Survey on Eye Movement Based Authentication Systems

Yun Zhang and Xuanqin Mou(✉)

Institute of Image Processing and Pattern Recognition,
Xi'an Jiaotong University, No. 28 West Xianning Road, Xi'an, China
{zhangyun2011,xqmou}@mail.xjtu.edu.cn

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 trading-off between the usability and the security of an authentication system. This paper conducts a comprehensive survey 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 data recognition. The features and functions of the EMBA modules are further analyzed. An emphasis is put 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 or security systems.

Keywords: Eye tracking · Authentication · Access control · Human computer interaction · Fixations · Saccades · Graphical password

1 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 an directly control tool, such as a non-touchable mouse pointer for the disable [1], and (2) analyzing eye movements to obtain the user's intention and then to facilitate the interaction environment, such as interactive graphical displays [2] and interface usability measurements [3-4]. 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 between the two features. First of all, from the perspective of interaction modality, eye tracking device is highly resistance to shoulder surfing which is done either by simply looking over a victims shoulder, or using technical devices like binoculars or miniature cameras to get the personal

H. Zha et al. (Eds.): CCCV 2015, Part I, CCIS 546, pp. 144–159, 2015.
DOI: 10.1007/978-3-662-48558-3_15

identification number (PIN) [5].Secondly, from the perspective of system usability, eye tracking based interaction is so different from the traditional alpha-number schemes that a new authentication mechanism such as a graphical based password system is more fitting for the human innate memory capability [6-9]. 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 sub-conscious viewing behaviors. Such information can be combined with other channels to enhance the validity of identification. This paper is structured as follows. Section 2 describes the three main aspects/modules of a general EMBA system and outlines the techniques and methodologies of each module. Section 3 reviews eight present EMBA systems by thoroughly discussing how the different modules are assembled together and how they affect the system performance. In Section 4, we further analyze the strengths and weaknesses of each module and reveal their coherent relationship in the EMBA framework. Section 5 concludes the paper with a summary of achievements and future research directions in this area.

2 Eye Movement Based Authentication Framework and Technical Modules

The general structure of an eye movement based authentication system is different from a conventional authentication system [10]. In spite of different applications, an EMBA system in general consists of the following three main modules:

1. Eye movement input modality
2. Eye movement interaction mechanism
3. Eye movement data recognition/identification

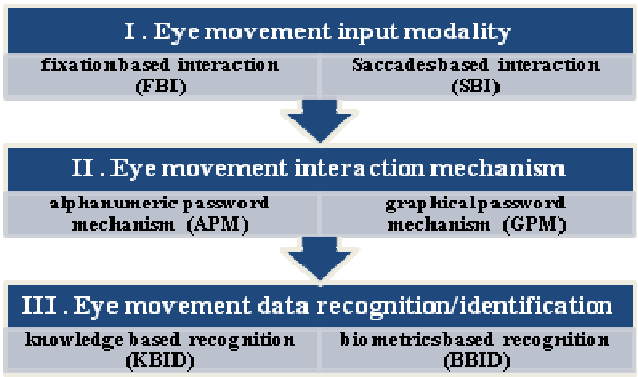


Fig. 1. The *EMBA framework and technical modules.*

As shown in Figure 1, the three modules are three main steps and elements to construct an EMBA system, which are all driven by the characteristics of eye movements and eye tracking device. In each module, we present the possible techniques and

methodologies which can be assembled together to form different functional EMBA systems.

Module 1

- Fixation-based interaction (FBI)
- Saccades-based interaction (SBI)

As previously mentioned, an authentication system is a special case of eye movement based HCI. Therefore, Module 1 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 decide the whole design of the system.

Fixation 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 [11]. Fixation-based interaction, or sometimes called "gaze-based interaction" [12], 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 are 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 [13]. 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 scanpath, which is an eye movement pattern consisted of series of saccades. Different patterns can be assigned to different input commands for HCI.

Module 2

- Alphanumeric password mechanism (APM)
- Graphical password mechanism (GPM)

As a novel element, eye tracking technology provides a new interaction mechanism to strengthen the existing authentication ones. For example, the alphanumeric password mechanism can be conveniently implemented by replacing a traditional input device with an eye tracker. The novel systems can effectively fight against the prevalent eavesdropping or spoofing problem which widely exists in the present system. Moreover, such "tradition mechanism + novel input (eye tracker)" not only reserves the well-established usability on a password system, but considerably increases the security as well.

