Enhancing CAPTCHA Using Eye Movement

Mr. Apichai Siripitakchai

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science and Information

Technology

Department of Mathematics and Computer Science

Faculty of Science

Chulalongkorn University

Academic Year 2017

Copyright of Chulalongkorn University

การปรับปรุงแคปชาโดยใช้การเคลื่อนไหวของตา

นายอภิชัย ศิริพิทักษ์ชัย

Thesis Title	Enhancing CAPTCHA Using Eye Movement
By	Mr. Apichai Siripitakchai
Field of Study	Computer Science and Information Technology
Thesis Advisor	Assistant Professor Suphakant Phimoltares, Ph.D.
Thesis Co-Advisor	Atchara Mahaweerawat, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

....Dean of the Faculty of Science

(Associate Professor Polkit Sangvanich, Ph.D.)

THESIS COMMITTEE

....Chairman

(Associate Professor Peraphon Sophatsathit, Ph.D.)

....Thesis Advisor

(Assistant Professor Suphakant Phimoltares, Ph.D.)

....Thesis Co-Advisor

(Atchara Mahaweerawat, Ph.D.)

....External Examiner

(Praisan Padungweang, Ph.D.)

อภิชัย ศิริพิทักษ์ชัย : การปรับปรุงแคปชาโดยใช้การเคลื่อนไหวของตา (Enhancing CAPTCHA Using Eye Movement) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. ดร. ศุภกานต์ พิมล ธเรศ, อ.ที่ปรึกษาวิทยานิพนธ์ร่วม: อ. ดร. อัจฉรา มหาวีรวัฒน์, 58 หน้า.

แคปชาเป็นวิธีที่ออกแบบเพื่อป้องกันการลงทะเบียนและการเข้าถึงอัตโนมัติ และยังสามารถแยกความแตกต่างระหว่างมนุษย์และโปรแกรมอัตโนมัติ (บอท) แคปชาเชื่อมต่อกับเซิร์ฟเวอร์แล้วเริ่มกระบวนการทวนสอบมนุษย์ ผู้ใช้ต้องตอบคำถามให้ถูกต้องหรือปฏิบัติตามคำสั่งเพื่อเข้าถึงระบบ อย่างไรก็ตามมีปัญหาเกิดขึ้นกับผู้ใช้งาน ตัวอย่างเช่น ข้อความสำหรับการทวนสอบมีความผิดเพี้ยนเกินไปที่แม้กระทั่งมนุษย์ไม่เข้าใจ หรือเกิดความสงสัยในประสิทธิผลของการป้องกันโปรแกรมคอมพิวเตอร์อัตโนมัติ จากเหตุผลเหล่านี้นักวิจัยจึงยังคงพัฒนาแคปชาให้ดีขึ้นและมีประสิทธิผลยิ่งขึ้น ในงานวิจัยนี้แคปชาที่นำเสนอทีเรียกว่าอายแคปชาผสมระหว่างแคปชากับเทคโนโลยีการเคลื่อนไหวของตา

อายแคปชา ประกอบด้วยส่วนประกอบที่สำคัญสามส่วน ส่วนประกอบแรกคือ แคปชาแบบปริศนา ส่วนที่สองคือการตรวจจับสายตาซึ่งขึ้นอยู่กับความสัมพันธ์ระหว่างตากับตำแหน่งบนจอภาพ องค์ประกอบสุดท้ายของวิธีการที่เสนอนี้คือการเคลื่อนที่ของดวงตาเพื่อเคลื่อนวัตถุไปยังทิศทางที่ต้องการ จากการทดลองและการวิเคราะห์ทางสถิติ วิธีการนี้สามารถปรับปรุงสมรรถนะของแคปชาในการแยกแยะระหว่างมนุษย์และบอท

ภาควิชา	คณิตศาสตร์และวิทยาการคอมพิวเตอร์	ลายมือชื่อนิสิต	....
		ลายมือชื่อ อ.ที่ปรึกษาหลัก	....
สาขาวิชา	วิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ	ลายมือชื่อ อ.ที่ปรึกษาร่วม	....
ปีการศึกษา	2560		

5672641023 : MAJOR COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

KEYWORDS: CAPTCHA / EYE MOVEMENT / GAZE DETECTION

APICHAI SIRIPITAKCHAI: Enhancing CAPTCHA Using Eye Movement. ADVISOR: ASST. PROF. SUPHAKANT PHIMOLTARES, Ph.D., CO-ADVISOR: DR. ATCHARA MAHAWEERAWAT, Ph.D., 58 pp.

CAPTCHA is a method designed to prevent automatic registration and access. It can distinguish between real human and automated program (BOT). CAPTCHA connects to a server and then starts human verification process. The user must answer a question correctly or follow an instruction in order to get access to the system. However, there are some problems occurred to users. For example, the verification text is too distorted that even real humans do not understand or the effectiveness of preventing an automated computer program is doubted. From these reasons, researchers are still developing CAPTCHA to make it better and more effective. In this research, the proposed CAPTCHA called EYE CAPTCHA is mixed between CAPTCHA and eye movement technology.

EYE CAPTCHA consists of three important components. The first component is the puzzle-based CAPTCHA. The second component is the gaze detection which is based on the relation between an eye and a position on the screen. The last component of this proposed method is the eye movement for moving objects to the desired direction. From an experiment and statistical analysis, this method can enhance the performance of CAPTCHA in distinguishing between humans and bots.

Department:	Mathematics and Computer Science	Student's Signature	....
Field of Study:	Computer Science and Information Technology	Advisor's Signature	....
Academic Year:	2017	Co-Advisor's Signature	....

ACKNOWLEDGEMENTS

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

CONTENTS

Content of Tables

Content of Figures

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

Chapter 1. Introduction

Nowadays the internet is widespread for people all over the world. It is very easy for everyone to access from almost everywhere. We have to accept that the internet has become a part of our everyday daily lives. Most of our activities can be facilitated by the internet, such as checking the weather, navigation, entertainment, news, and information. Accession to a website browser via the internet is a basic tool for many things, such as financial transaction, e-commerce, data, etc. As a result, the increase in the number of the internet users leads to private organizations and government organizations' attempts in changing the working process of how they can be presented to customers, opening access to internal data, and including other works in many different ways. These organizations change service channels by using a website to support their customers since it is easy to access. On the other hand, easy accession through the internet might lead to information security risk for users and organizations. There are several ways to help increase security such as verification and identification system. For example, there is a registration before accessing to a website for the safety of the user and the service system since some services have limited rights in getting free service per user and per day. So, some users attempt to exploit the offered free services by creating and applying duplicate users or attacking the system to get the no limit-services. Moreover, some people even attack websites by spam links. These behaviors could be improper accession and damage the system. Therefore, the process of system protection has to be taken into consideration.

CAPTCHA is one of the solutions for security on a website. It is a system which facilitates the measure of filtering whether an access to a website is made by actual humans or other automated program systems (BOT). It examines the differences between humans and bots by means of Turing Test. CAPTCHA's objective is to provide protection against automatic registration on websites, which commonly occurs because of the easy access on websites. Although some bots process the capabilities to pass through CAPTCHA system, CAPTCHA is still popular and is continuously being improved to protect websites in many different ways. As of today, there are many

different styles of CAPTCHAs to respond to each specific users' requirements for securities measures.

One of the most common style of CAPTCHA based authentication is biometrics. Biometrics is defined as the individual characteristics of a person. It is divided into two parts; physiological characteristics and behavioural characteristics. Examples of physiological characteristics are faces, fingerprints, hand geometries, iris, retinas, veins, voices, etc. Examples of behavioural characteristics are speech recognitions, signatures, keystrokes, among many others. Biometrics is applied for human authentication by serving as a process of individual identification using biological characteristics of a person. This provides reliability in addition to safety. From biometric authentication principals, biometrics serves as an alternative in security protection systems.

This research intends to use an individual's characteristic verification mixed with CAPTCHA as biometric authentication before granting access of the system to a user. Through research, it is discovered that eye movements and gaze detections can express the unique biological characteristics of a person; thus is selected as a topic of research for biometric authentication. An eye movement and a gaze detection will be applied along with the security protection system for filtering and differentiating real human users from program systems (BOT) attempting to access a website. This has potential in increasing the efficiency of the protection system and allows for easier user's usability in installing and accessing the system.

This research proposes an implementation of biometric authentication for CAPTCHA creation by using features of the eye movement and gaze detection. This method is used to analyse data from real humans and aims to increase the performance of preventing the attacks from BOTs.

1.1. Objective

1. To propose an implementation of biometric authentication based on eye movement characteristics to create CAPTCHA for spamming agents' attacks prevention.

2. To improve the performance of human verification with CAPTCHA.

1.2. Problem formulation

1. How to design a method that increases the performance of CAPTCHA in preventing the attacks from BOTs?
2. How to apply eye movement technology in CAPTCHA?
3. How to evaluate the proposed authentication prototype?

1.3. Scope of thesis

1. The frame rate of camera in this prototype is not greater than 30 fps. While the resolution is between 320 x 240 pixels and 1280 x 1024 pixels.
2. The image size of CAPTCHA is at least 720x480 pixel with 72 dpi.
3. The prototype is evaluated by the satisfaction analysis and the in-depth interview.

1.4. Expected Outcomes

This research aims to implement the biometric authentication in order to create CAPTCHA that uses features of the gaze detections and eye movements. The prototype constructed from the proposed method is expected to increase the performance of CAPTCHA in analyzing and distinguishing humans and machines.

Chapter 2. Theoretical Backgrounds

This Chapter describes and explains the details of the background knowledge for the EYE CAPTCHA. It consists of CAPTCHA, biometric authentication, and eye movement.

2.1. CAPTCHA

CAPTCHA stands for "Completely Automated Public Turing Test to tell Computers and Humans Apart". It is used as a tool to test the differences between authentic users (humans) and computer programs (BOTS). It is commonly applied onto websites. CATCHA was invented by Luis von Ahn, Manuel Blum, Nicholas Hopper, and John Langford of Carnegie Mellon University in 2000. Its basic advantages are automatic system access protection, spam rejection, etc. However, in practical terms, the CAPTCHA system always prevents issuing too many commands. It can be described by Figure 1, which illustrates the process of CAPTCHA system [1].
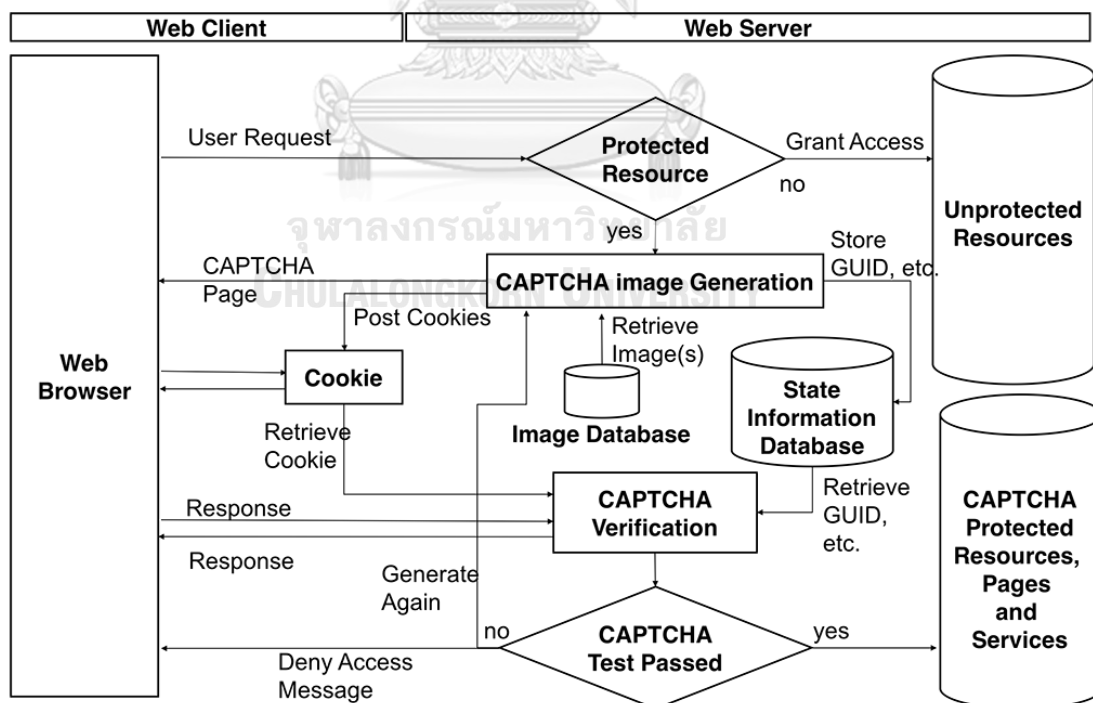
Figure 1. Process of CAPTCHA system.

