccades. Different patterns can be assigned to different input commands for HCI.

B. Eye movement interaction mechanism

Eye tracking technology provides a new interaction mechanism to strengthen the existing security techniques. Despite its simplicity, alphanumeric password constantly suffers from prevalent eavesdropping or spoofing problem, moreover, its security and usability always conflict with each other. People are not good at remembering the safe but long PIN number. An alternation is graphical password, which is first proposed by Greg Blonder [8] to replace the precise recall of a PIN by image recognition. It is a skill at which humans are proficient. The tradeoff, whereas, is that graphical password seems more vulnerable to shoulder surfing attack. For instance, the larger image interface can be more exposed to those malicious attacks, despite the potential bigger password space. Equipped with eye tracking techniques, EMBA systems provide a feasible solution. By combining “tradition mechanism” with “novel input (eye tracker)”, both of the password system not only reserve the well-established usability but considerably increase their security as well.

C. Eye movement data recognition/identification

The first two modules are to select and collect the eye movement data for EMBA system. The last module’s function is to process those data to authenticate the user.

Knowledge-based mechanisms [15] are the most widely used identification method today. The user needs to remember the PIN or password and the system verifies an encrypted version of the user input to a stored encrypted copy. Biometrics based authentication is another option which uses physical /or behavioral (learned) characteristics to replace the PIN/password [16]. Eye movement characterizes human’s physiological and perceptual behaviors at the same time, which constitutes a rich source of personal characteristics and features. Exploration of such a source may lead to a new approach for foolproof or multivariate dynamic identification systems.

CASES STUDY

No matter how an EMBA system is designed, it is a special case of eye movement based HCI. Consequently, the following six cases are categorized by their eye movement input modalities to explain (1) how the three modules of the EMBA system are working together and (2) what are the detailed techniques and methodologies within each module.

D. Fixation based interaction

Kumar and their group proposed a “fixation based interaction + alphanumeric password mechanism + knowledge based identification” prototype. Their system, named EyePassword, retains the traditional alphanumeric password mechanism in order to reduce shoulder surfing attacks [17]. EyePassword uses the on-screen keyboard and tracks the users’ fixations as the password entry. In doing so, their EMBA system retains the simplicity of a traditional password scheme. The only difference to the user is to enter the passwords by “looking at them” instead of “clicking them”. To enhance the fixation-based interaction, the authors developed a series of designs of different target sizes, keyboard layouts, trigger mechanisms and feedbacks. The first two parameters need to be optimized to overcome the eye tracker’s limitation on resolution and accuracy. The second two approaches are proposed to solve the problems in active vision control. The purpose is to track data for an eye tracking system without ambiguity. As a typical knowledge-based identification, EyePassword is a most straightforward application of eye tracking techniques in the authentication system. It retains the established user’s habits while making the stealing virtually impractical in the fixation-based interaction.

Maeder et al. [18] and Hoanca et al. [19] proposed two “fixation based interaction + graphical password mechanism + knowledge based identification” prototypes. Different from Kumar’s system, their design is motivated by the graphical password mechanism. Maeder et al.’s work uses a nature image instead of an on-screen keyboard. The visual objects or features of the image serve as the symbol set. The user just fixates in a specified sequence on those features or objects to input the PIN. In order to distinguish possible image objects from the other regions, the image is superimposed with 3x3 non-uniform grids to help identify the distinctive fixations and gazes. Hoanca’s work is based on a well-known graphical password Passfaces[20]. Instead of a nature image, the Passfaces interface is composed of human faces pictures, usually 3x3 tiles. The user is asked to fixate on the prescribed faces among the decoy ones for authentication. Such technique is based on the assumption that people can recall human faces better than any other pictures. Hoanca’s contribution is to use eye tracking in Passfaces and to refine the authentication algorithm. Furthermore, such kind of interfaces provide a predictable object’s location and the error area, which may increase the certainty of the user’s attentive fixations.