Alternatively, a graphical password mechanism equipped with eye tracking technology could be a feasible solution not only to security problems, but also usability problems as well. Graphical password is first proposed by Greg Blonder [6] to replace the precise recall of a PIN by image recognition, a skill at which humans are proficient [14]. Whereas, the tradeoff 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 [15]. When combined with eye tracker, such mechanism can easily bypass the disadvantage of graphical password and make best use of their advantages.

Module 3

- Knowledge-based identification (KBID)
- Biometrics-based identification (BBID)

After the first two steps to select and collect the eye movement data, the other aspect of authentication system design is to process the data to authenticate the user.

Knowledge-based mechanisms [16] 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 [17]. Eye movement characterizes human's physiological and perceptual behaviors in 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.

3 Cases Study

In this section, a comprehensive analysis of EMBA systems is given by analyzing eight cases in five types module combination (in fact, there are 2x2x2, eight combinations of two approaches in each of three modules. Heretofore, the present's cases have only covered 5 of them). The survey emphases (1) how the three modules of the EMBA system are working together and (2) what are the detailed techniques and methodologies within each module.

3.1 FBI + APM + KBID

Kumar and their group proposed a fixation-based authentication prototype *EyePassword* mainly to reduce shoulder surfing [18]. Their system retains the traditional alphanumeric password mechanism, as illustrated in Figure 2. *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 to resolution and accuracy. The second two approaches are proposed to solve the problems in active vision control. The purpose is to disambiguating tracking data for an eye tracking system.

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 makes the stealing virtually impractical in the fixation-based interaction. The authors also conducted usability studies to compare the fixation-based control and a normal keyboard. The result shows that an eye tracking method needs a longer time than using a keyboard. However, the error rate is quite similar and most of the subjects tested prefer the fixation-based interaction over the traditional ones. According to a recent report, the concept of *EyePassword* has already been converted into real products.

(a) (b)

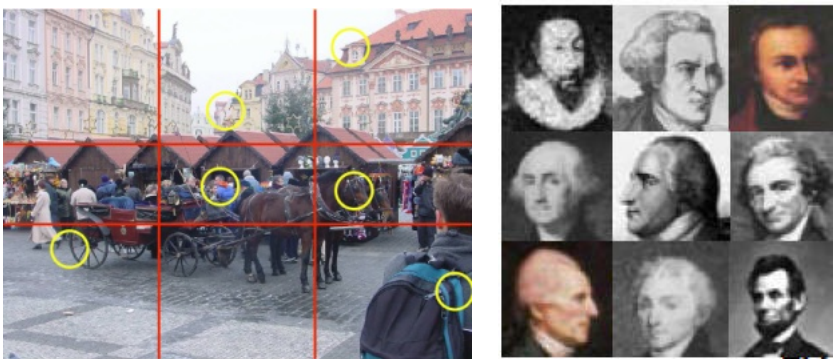
Fig. 2. On-screen keyboard of *EyePassword* (a) The alphabetic layout with gaze points superimposed; (b) Keypad layout for a practical ATM application.

3.2 FBI + GPM + KBID

Maeder et al.[19] and Hoanca et al.[20] also proposed fixation-based password systems which are different from Kumar's system although two were all motivated by the graphical password mechanism. Maeder et al's work uses a nature image instead of an on-screen keyboard. The visual features or objects 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 (Figure 3(a)) to help identify the distinctive fixations and gazes.

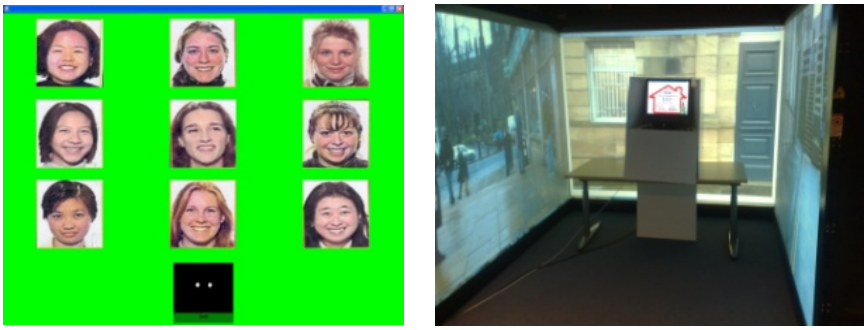
Hoanca's work is based on a well known graphical password *Passfaces*[1]. Instead of a nature image, the *Passfaces* interface is composed of human faces pictures, usually 3x3 tiles (Figure 3(b)). The user is asked to fixate on the prescribed faces among the decoy ones for authentication. Such technique 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 interface provides a predictable object's location and the error area, which may increase the certainty of the user's attentive fixations.