In Figure 1, at the start of the process, the user enters to a web page through a web browser and sends a request for the system to grant access to a web server. Then the server generates a web page with CAPTCHA in response to the user's request to the web page to be displayed. The user needs to solve CAPTCHA solution and submits that CAPTCHA answer to the server for verification. Then, the server checks the answer for authentication. If it is correct, it will send the web page to render and embed CAPTCHA cookie into the web browser. If it is wrong, it will restart the process from the beginning.

2.2. Biometric authentication

Biometrics is a technology of analysis of physical or behavioral characteristics of each individual which is used to confirm a person's identity. There are two major categories of biometric technology; physiological measurement and behavioral measurement. Thus, biometric authentication is the process of comparing two sets of data; in Figure 2, at the beginning, the system accepts the user's biometrics and pass it on for matching with the template stored within the system in order to determine the resemblances and make a decision whether to grant access. Currently, biometric authentication has become a common method for authentication. In addition to security purpose, it is difficult to fake individual biological characteristics. It is also accepted that the biometric verification is easy and convenient to process [2]. The process of biometric authentication can be illustrated as shown in Figure 2.
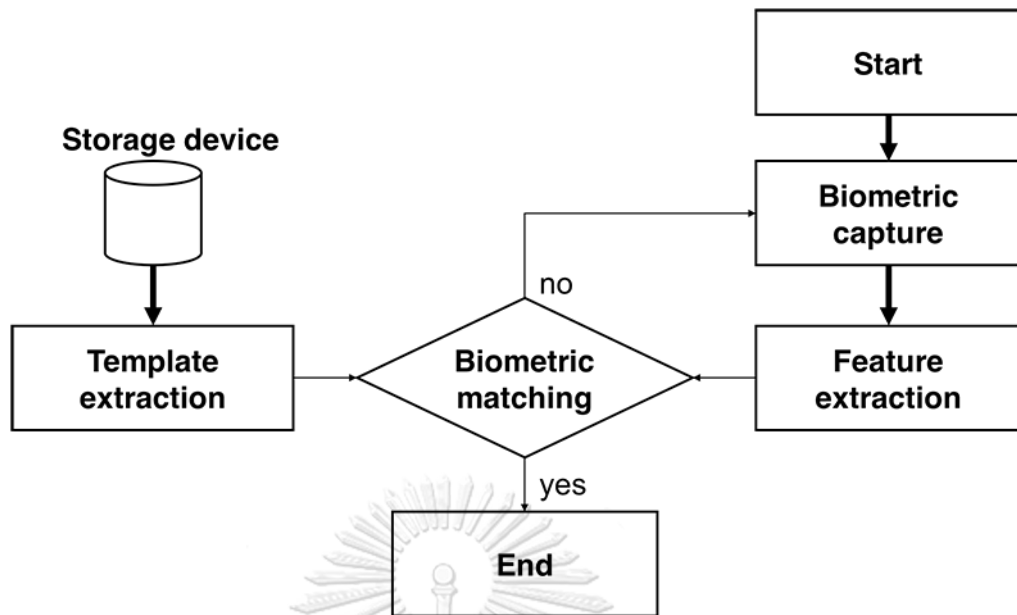
Figure 2. The process of biometric authentication.

There are quite a few types of identifying a user by using biometric method. Below are the most popular biometric authentication technologies.

2.2.1. Fingerprint

It processes in the form of raised areas and branches in human fingerprints Fingerprint scanning is shown in Figure 3 [3].

Figure 3. Fingerprint scanning.

2.2.2. Eye scanning

It uses the ring-shaped region surrounding the pupil of an eye. An eye is the most reliable body part for biometric authentication. The parts that are mostly and commonly used are the retina and the iris. Eye scanning [4] is shown in Figure 4.

Figure 4. Eye scanning.

2.2.3. Voice recognition

A system relies on the characteristics of a voice. Voice recognition uses the properties of inflections, tone, and accent as shown in Figure 5 [5].
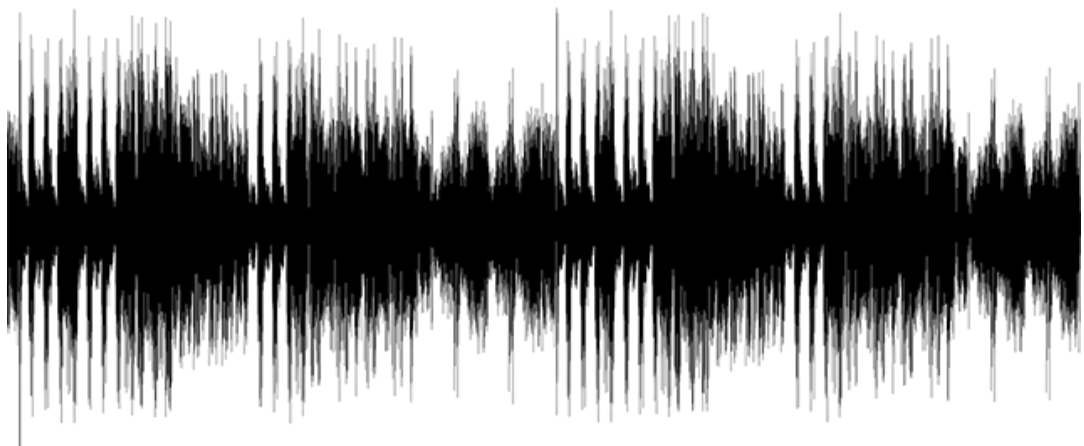
Figure 5. Sound wave.

2.2.4. Eye movement

Eye movement is a movement of an eye by muscles innervated by cranial nerves. Eye movement [6] has four basic types that is saccades, smooth pursuit movements, vergence movements, and vestibulo-ocular movements.

2.2.5. Saccades

Saccades are fast-moving eyes that immediately change the point of fixation. The time course of a saccades sight movement is shown in Figure 6.
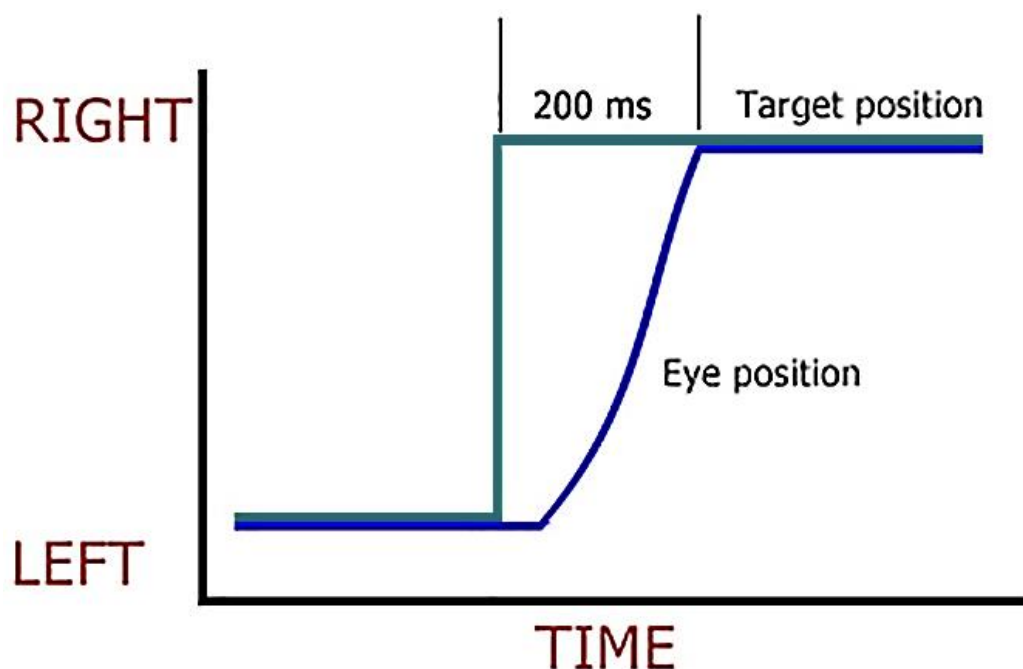
Figure 6. The saccadic eye movement.

2.2.6. Smooth pursuit movements

Tracking movements of the eyes is a smooth pursuit of movements. It is designed for keeping a moving stimulus on the fovea. The movement is subject to voluntary control in the sense that the observers can choose whether to track or not to track a moving impulse. In simpler terms, this means that when a human's eyesight is focused on an object, as the object moves in it's distinguish motion, the eyes watching the object will also follow to keep the object in sight. Thus creating a smooth movement of the eyesight along with objects. Figure 7 explains the definition of smooth pursuit of eye movements, where the red lines represent the movement of the human eyes and the blue lines represent the actual movements of the objects in term degrees. As

shown in the Figure, the two color lines are almost overlapped. The meaning of the overlapping lines is that as the objects are moving the human eyes are also following the objects through the movements.
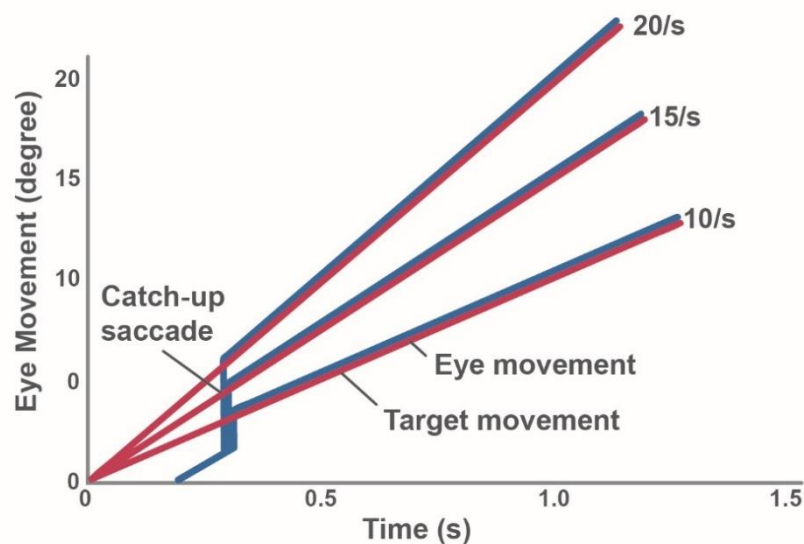
Figure 7. The smooth pursuit of eye movements.

