AUTHENTICATION INDICATORS USING BIO-DETECTION FUNCTION WITH TEXT-BASED CAPTCHA

Miss Nilobon Nanglae

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 2013

ตัวชี้วัดบอกการระบุตัวตนโดยใช้ฟังก์ชันการตรวจหาเชิงชีวภาพร่วมกับ CAPTCHA เชิงข้อความ

นางสาวนิโลบล นางแล

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2556

Thesis Title	AUTHENTICATION INDICATORS USING BIO-DETECTION FUNCTION WITH TEXT-BASED CAPTCHA
By	Miss Nilobon Nanglae
Field of Study	Computer Science and Information Technology
Thesis Advisor	Assistant Professor Pattarasinee Bhattarakosol, 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

(Professor Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

....Chairman

(Assistant Professor Nagul Cooharojananone, Ph.D.)

....Thesis Advisor

(Assistant Professor Pattarasinee Bhattarakosol, Ph.D.)

....External Examiner

(Kanokwan Atchariyachanvanich, Ph.D.)

นิโลบล นางแล : ตัวชี้วัดบอกการระบุตัวตนโดยใช้ฟังก์ชันการตรวจหาเชิงชีวภาพร่วมกับ CAPTCHA เชิงข้อความ. (AUTHENTICATION INDICATORS USING BIO-DETECTION FUNCTION WITH TEXT-BASED CAPTCHA) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. ดร. ภัทรสินี ภัทรโกศล, 77 หน้า.

ในปัจจุบันCAPTCHA ซึ่งย่อมาจาก Completely Automated Public Turing Computer and Humans Apart เป็นเครื่องมือสาคัญที่ช่วยป้องกันการรุกรานของโปรแกรมอัตโนมัติ ในการเข้าสู่ระบบอินเตอร์เน็ต CAPTCHA ถูกสร้างขึ้นมาเพื่อว่าเป็นมนุษย์หรือโปรแกรมอัตโนมัติ นักวิจัยหลากลายท่านได้คิดค้นCAPTCHA ในรูปแบบต่างๆ เช่น CAPTCHAเชิงข้อความ CAPTCHAเชิงรูปภาพ CAPTCHAเชิงเสียง ดังนั้น CAPTCHAรูปแบบที่ได้กล่าวมาสามารถจำแนกได้เฉพาะโปรแกรมอัตโนมัติแต่ไม่สามารถจำแนกผู้รุกรานที่เป็นมนุษย์ได้ ซึ่งการวิจัยในครั้งนี้ได้เสนอCAPTCHAรูปแบบใหม่ที่รวมกับชีวภาพของมนุษย์เพื่อป้องกันปัญหาดังกล่าว ในการศึกษาครั้งนี้จะพิสูจน์ความเป็นเอกลักษณ์ของแต่ละตัวบุคคล โดยวัดจาก อายุ เพศ การรับรู้ของสี อาชีพ และการพิมพ์ถูกผิด ผลที่ได้สามารถนำมาพัฒนาCAPTCHAรูปแบบโดยใช้ฟังชันก์การตรวจหาเชิงชีวภาพสำหรับการระบุตัวตนของมนุษย์

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์

สาขาวิชา วิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ

ปีการศึกษา 2556

ลายมือชื่อนิสิต ....

ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก ....

5572631723 : MAJOR COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
KEYWORDS: CAPTCHAS / TEXT-BASED CAPTCHA / BIO-DETECTION FUNCTION

NILOBON NANGLAE: AUTHENTICATION INDICATORS USING BIO-DETECTION FUNCTION WITH TEXT-BASED CAPTCHA. ADVISOR: ASST. PROF. PH. PATTARASINEE BHATTARAKOSOL, Ph.D., 77 pp.

Currently, CAPTCHA (Completely Automated Public Turing test to tell Computer and Human Apart) is used in the daily life before the Internet accessing for preventing automatic programs illegally access web services. CAPTCHA was introduced to identify human or computer program automatically. Many researchers proposed several of CAPTCHA techniques to protect bots, as Text-based CAPTCHA, Audio-based CAPTCHA, Image-based CAPTCHA or Puzzle-based CAPTCHA. Those techniques are able to solve only automatically program but cannot protect system from the 3rd party. This study suggests the combination of biometric of human and CAPTCHA system to protect serious problem. The concept is to prove the uniqueness of human by measuring age, gender, color detection, occupation, timestamp, and correctness of typing. The result leads to the creation of a new way CAPTCHA system that embedded with a suitable bio-detection function to be authenticated as a human user.

Department:	Mathematics and Computer Science	Student's Signature	....
		Advisor's Signature	....
Field of Study:	Computer Science and Information Technology		
Academic Year:	2013		

ACKNOWLEDGEMENTS

I would like to express my thankfulness to the people who have helped me most throughout my thesis. I am sincerely grateful to my professor Assist Prof. Dr. Pattarasinee Bhattarakosol for helpful guidance and encouragement; therefore, I am particularly obliged for the valuable assistance given contributions through constructive suggestions and recommendations. In addition, I would like to thank the thesis committees, Assistant Professor Dr. Nagul Cooharojananon and Dr. Kanokwan Atchariyachanvanich for sparing the their precious time for thesis examinations and for their invaluable comments. Moreover, I would like to thank Dr.Pakawan Paksee for suggestion in data analysis and Weka program.

Finally, my graduation would not have been achieved without best wish from my parents for helped me in everything and always giving me greatest love and willpower until completion of my study. I also would like to thank all my friends for helpful and encouragement.

CONTENTS

Page

LIST OF TABLE

Page

LIST OF FIGURE

CHAPTER 1
INTRODUCTION

This chapter states the interested problem in Section 1.1, and then the problem formulation and motivation are described in Section 1.2. In Section 1.3 and Section 1.4, the objective, and the scope and constraint of the thesis will be discussed respectively, followed by benefit and expected outcomes in Section 1.4. Then definitions of technical term in Section 1.6 and the structure of thesis in Section 1.7

1.1 Background and Importance

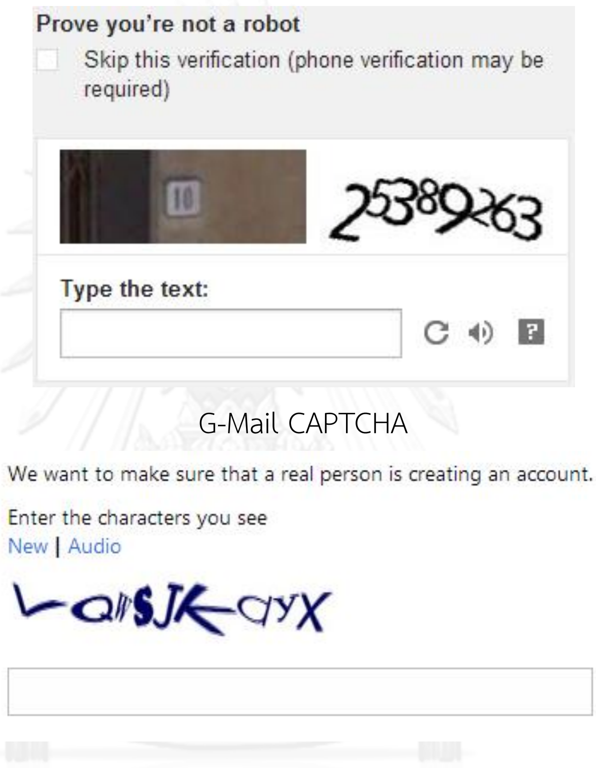
Currently, security is a major role whenever a website is accessed because the important data or individual information is published. There are various types of attackers over the Internet, such as bots, spam or malicious automated programs. These attackers become a serious problem for all Internet users.

It is deniable that the Internet has a major role in human living in every day's life. Most data are stored and retrieved from time to time over the network across organizations, even across the world. Since there are various types of illegal impostors, thus, the protection system is implemented using varieties techniques. The most basic one is the use of password authentication system. This authentication system can be said as the oldest life-long serving for human's use. Unfortunately, it is not sufficient to satisfy the security level of organizations.