[1] http://www.realuser.com/



(a) (b)

Fig. 3. (a) Prague image used in the experiments with a non-uniform 3x3 grid superimposed on the image. (b) On tiled face images, the user selects a face out of a series of faces for their password



(a) (b)

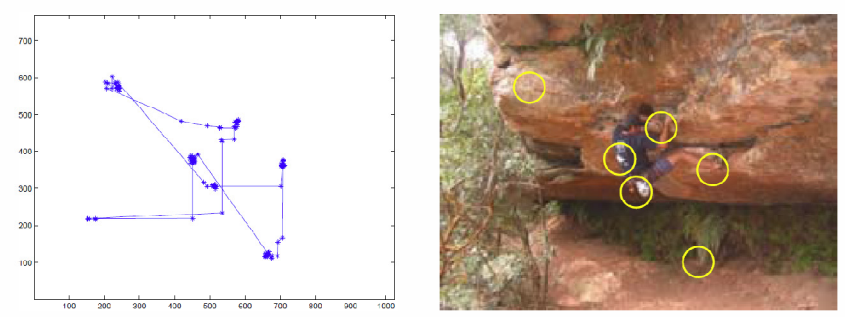
Fig. 4. Dunphy et al.'s gaze-contingent passwords at ATM. (a) The password interface; (b) The simulated ATM scenario in the lab.

Another case in this category is work from Dunphy et al.[21] whose contribution is to implement the (FBI + GPM + KBID) system to a real ATM password system (Figure 4). Based on the *Passfaces* design, they created a naturalistic ATM setting with similar sight, sounds and operation experience by using the video technique in the lab. A study on twenty users showed that the participants felt ease with the eye tracker. Another conclusion drawn is that the public environment does not cause undue distraction of user's fixations, which demonstrates the feasibility and practicability of an EMBA system.

3.3 FBI + GPM + BBID

Using eyes to perform human identification in biometric methods has a long tradition such as iris pattern recognition and retina scanning. However, the ideal forms of biometrics would be based on non-visible and non-physiological information hidden

within the person, such as the behavior or cognitive processes of a human being. Different from their previous model discussed in Section 3.2, Maeder and Fookes [22] presented a visual attention based biometric identification. As shown in Figure 5, the fixation permits a subject to view an AOI near the center 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 are processed to find the individual features. In a conscious/overt viewing test, the fixation locations are prescribed (the yellow circles in Figure 5), while in a sub-conscious /covert test, the user just view the picture naturally without a clear task. 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 expected to be carried out to solve the problems with identification and validation, which are the two basic issues of a biometric system.



(a) (b)

Fig. 5. Maeder et al.'s visual attention approach for biometric identification. (a) and (b) are the examples of a participant's gazes data and the corresponding viewing points which are used for personal authentication.

3.4 SBI + APM + KBID

De Luca et al.[23-24] proposed a saccade-based password system *EyePass*, which use "gaze gesture" to reduce the likelihood of shoulder surfing in public terminals. Gaze gesture, first proposed by Drewes and Schmidt [25], is a series of eye movement patterns each of which is formed by consecutive saccades. The concept was originated from the mouse gesture2 in the Firefox web browser.

As shown in Figure 6, EyePass uses alphanumeric password mechanism which is based on EdgeWrite [26]. 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. For the system, decryption is done by using a two-step recognition

[2] http://optimoz.mozdev.org/gestures/

algorithm. Firstly, it needs to extract each sub-gesture or stroke from the input gaze points; secondly, it needs to assemble those recognized strokes together and map them to the given gesture pattern. In EyePass, a "press button" motion is added to help the recognition of eye strokes, which require the user to hold the button during the performing to indicate they are trying to enter an authentication token. 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.