2.2.7. Vergence movements

Vergence movements are the simultaneous movements of both eyes. The position of each eye aligns with the targets located at different distances from the observer. Both eyes move in the same direction and vergence movements are associated either by a convergence or divergence of the eyesight. This allows for each eye to see an object and determine whether it is nearer or farther away from the eyes as illustrated in Figure 8 [7]. Convergence is one of three reflexive visual responding to humans' interests in nearby objects. The other components of the group of the reflex triad are accommodation of the lens, which brings the object into focus, and pupillary constriction. This increases the depth of field and sharpens the image on the retina.
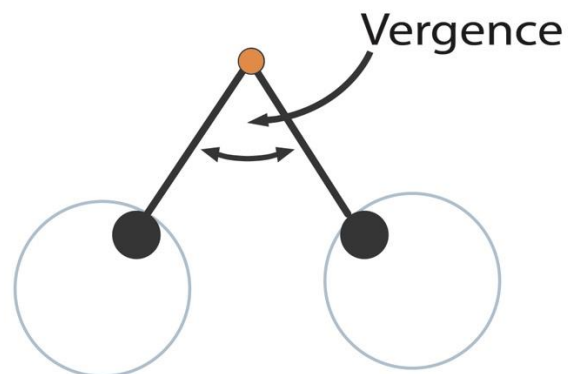
Figure 8. A vergence eye movements.

In Figure 8, the two circles with inner black circles represent the eyes making a vision on to an object of interests represented in an orange circle.

2.2.8. Vestibulo-ocular movements

Movements of Vestibulo-ocular reflex of eyes are associated with the outside world. As head movements can cause erratic movements of the focused objects, an example is when a camera is attempting to take photos on unstable platform, the image taken can be out of the camera's focal point. Similarly in humans' vision system, to handle the unstable movements of the eyesight, Vestibulo-ocular movements provides humans the ability to see everything precisely as the eyesight of human are unstable through body and head movements.

Chapter 3. Related Works

In this research, we divide three parts of the related works namely CAPTCHA, the biometric and the eye movement.

3.1. CAPTCHA

Today, the internet is almost in every activity in our lives. It can be used for many things such as hotel booking, food ordering, information searching, etc. It is mainly used via a website as well. Websites have become the basis for usage. But, the rapid advancement of technology and techniques has increased the vulnerabilities of websites and systems. It allows a harmful person to hack or attack a system. According to Acunetix web application vulnerability report in 2016, more than 55% of websites have one or more vulnerabilities, growing by 9% over 2015's report. 84% were susceptible to at least one medium-severity vulnerability [8].

CAPTCHA technology is a tool for an experiment called the Turing Test. It proposes the test as a way to examine whether the user is a real human. CAPTCHA is commonly used to apply on systems and websites, i.e., to prevent spams, stop a Distributed Denial of Services (DDos) attacks, deter spammers, decelerate a new page creation or adding an external link to a page or spam posting to forums, and defend against the web scraping [1]. CAPTCHA is popular for applying on websites. Websites which are content subscription sites, forums, social networks, and blogs because of its usability and simplicity. CAPTCHA has a variety of styles, depending on the types of its presentation. CAPTCHA can be simply classified into five categories ranged by its popularity as presented as follows [9].

3.1.1. Text-based CAPTCHA

This is the most popular category of CAPTCHA for registration forms on websites. It contains an image of numbers, an image of characters, or both. The system shows an image and a textbox. A user can pass the system by typing the characters he sees in the picture into the textbox. Figure 9 depicts an example of text-based CAPTCHA [10].

Figure 9. Text-based CAPTCHA.

Because of its simplicity, it is easy to use and implement this CAPTCHA. Therefore, it is easily attacked by many methods such as Optical Character Recognition (OCR) techniques, Template Matching Correlation (TMC) technique. To avoid the problem of CAPTCHA solving techniques, many researchers have improved text-based CAPTCHA by using complicated variation such as applying noise and distorting the image to the sequence [11, 12]. These have an impact on identifying correct numbers or characters by a human.

3.1.2. Image-based CAPTCHA

Image-based CAPTCHA is required to match image according to a text instruction or an image instruction [10]. To attack this CAPTCHA, the image recognition must be used to extract the meaning of each image. For example, research of David Lorenzi et al., they used image recognition techniques to attack the image-based CAPTCHA [13]. Moreover, in case that selects an image from an instruction, the OCR is still important. It works collaboratively with the image recognition to attack a system. In the other words, the system understands the meaning of the command and of the image and can match both. The examples of image-based CAPTCHA are depicted as shown in Figure 10 and Figure 11.
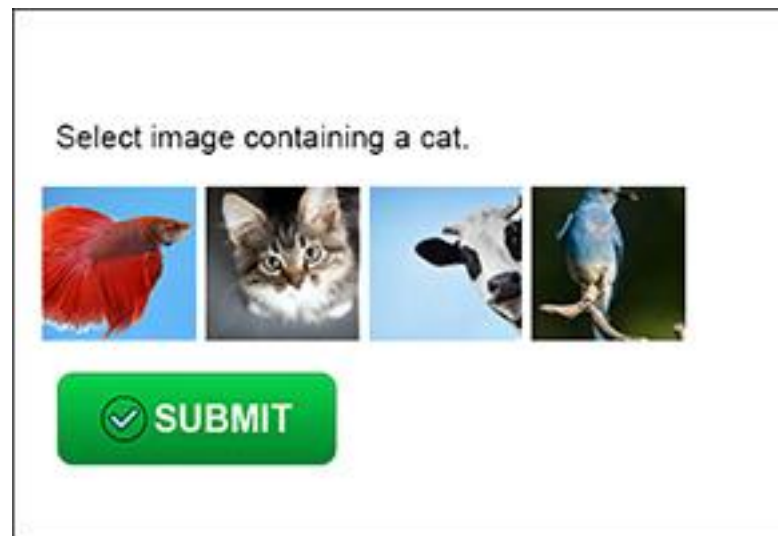
Figure 10. Image-based CAPTCHA in which the image is chosen according to the text instruction.

Figure 11. Image-based CAPTCHA in which the similar image is chosen to match another image in the instruction.

However, there are some weaknesses. For example, increasing security such as blurring, noise, or illumination effects may make CAPTCHA difficult to be solved by some users who have poor eyesight. Consequently, Bin B. Zhu et al. developed CORTCHA framework as a new CAPTCHA with higher security. CORTCHA is abbreviated from Context-based Object Recognition to Tell Computers and Humans Apart. The advantage of this research is the ability to effectively handle machine learning attacks [14]. However, it takes a lot of time to complete the task.

3.1.3. Audio-based CAPTCHA

Audio-based CAPTCHA is a dataset of sounds of words or phrases including characters and numbers. A user listens to a sound of characters and numbers from a speaker. After that, the user must type characters, numbers, or both into a textbox. The working process of the audio-based CAPTCHA is similar to the visual CAPTCHA, but it is more difficult than the visual CAPTCHA. This CAPTHCA is designed for a group of visually impaired users who use screen-reader programs. An example of this CAPTCHA is shown in Figure 12.
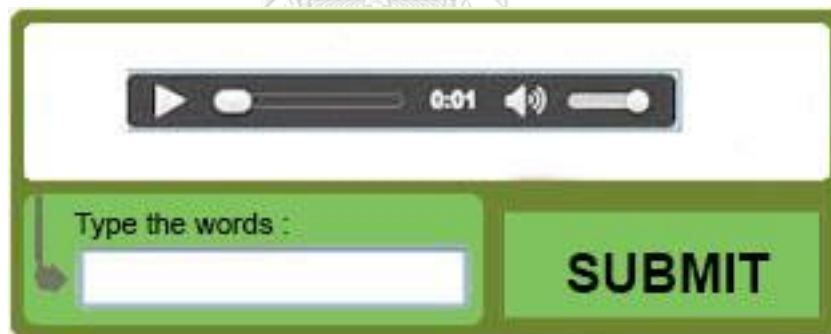
Figure 12. Audio-based CAPTCHA.

There are still some problems with this type of audio-based CAPTCHA. The user must understand English language. Especially, they must understand what they hear and must also spell it correctly [15]. Moreover, the speaker or headphone are the key component in this kind of audio-based CAPTCHA.

3.1.4. Video-based CAPTCHA

Video-based CAPTCHA technology substitutes a brief video display of characters for a wavy line of letters. This category is quite new and its creators claim that it is also much more secure. Users can be proved by filling a sequence of red characters from a video into a text box. The example of video-based CAPTCHA is depicted as shown in Figure 13.

Figure 13. Video-based CAPTCHA.

Despite the increased safety, there are still some problems. The size of the video file is large and it effects the loading time of the website, including waiting time for the red characters to show up [16].

3.1.5. Puzzle-based CAPTCHA

Puzzle-based CAPTCHA is adapted from the image-based CAPTCHA. It works as a puzzle game. When an instructions appears on the screen, and users are asked for solving a puzzle for proving themselves under the assumption that computers cannot solve the task as humans do. By the way, sometimes the random puzzles are too difficult to solve in a limited time [17]. Figure 14 shows the example of puzzle-based CAPTCHA.

Complete the jigsaw.

Figure 14. Puzzle-based CAPTCHA.

There are still a lot of researchers and developers who are developing CAPTCHA system. They try to improve and develop CAPTHCA in various issues such as performance, accuracy, workflow and applying new techniques. These techniques include machine learning, cloud techonology, mobile technology, and biometrics. For example, Brian M. Powell et al. used CAPTCHA based on multibiometrics to get better online security [18]. Since fingerprints, faces, and eyes are hardly detected by the computer program, they used images of faces, fingerprints, and eyes for generating CAPTCHA mixing with images distortion background. The results show that human success rates are above 80%, while success rates for anti-attack are 100%. For mobile devices and tablets, Mitsuo Okada and Sakito Matsuyama created a CAPTCHA [19]. They used distorted background to hide multiple images and text. A user has to use the finger to move the hidden objects. The objects become visible once they are overlapped. Then, a user (the human) verification is completed after they can overlap the objects. Anjitha K and Rijin I K A presented an enhanced security of CAPTCHA as

gRaphical Passwords (CaRP) [20]. Their system comprises CaRP and motion-based CAPTCHA, which relies on video technology. The gRaphical Passwords is a technique for authentication by clicking on the image as the password. CAPTCHA features such as color, size, and shape can also be changed.