The fundamental problem of using password is that the login password was hacked by malicious software and the password will be uncovered. As a result, this intrude program can access the data without permission by emulating human login process. As a consequence, CAPTCHA, Completely Automated Public Turing test to tell Computer and Humans Apart, was implemented in the year 2000 by Luis von Ahn et. al. [1] to protect this unwanted situation. This technique identifies whether human or software program has accessed to the service over the Internet. CAPTCHA is an automatic test design for asking the user to complete a simple test, which most of human can pass, in the other way computer program cannot pass [2] [3]. CAPTCHA is a mechanism that uses to distinguish human from current computer program by asking user to solve a question [4]. A good of CAPTCHAR should be [5] [6] [7] [8]:

generated automatically CAPTCHA quick and easy to solve mostly accept human and reject bots

So, CAPTCHA technology is widely used for online polls should be ensure human vote or not, proving human before getting email service account, against email from worms and spam and prevent search engine from a private web site [9] [10].



Prove you're not a robot

□ Skip this verification (phone verification may be required)

Type the text:

G-Mail CAPTCHA

We want to make sure that a real person is creating an account.

Enter the characters you see

New | Audio

Hotmail CAPTCHA

Figure 1.1 Example of CAPTCHA

Figure 1.1 shows the example of CAPTCHA that is implemented by popular web based services, such as Gmail account or Hotmail account, etc. Those websites use CAPTCHA as a standard security technology to make sure that the real human is creating free email service account and malicious computer programs are protected to aggregate spam mail.

CAPTCHAs are most likely Turing Tests in distinguish human from computer [9]. Turing proposed Turing Test that provides the method to distinguish between human and machine by asking a series of questions between two players and distinguish them, which one is human and another is computer program since the machine cannot have a thought [11]. Thus, Turing test is an important mechanism to determine between human and software programs.

According to the objective of CAPTCHA that is applied to distinguish between human and bots, generated test or problem must be solved by most of human but not for bots. Thus, many researchers design test to prevent these bots under the condition that difficult to automatic program to solve but easy for human. The tests mostly consist of either alphabets, numbers, images, or sound with noise.

There are exiting CAPTCHA mechanisms that can separate into three main categories as Text-based CAPTCHA, Image-based CAPTCHA and Sound-based CAPCHA [12] [13].

First, Text-based CAPTCHA is the most widely used in webpage. It is the easiest and simplest to be implemented. The Text-based CAPTCHA asks user to type randomly words or letters that consist of noise, distortion, blurring letters and rotates letters with variety angles, on screen [14]. Make difficult Text-based CAPTCHA for prevent bots, also difficult for human as well [8]. Moreover, OCR or Optical Character Recognition technique was implemented to break Text-based CAPTCHA that translates image into a form which bots can read [15].

Second, Image-based CAPTCHA was introduced after problems of Text-based CAPTCHA were uncovered. This technique requires users to enter the right labeled of the presented image, or adjust rotated images to the right position [16] [17]. To break Image-based CAPTCHA was using Image Processing technique by bots or time consuming. So, human can solve that quickly, if any spend more time or cannot solve [15]. In additional, the Image-based is not suitable for persons who have difficulty in understanding or interpreting the image to answer questions. This is the serious problem of the Image-based CAPTCHA.

The last CAPTCHA technique is the Sound-based CAPTCHA, which was design based on the audiometry perception of human users. The Sound-based CAPTCHA technique is developed for a specific group who has eye vision problem. This technique can classify into two categories. The first ones, human heard the sound clip that pronounces letters or numbers, including the background noise. The second ones, the sound was offer with an image that relate to the sound [18] [19] [20]. In addition, this technique can eliminate a problem that is gap between blindness and normal people [21].

Besides these three main categories of CAPTCHA technique, there are researchers introduce other types of CAPTCHA techniques for protecting automatic programs.

Figure 1.2 represents an example of Text-based CAPTCHA, and Figure 1.3, 1.4 represent examples of Image-based CAPTCHA. Those are using to ensure that only human access on websites, not spam or automatic programs.

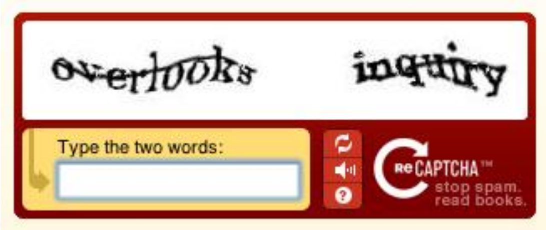


Figure 1.2 Example of Text-based CAPTCHA [22]

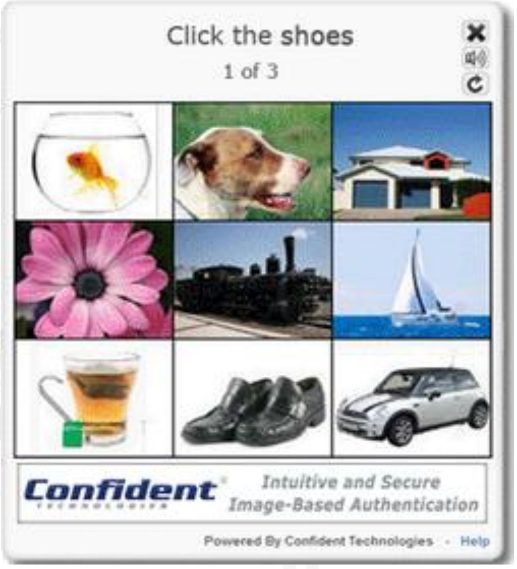

Click the shoes
1 of 3
Confident
TECHNOLOGIES
Intuitive and Secure
Image-Based Authentication
Powered By Confident Technologies · Help

Figure 1.3 Example of Image-based CATPCHA [23]

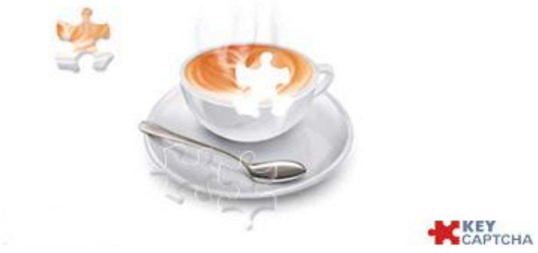


Figure 1.4 Example of Image-based CAPTCHA [24]

CAPTCHA was proposed for distinguish human from automatic programs and there are different types of CAPTCHAs to serve security needs for different personality uses. Nevertheless, this CAPTCHA cannot distinguish illegal users and the authenticated one. The intruder human so called "the 3rd party human CAPTCHA attacks" to break CAPTCHAs testing [25]. So, this type of attacks of CAPTCHAs is difficult to prevent [26]. As the fact that, each person has unique behavior and specific recognition capability. Thus, these abilities should be applied to identify a personality of a person as same as other biometric data, such as fingerprint, and face recognition those are applied in the authentication process. Consequently, from some studies, the correctness of typing CAPTCHA is based on personal impacts, such as personal characteristics, gender and education. So, these factors have impacts to the correctness of typing [27]. Furthermore, the combination of numbers, background colors, and consuming times for solving CAPTCHA has influenced to the correctness of typing CAPTCHA [28]. In addition, human's profile and the set of representation numbers in each position, have affects to entering to the required system [29]. In addition, an effect from aging of users' visibility towards alphabets and background contrast color in web site was proven [30].

According to the users' characteristics based on CAPTCHA mentioned above, this research has an aim to expand the use of Text-based CAPTCHA into the authentication system using combinations of human's capabilities and CAPTCHA abilities to identify an intruder from the authenticated one. The bio-detection functionalities metrics are values that measure for typing correctness, ageing, gender, vision perception, timestamp and position represented. Moreover, the experiment was implemented using only 4-digit random number. However, there are various factors related to the personal identification. Thus, the results from this experiment indicate some significant factors that can be applied to the authentication system.