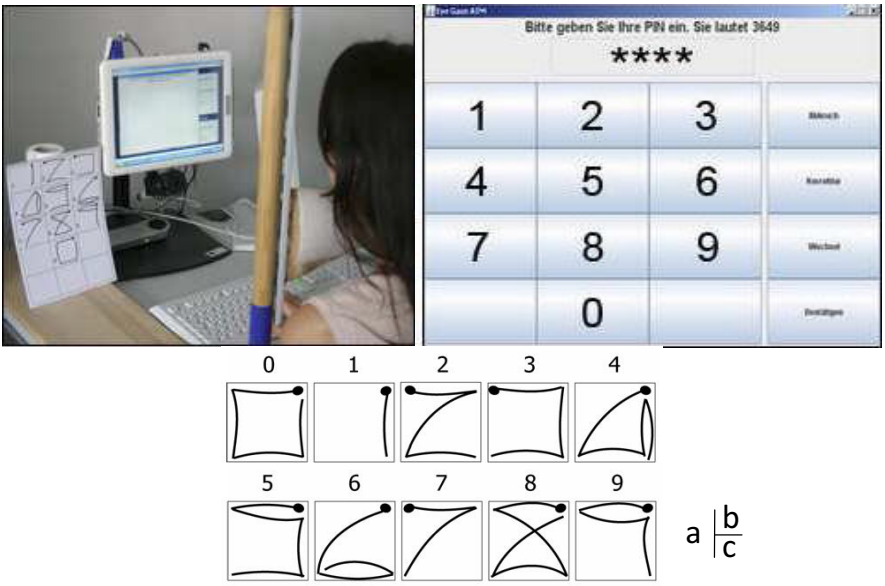


Fig. 6. The EyePass system. (a) The lab setting; (b) The screenshot of the prototype; (c) The numeric gaze gestures used for the prototype.

3.5 SBI + GPM + BBID

Saccades can also be used in a biometric-based authentication system. Kasprowski and Ober [27] provided a scheme based on the "dynamic" physiological properties of eye movements. As the saying goes, the eye is "the window to our mind". Eye movements may encode muscle activities and brain information simultaneously. The fixation-based biometric approach discussed in Section 3.3 (FBI + GPM + BBID) recognizes individuals by their cognitive processes, which is paid more attention to "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.

As shown in Figure 7, to avoid the 'learning effects', a 3x3 'jumping point' design is chosen as a visual stimulus to generate a series of saccades. Reaction times and drifts during the eye calibrations are recorded to extract the distinctive and permanent features which have exactly the same values for the same person in every experiment.

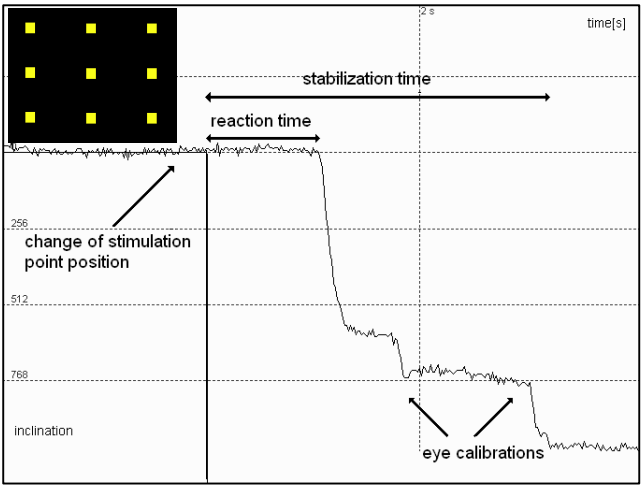


Fig. 7. Explanation of Kasprowski and Ober's work . The 3x3 matrix with the "jumping point" stimuli shown on the top left. The rest of display depicts the definition of the reaction time and the stabilization time.

The similar work was also done by Bednarik et al. [28], in which they extracted the features including pupil sizes, gaze velocities and the distances of infrared reflections of the eyes. Figure 8 shows eight vision stimuli proposed by Bednarik et al. Although these two pieces of pioneering research work furnished the possibility of such a new authentication mechanism, there is still a long way to go from a good idea to a reliable methodology. The issues such as how to acquire the most informative features and how to establish the recognition model need to be addressed in the future.

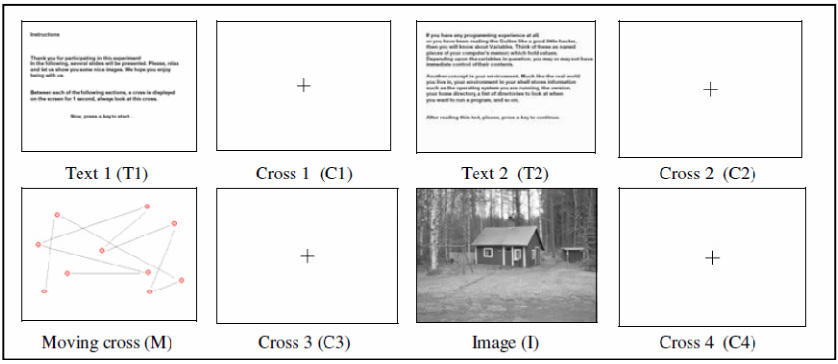


Fig. 8. Explanation of Bednarik et al.'s work. The eight vision stimulus including texts, image, static and dynamic crosses are used to extract biometric information of personal eye movements.