3.2. Eye Movement

Biometrics is measurement, calculation, and analysis of human physical and behavioral characteristics. The usage of biometrics can be applied in the authentication. Biometric authentication is a technology of security process based on identification or verification through at least one biological feature. It has various authentication methods such as identifying a person and biometric matching. It can be applied to security applications that need accuracy and reliability. There are many features used for biometrics authentication such as fingerprint, face, palm-print, hand geometry, iris, and voice [21]. In addition, many biological features can work together in multiple systems or can be applied to many applications. For example, a web-based multimodal biometric authentication, which consists of Electroencephalography (EEG), face recognition, and SMS token. Three categories are used as the authentication weight for access. It was proposed by Ghada Al-Hudhad et al [22]. Figure 15 shows the system of a web-based multimodal biometric authentication.
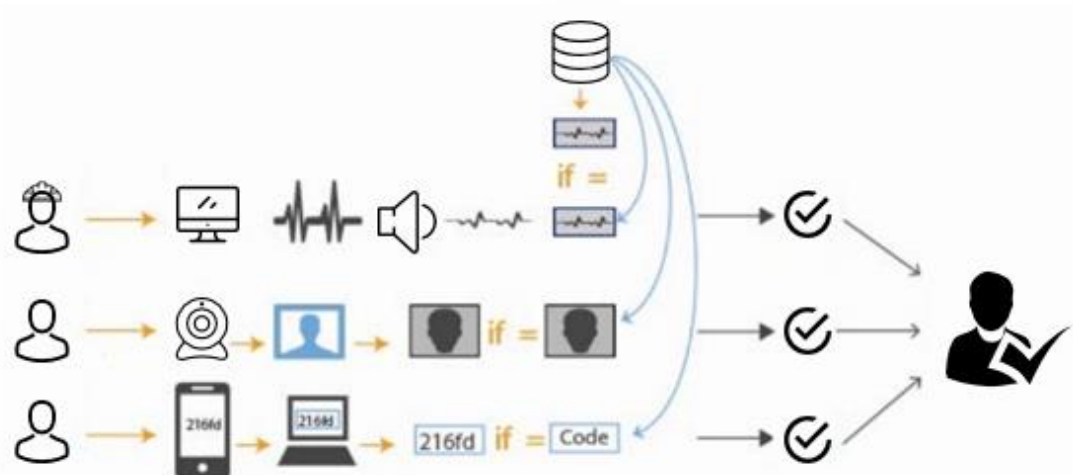
Figure 15. A web-based multimodal biometric authentication.

One of the key features of identification is eye movement. Eye movement is one characteristic that can be used for biometric authentication. There are many researches related to the use of eye movement in identifying people. Akram Bayat and Marc Pomplun [23] proposed the analysis of the users' behaviors by using tracking during reading. They used fixation duration method, pupil size, and reading speed for eye-tracking measurement. From the result, it indicates that the eye movement and pupil size have impacts on individual differences. Pawel Kasprowski and Katarzyna Harezlak [24] showed the results of verification and identification of the eye movement from the competition. They chose the best five results and algorithms among all participants in terms of recognition rate, memory effect, and data dependency.

According to several researches in the eye movement, eye tracking, and eye detection, reliability, easiness, fast processing, and ease of use are concerned. Eye gaze is a key part of eye movement tracking by detecting eye and predicting the position of the eye matching with the screen. Dat Tien Nguyen et al. [20] presented a method for head pose estimation in smart TV using a new gaze detection method based on face ROI extraction. In this method, they combined the boundary of the face and the shoulder line to estimate the head pose shown in Figure 16.
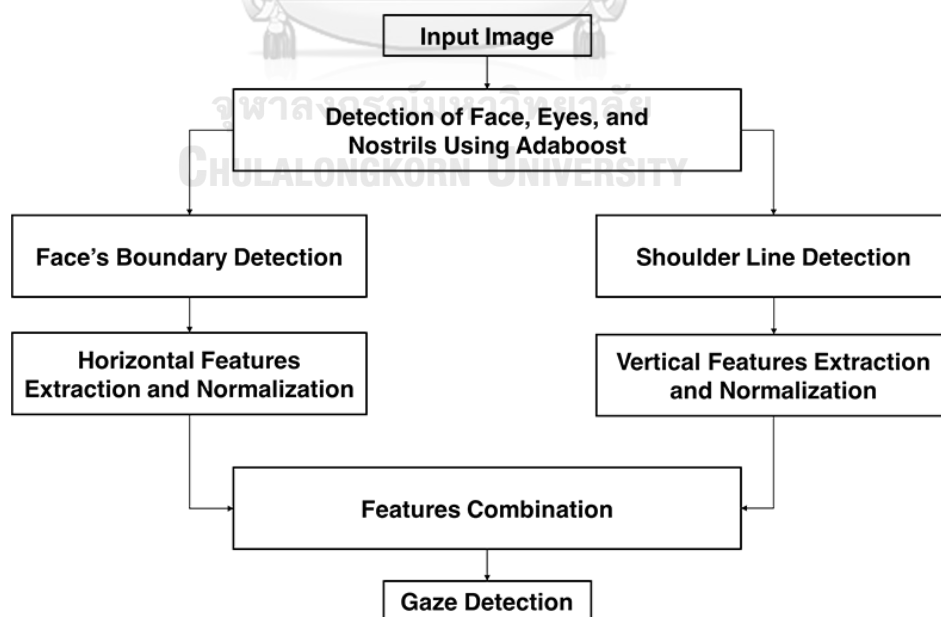
Figure 16. The overall procedure of pose estimation in smart TV

Ba Linh Nguyen [25] proposed the real-time eye gaze tracking technique using Haar-like features, Lucas-Kanade algorithm, and Gaussian process regression. First, they used Haar-like features to detect eyes. After that, they used Lucas kanade algorithm for eye tracking. Lastly, they used Gaussian process for eye gaze detecting. In addition, the movement of the head and eyes will be calculated and analyzed for greater accuracy. Chunning Meng and Xuepeng Zhao proposed the convolutional neural network (CNN) for analyzing webcam-based eye movement [26]. The CNN is used to estimate the movement of the eye by training the eye properties collected from five points as shown in Figure 23. Points A and B are inner and outer corners, Points C and D are centers of upper and lower eyelids. Point E is a center of iris.
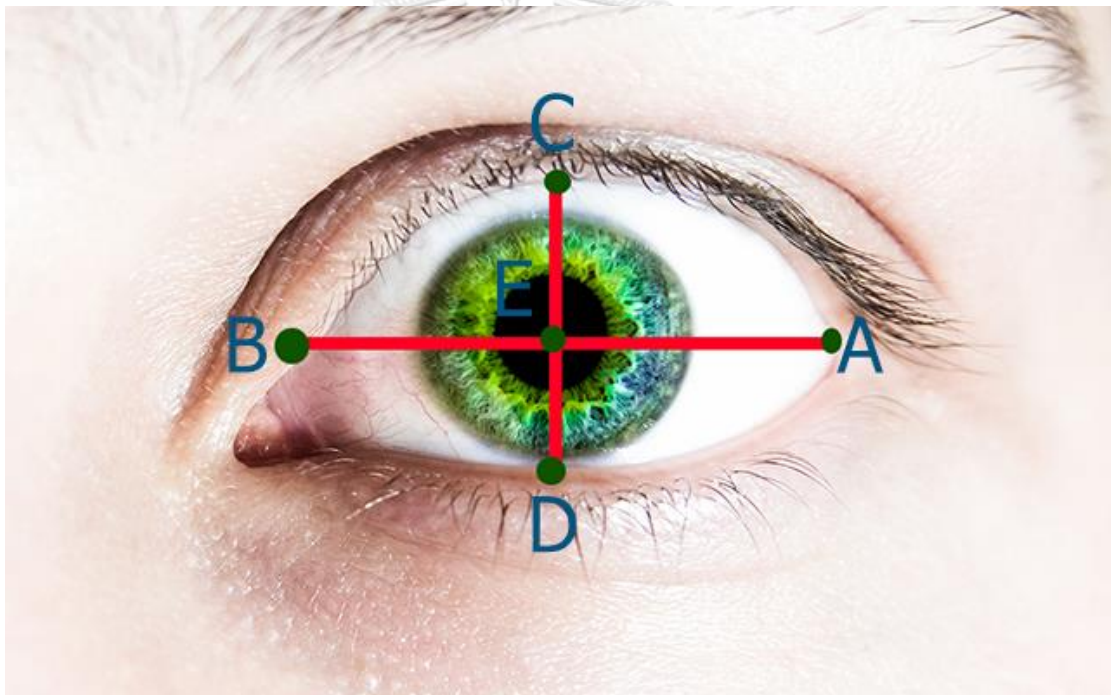
Figure 17. Eye feature point [4].

In the proposed prototype, the WebGazer library proposed by Alexandra Papoutsaki et al. [27] and integrated into the website for eye detection and gaze interaction in real-time is used. Two most important modules of webgazer are eye detector and gaze estimator using analysis information of interactions between user and screen.

Chapter 4. Proposed Method

From the previous Chapter, CAPTCHAs and the eye movements play a major role in the part of human verification. Both are used to increase accuracy and enhancement in the protection against unwanted computer programs. In this study, CAPTCHA is introduced based on the detection and movement of the eyes that can subrogate existing CAPTCHA. This proposed technique applies CAPTCHA in relation to puzzle-based CAPTCHA and image-based CAPTCHA to capitalize on the strong points of these two CAPTCHAs. This method is called "EYE CAPTCHA" since both of gaze detection and eye movement are adopted. This proposed method consists of the following five main steps.

1. Train and feed data into local storage.
2. Create the EYE CAPTCHA.
3. Detect a user's gaze.
4. Ask a user move an answer object to the destination using his/her eyes.
5. Check the result.
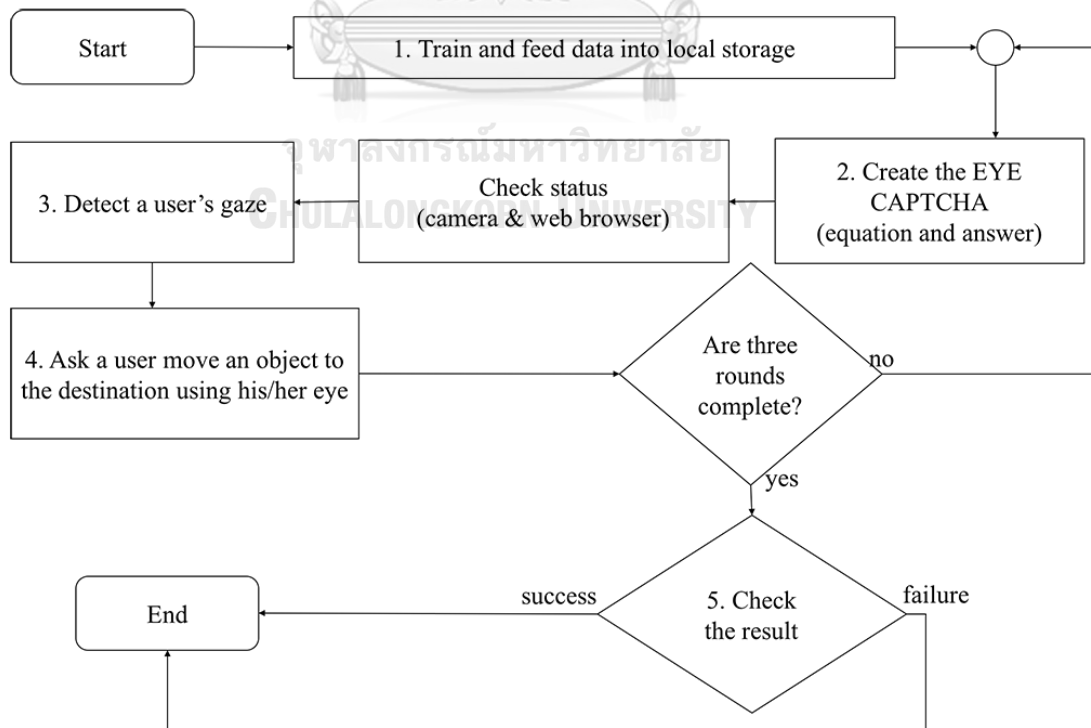
Figure 18. The proposed method.