Different from the previous two cases, Maeder and Fookes[21] presented a visual attention based biometric identification, which is featured by “fixation based interaction + graphical password mechanism + biometrics based identification”. Usually fixation permits a subject to view an AOI near the centre of the field with a high resolution, which is known as foveal. In this respect, visual attention acts as a “spotlight”, and by analyzing the spatial and temporal patterns of fixation sequences, the traits of overt or cover viewing
behaviors can be disclosed. The authors undertook a set of conscious and sub-conscious viewing experiments and the eye movement patterns were processed to find the individual features. They estimated the number of fixations, the order of fixations, the first five fixations and their numbers of revisits. The preliminary statistics of fixations show greater intra variances than inner variances. However, further work is needed to solve the problems with identification and validation, which are the two basic issues of a biometric system.

E. Saccades based interaction

De Luca et al. [22, 23] proposed a “saccades based interaction + alphanumeric password mechanism + knowledge based identification” system named EyePass. It utilizes the concept of “gaze gesture” to reduce the possibility of shoulder surfing in public terminals. Gaze gesture, first proposed by Drewes and Schmidt [24], is a series of eye movement patterns, each formed by consecutive saccades. The concept originated from the mouse gesture in the Firefox web browser. Based on EdgeWrite [25], the user should follow the prescriptive eye movement pattern of the corresponding digit to encrypt the entry just like mouse or pen strokes on a tablet PC. The preliminary user study shows that the gaze gesture is a suitable method for PIN entry and such a method potentially has a better memorability than the gestures used by the tablet PC.

Saccades can also be used in a biometric based authentication system. Kasprowski and Ober [26] provided a “saccades based interaction + graphical password mechanism + biometric based identification” scheme, which applied the “dynamic” physiological properties of eye movements. The fixation based biometric approach discussed in Section III-A recognizes an individual by his cognitive processes, which is more on “where” the persons are looking at. By contrast, the saccades based biometric approach recognizes individuals by their viewing behavioral traits, which focuses on “how” they are viewing the pictures. In this regard, it is closely comparable to biometric traits such as signature, keystroke and gait.

DISCUSSION

Although the classifications here are subjective, the aim is to bring out those significant modules or factors of the EMBA system design, and to give a systemic perspective on the state of the art technology and possible future development. According to the six typical cases, the EMBA system is firstly highlighted by two different types of eye movements: fixation and saccades. Just as languages are important to human communication, so are such medium to eye movement based interaction. Fixation is the most utilized feature in both HCI and EMBA systems to date. However, saccades based interaction has some unique features. Take “gaze gesture” as a typical example, it is free from the calibration shift and does not demand high spatial and temporal resolutions for an eye tracker because the recognition of the user eye movement can be assisted by the HCI design.

Once the input modality is set, the corresponding interaction mechanism and data processing methodology can be developed based on it. Generally speaking, more EMBA systems use the graphical password mechanism instead of the alphanumeric password mechanism. Because, on the one hand, eye tracking can fight well against the shoulder surfing problem which is an intrinsic one in graphical password. On the other hand, the increasingly mature graphical password helps to develop a platform to introduce eye controlled input devices, whose schemes are to replace the precise recall of alphanumeric password entry with the imprecise recognition of the images. A comprehensive survey with detailed analysis on graphical password can be found in [27].

In the last module of an EMBA system, knowledge based identification is the most straightforward and convenient authentication method. However, its weaknesses are apparent, such as difficulty to memorize, and being vulnerable to social engineering which refers to trick someone into disclose a password than to spend the effort to hack into the system. To biometrics based identification, eye movements are sorts of dynamic and living-body biometric traits, which are non-intrusive and very difficult to be forged, yet such techniques are still at a very primary stage. There are a few open questions: (1) What kinds of eye movement modalities should be enrolled? (2) What templates should be formed from the enrollee’s data? and (3) How a live eye movement data is matched against one or many templates in the system database? More research and studies along this direction are expected to come in the future.