4 Discussion

Although the classifications here are artificial, 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. Table 1 summarizes the current situations of all possible eight combinations of three modules.

Table 1. Systemic perspective on the EMBA system

	Fixation-based interaction	Saccades-based interaction	Row Sum
APM + KBID	√ (1 case)	√ (1 case)	25%
APM + BBID	×	×	
GPM + KBID	√ (3 cases)	×	75%
GPM + BBID	√ (1 case)	√ (2 cases)	
Colum Sum	**62.5%**	**37.5%**	

(APM: alphanumeric password mechanism; GPM: graphical password mechanism; KBID: knowledge-based identification; BBID: biometrics-based identification; "√": application cases reported "×": no application case reported).

4.1 Fixation vs. Saccade

Column-wisely, 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 (67.5%) to date. However, saccades-based interaction has some unique features. Take "gaze gesture" as a typical example, the advantages and disadvantages are given as follows:

Advantages

- It is free from the calibration shift; sometimes it even does not need a calibration. For example, gaze gesture is based on relative eye movement patterns but not absolute gaze positions.
- It 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. For example, in Drewes and Schmidt's case, eye gestures can be as large as 10°visual angle and the sampling interval can be a few hundred milliseconds.

Disadvantages

- It needs the user to practice and perform those gestures correctly, which is not natural but a technical eye movement. By contrast, the fixation-based interaction is more intuitive and direct.
- It may need some efforts for a user to remember the "gaze gesture table" which maps gestures to the computer commands (Figure 6(c)). However, the application

to a password system benefits from a relatively small gesture table. According to De Luca et al.'s online survey, the user may feel ease to perform gaze gesture.

4.2 APM vs. GPM and KBID vs. BBID

Once the input modality is set, the corresponding interaction mechanism and data processing methodology can be developed based on it. From Table 1, we can see that 75% of 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 help to develop a platform to introduce eye controlled input devices, whose schemes is 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 [29].

Eye tracking technology can be combined with either knowledge-based identification or biometrics-based identification. While KBID is the most straightforward and convenient authentication method, its weaknesses are apparent, such as difficulty to memorize, being vulnerable to social engineering which refers to trick someone into disclose a password than to spend the effort to hack into the system. Combined with eye tracking technology, some pragmatic solutions can be developed. For example, (GPM + KBID) has a feature of being easy to memorize passwords but being difficult to be divulged. This is because the validation operations can be conducted by eyes and graphical password is difficult to write down or to describe to somebody else. Although no (SBI+ GPM + KBID) has been reported to date, such direction is worth exploiting, which may result in a perfect combination of dynamic eye movement' characteristics in an authentication system.

BBID is based on something you are or something you do, which cannot be lost or forgotten, be written down or stolen by social engineering. An important issue in BBID is clonability. Obtaining a copy of an individual's fingerprint can be trivial, even the trick of iris images is not difficult. Another problem is the measurement of physical features may be intrusive to users. Eye movements are sorts of dynamic and living-body biometric traits, which are non-intrusive and very difficult to be forged. Such good properties have already been demonstrated in the (GPM+BBID) cases reported. However, BBID with eye tracking technology is still at a very primary stage. There are a few questions needed to be answered: (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.

4.3 Summary and Comparison of State-of-the-Art EMBA Systems Technical Details

Though still in its infancy, the field of eye movement based authentication is growing rapidly. To facilitate the others who are interested in the study and application on such field, we gather all the experiment conditions and technical details of latest eye movement based authentication systems cases in the survey into Table 2. The main

purpose of the table is to provide a substantial and extensive reference for other peers to conveniently setup a EMBA system based on the prior's empirical data.

The first row of the table divides the EMBA into two categories: fixation-based and saccades-based password system. Then all the eight cases discussed in section 3 are classified in the two categories with their five types of features, which are abbreviated as follows:

- **T1:** FBI + APM + KBID = fixation-based interaction + alphanumeric password mechanism + knowledge-based identification
- **T2:** FBI + GPM + KBID = fixation-based interaction + graphical password mechanism + knowledge-based identification
- **T3:** FBI + GPM + BBID = fixation-based interaction + graphical password mechanism + biometrics-based identification
- **T4:** SBI + APM + KBID = saccades-based interaction + alphanumeric password mechanism + knowledge-based identification
- **T5:** SBI + GPM + BBID = saccades-based interaction + graphical password mechanism + biometrics-based identification