1.2 Problem Formulation and Motivation

Presently, CAPTCHA is used in the daily life before access the Internet for preventing automatic programs illegally access web services. Many researchers proposed several CAPTCHA techniques to protect bots, such as Text-based CAPTCHA, Sound-based CAPTCHA, and Image-based CAPTCHA. Those techniques are able to solve only automatically program but cannot protect from the 3rd party human. Therefore, generating the Text-based CAPTCHA combining with human' biometrics should be able to protect this serious problem. The concept of this research is to prove the uniqueness of human by measuring age, gender, color detection, occupation, timestamp and correctness of typing.

1.3 Objective

The main objective of this research is to determine the bio-detection function metrics based on Text-based CAPTCHA that affects to the human's vision. In addition, the difference biometrics of bio-detection function of each person using Text-based CAPTCHA will be identified so that an authentication method using Text-based CAPTCHA can be achieved.

1.4 Scope of thesis and constraint

In this experiment mainly focus only Text-based CAPTCHA and scope of thesis and constrained are described as follows:

1. Experimental system to implement Text-based CAPCHA using adobe CS5.5 under PHP web environment.
2. The Text-based CAPTCHA was generated randomly from the experiment.
3. The samples are collected from Thai nationality, which is set to be 100 participants.
4. Collected demographic information are as follow:
    - Age of participant between 10 to 60 years old and above,
    - Gender: male and female,
    - Occupation environments as student, merchant, officer, government and unemployed,
    - eye problem of each participants as color blindness and eye-sight,
    - time of typing in each position's character of CAPTCHA within two months,
    - All participants are Thai citizen only.

1.5 Benefit or Expected Outcomes

This research proposes an authentication method using Text-based CAPTCHA. The fundamental result is to identify factors that support bots protection. The additional outcome is the ability to classify the authentication person from 3rd party attacks.

1.6 Definition

CAPTCHA: CAPTCHA (Completely Automated Public Turing test to tell Computer and Humans Apart) is a program that differentiates human from computer by generating and presenting a test that only humans can solve and no computers or automated software can.

BDF: BDF (Bio-Detection Function) is to identify the authorized from an unauthorized person using combinations of CAPTCHA attributes and human's capabilities.

KPI: (Key Point Index) is the input time that a person uses when typing a CAPTCHA.

1.7 Structure of the Thesis

The rest of this thesis is organized as follows. Chapter 2 provides the fundamental knowledge and the literature review for the thesis. Then, Chapter 3 describes the research methodology followed by showing the experimental and results in Chapter 4. Finally, discussion and conclusions are drawn in Chapter 5.

CHAPTER 2
FUNDAMENTAL KNOWLEDGE AND LITERATURE

This chapter provides fundamental knowledge and reviews of some related works. First, Section 2.1, the general knowledge in CAPTCHA is presented. Then, the needs of computer security and authentication methods are elaborated in Section 2.2. Finally, some literature reviews are drawn in Section 2.3.

2.1 Computer Security and Authentication System

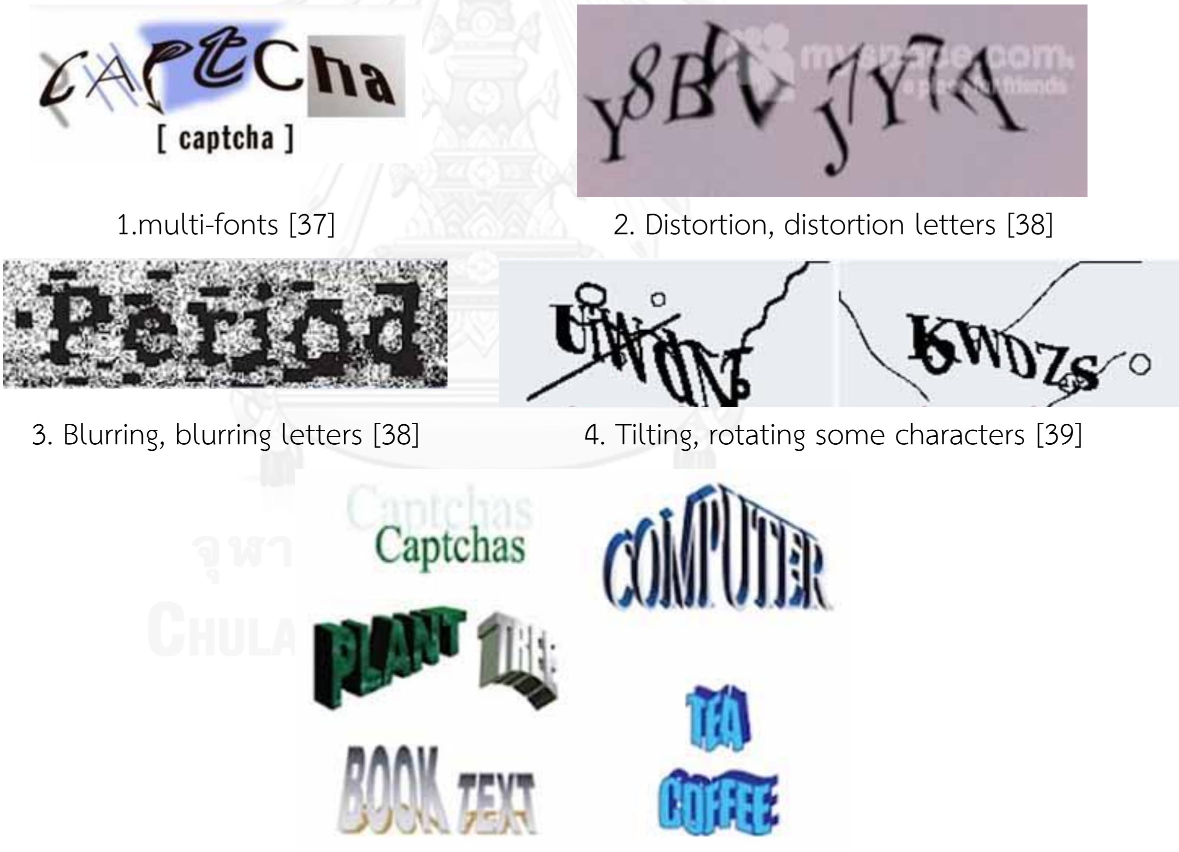
Computer security is the process to prevent and detect unauthorized access system. In order to control the accessibility to the system, Password security as user id and password is the most popular method. While logging to the system, the user must inform the system for who they are; and then, the system proves that the accessing user is the right person. So, to prove that the user has been authorized, there are two steps to be applied. Firstly, the identification process to inform the system for who they are; secondly, the authentication process to prove that the user is an authorized person. The three ways to classify a person as follow.

1. Asking for what the person knows, such as IDs and password, personal identification number.
2. Looking for what the person owns, such as ATM card, smart card.
3. Identify for whom the person is, such as biometric behavior, characteristic

Biometrics is automated methods to recognize person based on a personal physical and behavior characteristic that make uniqueness of each person [31] [32]. The advantage of biometric characteristic is that it is hardly change in a short time, so it is applied for the authentication process [33]; for examples figure print, face recognition, hand geometry technology, iris technology, retina geometry technology, DNA, speaker recognition technique and signature verification technique [34] [35]. These techniques need a learning process from samples. Therefore, it is not perfect due to poor quality of biometric samples and the complexity of biometric authentication equipment [34]. Nonetheless, a technique as keystroke dynamics, one of the biometric authentication mechanisms, refers to the process of analyzing the keyboard typing based on the habitual rhythm patterns. As a result, this technique does not require any special devices. Thus, it causes the low deployment cost [36] [37].

2.2 CAPTCHA

According to the external intrusion of malicious programs through the login page of any private systems, CAPTCHA has been implemented for a simple security system cooperated with the password using. However, users over the computer world have different abilities. Some are blind, some have a vision problem, and some have the reading problem. Thus, there are three types of CAPTCHA are implement recently: the Text-based CAPTCHA, the Image-based CAPTCHA, and the Sound-based CAPTCHA.



1.multi-fonts [37]

2. Distortion, distortion letters [38]

3. Blurring, blurring letters [38]

4. Tilting, rotating some characters [39]

5. many size of fonts [38]

Figure 2.1 Examples of CAPTCHA Styles.