In order to facilitate reading and understanding, we carefully and detailed collected the eye tracking experimental conditions and technical details of all the six cases and outlined them in Table 1.

CONCLUSION

The Eye Movement Based Authentication (EMBA) system is still in its infancy. Most of the reported cases are just prototypes without providing substantial system error analysis (e.g. FAR and FMR) and extensive usability test. The past decade has seen a growing interest in eye tracking technology, accompanied by the emergence of non-expensive but easy to use eye trackers [28], which will provide a more robust data sampling, analyzing, and transferring platform. In summary, eye movement-based authentication techniques are very promising but more research and development is needed to be pursued in order to achieve a higher level of maturity and usability.

ACKNOWLEDGMENT

The work reported in this paper is substantially supported by a PolyU research grant (project code: G-U750).

REFERENCES

The OBER2 system is an infrared oculography (IROG) based system, more details can be found in [29].

**Table I. Experimental Conditions and Technical Details of EMST**

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Fixation based interaction</th>
<th>Saccades based interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>alphanumeric password</td>
<td>graphical password</td>
</tr>
<tr>
<td></td>
<td>knowledge based identification</td>
<td>knowledge based identification</td>
</tr>
<tr>
<td>Cases</td>
<td>Kumar et al.</td>
<td>Maeder et al.</td>
</tr>
<tr>
<td></td>
<td>Hoanca et al.</td>
<td>De Luca et al.</td>
</tr>
<tr>
<td>Eye Tracker</td>
<td>Tobii 1750</td>
<td>Eye Tech</td>
</tr>
<tr>
<td></td>
<td>Eye Response Technologies</td>
<td>ERAICA</td>
</tr>
<tr>
<td></td>
<td>ERICA</td>
<td>OBER2 [2]</td>
</tr>
<tr>
<td>Accuracy</td>
<td>0.5 deg</td>
<td>1.0 deg</td>
</tr>
<tr>
<td></td>
<td>±0.5 deg</td>
<td>±0.5 deg</td>
</tr>
<tr>
<td>Frame rate</td>
<td>50 Hz</td>
<td>15 Hz</td>
</tr>
<tr>
<td></td>
<td>60 Hz</td>
<td>60 Hz</td>
</tr>
<tr>
<td>Interface</td>
<td>1280x1024 pixels at 96 dpi</td>
<td>1024x768 pixels at 96 dpi</td>
</tr>
<tr>
<td></td>
<td>1024 x768 pixels at 106dpi</td>
<td>730 x 450 pixels at 106dpi</td>
</tr>
<tr>
<td>Viewing distance</td>
<td>50 cm</td>
<td>60 cm</td>
</tr>
<tr>
<td>Visual angle ranges for viewing (WSI)</td>
<td>±18.7 deg x 15.2 deg</td>
<td>±15 deg x 10 deg</td>
</tr>
<tr>
<td></td>
<td>±14 deg x 11 deg</td>
<td>±11 deg x 6.25 deg</td>
</tr>
<tr>
<td>Target size/area</td>
<td>84 pix each with 12 pix interval</td>
<td>averagely 341 x 256 pixels</td>
</tr>
<tr>
<td></td>
<td>96 X 96 pixels</td>
<td>180 x 90 pixels</td>
</tr>
<tr>
<td>Target visual angle</td>
<td>±1.275 deg</td>
<td>±1.375 deg</td>
</tr>
<tr>
<td></td>
<td>uneven</td>
<td>± 2.5 x 1.5 deg</td>
</tr>
</tbody>
</table>

[1] Another case from Maeder and Fookes uses the same experimental setups, which technically featured as “fixation based interaction + graphical password mechanism + biometrics based identification”.

[2] The OBER2 system is an infrared oculography (IROG) based system, more details can be find in [29].