The second row is the eight specific EMBA systems which belong to five type and two categories. For example, case "Kumar et al." belongs to T1, type "fixation-based interaction + alphanumeric password mechanism + knowledge-based identification", and category "Fixation-based password". Column-wisely, each column is the collection of the technical features of one case .The first column represents nice types of the technical features of EMBA system, which are explained as follows

1. **Eye Tracker:** The cases' use what kind of state-of-the-art eye tracker models. While most of them are commercial ones, there is still self-developed eye tracker, such as OBER2, used in the prototype system.
2. **Accuracy:** The maximum precision of view angle the eye tracker models can reach .
3. **Frame rate**: The sampling rate of the eye tracker models. Usually it covers from 10Hz ~3000Hz. The rate around 30Hz~120Hz are mostly used in HCI system.
4. **Interface** : Here means the size of interaction screen and its resolution. It is an important factor, because it directly affects the interaction precision and interface design. Generally speaking, the larger the better the user experience is, and the higher input precision the system can get.
5. **Viewing distance:** means the distance between the user and the eye tracker. Such item is also an important factor to be considered, because there are objective distance measurement limitations in all eye trackers. They cannot be too closer or too far. The empirical distance value is between 40cm~70cm.
6. **Visual angle ranges for viewing (WxH) :** It means the how wide and large the user's visual field is in the current case. WxH represent Width x Height. It is another measuring unit by means of feature "interface" and "viewing distance".
7. **Target size/area:** It means the size of the button or the graphical pattern to be triggered by the eye movement. It is a feature to reflect the design and interaction friendliness. The general attribute of the target size is similar to those of the feature "interface".

Table 2. Experimental conditions and technical details of EMBA systems

Techniques	**Fixation-based password**				**Saccades-based password**		
	T1	**T2**			**T4**	**T5**	
Cases	Kumar et al.	Maeder et al.[1] **(T2 & T3)**	Hoanca et al.	Dunphy et al.	De Luca et al.	Kasprowski and Ober	Bednarik et al.
Eye Tracker	Tobii 1750	Eye Tech	Eye Response Technologies ERICA	Tobii X50	Eye Response Technologies ERICA	OBER2 [2]	Tobii 1750
Accuracy	0.5 deg	1.0 deg	±0.5 deg	0.5 ~ 0.7 deg	±0.5 deg	±0.5 deg	0.5 deg
Frame rate	50 Hz	15 Hz	60 Hz	50 Hz	60 Hz	250 Hz	50 Hz
Interface	1280x1024 pixels at 96 dpi	1024 x768 pixels at 96 dpi	1024 x768 pixels at 106dpi	≤1280x 1024 pixels at 96 dpi	730 x 450 pixels at 106dpi	Targets are 3x3 dynamic jumping ball	1280x1024 pixels at 96 dpi
Viewing distance	50 cm	60 cm	48 cm±2 cm	30 cm-50 cm away	48 cm±2 cm	2048 gaze points positions of both eye are sampled in 8128 ms	80 cm with chinrest
Visual angle ranges for viewing (WxH)	±18.7 deg x 15.2 deg	±15 deg x10 deg	±14 deg x 11 deg	≤±18 deg x15deg	±11 deg x 6.25 deg		Multi-targets including: text, images, static and dynamic cross marks
Target size/area	84 pix/each with 12 pix interval	averagely 341x 256 pixels	96 X 96 pixels	196 pix/each with 196 pix interval	180 x 90 pixels		
Target visual angle	±1.275 deg	uneven	±1.375 deg	±1.5 deg	± 2.5 x 1.5 deg		

[1] Maeder et al.'s cases of T2 [Maeder et al. 2004] and T3 [Maeder and Fookes.2003] use the same experimental setups. The difference is in the use of "targets". T3 used the natural objects of the image whose visual angles are not fixed.

[2] The OBER2 system is an infrared oculography (IROG) based system, more details can be find in [Ober et al. 1997].

8. **Target visual angle:** It means the how wide and large the user's visual field is on each interactive target. It is another measuring unit by means of "interface" and "viewing distance".

All these features are main components of an EMBA system. When we analyze an existing EMBA system or build a new one, these features are essential factors should be taken into account. The function of table 2 is to list all those features of current cases together to facilitate future reference and experiment comparison.

5 Conclusion

The past decade has seen a wide variety of applications on eye movement based HCI. In the application for authentication, the strengths of eye tracking technology are substantial. The most immediate benefit is that the eye movement based interaction is immune from shoulder surfing or other trickery for the purpose of password stealing at public terminals.