The entire flow of procedure for the EYE CAPTCHA system is illustrated in Figure 18. All the steps are described in details below.

4.1. Train and feed data into local storage

When users access a website with the EYE CAPTCHA, the authentication system will start automatically. This website shows the first page of the EYE CAPTCHA system as in Figure 19. It will show start button on a center of the screen of the desktop.

Figure 19. The first page of the EYE CAPTCHA system.

First, the system will check whether previous training data is available. The data is the information of the positioning of the user's eyes, whether they match with the position of the object on the viewed screen. The object is stored in an array format in a cache memory of the web browser on computer. The default of local storage for each browser is at least 5 MB buffer in the browser. This information will never be transferred to the server. If there is no training information within the local storage, the system will use a default training dataset loaded to the local storage. When users use this system, it will automatically update the training data every time deploying the current users' information for next opportunities.

Note: The training data is calibrated gaze detection matching with a position on screen through user interactions. It consists of JSON format data of the eye position on the

screen matching with the position of the object. The structure of collected data is shown below.

Structure of collected data:

{

        'Positions': The position (X, Y) on the screen that a user is looking at,

        'Width': width of pixel data,

        'X': calibrate position X between the eyes of the user and the screen,

        'Y': calibrate position Y between the eyes of the user and the screen,

        'Type': type of data,

        'Timestamp': time

}

4.2. Create the EYE CAPTCHA

By pressing the start button, the system will begin the process, as shown in Figure 18. In this step, the system does a parallel process. First, the system will generate an equation with four choices as answers. The equation is initialized at the middle of the screen. Likewise, each answer is displayed at each corner of the screen as shown in Figure 20.

Figure 20. The step of creating the EYE CAPTCHA.

At the same time, the system will check the status of the camera and web browser. It is investigated to ensure the readiness of gaze detection.

4.3. Detect a user's gaze

From Step 2, once everything is ready, the system will detect the user's eyes through the web-camera and locate the position of the eyes in respect to the screen. To detect the user's eyes for authentication, first and foremost, the system needs to determine the detection of each features of a human's face. Thus face detection needs to be implemented. Through face detection, the system can filter out unnecessary features of the face, such as mouth and nose, to focus the detection to only the location surrounding the eyes. Once the information of the eyes are detected, pupils can also be detected for further analysis. The X, Y coordinates of the pupils are analyzed in correlation to information that has been stored in data storage i.e. calibrate (training) data. If the coordinates of the user's detected pupils match to one of the training data within the data storage, the position on the screen where the user is gazing at can be predicted.

Face detection is implemented by using the following open source libraries:

1. js-objectdetect [27]
2. tracking.js [28]
3. clmtrackr [29]

The js-objectdetect and tracking.js libraries are used to detect features on the face; mouth, eyes, and nose. Once these features has been detected, the libraries return rectangle marks covering these facial features. In cases where the user's detected face is not in upright position, clmtrackr is applied to adjust the shape positioning to be more upright for further analysis. With these three libraries, the system has filtered out other unnecessary features of the face, leaving only the data on eyes for the next process. To process the acquired eyes data, WebGazer library [30] is implemented.

There are three assumptions within this study concerning eye detection:

1. The iris is dark,
2. It is a circle, and
3. It is located at the middle.

If the system cannot detect the eyes of a user following the proposed assumptions, the system will response to the user by showing a notification on the screen.

4.4. Ask a user to use his/her to move an answer object to the destination

The system detects a user's eyes relatively to the X, Y coordinates on the screen. In each round, the system will be completed when the answer is moved to the center of the screen by the user's gazing on the correct answer as shown in Figure 21.
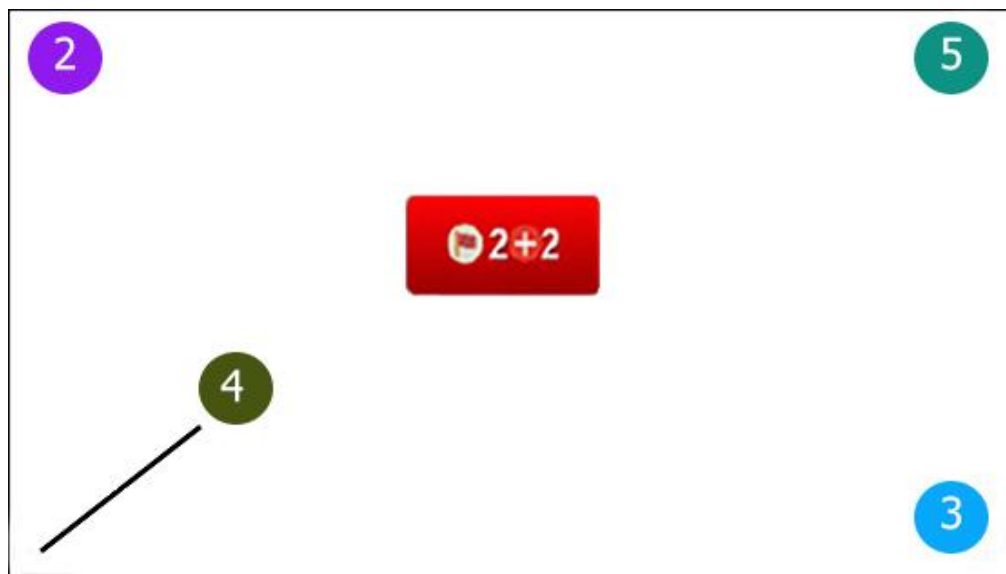
Figure 21. The step of ask a user to user his/her to move an answer object to the destination.

In this step, the system works by focusing user's gaze on the correct answer to be moved to the center of the screen following the user's eyesight. First of all, the system needs to determine that the user is gazing at the position of the answer by matching user's gaze to the position on the screen of the answer. In this case, to be considered as a gaze, only if the user's eyes focus on the answer for more than 500ms. Only then will the answer starts to move, following the user's eyesight bringing the answer to the center of the screen.

An inspection of the system in each round is accomplished when an answer is moved to the center of the screen by the user's eyesight. When a user moves the answer to the target, the system will save all information as a log file. This file contains the position, the path, the location, and the timestamp as the answer of each round

to be processed in the next step. This step is considered to be finished when the user selects the correct answer for at least two times out of three tries. If the user selects the correct answer within the first two tries, the third round is not necessary.

4.5. Check the result

The step of verification is performed based on interactive information such as the answer, timestamp, and some errors. The system will proceed information to identify if it is a human or a bot. To decide whether it is a human's interaction, there must be at least two correct answers from 3 rounds. Also, the completion time should be reasonable due to the average time in each round of participants plus or minus standard deviation of 200ms [32]. This average time is updated all the time along with the number of users. After analyzing the information, the system will report the conclusion whether the user is a real human or a failure case that the bot tries to fake to access the system. Figure 22 shows an examples of conclusion report of the system.
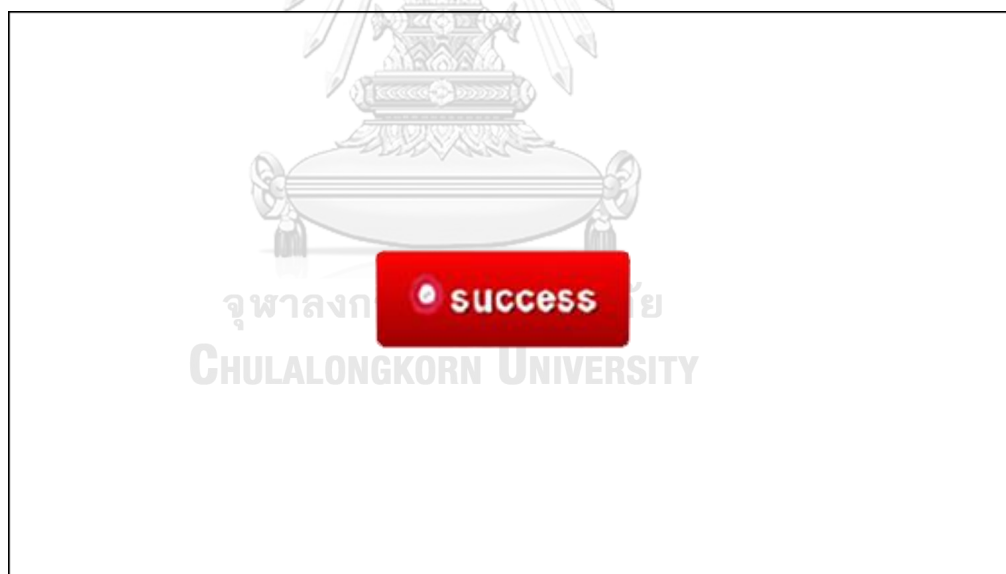
Figure 22. Result of the EYE CAPTCHA.

In order to measure the satisfaction of the EYE CAPTCHA, the proposed method uses three groups of satisfaction measurements including work process, appearance, and gratification. The results of these measurements are shown in Chapter 5.

Chapter 5. Experiments and Results

This Chapter can be separated into five parts. Part I is the general information about the experimental setup and collected information in the research. Part II, the proposed process compared with the traditional process by the statistical method. Part III is the analysis of the result of Part II. Part IV, the limitation of the proposed method. The final Part is feedback from participants.

5.1. Experimental Setup

The background environment of the proposed system is shown in Table 1 while the general information of data collection is shown in Table 2. The form of questionnaire and raw data are presented in the appendix.

Table 1. Background environment.

Hardware Specification	Detail
Processor	2.70GHz Intel Core i5
Memory	8GB 1867 MHz DD3
Graphics	Intel Iris Graphics 6100 1536 MB
OS	macOS High Sierra
Displays resolution	2560 x 1600
Camera	720p FaceTime HD camera
Browser	Chorme version 62.0.3202.75 (64 bit)

Table 2. Frequency of participants' characteristics.

Gender	Number
Male	34
Females	23
Age (years)	Frequency
<20	5
20-25	13
26-30	20

31-35	18
>35	1
Education	**Number**
Under Bachelor Degree	4
Bachelor's Degree	37
Master's Degree	16
Doctoral's Degree	0

The overall satisfaction measurements of the proposed system in terms of the work process, appearance, and gratification are detailed in Table 3.

Table 3. Overall satisfaction measurements.

Group	Issue	Description
1. Work process (Step by step)	1	Minimal and simple procedure
	2	User-friendly process
	3	Appropriate technique
2. Appearance	4	Optimal UX & UI
	5	Using modern technology
	6	Meaningful interface
3. Gratification	7	Usage Overview
	8	Appropriate user's interaction
	9	Conformance with task's objective
	10	Applicable in real life

From Chapter 4, the prototype is mainly implemented using JavaScript. The proposed system attempts to automatically check the environment within the system and to define default data of the predicted positions of the pupils on the screen. The measurements in Table 3 are used as the users' satisfaction survey. A user is required to give the score for each issue, ranging from least satisfactory, as number one to the most satisfactory, as number four.

The next section will explain the users' satisfaction on the EYE CAPTCHA compared to other traditional CAPTCHAs.