Simple CAPTCHA or Text-based CAPTCHA uses series of letters that include warping or adding distracting background [16]. The varieties of their designs are classified by [14] as follow. These designs are shown in Figure 2.1.

1. Multi-fonts, using many types of font
2. Fonts size, many size of fonts in CAPTCHA
3. Blurring, blurring letters
4. Distortion, distortion letters
5. Tilting, rotating some characters in CAPTCHA in many angles.

Even though there are three different types of CAPTCHA, the Text-based CAPTCHA has been chosen to implement in many popular web sites, such as Google, Yahoo, or Facebook, etc. One similarity among these Text-based is that some CAPTCHA is unable to be read or decoded, too complicated or annoying to solve by human. Therefore, users might ignore this CAPTCHA and wait for a new line.

Different from the Text-based, the Image-based CAPTCHA are implemented in some interesting webs. This type of CAPTCHA is presented using image of some objects, with a question to be answered; users must answer questions based on the presented image. However, the problem of answering questions based on the image might be depended on the intelligence and experiences of users. Therefore, this Image-based CAPTCHA might not be suitable for uneducated or low-educated users. Jison Zhang and Xingfen Wang recommended a good CAPTCHA should base on multi characters in the CAPTCHA and connecting or overlap in each CAPTCHA and various color with text and background color [40].

RiZwan ur Rahman and friends created dynamic Image-based CAPTCHA, based on tree layer: the image access layer, the image process layer, and the presentation layer. This CAPTCHA proposes a system that is easy for human to answer, but in the same time difficult for malicious cracking [41]. Hussan Hajjdiab and Ashraf Khalil [8] said about image matching problem in Image-based mechanism as camera calibration, 3D object reconstruction, obstacle detection, motion estimation, and object tracking. So, they propose a new image matching CAPTCHA that does not require any database of images.

Though the first two types of CAPTCHA are implemented and used by various systems, these two techniques are not suitable for people who are blind or vision problems. Thus, the Sound-based CAPTCHA was proposed and implemented for this specific group. The implementation of the Sound-based CAPTCHA is the integration between vocal and noise. As a consequence, the difficulty in distinguishing the real value of CAPTCHA occurs; users must type the correct value of the presented CAPTCHA based on the sound they have heard.

Based on three types of CAPTCHA presented above, there is no CAPTCHA style that is suitable for every person or every capability. In addition, some implemented CAPTCHA can obstruct legal users from accessing their own system. Moreover, some simple CAPTCHA styles are able to be solved by a specific program [42].

CAPTCHA doesn't be used in only website but they can be used in any smart phones. Isaonas Polakis and friends studied Phone CAPTCHA that protects automatic program callers. They build functional that calls center to prevent landlines devices from DIAL attacks. As a consequence, all callers must answer CAPTCHA puzzle by phone. Whenever the caller answers wrong, the call will be terminated [43]. Moreover, CAPTCHA is also implemented in to e-banking. Shujun Li and friends tried to uncover patterns of CAPTCHA techniques that can break all malicious programs with the success rate close to 100 percent [44].

According to the study of Jeff Yan and Ahmad Salah El Ahmad, it is stated that some spammers hire cheap labor to answer the CAPTCHA in order to break the system [45].

2.3 Related Works

2.3.1 Related Works and Improvements of Computer Security

Computer security is about the process to prevent and detect unauthorized access of a computer, including applications and data. Detection system helps determining illegal users when system was intruded. The protection mechanisms have been widely implemented in recent year since problems of stealing information or machine annihilation arise. Butler W. Lampson [46] said that the number of computer users is increasing rapidly. So, screening valid users from unauthorized users becomes a serious issue. Thus, the computer security turned to be an essential mechanism for accessing computers of users [47].

After realizing that the computer must be protected, various protection methods are proposed, both physical and logical. As a result, the computer system and all stored data have been protected. Details of these protections are described below.

Physical Protection

The physical protection for a prohibited access related to various methods, such as hiring guards, the implementation of a closed circuit television (CCTV), the implementation of an accessing room policy, etc. This protection can protect only when the system is only approached by human. Unfortunately, these physical intrusions are not a serious problem of all computer users unlike the logical invasion.

Logical Protection

Besides the physical protection, the logical roles are also vital. The logical issue uses the software protection method because the invasion occurs from malicious software. The efficiency of unwanted software was developed as same as the development of the logical protection techniques. A research in computer security mentioned that these intrusions exist according to the monetary gains [48]. Thus, many more anti-virus, data security software, firewalls are established to prevent this unlawful situation [49].

Originally, the prevention of each computer was relied on the use of password for logical protection and key card for physical protection. For example, the smart card was proposed by [50] for the financial protection of electronic transaction of banks. This prevention must be performed when users want to access the system or stored data. This process performed by a system that is called as the authentication system. The improvement of this system has various alternatives, such as the use of passwords, the use of biometrics, and the use of a smartcard.

2.3.2 Related Works and Improvements of the Authentication System

Presently, people use computer for every action of lives. Therefore, the computer technology has been developed for various purposes with various supporting software. As mentioned previously, the identification of users must be performed before entering the secured system. Unluckily, attackers can emulate themselves as the authentication ones, even trace for the entering passwords of users using illegal screen emulation. As a result, all protected objects are unsecured.

Under the use of password authentication, Faid Alolul and Wassim El-Hajj [51] proposed the one time password (OTP) on the mobile phone instead of a keycard. This method is easy to use, secure and cheap since it is based on SMS-based approach as ATM machines. Though, the password-based authentication system is very popular but it is not strong because hackers can steal or guess the value of the password using many techniques. In addition, the weakness of using passwords depends on the complication of the password's value; easy to remember, easy to be hacked. Thus, to create complications of a password, several alphabets, many space size and variety of lengths are applied [52]. In addition, Swapnaja, et al. concluded that using passwords in an authentication system leads to various kinds of risks. For examples, passwords are copied by hackers, users lost or forgot their passwords because it is too long to remember. According to these reasons, some biometrics are applied for enhancing the security of the authentication system [53].

A biometrics authentication is a technology for personal identification based on physical appearances, including personal behaviors. Nevertheless, the physical appearances or personal characteristics are dynamic. Thus, currently, only some bioinformation are applied to be biometrics, such as fingerprint, voiceprint, facial, retina, iris scanning, or signatures. Even so, this biometrics may have some defects since these values can be changed by external factors. For example, the change of users' faces is based on users' ages. Therefore, there is no permanent value of each biometric according to the change of time.

As a results from many researches, the fingerprint technique is quite reliable since there is a proof that the fingerprint patterns of each person is unique. For example, fingerprint patterns are unique and persistent intrinsic characteristic of each person that can distinguish one person from another person. Vladimir I. Ivanov and John S. Baras combined fingerprint scanner and biometrics authentication for high securing in authentication systems, which call "bipartite authentication" that verifies both, identity user and the identity's fingerprint scanner [54].

Iris technique, iris is the color ring of textured tissue that surrounds the pupil of the eye. Both iris of a person have difference iris patterns, left and right is different. Each iris is a unique structure. ZHOU Hu-Lin and XIE Mei studied iris technique authentication using image matching method of iris from database one by one [55].

Palm vein technique is based on the fact that the vein pattern in person body is distinctive for all individuals. The vein under skin absorbs infrared rays by the vein authentication device, a dark pattern image as the blood vessel pattern of the palm appeared. After that this appearance will be matching with the previous palm in the stage [56]. The hand vein authentication uses for the door handling without entering password as well as preventing of stolen or forged the keys [57].

2.3.3 Related Works and Improvements of CAPTCHA

Since the Internet becomes a part of human's life, computer security also becomes an important issue for every Internet user. This is because all data over the Internet must be protected from hackers. Therefore, CAPTCHA, a common technique that insists users to enter a set of text before entering to the system was proposed by Luis Von Ahn [58]. The objective of this system asks users to answer the question that is easy to answer, while computer or automatic spam cannot [59]. Fortunately, this technique seems to work well for years and is widely used in every system protection as a basic protection mechanism after users enter their passwords.