Generally speaking, the current Eye Movement Based Authentication (EMBA) techniques are still immature. One of future developments can come from the direction of eye movement interaction mechanism. Normally, eye behaviors include both voluntary (conscious) and involuntary (sub-conscious) movements. Voluntary eye movements are more often used on the computer user interface, although involuntary eye movements can also be used. In both interface designs, the PIN is encrypted by the eye movements. The difference is that, in the voluntary case, the PIN is consciously inputted by the eye, whereas in the involuntary case, the PIN is interpreted from the natural eye movement data. Among the eight cases reviewed in this paper, there is only one case which is based on involuntary eye movements: (FBI + GPM + BBID) discussed in Section 3.3. In fact, eye movements convey physiological and perceptual information concurrently, which are good sources of physiological biometrics as well as behavioral biometrics. For example, the traits of extra-ocular muscle movements are different from one person to another. On the other hand, the cognition process expressed by the eye movements is qualitatively distinct from each other. Such a complex biometric traits have not been well developed yet, which may bring a new direction to the next generation of biometric identification.

The other direction is to develop multichannel or multimodal authentication systems. One possible combination is "iris/face + eye movement". In such a multichannel system, high-quality digital cameras may collect iris, human face, and eye movement data simultaneously. Another possible combination is (KBID + BBID). For example, in the case of *EyePassword* discussed in Section 3.1, the eye movements can not only be used to input the password, but also be used as a biometric pattern. Both the knowledge-based and biometric-based identifications can be performed at the same time. Such a new multimode *EyePassword* can fill the blank "FBI+APM + BBID" in Table 1. In the same manner, a multimode *Eyepass* discussed in Section 3.4 can fill the blank of "SBI+APM + BBID".

In summary, eye movement based authentication techniques are very promising but more research and user studies are required in order to achieve a higher level of maturity and usefulness.

References

1. Duchowski, A.T.: Eye Tracking Methodology: Theory and Practice. Springer-Verlag New York Inc., Secaucus (2003)
2. O'sullivan, C., Dingliana, J., Howlett, S.: Eye-movements and Interactive Graphics (2003)
3. Parkhurst, D., Culurciello, E., Niebur, E.: Evaluating variable resolution displays with visual search: task performance and eye movements. In: ETRA 2000: Proceedings of the 2000 Symposium on Eye Tracking Research & Applications, Palm Beach Gardens, Florida, United States, pp. 105–109. ACM, New York (2000)
4. Loschky, L.C., Mcconkie, G.W.: User performance with gaze contingent multiresolutional displays. In: ETRA 2000: Proceedings of the 2000 Symposium on Eye tracking Research & Applications, Palm Beach Gardens, Florida, United States, pp. 97–103. ACM, New York (2000)
5. Li, Z., Sun, Q., Lian, Y., Giusto, D.D.: An association-based graphical password design resistant to shoulder-surfing attack. In: IEEE International Conference on Multimedia and Expo., ICME 2005, pp. 245–8 (2005)
6. Blonder, G.E.: Graphical Password, United State Patent, 5559961 (1996)
7. Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D.: The design and analysis of graphical passwords. In: SSYM 1999: Proceedings of the 8th Conference on USENIX Security Symposium, Washington, D.C., pp.1–1. USENIX Association, Berkeley (1999)
8. Dhamija, R., Perrig, A.: Déjà Vu: a user study using images for authentication. In: SSYM 2000: Proceedings of the 9th Conference on USENIX Security Symposium, Denver, Colorado, pp. 4–4. USENIX Association, Berkeley (2000)
9. Sabzevar, A.P., Stavrou, A.: Universal multi-factor authentication using graphical passwords. In: SITIS 2008: Proceedings of the 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems, pp. 625–632. IEEE Computer Society, Washington, DC (2008)
10. Jobusch, D.L., Oldenhoeft, A.E.: A survey of password mechanisms: weaknesses and potential improvement, part 1 & 2. Comput. Secur. **8**, 587–601 (1989)
11. Poole, A., Ball, L.: Eye tracking in human-computer interaction and usability research: current status and future prospects. In: Ghaoui, C. (ed.) Encyclopedia of Human Computer Interaction. IGI Global (2005)
12. Jacob, R., Karn, K.: Eye tracking in human-computer interaction and usability research: ready to deliver the promises. In: Hyona, J., Radach, R., Deubel, H. (eds.) The Mind's Eye: Cognitive and Applied Aspects of Eye Movement Research. Elsevier Science, Oxford (2003)
13. Qvarfordt, P., Zhai, S.: Conversing with the user based on eye-gaze patterns. In: CHI 2005: Proceedings of the SIGCHI Conference on Human Factors In Computing Systems, Portland, Oregon, USA, pp. 221–230. ACM, New York (2005)
14. Weinshall, D., Kirkpatrick, S.: Passwords you'll never forget, but can't recall. In: CHI 2004 Extended Abstracts on Human Factors in Computing Systems, Vienna, Austria, pp. 1399–1402. ACM, New York (2004)
15. Wiedenbeck, S., Waters, J., Sobrado, L., Birget, J.: Design and evaluation of a shoulder-surfing resistant graphical password scheme. In: AVI 2006: Proceedings of the Working Conference On Advanced Visual Interfaces, Venezia, Italy, pp. 177–184. ACM, New York (2006)
16. Patrick, A.S., Long, A.C., Flinn, S.: HCI and security systems. In: CHI 2003 Extended Abstracts On Human Factors In Computing Systems, Ft. Lauderdale, Florida, USA, pp. 1056–1057. ACM, New York (2003)