5.2. Evaluation

The t-test is used for independent two-sample comparison. In this case, it is a comparison on the EYE CAPTCHA.

In case $\sigma_1^2 = \sigma_2^2$, use the formula

$$t = \frac{X_1 - X_2}{\sqrt{S_p^2(\frac{1}{n_1} + \frac{1}{n_2})}}$$
(5.1)

$$df = n_1 + n_2 - 2$$
(5.2)

where X_1 and X_2 are the means of sample values of group 1 and group 2, respectively. df Is degree of freedom.

S_p^2 is a pooled variance that is calculated by the following equation.

$$S_p^2 = \frac{(n_1 - 1)S_1^2 + (n_2 - 1)S_2^2}{n_1 + n_2 - 2}$$
(5.3)

where n_1 and n_2 are the number of sample values of group 1 and group 2, respectively.

In case $\sigma_1^2 \neq \sigma_2^2$, use the formula

$$t = \frac{X_1 - X_2}{(\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2})}$$
(5.4)

and

$$df = \frac{\left(\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}\right)^2}{\frac{(\frac{S_1^2}{n_1})^2}{n_1 - 1} + \frac{(\frac{S_2^2}{n_2})^2}{n_2 - 1}}$$
(5.5)

where X_1 and X_2 are the mean of sample value of group 1 and group 2, respectively. df is degree of freedom

S_p^2 is a pooled variance

$$S_p^2 = \frac{(n_1 - 1)S_1^2 + (n_2 - 1)S_2^2}{n_1 + n_2 - 2} \tag{5.6}$$

where n_1 and n_2 are the number of sample value of group 1 and group 2, respectively

5.3. Analysis

For evaluation and analysis of this work, work process, appearance, and gratification are used to measure the satisfaction of each group and issue. Table 4 provides the mean of satisfaction score of both traditional version and new version of CAPTCHA.

Table 4. Mean and standard deviation values of satisfaction of the ten issues, three groups, and overall system.

Groups		Mean		Standard Deviation	
		Old	New	Old	New
Overall		2.68	2.86	.736	.718
Groups	Group 1	2.68	2.72	.720	.703
	Group 2	2.56	2.93	.668	.548
	Group 3	2.74	2.89	.684	.648
Issues	Issue 1	2.61	2.65	.861	.767
	Issue 2	2.81	2.68	.811	.805
	Issue 3	2.79	2.81	.840	.833
	Issue 4	2.60	2.82	.842	.710
	Issue 5	2.44	3.28	.846	.726
	Issue 6	2.70	2.79	.772	.700
	Issue 7	2.63	2.67	.698	.787
	Issue 8	2.61	2.70	.796	.654
	Issue 9	2.70	2.98	.778	.719
	Issue 10	2.72	2.72	.774	.881

New - EYE CAPTCHA
Old – Traditional CAPTCHA

Table 4 shows the EYE CAPTCHA comparison score for new and existing CAPTCHA method, as labeled as old, in three different categories; overall, groups, and issues.

The mean score of overall satisfaction of the EYE CAPTCHA is higher than that of the traditional CAPTCHA. In more detail, the mean scores of the EYE CAPTCHA satisfaction results of appearance (group 2) and gratification (group 3), are higher than those of traditional CAPTCHA. However, when considering from the mean score of the work process (group 1), it is slightly less than that of the traditional CAPTCHA. This might be caused by its complication of the work process. For each group, the standard deviation (SD) of the EYE CAPTCHA is lower than that of the traditional CAPTCHA because most users have the same level of satisfaction in the EYE CAPTCHA. However, with the view of issues, the EYE CAPTCHA outperforms the traditional CAPTCHA in nine issues. Except issue 2, the user-friendly process of the traditional system is better than the EYE CAPTCHA since the score is slightly less than the traditional CAPTCHA. It may be because the users are unfamiliar with the novelty and difference of the EYE CAPTCHA system. Also, the time spent on the validation process of the traditional CAPTCHA is low and the traditional CAPTHCA is easy to be completed. However, the users can finish the task faster if they frequently use the CAPTCHA.

The comparison between the EYE CAPTCHA and the traditional CAPTCHA is considered and discussed. In this thesis, Independent Sample t-test is used to evaluate and analyze the satisfaction of the users. The table consists of t-test, P-value (Sig.), mean difference, and confidence interval of the difference. t-test is used for the mean difference testing between the null hypothesis (H0) and the alternative hypothesis (H1). A P-value is used to evaluate and analyze the difference in two groups.

Table 5 shows the statistics of users' overall satisfaction. The result consists of a frequency of participants, mean values, standard deviations, and the standard deviation error mean. The mean score of the EYE CAPTCHA is higher than that of traditional CAPTCHA whilst the standard deviation of the EYE CAPTCHA is slightly less than that of the traditional CAPTCHA. In other words, between the two groups, most users have the same level of satisfaction in regards to the EYE CAPTCHA.

Table 5. Group statistics of questionnaire (Overall).

Groups Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.86	.718	.095
Traditional CAPTCHA	57	2.68	.736	.097

Table 6 shows the overall of the questionnaire in terms of comparison between the two CAPTCHA hypotheses, where the hypotheses are defined as follows:

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

The acquired P-value of 0.200 is higher than the defined significance level of 0.05. Therefore, it is reasonable for the null hypothesis to be accepted at 95% of the confidence interval between the hypotheses. In other words, there is no significant difference. From analysis, it can be concluded that the overall process of the EYE CAPTCHA is not different from overall process of traditional CAPTCHA. This means that traditional CAPTCHA can be replaced by the EYE CAPTCHA. In addition, it can be perceived that users feel marginally better about the EYE CAPTCHA than the traditional CAPTCHAs.

Table 6. Independent samples test of questionnaire (Overall).

	t-test for Equality of Means						
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
						Lower	Upper
Score	1.288	112	.200	.175	.136	-.094	.445

Table 7 shows the different statistics of the work process acquired in the proposed system. The evaluation consists of a frequency of participant, mean value, standard deviation, and standard deviation error mean. The experiments resulted in a higher mean score of work process for the EYE CAPTCHA in comparison to that of traditional CAPTCHA. While in contrast, the standard deviation of the EYE CAPTCHA is

to some degree less than traditional CAPTCHA. The meaning of the result is that there is not much of a difference in the users' preference between the two.

Table 7. Group statistics of group 1 (work process).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.72	.703	.099
Traditional CAPTCHA	57	2.68	.720	.094

Table 8 details comparisons of the work processes (Groups 1). The hypotheses are defined similar to Table 6 as follow:

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

The P-value of 0.798 is higher than the significance level of 0.05. The null hypothesis can be accepted at 95% of the confidence interval, which means, there is no significant difference between the EYE CAPTCHA and tradition CAPTCHA. It can be concluded that work process procedure of the EYE CAPTCHA is not different from work process procedure of traditional CAPTCHA. Thus, traditional CAPTCHA can be replaced with the EYE CAPTCHA. Based on the analysis, it can be determined that users views the EYE CAPTCHA as a bit more preferable comparing to the traditional one.

Table 8. Independent samples test of group 1 (work process).

	t-test for Equality of Means						
						95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Score	.256	112	.798	.035	.137	-.236	.306

Table 9 shows statistics of the appearance. The mean score of the EYE CAPTCHA is superior to traditional CAPTCHA. Also, the standard deviation of the EYE CAPTCHA is slightly less than that of the traditional CAPTCHA. In conclusion, most users feels comfortable with the level of satisfaction in the EYE CAPTCHA.

Table 9. Group statistics of group 2 (Appearance).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.93	.548	.079
Traditional CAPTCHA	57	2.56	.668	.100

Table 10 displays appearance comparison (Groups 2). The hypotheses are defined as follows.

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

The P-value is 0.005, this is considered to be minor comparing to the significance level of 0.05. Therefore, the null hypothesis can be rejected at 95% of the confidence interval. From this reason, it can be concluded that the appearance of the EYE CAPTCHA is different from that of the existing CAPTCHA. This reason might be because the EYE CAPTCHA is new to the users. They might feel unfamiliar with the process.

Table 10. Independent samples test of group 2 (Appearance).

	t-test for Equality of Means						
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
						Lower	Upper
Score	2.893	112	.005	.368	.127	.116	.621

The statistics of gratification is displayed in Table 11. It consists of a frequency of participant, mean value, standard deviation, and standard deviation error mean. The mean value of the EYE CAPTCHA is higher than that of traditional CAPTCHA. The

standard deviation of the EYE CAPTCHA is lower than traditional CAPTCHA. In other words, the user feels satisfied with the gratification of the EYE CAPTCHA.

Table 11. Group statistics of group 3 (Gratification).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.89	.648	.099
Traditional CAPTCHA	57	2.74	.684	.095

Table 12 shows gratification (Groups 3) comparison. The hypotheses are defined as follows.

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

From the result in Table 12, the P-value of gratification is higher than 0.05, meaning that the null hypothesis can be accepted at 95% of the confidence interval. Hence, there is no significant difference. It can be concluded that gratification of the EYE CAPTCHA is similar to traditional CAPTCHA. The traditional CAPTCHA can be replaced by the EYE CAPTCHA.

Table 12. Independent samples test of group 3 (Gratification).

	t-test for Equality of Means						
						95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Score	1.148	112	.254	.158	.138	-.115	.430

Table 13 shows the statistics of the minimal and simple procedure. The table consists of the frequency of participants, mean value, standard deviation, and standard deviation error mean. The mean score of the EYE CAPTCHA is higher than that of the traditional CAPTCHA. The standard deviation of the EYE CAPTCHA is less than the traditional CAPTCHA, which means that the EYE CAPTCHA is suitable for the users as well and that the users feels comfortable using it.

Table 13. Group statistics of issue 1 (Minimal and simple procedure).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.65	.767	.102
Traditional CAPTCHA	57	2.61	.861	.114

Table 14 shows minimal and simple procedure (issue 1) comparison. The hypotheses can be defined as follows.

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

The P-value of 0.819 is higher than the significance level of 0.05, therefore, the null hypothesis can be accepted at 95% of the confidence interval of the difference. In other words, there is no significant difference. From the above analysis, it can be concluded that minimal and simple procedure of the EYE CAPTCHA is not different from minimal and simple procedure of traditional CAPTCHA. In other words, the traditional CAPTCHA can be replaced by the EYE CAPTCHA. In addition, based on the statistical analysis, it seems like users start to feel a little better about the EYE CAPTCHA than the traditional one.

Table 14. Independent samples test of issue 1 (Minimal and simple procedure).

		t-test for Equality of Means					
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
						Lower	Upper
Score	.230	112	.819	.035	.153	-.268	.338

Table 15 shows statistics of the user-friendly process. It uses a frequency of participant, mean value, standard deviation, and standard deviation error mean as default values in determining the user-friendly process of the t-test value. From the result, the mean value of the EYE CAPTCHA is slightly less than traditional CAPTCHA. This might be caused of not familiar with the system process by the users.

Table 15. Group statistics of issue 2 (User-friendly process).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.68	.805	.107
Traditional CAPTCHA	57	2.81	.811	.107

Table 16 shows the user-friendly process of the questionnaire in terms of comparison between the two CAPTCHA hypotheses, where the hypotheses are defined as follows:

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

The acquired P-value of 0.200 is higher than the defined significance level of 0.05. Therefore, it is reasonable for the null hypothesis to be accepted at 95% of the confidence interval between the hypotheses. In other words, there is no significant difference. From analysis, it can be concluded that the user-friendly process of the EYE CAPTCHA is not different from overall process of traditional CAPTCHA. This means that traditional CAPTCHA can be replaced by the EYE CAPTCHA.