According to its efficiency, CAPTCHA has been a challenge opportunity for any hackers to break this protection mechanism. Therefore, various designs of CAPTCHA styles have been developed. As mention earlier, CAPTCHA technology can be classified in three categories: Text-based CAPTCHA, Image-based CAPTCHA, and Sound-based CAPTCHA.

A Text-based CAPTCHA, the most popular use CAPTCHA, is created by a computer program by random selecting a sequence of letters, rotate them, adding distorting, and adding noise. Since this CAPTCHA style looks simple and easy, the authentication system with embedded CAPTCHA as the additional process is continuously increasing [60] [61] [62]. The weakness of Text-based CAPTCHA is bots or automatics program can read the distorted a sequence of letters, or remove noise and distorting using optical character recognition (OCR) [63] [13]. Although there is a significant problem of CAPTCHA according to OCR usage from bots, many popular websites still implement Text-based CAPTCHA, such as Hotmail, Google, Yahoo or Facebook [13]. Nevertheless, in some generated CAPTCHA styles, their presentations are not friendly to human and persuade users to abandon the system without intension.

Similar to other protection mechanisms, while CAPTCHA protection technique is developed, CAPTCHA-attack algorithms are concurrently developed. Cui et.al [64] had summarized that there are four CAPTCHA attack methods. The first two methods are statistical-based method named as anti-noise and anti-jamming capability. The third method is the combination of the first two that becomes an interesting research topic as same as the forth method which is the application in the area of neural network.

As a result of attacker's effort, CAPTCHA system intends to create reading difficulty in CAPTCHA text by systematically adding noise and distortion. A new form of CAPTCHA is a complexity image of a distorted letters for users to type [65] [66] [63] [67]. CAPTCHAs are invented in variety forms. Shape CAPTCHA [64] is obtained from transforming various shapes using Gestalt and Geon principles while spatial CAPTCHA is a text image that is derived from three-dimensional model.

An interesting CAPTCHA is the speech CAPTCHA that is implemented for blind people. This is a kind of Sound-based CAPTCHA. This technique is proposed in the year 2007 in order to bind the gap between blind people and normal people [21]. The objective of the Sound-based CAPTCHA is developed to serve blind persons so they can equally use a secure computer. The system will pronounce the letter and the blind person must press the right keyboard according to the hearing vocal.

After a long use of CAPTCHA, the 3rd party attack problem begins to arise. Therefore, Chirstopher F. Tuner [26] introduced an iCAPTCHA system to protect this serious problem caused by human intrusion. The concept of this technique is the correctness of the input sequence comparing with the CAPTCHA image appeared on the screen.

In additional, according for a good characteristic of CAPTCHA that mention earlier, there are some similarity rules for CAPTCHA design to increase success rate of protect bots and friendly for human. Table 2.1 demonstrates the existing CAPTCHA techniques that rely on the characteristics of a good CAPTCHA.

Table 2.1 The exit CAPTCHA techniques that rely on a good CAPTCHA

CAPTCHA technique	A good CAPTCHA should be			Protect the 3^{rd} party human attack
	Generated automatically	Quick and easy to solve	Mostly accept human and reject bots	
Image based CAPTCHA using jigsaw puzzle [13]	√	√	√	–
What’s up CAPTCHA based on image orientation [16]	√	√	√	–
Advanced collage CAPTCHA by M. Shirali-Shahreza [17]	√	√	√	–
Image matching CAPTCHAs [8]	√	√	√	–
Image CAPTCHA based on human understanding [15]	√	√	√	–
Audio CAPTCHA by Haichang Gao [18]	√	√	√	–
Sequenced Tagged CAPTCHA [19]	√	√	√	–
CAPTCHA for blind people by M. Shirali-Shahreza [21]	√	–	√	–
GeoCAPTCHA by Te-En Wei [25]	√	√	√	√
iCAPTCHA by Huy D. Truong [26]	√	√	√	√

CHAPTER 3
RESEARCH METHODOLOGY

This chapter describes the CAPTCHA with propose method by combining simple Text-based CAPTCHA with human' capabilities, color detection, timestamp, and position of appearance. Moreover, the results that show how to propose method is superior to other CAPTCHA techniques are demonstrated. Section 3.1 describes the demographic information, following with Section 3.2 for CAPTCHA Generating and Data Grouping.

In order to prove the BDF of each participant is different when entering CAPTCHA, there are two main processes that must be established. The first process is to define all interesting attributes related to the participant's information profile or demographic information. This process will collect fundamental information of participant that might have impacts to the collected data in the second phase, such as age, gender and occupation. The second process is to define the sample behavior with respect to the presented CAPTCHA. This process collects all information that can be measured from the participant's reacting in the CAPTCHA system. Presently, many researchers proposed a variety of CAPTCHA, such as Text-based CAPTCHA, Image-based CAPTCHA and more. Nevertheless, Text-based CAPTCHA is the most widely used for identify human computer users, and secondly it is easy to be generated and easy to be designed. Thus, this research will experiment on Text-based CAPTCHA only.

When data collected from participants in various places according to the personal corporation, a web page questionnaire and CAPTCHA simulation system are implemented. The web implementation uses PHP and runs on a server that can be accessed via the Internet. The architecture of the experimental system is presented in Figure 3.1.