17. Faundez Zanuy, M.: Biometric security technology. IEEE Aerospace and Electronic Systems Magazine **21**, 15–26 (2006)
18. Kumar, M., Garfinkel, T., Boneh, D., Winograd, T.: Reducing shoulder-surfing by using gaze-based password entry. In: SOUPS 2007: Proceedings of the 3rd Symposium on Usable Privacy And Security, Pittsburgh, Pennsylvania, pp 13–19. ACM, New York (2007)
19. Maeder, A.J., Fookes, C.B., Sridharan, S.: Gaze based user authentication for personal computer applications (2004)
20. Hoanca, B., Mock, K.: Secure graphical password system for high traffic public areas. In: ETRA 2006: Proceedings of the 2006 symposium on Eye Tracking Research \& Applications, San Diego, California, pp. 35–35. ACM, New York (2006)
21. Dunphy, P., Fitch, A., Olivier, P.: Gaze-Contingent Passwords at the ATM. Czech Republic, Prague, pp. 50–62, September 2–3, 2008
22. Maeder, A.J., Fookes, C.B.: A visual attention approach to personal identification. In: Eighth Australian and New Zealand Intelligent Information Systems Conference, December 10–12, 2003
23. De Luca, A., Weiss, R., Drewes, H.: Evaluation of eye-gaze interaction methods for security enhanced PIN-entry. In: OZCHI 2007: Proceedings of the 19th Australasian Conference on Computer-Human Interaction, Adelaide, Australia, pp. 199–202. ACM, New York (2007)
24. De Luca, A., Weiss, R., Hußmann, H., An, X.: Eyepass - eye-stroke authentication for public terminals. In: CHI 2008 Extended Abstracts on Human Factors in Computing Systems, Florence, Italy, pp. 3003–3008. ACM, New York (2008)
25. Drewes, H., Schmidt, A.: Interacting with the computer using gaze gestures. In: Baranauskas, C., Abascal, J., Barbosa, S.D.J. (eds.) INTERACT 2007. LNCS, vol. 4663, pp. 475–488. Springer, Heidelberg (2007)
26. Wobbrock, J.O., Myers, B.A., Kembel, J.A.: Edgewrite: a stylus-based text entry method designed for high accuracy and stability of motion. In: UIST 2003: Proceedings of the 16th annual ACM symposium on User Interface Software and Technology, Vancouver, Canada, pp. 61–70. ACM, New York (2003)
27. Ober, J., Hajda, J., Loska, J., Jamicki, M.: Application of eye movement measuring system OBER 2 to medicine and technology. In: Andresen, B.F., Scholl, M.S. (eds.) Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series; Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, pp. 327–336, August 1997
28. Bednarik, R., Kinnunen, T., Mihaila, A., Fränti, P.: Eye-movements as a biometric. In: Kalviainen, H., Parkkinen, J., Kaarna, A. (eds.) SCIA 2005. LNCS, vol. 3540, pp. 780–789. Springer, Heidelberg (2005)
29. Suo, X., Zhu, Y., Owen, G.: Graphical passwords: a survey, 10 pp. (2005)
30. Kasprowski, P., Ober, J.: Eye movements in biometrics. In: Maltoni, D., Jain, A.K. (eds.) BioAW 2004. LNCS, vol. 3087, pp. 248–258. Springer, Heidelberg (2004)
31. Surakka, V., Illi, M., Isokoski, P., Hyönä, J., Radach, R., Deubel, H.: Voluntary eye movements in human-computer interaction. Elsevier Science, Oxford (2003)
32. Zhu, Z., Ji, Q.: Eye and gaze tracking for interactive graphic display. Machine Vision and Applications **15**, 139–148 (2004)