Table 16. Independent samples test of issue 2 (User-friendly process).

	t-test for Equality of Means						
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
						Lower	Upper
Score	-.811	112	.419	-.123	.151	-.423	.177

The statistics of the appropriate technique is displayed in Table 17. It consists of a frequency of participant, mean value, standard deviation, and standard deviation error mean. The mean value of the EYE CAPTCHA is higher than that of traditional CAPTCHA. The standard deviation of the EYE CAPTCHA is lower than traditional CAPTCHA. In other words, the user feels satisfied with the appropriate technique of the EYE CAPTCHA.

Table 17. Group statistics of issue 3 (Appropriate technique).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.81	.833	.110
Traditional CAPTCHA	57	2.79	.840	.111

Table 18 details comparisons of appropriate technique (Issue 3). The hypotheses are defined similar to Table 16 as follow:

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

The P-value of 0.911 is higher than the significance level of 0.05, which means that the null hypothesis can be accepted at 95% of the confidence interval which means there is no significant difference between the EYE CAPTCHA and tradition CAPTCHA. It can be concluded that appropriate technique of the EYE CAPTCHA is not different from work process procedure of traditional CAPTCHA. This means that traditional CAPTCHA can be replaced with the EYE CAPTCHA. Based on the analysis, it can be determined that user's views the EYE CAPTCHA as a bit more preferable comparing to the traditional one.

Table 18. Independent samples test of issue 3 (Appropriate technique).

	t-test for Equality of Means						
						95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Score	.112	112	.911	.018	.157	-.293	.328

Table 19 shows the different statistics of the UX & UI acquired in the proposed system. The evaluation consists of a frequency of participant, mean value, standard deviation, and standard deviation error mean. The experiments resulted in a higher mean score of UX & UI for the EYE CAPTCHA in comparison to that of traditional CAPTCHA. While in contrast, the standard deviation of the EYE CAPTCHA is to some

degree less than that of traditional CAPTCHA. The meaning of the result is that there is not much of a difference in the users' preference between the two.

Table 19. Group statistics of issue 4 (Optimal UX & UI).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.82	.710	.094
Traditional CAPTCHA	57	2.60	.842	.112

Table 20 shows UX & UI (Issue 4) comparison. The hypotheses are defined as follows.

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

From the result in Table 20, the P-value of gratification is higher than 0.05, meaning that the null hypothesis can be accepted at 95% of the confidence interval. Hence, there is no significant difference. It can be concluded that gratification of the EYE CAPTCHA is similar to traditional CAPTCHA. Traditional CAPTCHA can be replaced by the EYE CAPTCHA.

Table 20. Independent samples test of issue 4 (Optimal UX & UI).

	t-test for Equality of Means						
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
						Lower	Upper
Score	1.563	112	.121	.228	.146	-.061	.517

Table 21 shows the different statistics of the using modern technology acquired in the proposed system. The evaluation consists of a frequency of participant, mean value, standard deviation, and standard deviation error mean. The experiments resulted in a higher mean score of the using modern technology for the EYE CAPTCHA in comparison to that of traditional CAPTCHA. While in contrast, the standard deviation of the EYE CAPTCHA is to some degree less than traditional CAPTCHA. The meaning of

the result is that there is not much of a difference in the users' preference between the two.

Table 21. Group statistics of issue 5 (Using modern technology).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	3.28	.726	.096
Traditional CAPTCHA	57	2.44	.846	.112

Table 22 displays using modern technology (Issue 5). The hypotheses are defined as follows.

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

The P-value is 0.005, this is considered to be minor comparing to the significance level of 0.05. Therefore, the null hypothesis can be rejected at 95% of the confidence interval. From this reason, it can be concluded that using modern technology of the EYE CAPTCHA is different from that of the existing CAPTCHA. This reason might be because the EYE CAPTCHA is new and nobody applies the eye movement to the CAPTCHA.

Table 22. Independent samples test of issue 5 (Using modern technology).

	t-test for Equality of Means						
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
						Lower	Upper
Score	5.705	112	.000	.842	.148	.559	1.135

The statistics of meaningful interface is displayed in Table 23. It consists of a frequency of participant, mean value, standard deviation, and standard deviation error mean. From the result in Table 23, the mean value of the EYE CAPTCHA is higher than that of traditional CAPTCHA. The standard deviation of the EYE CAPTCHA is lower than

the traditional CAPTCHA. In other words, the user feels satisfied with the meaningful interface of the EYE CAPTCHA.

Table 23. Group statistics of issue 6 (Meaningful interface).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.79	.700	.093
Traditional CAPTCHA	57	2.70	.778	.103

Table 24 shows meaningful interface (issue 6) comparison. The hypotheses can be defined as follows.

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

The P-value of 0.528 is higher than the significance level of 0.05, therefore, the null hypothesis can be accepted at 95% of the confidence interval of the difference. In other words, there is no significant difference. From the above analysis, it can be concluded that meaningful interface of the EYE CAPTCHA is not different from the meaningful interface of traditional CAPTCHA. In other words, the traditional CAPTCHA can be replaced by the EYE CAPTCHA. In addition, based on the statistical analysis, it seems like users start to feel a little better about the EYE CAPTCHA than the traditional one.

Table 24. Independent samples test of issue 6 (Meaningful interface).

	t-test for Equality of Means						
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
						Lower	Upper
Score	.632	112	.528	.088	.139	-.187	.363

The statistics of usage overview displays in Table 25. It consists of a frequency of participant, mean value, standard deviation, and standard deviation error mean. The mean value and standard deviation of the EYE CAPTCHA are higher than those of

traditional CAPTCHA. In other words, the user feels satisfied with the usage overview of the EYE CAPTCHA.

Table 25. Group statistics of issue 7 (Usage Overview).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.67	.787	.104
Traditional CAPTCHA	57	2.63	.698	.092

Table 26 shows the usage overview of the questionnaire in terms of comparison between the two CAPTCHA hypotheses, where the hypotheses are defined as follows:

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

The acquired P-value of 0. 802 is higher than the defined significance level of 0.05. Therefore, it is reasonable for the null hypothesis to be accepted at 95% of the confidence interval between the hypotheses. In other words, there is no significant difference. From analysis, it can be concluded that the usage overview process of the EYE CAPTCHA is not different from the usage overview of traditional CAPTCHA. This means that traditional CAPTCHA can be replaced by the EYE CAPTCHA. In addition, it can be perceived that users feel marginally better about the EYE CAPTCHA than the traditional CAPTCHAs.

Table 26. Independent samples test of issue 7 (Usage Overview).

	t-test for Equality of Means						
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
						Lower	Upper
Score	.252	112	.802	.035	.139	-.241	.311

Table 27 shows the different statistics of the appropriate user's interaction acquired in the proposed system. The evaluation consists of a frequency of participant, mean value, standard deviation, and standard deviation error mean. The experiments

resulted in a higher mean score of the appropriate user's interaction for the EYE CAPTCHA in comparison to that of traditional CAPTCHA. While in contrast, the standard deviation of the EYE CAPTCHA is to some degree less than traditional CAPTCHA. The meaning of the result is that there is not much of a difference in the users' preference between the two.

Table 27. Group statistics of issue 8 (Appropriate user's interaction).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.70	.654	.087
Traditional CAPTCHA	57	2.61	.796	.105

Table 28 shows appropriate user's interaction (issue 8) comparison. The hypotheses can be defined as follows.

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

The P-value of 0.522 is higher than the significance level of 0.05, therefore, the null hypothesis can be accepted at 95% of the confidence interval of the difference. In other words, there is no significant difference. From the above analysis, it can be concluded that the appropriate user's interaction of the EYE CAPTCHA is not different from appropriate user's interaction of traditional CAPTCHA. In other words, the traditional CAPTCHA can be replaced by the EYE CAPTCHA. In addition, based on the statistical analysis, it seems like users start to feel a little better about the EYE CAPTCHA than the traditional one.

Table 28. Independent samples test of issue 8 (Appropriate user's interaction).

	t-test for Equality of Means						
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
						Lower	Upper
Score	.643	112	.522	.088	.136	-.183	.358

Table 29 shows the statistics of the conformance with task's objective. The table consists of the frequency of participants, mean value, standard deviation, and standard deviation error mean. The mean score of the EYE CAPTCHA is higher than that of the traditional CAPTCHA. The standard deviation of the EYE CAPTCHA is less than the traditional CAPTCHA, which means that the EYE CAPTCHA is suitable for the users as well and that the users feels comfortable using it.

Table 29. Group statistics of issue 9 (Conformance with task's objective).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.98	.719	.095
Traditional CAPTCHA	57	2.70	.778	.103

Table 30 displays conformance with task's objective (Issue 9). The hypotheses are defined as follows.

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

The P-value is 0.005, this is considered to be minor comparing to the significance level of 0.05. Therefore, the null hypothesis can be rejected at 95% of the confidence interval. From this reason, it can be concluded that the appearance of the EYE CAPTCHA is different from that of the existing CAPTCHA. This reason might be because the users feels more safety to use the EYE CAPTCHA to access a system.

Table 30. Independent samples test of issue 9 (Conformance with task's objective).

	t-test for Equality of Means						
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
						Lower	Upper
Score	1.999	112	.048	.281	.140	.003	.559

Table 31 shows the different statistics of the applicable in real life acquired in the proposed system. The evaluation consists of a frequency of participant, mean

value, standard deviation, and standard deviation error mean. The experiments resulted in a same level of mean score of the applicable in real life for the EYE CAPTCHA in comparison to that of traditional CAPTCHA. While in contrast, the standard deviation of the EYE CAPTCHA is to some degree higher than traditional CAPTCHA. The meaning of the result is that there is not much of a difference in the users' preference between the two.

Table 31. Group statistics of issue 10 (Applicable in real life).

Group Statistics				
GROUP	N	Mean	Std. Deviation	Std. Error Mean
EYE CAPTCHA	57	2.72	.881	.117
Traditional CAPTCHA	57	2.72	.774	.102

Table 32 shows the applicable in real life (issue 10) of the questionnaire in terms of comparison between the two CAPTCHA hypotheses, where the hypotheses are defined as follows:

H_0: EYE CAPTCHA and the traditional CAPTCHA are the same.

H_1: EYE CAPTCHA and the traditional CAPTCHA are different.

The acquired P-value of 1.000 is higher than the defined significance level of 0.05. Therefore, it is reasonable for the null hypothesis to be accepted at 95% of the confidence interval between the hypotheses. In other words, there is no significant difference. From analysis, it can be concluded that the applicable in real life of the EYE CAPTCHA is not different from overall process of traditional CAPTCHA. This means that traditional CAPTCHA can be replaced by the EYE CAPTCHA.

Table 32. Independent samples test of issue 10 (Applicable in real life).

	t-test for Equality of Means						
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
						Lower	Upper
Score	.000	112	1.000	.000	.155	-.308	.308

5.4. Limitations

The proposed CAPTCHA cannot distinguish between glimpse and gaze. Moreover, the movement for answering is restricted. It needs to go right away to the destination only at the middle of screen.