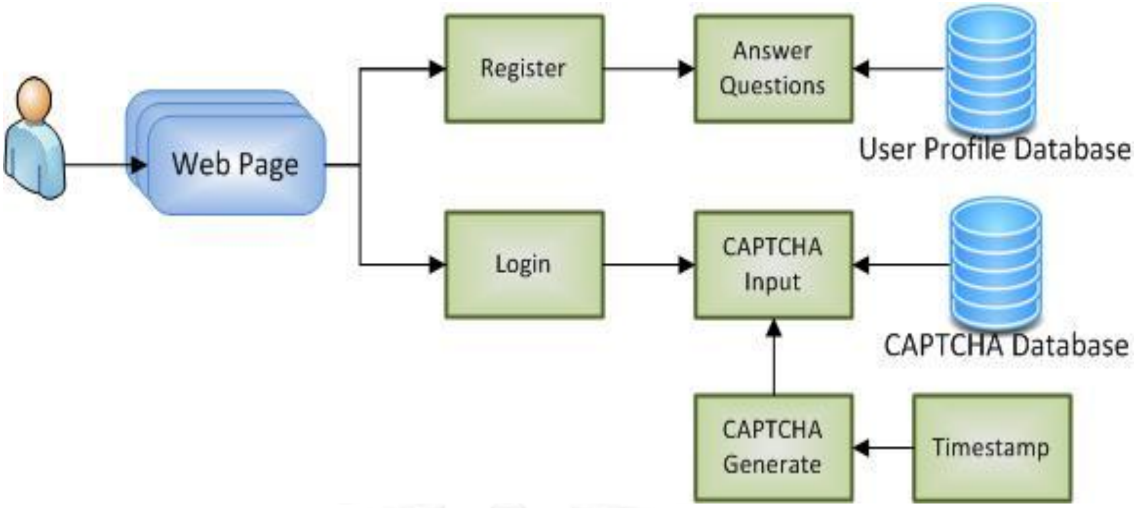


Figure 3.1 The Data Collecting System Architecture

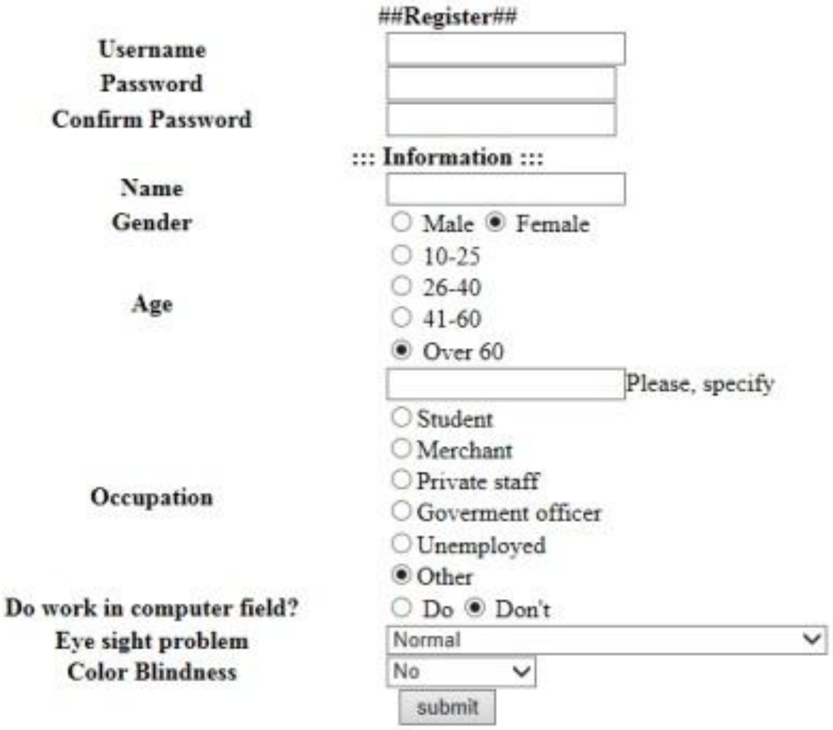
As previously mentioned, there are two phases that samples must enter. The first phase is to collect the demographic of each sample and the second phase is to collect data related to the typing of simulated CAPTCHA.

According to Figure 3.1, the first phase consists of two processes: the register, and the answer questionnaires. This phase is the demographic data collection phase, will be described in the following paragraph. The second phase consists of four processes: the Login, the CAPTCHA Generating, the timestamp, and the CAPTCHA input processes. However, within these four processes, there are 2 tasks to be performed by the data collecting system: the CAPTCHA Generating, and the timestamp. Details of this second phase will be elaborated in the following content.

After the data collection system is fully implemented, an announcement asking for collaboration was distributed over many organizations using personal contacts. These personal contacts were obtained from government staff and family members. All collecting information from both phases and collection processes are displayed in the following section.

3.1 Demographic Information

In the first phase of data collection starts with each participant registers to the system before passing to the second phase of the experiment. The entering information is an important factor that is used in the analytical phase of participants' characteristics. These characteristics are applied to support the conclusion that each person has unique characteristics. Figure 3.2 shows the input screen of the first phase.



##Register##

Username	
Password	
Confirm Password	

::: Information :::

Name	
Gender	○ Male ● Female
Age	○ 10-25 ○ 26-40 ○ 41-60 ● Over 60
	Please, specify
Occupation	○ Student ○ Merchant ○ Private staff ○ Goverment officer ○ Unemployed ● Other
Do work in computer field?	○ Do ● Don't
Eye sight problem	Normal
Color Blindness	No

Figure 3.2 Register form of Demographics' participants

According to Figure 3.2, the participant must setup his/her username and password. Then, a personal demographic must be selected from the on screen displayed choices. Thus, data that each participant has to provide are listed as follow.

- Username
- Password
- Age group: This information can be used to classify the overall vision of users related to the presented CAPTCHA under different age groups. Ages are separated into 4 groups: young, middle-age, adult, and elderly as belong.
    - 10-25
    - 26-40

  - 41-60
  - Over 60

- Gender: This information can be used to differentiate the typing ability based on different genders.
- Occupation: This information can be used to differentiate the familiarization of computer usage and keyboard.
  - Student
  - Merchant
  - Private Staff
  - Government Officer
  - Unemployed
  - Other
- Work in Computer field: This information identifies participants who work in the computer field. This information can used to differentiate the professional of typing on keyboard.
  - Do
  - Don't
- Eye Sight problem: This information indicates the visual difficulties of each participant towards the displayed CAPTCHA. The most common eye sight error may include:
  - Myopia
  - Hyperopia
  - Astigmatism
  - Myopia and Hyperopia
  - Hyperopia and Astigmatism
  - Myopia, Hyperopia and Astigmatism
- Color Blindness is the color vision problem. This information can be used to differentiate kinds of color problem that affects to the ability of typing difficulty.

- Non
- Red-Green
- Blue-Yellow
- Not sure

After completing this phase, all information of participants will be recorded into the User Profile Databases (UPDB). Moreover, each participant will have individual login and password for continuing to the second phase as follows.

In additional, Jain et al. introduced soft biometric which is a characteristic that provide information about user as gender, eye color, ethnicity, height, weight [68]. Some researchers studied faces recognize using factor as age, race, gender, skin and glasses, those can affect the biometric system [69]. So, that information can infer to biometric identifiers [70].

Consequently, this research uses soft biometrics to identity participant as age, gender and eyes problem from the participants during an online questionnaires process, to compile with biometrics information during each participant typing CAPTCHA system. On the other hand, time when a participant type each CAPTCHA's character call interleave time. The interleave time has impact when participant type difference characters in difference person. This information can also provide into biometrics identifiers.

3.2 CAPTCHA Generating and Data Grouping

With the defined login and password in the first phase, all participants will enter to the second phase to solve the CAPTCHA testing. All characters of CAPTCHAs are randomly selected by CAPTCHA generating module embedded within the web application. In addition, RGB colors will be applied to the CAPTCHA generating module to simulate the real basic CAPTCHA using over the Internet. These RGB values will be used to distinguish the personal's perception.

This experiment does not only generate CAPTCHA and measure the correctness of sample's typing, but also collect two significant time values: an individual typing time of each position of typing CAPTCHA, and total typing time. Collecting details are described below.

3.2.1 CAPTCHA Text

The Text-based CAPTCHA is implemented as a 4-digits number, values between 0-9. This 4-digit number was present, using the BrowalliaUPC font with a font size of 96.0 point and regular format text, without italic, underline nor rotates. Each participant was asked to solve 30 CAPTCHA questions of each round. In addition, there is no duplicated number and all positions of CAPTCHA are randomly. Figure 3.3 below show the sample of the Text-based CAPTCHA generated by the CAPTCHA system.

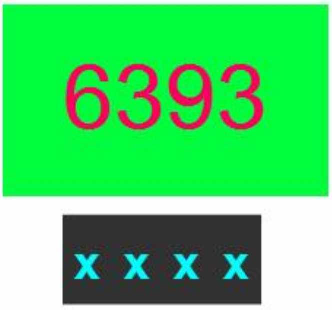


Figure 3.3 Sample of CAPTCHA that generated by the CAPTCHA system

3.2.2 Color Categories

One of the significant factors that is considered in this research is color, both foreground and background. A variety color models are displayed for human perception, such as RBG color model, CMY color model, CMTK color model and more. This study uses a simple RGB (Red-Green-Blue) color model that usually represents and displays images on the computer terminal; three primary colors are red, green, and blue. Although there are various combinations of the color's tone obtained from RGB, as shown in Table 3.1, this research had grouped all different tones of colors to be 9 different groups, as shown in Table 3.2.

Table 3.1 Group of code color

Color	Code Color
RED	#FF002F, #FF001F, #FF000F, #FF0000, #FF0F00, #FF1F00, #FF2F00, #FF3F00, #FF4F00, #FF5F00, #FF6F00, #FF7F00, #FF8F00, #FF9F00, #FFAF00, #FFBF00
YELLOW	#FFCF00, #FFDF00, #FFEF00, #FFFF00, #EFFF00, #DFFF00, #CFFF00, #BFFF00
GREEN	#AFFF00,#9FFF00,#8FFF00,#7FFF00,#6FFF00,#5FFF00,#4FFF00,#3FFF00,#2FFF00, #1FFF00,#0FFF00,#00FF00,#00FF0F,#00FF1F,#00FF2F,#00FF3F
CYAN	#00FF4F,#00FF5F,#00FF6F,#00FF7F,#00FF8F,#00FF9F,#00FFAF,#00FFBF,#00FFCF, #00FFDF,#00FFEF,#00FFFF,#00EFFF,#00DFFF,#00CFFF,#00BFFF
BLUE	#00AFFF,#009FFF,#008FFF,#007FFF,#006FFF,#005FFF,#004FFF,#003FFF,#002FFF, #001FFF,#000FFF,#0000FF,#0F00FF,#1F00FF,#2F00FF,#3F00FF
MAGENTA	#4F00FF,#5F00FF,#6F00FF,#7F00FF,#8F00FF,#005FFF,#AF00FF,#BF00FF,#CF00FF, #DF00FF,#EF00FF,#FF00FF,#FF00EF,#FF00DF,#FF00CF,#FF00BF,#FF00AF,#FF009F, #FF008F,#FF007F,#FF006F,#FF005F,#FF004F,#FF003F
GRAY	#BFBFBF,#9F9F9F,#7F7F7F,#5F5F5F,#3F3F3F,#1F1F1F
BLACK	#000000
WHITE	#FFFFFF

Table 3.2 The 9 main colors

Main Color Code	Name of Color	Color
1	Red	🟥
2	Yellow	🟨
3	Green	🟩
4	Cyan	🟦
5	Blue	🟦
6	Magenta	🟪
7	White	⬜
8	Gray	◼
9	Black	⬛

3.2.3 Counting Time

When each participant typed CAPTCHAs, two phases of the system are performed as described below.

- This system measures the individual typing time based on each position of typing CAPTCHA. Figure 3.4 represents individual counting of each CAPTCHA. Locating at the sprit time for button situation - 3.166, 0.988, 0.894 and 0.578 were the time when the user pressed the 1st, 2nd, 3rd and 4th buttons, respectively. The time commenced when CAPTCHA was presented until the first position completely pressed. This process repeats until the last character was completely pressed.
- The total typing time of CAPTCHA is the total time when every position of typing CAPTCHA is completed. Referring to Figure 3.4, the total time of typing this CAPTCHA is 5.626 seconds. This process starts counting when the CAPTCHA was presented until all positions are filled.

In addition, the total time of counting and the individual time of counting will be stored in the database as same as the result of typing. When participants enter the correct CAPTCHA, the system will record a “true” response. If not, the system will record a “false” response.

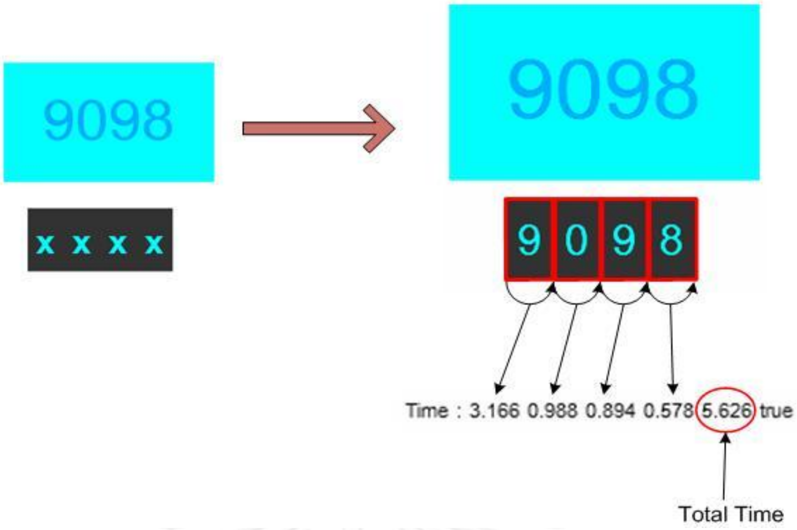


Figure 3.4 Time of typing CAPTCHA

Referring to Figure 3.4, all participants are able to type the CAPTCHA within 24 hours a day. Thus, the collecting time is divided into six periods, as follow.

- Period 1 is 06.01 am-08.00 am,
- Period 2 is 08.01 am-12.00 pm,
- Period 3 is 12.01 pm-1.00 pm,
- Period 4 is 01.01 pm-4.00 pm,
- Period 5 is 04.01 pm.-8.00 pm.,
- Period 6 is 08.01 pm-06.00 am.

These time period will be recorded into the database as same as other biometrics.

Figure 3.5 represents step of taking CAPTCHA system. Most participants must complete the CAPTCHA system according to three phases. The first phase consists of the registering and answering questionnaires via the web page, this phase collects the demographic information of each participant. The data that was collected such as username password, age, gender, occupation and eye problem. Then, the second phase is logging in to the simulated CAPTCHA testing. Before starting the CAPTCHA testing, each participant must enter the username and the password. The last phase is the CAPTCHA testing, each participant must enter number according to 30 CAPTCHAs questions for each round which combining with color on foreground and background.

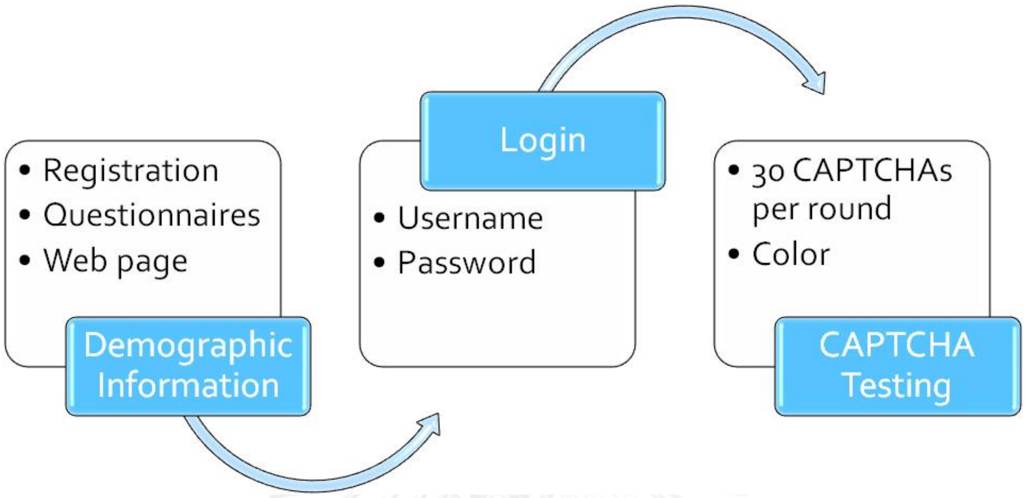


Figure 3.5 Research Methodology

CHAPTER 4
EXPERIMENTAL AND RESULTS

This chapter describes the analysis and the results. It has been divided into sections where in Section 4.1 describes the fundamental results of demographic data and Section 4.2 elaborates the analysis for factor finding. The last section is Section 4.3 that draws the results from Weka.

4.1 Fundamental Results of Demographic Data

First, look into the demographic data of participants selected for the experiment. Total of 100 participants were collected between June-July 2011 and details of the collected data mention as follow.

- Each participant must answer 30 different CAPTCHAs randomly per day, over the course of 15 days.
- 100 participants with 56 females and 44 males, ages between 10 and 60 years old.
- 50% of the participants have normal eye sight while 20% are short eye sight problem, and the rest have astigmatism and hyperopia.
- None of participant had color blindness.

4.2 Analysis for Factor finding

This section is analysis part for determining significant factors that relate to correctness of CAPTCHA typing. There are three main factors to be analyzed. The first, factor focuses in the demographic information of participants that has an impact for the typing while the second factor focuses in the characteristic of the presented CAPTCHA. And the last ones, the factor focuses in colors of CAPTCHAs that affect to vision perception of each participant.

4.2.1 Demographic information effect

Based on the information that collected from all participants, all 45,000 records for analysis significant of participants. Then, using Chi-square Cross Tabulation method identifies the uniqueness of each characteristic's participant. This statistical analysis uses the significant level of 0.05(α) because the impacts from these factors have mild damages. The results are summarized as below.

4.2.1.1 Age with period of time

Since the data were collected during 6 periods of a course per day, the analytical result shows that during the period of time at 8.01 pm.to 06.00 am., the participants who have age between 10 to 25 years old have chances to type mistake higher than other period of time and also this age of participants have chances to type correct more than other period of time, with p-value = 0.00 < 0.05(α). According Table A1 and Table A2, the results of the relation between periods of time is drawn and the final status and the result of Chi-Square Test are presented respectively.