5.5. Feedback

Comments and suggestions from users who have tried the EYE CAPTCHA system are described as follows.

1. The EYE CAPTCHA takes a long time for verification. It is not comfortable.
2. There are still limitations for the blind.
3. A user still feels that the traditional system is faster to be completed than the proposed system.
4. The response of the eye movement is quite slow.
5. The EYE CAPTCHA is not precise.
6. The EYE CAPTCHA cause eyesore since it requires a lot of eye movement and gazing.
7. More precision between the point of screen and the point of gaze is required.
8. Slower process for the next rounds of testing is needed.
9. The respond of movement should be faster.
10. User Interface should be improved.
11. User would like to choose the picture which same meaning as instruction rather than solving the equations.

Chapter 6. Conclusion and Future Research

6.1. Summary of research

Generally, CAPTCHA is a tool for separating between humans and computer programs (BOT). It can protect a website or a system from automated programs or harmful users. It is the first choice for protecting an automatic registration form on the website. Since the existing CAPTCHAs have some limitations, the new CAPTCHA called the EYE CAPTCHA is developed under eye movement technology.

The objective in designing the EYE CAPTCHA is associated in terms of safety, easy usage, and interchangeability with the old CAPTCHA. From the analysis of results, the EYE CAPTCHA can be replaced to the original CAPTCHA.

6.2. Future work

For future research, some issues of the EYE CAPTCHA can be improved such as responsiveness of eye movement, user friendliness, and accuracies of matching gaze and position on the screen and distinguishing between human and bot. Moreover, eye movement can also be combined with other biometric technology to improve the CAPTCHA.

REFERENCES

[1]   L. V. Ahn, M. Blum, and J. Langford, "Telling humans and computers apart automatically," Communications of the ACM, vol. 47, no. 2, pp. 56 – 60, 2004.

[2]   H. Saevanee and P. Bhatarakosol, "User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device," in Proceedings of the International Conference on Computer and Electrical Engineering (ICCEE), 2008, Phuket, Thailand, pp. 82 - 86.

[3]   Pixabay.com, 'Free image on pixabay – Fingerprint, Touch, Crime, Criminal', 2017. [Online]. Available: https://pixabay.com/en/fingerprint-touch-crime-criminal-150159/. [Access: 2-Nov-2017].

[4]   Stocksnap.io, 'Free image of eye, green, face – StockSnap.io', 2017. [Online]. Available: https://stocksnap.io/photo/OUH9F7WAG7/. [Access: 2-Nov-2017].

[5]   Pixabay.com, 'Free image on pixabay – Audio, Aural, Ear, Hearing, Music', 2017. [Online]. Available: https://pixabay.com/en/audio-aural-ear-hearing-music-2028515/. [Access: 2-Nov-2017].

[6]   P. Satam, D. Kelly, and S. Hariri, "Anomaly behavior analysis of website vulnerability and security," in Proceedings of the 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 2016, pp. 1 - 7.

[7]   Schorlab.berkeley.edu, 'Vergence eye movements', 2017. [Online]. Available: http://schorlab.berkeley.edu/vilis/vergence.htm. [Access: 2-Nov-2017].

[8]   Acunetix, 'Acunetix Web Application Vulnerability Report 2016 - Acunetix', 2017. [Online]. Available: https://www.acunetix.com/acunetix-web-application-vulnerability-report-2016/. [Access: 2-Nov-2017].

[9]   P. K. Kulluru, T. Shaikh, S. Bidwai, A. Mannarwar, and K. Shamlani, "Survey of different types of CAPTCHA," in Proceedings of International Conference on

Advances in Computing, Communication and Networking (ICACCA), Dehradun, India, 2016, pp. 19 – 21.

[10]   R. ur Rahman, D. S. Tomar, and S. Das, "Dynamic image based CAPTCHA," in Proceedings of the International conference on Communication System and Network (CSNT), Rajkot, India, 2012, pp. 90 – 94.

[11]   E. Bursztein, M. Martin, and J. Mitchell, "Text-based CAPTCHA strengths and weaknesses," in Proceedings of the 18th ACM conference on Computer and communications security (CCS), Chicago, Illinois, USA, 2011, pp. 125 – 138.

[12]   X. Ling-Zi and Z. Yi-Chun, "A case study of text-based CAPTCHA attacks," in Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Sanya, China, 2012, pp. 121 – 124.

[13]   D. Lorenzi, J. Vaidya, E. Uzun, S. Sural, and V. Atluri, "Attacking image besed CAPTCHAs using image recognition recognition techniques," in Proceeding of the 8th International Conference on Information Systems Security (ICISS), Guwahati, India, 2012, pp. 327-342.

[14]   B. B. Zhu, J. Yan, Q. Li, C. Yang, J. Liu, N. Xu, M. Yi, and K. Cai, "Attacks and design of image recognition CAPTCHAs," in Proceedings of the 17th ACM Conference on Computter and Communications Security (EuroS&P), Chicago, Illinois, USA, 2010, pp. 187–200.

[15]   H. Gao, H. Liu, D. Yao, X. Liu, and U. Aickelin, "An audio CAPTCHA to distinguish humans from computers," in Processding of Third International Symposium on Electronic Commerce and Security (ISECS), Guangzhou, China, 2010, pp. 265 – 269.

[16]   N. M. Al-Fannah, "Using aesthetic judgements to distinguish between humans and computers," Cornell University, ArXiv:1704.02972, 2017.

[17]   F. A. B. H. Ali and F. Bt. Karim, "Development of CAPTCHA system based on puzzle," in Proceedings of the International Conference on Computer, Communications, and Control Technology (I4CT), Langkawi, Malaysia, 2014, pp. 426 – 428.

[18]   B. M. Powel, A. Kumar, J. Thapar, G. Goswami, M. Vatsa, R. Singh, and A. Noore, "A multibiometrics-base CAPTCHA for Improved online security," in Proceedings of the 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, USA, 2016, pp. 1 – 8.

[19]   M. Okada and S. Matsuyama, "New CAPTCHA for smartphones and tablet PC," in Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 2012, pp. 34 – 35.

[20]   K. Anjitha and I. K. Rijin, "Captcha as graphical password-enhanced with video-based captcha for secure services," in Proceedings of the International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Davangere, India, 2015, pp. 213 – 217.

[21]   A. Babich, "Biometric authenticaltion. Types of biometric identifiers," Haaga-Helia University of Applied Sciences, 2012.

[22]   G. Al-Hudhud, E. Alarfag, S. Alkahtani, A. Alaskar, B. Almashari, and H. Almashari, "Web-based multimodal biometric authentication application," in Proceedings of the 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), Riyadh, Saudi Arabia, 2015, pp. 1 – 8.

[23]   A. Bayat and M. Pomplun, "The influence of text difficulty level and topic on eye-movement behavior and pupil size during reading," in Proceedings of the 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS), Tehran, Iran, 2016, pp. 1 – 5.

[19]   P. Kasprowski and K. Harezlak, "The second eye movement verification and identification competition," in Proceedings of the International Joint Conference on Biometrics (IJCB), Clearwater, FL, USA, 2014, pp 1-6.

[24]   D. T. Nguyen, K. Y. Shin, W. O. Lee, Y. G. Kim, K. Wan, H. G. Hong, K. R. Park, C. Oh, H. Lee, and Y. Jeong, "Gaze detectin based on head pose estimation in smart TV," in Proceeding of the International Conference on ICT Convergence (ICTC), Jeju, South Korea, 2013, pp. 283 – 288.

[25] B. L. Nguyen, "Eye gaze tracking," in Proceedings of the International Conference on Computing and Communication Technologies (IEE-RIVF), Da Nang, Vietnam, 2009, pp.1 – 4.

[26] C. Meng and X. Zhao, "Webcam-Based Eye Movement Analysis Using CNN," IEEE Access, vol. 5, pp. 19581 – 19587, 2017.

[27] M. Tschirsich. Js-objectdetect: Computer vision in your browser - javascript real-time object detection. https://github.com/mtschirs/js-objectdetect, 2012. [Online; accessed 2015-08-15].

[28] E. Lundgren, T. Rocha, Z. Rocha, P. Carvalho, and M. Bello. tracking.js: A modern approach for Computer Vision on the web. http://trackingjs.com/, 2014. [Online; accessed 2015- 05-15].

[29] A. Mathias. clmtrackr: Javascript library for precise tracking of facial features via Constrained Lo- cal Models. https://github.com/auduno/clmtrackr, 2014. [Online; accessed 2015-07-08].

[30] A. Papoutsaki, P. Sangkloy, J. Laskey, N. Daskalova, J. Huang, and J. Hays, "WebGazer: scalable webcam eye tracking using user Interactions," in Proceedings of the Twenty-Fifth International Joint Conference on Artificial Interlligence (IJCAI), New York, USA, 2016, pp. 3839 – 3845.

[31] A. E. Hoerl and R. W. Kennard, "Ridge Regression: Biased Estimation for Nonorthogonal Problems," American Statistical Association and American Society for Quality, vol. 12, no. 1, pp. 55 – 67, 1970.

[32] C. Ghaoui, "Human Computer Interaction," The Encyclopedia of Human-Computeer interaction, vol. 2, pp. 21 – 62, 20

APPENDIX

The EYE CAPTCHA satisfaction survey

GENERAL INFOMATION

GENDER ◯ MALE ◯ FEMALE

AGE ◯ less than 20 years ◯ 20 – 25 years

◯ 26 – 30 years

◯ 31 – 35 years ◯ more than 35 years

EDUCATION ◯ Below Bachelor's Degree ◯ Bachelor's Degree

◯ Master's Degree ◯ PhD

General understanding about CAPTCHA

1. Knowledge of the CAPTCHA of the user ◯ YES ◯ NO

2. Experience using CAPTCHA (Please specify number of years) …………years

* Note: 1 is minimum and 4 is maximum

Table 1: Assessment table of understanding about security

List of issues	Level			
	1	2	3	4
1. User understands web security and computer security				
2. User understands identification and verification				

Table 2: Quality assessment table of the EYE CAPTCHA

List of issues	Level			
	1	2	3	4
1. The accuracy of the system				
2. The appropriate time for the work process				
3. User feels more safety in data and accessing to the system when the EYE CAPTCHA is used instead of traditional CAPTCHA				

Figure 23. Page 1 of the EYE CAPTCHA satisfaction survey.

Table 3: Performance and satisfaction assessment table comparing between EYE CAPTCHA and traditional CAPTCHA.

List of Issues	Level EYE CAPTCHA				Level traditional CAPTCHA			
	1	2	3	4	1	2	3	4
Work process (Step-by-step)								
1. Minimal and simple procedure								
2. User-friendly process								
3. Appropriate technique								
Appearance								
1. Optimal UX & UI								
2. Using modern technology								
3. Meaningful interface								
Gratification								
1. Usage overview								
2. Appropriate user's interaction								
3. Conformance with task's objective								
4. Applicable in real life								

SUGGESTION:……

……….

……….

Figure 24. Page 2 of the EYE CAPTCHA satisfaction survey.

VITA

Name: Apichai Siripitakchai

Affiliation: Advanced Virtual and Intelligent Computing (AVIC) Center, Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Thailand

Work: I have been working for Ewit Company Limited in Research and Development Division as a Supervisor. The responsibility is monitoring the standardization and implement in order to create the software and service.

Education: I have received a Bachelor's Degree in Computer Science from Silpakorn University in 2006.