According to the analysis results mentioned above, it is clear that times play a major role towards the correctness of sample typing. A reason might be that the samples might require more time, in order to adjust their eyes to a computer monitor. However, there is no significant difference of mistyping in other periods of the day. In addition, people age between of 10 and 25 years which are the studying ages, the correctness of them is lower than older people according to their responsibility.

4.2.1.2 Gender with period of time

The results represent that between period of time 08.01 pm to 06.11 am, participants who are male, who have chance to type CAPTCHA correctly with 32.18% more than female participants. Nevertheless, the ratio of incorrect typing in the same period of time is also higher than other periods of time, with p-value = 0.00 < 0.05 (α). According to the Table A3 and Table A4, the correctness by period of time related with genders was presented following with the result of Chi-Square Tests.

According to the analysis results mentioned above, male have mistype more than female, and also type correctly more that female as well as.

4.2.1.3 Occupation with period of time

Occupation refer to background of the participants is another important impact to typing correctness of the Text-based CAPTCHA. It determines there are skills to use the equipment or the infrastructures in IT environment. Therefore, participants of different occupation as student, private staff, government officer, merchant and other occupation have been different working in environment.

From the result of Chi-square cross tabulation analysis represents, the private staff who is working in computer field tended to make mistype more than other occupations during that time and also make correct type more than other occupation with the same period of time, with p-value = 0.303 > 0.05(α). According to Table A5 and Table A6, the correctness by period of time with occupation and the result of Chi-Square Tests are presented respectively.

4.2.1.4. Occupation in computer field with period of time

From the result of Chi-square cross tabulation analysis with p-value = 0.045 < 0.05(α), the student who is working in the computer field tended to type correctly more than other occupations during period time of 08.01 pm to 06.00, according to the Table A7 and Table A8.

4.2.2 Effects from Characters and Its Position

This experiment runs only 4-digit numeric CAPTCHA using 9 color groups. Therefore, this research will analyze only positions of the presented numbers, running from 0-9. The analysis method is Least Square Different (LSD) using 0.05 significant level (α). The analysis uses the time capturing from participants' typing on each character.

In the first position, the analytical results show that number 1 and 7 cause significant different in the average typing time more than other numbers, p-value< 0.05(α). Additionally, numbers 0, 1, 3, 5, 6, 7, 8, and 9 cause significant differences in the average typing times in the second position, with p-value < 0.05(α); number 2, and 4 have no significant differences in the average typing times, as shown in Table A9.

Similar to the second position, and the third position, the numbers 0, 1, 3, 5, 7, and 8 cause significant differences of the average typing times, with p-value <

0.05(α), while numbers 2, 4, and 9 have no significance differences of the average typing times, as shown in Table A10 and Table A11 respectively.

For the last position, position 4, with p-value > 0.05(α), the numbers that have no significance difference in the average typing time is every number, except numbers 3, 4, and 5, as shown in Table A12 respectively.

Based on the above results, it is interesting that each character in each position can cause time differences while types. Therefore, in order to identify a person from another, the numbers that cause time differences in each individual position should be used rather than numbers that have no significant.

4.2.3 Effect from Color and Its Position

The test for correctness of the typing CAPTCHA against the real CAPTCHA value can be concluded that the right input from users is depended on every factor which is character color, background, position of the text, typing time, numeric value of CAPTCHA. This means a volunteer will put the right CAPTCHA if the text color and background color are the right color for the particular person, including that the number of the CAPTCHA presented in each position is easy to be read and he/she has time to type. When the data was analyzed with Chi-Square, the results have shown that every factor has significant level equal to zero < α = 0.05.

In addition, this research has found that there is a relationship between background color and text color towards the correctness of the CAPTCHA with significant level equal to zero < α = 0.05. For example, the Green background and Green character, most of volunteers answer in right, among 8.69%, the sample character color and background of the shade of green color that participants have mistype as represent in Table 4.1. Thus, the proper color matching supports the BDF of users as the Table A13.

Table 4.1 The shade of green color

No.	Color	No.	Color
1	🟩	14	🟩
2	🟩	15	🟩
3	🟩	16	🟩
4	🟩	17	🟩
5	🟩	18	🟩
6	🟩	19	🟩
7	🟩	20	🟩
8	🟩	21	🟩
9	🟩	22	🟩
10	🟩	23	🟩
11	🟩	24	🟩
12	🟩	25	🟩
13	🟩		

When considering the capability of eye detection without consideration of color's effect, the experiment has shown that position of numbers in CAPTCHA is related to the correctness of typing with significant level equal to zero < α = 0.05.

According to Table A14 represents the number "2" in the fourth position has 3.49% incorrect typing. The number "9" in the second position has 2.58% of correct typing. So, setting up some numbers in some specific positions might be able to classify a person according to the vision they have seen and typed.

Furthermore follow as the Table A15, the similarity is shape of numbers is another influencer to the correct or incorrect typing. For example, 0.061% of people type the number "1" as the number "4", 0.48% of people type the number "0" as the number "1", as well as type the number "3" as the number "2" and type the number "2" as the number "3". Furthermore, 0.049% of people see the number "9" as the number "8". Nevertheless, there is an observation that the mistyping can occur in two situations. The first situation is the similarity of the character, such as number "1" might look like number "4". The second situation is the position of the figure pressed on the keyboard, such as the case of mistyping between number “2” and number “3”.

Although there is an assumption that the time period might have effect in the ability of BDF, the result of this study has shown that the correctness of typing CAPTCHA still remains although the typing time occurs in various interval with significant level 0.00 < α = 0.05. Therefore, the BDF of human will not change according to the time interval.

4.2.4 Effect from Color and Its Position

The experiment measures the individual typing and total typing time of CAPTCHAs. So this paper will analyze the time spending on the CAPTCHA system with other factors as CAPTCHA keys, the period of times, the final status, and the eyes problem. The analysis method is the General linear models (GLM) using 0.05 significant level (α).

4.2.4.1 Time spent with key CAPTCHA

According to Table A17, the analytical results of the effects of time spent and typing CAPTCHAs are derived. The results found that the time spent to type CAPTCHA on the third position is significant different from typing times with *F* is equal to 23.563 and Sig. p = 0.000 < 0.05 (α). On the other hand, the typing time of other positions has no significant different, with Sig. p > 0.05(α). Therefore, time influences the typing CAPTCHA in the third position.

A reason to explain the results above might be that participants may only remember the first and the second of CAPTCHA numbers on their first sight, typing them first. After that they read the last two position of CAPTCHA in the third and the fourth positions; then type them. So, participants require more time to read CAPTCHA on the third and the fourth position, those causes to the third position of the CAPTCHA has significance.

4.2.4.2 Time spent with period of time

Since the data were collected during 6 periods of a course per day. Therefore, this research will analyze the relation between a period of time and the time spent in all the position of CAPTCHA. The analytical results from Table A18 shows that, at the third position, *F* is equal to 134.687 and Sig. p= 0.000< 0.05 (α) while there is no significant difference based on other positions. Consequently, the period time has influence on the typing CAPTCHA in the third position.

4.2.4.3 Time spent with eyes problem Time spent with final status

While participants filled in an online questionnaire, they must answer the question about their eyesight problem as myopia, hyperopia and astigmatism. Thus, this section analyzed the relation between time spent to type CAPTCHAs and eyesight problem. The analytical result presented in Table A19 indicates that at the third position, F is equal to 414.562 and Sig. p= 0.000< 0.05 (α). This result means in the third position, eyesight problem has influence of typing in the third position. Furthermore, the analytical results from Table A20 shows that F is equal to 3.935 and Sig. 0.001, so that Sig. is less than significant level (0.05). According to Table A20, eyes sight problem has influence on typing CAPTCHA in the fourth position.

4.2.4.4 Time spent with Correctness

When participants enter the CAPTCHAs, the system will check the correctness of typing CAPTCHAs. If the typed values match with the presented CAPTCHAs, the system will record a “true”, else the system will record a “false”. Thus, this research consider that time spent has affect to the correctness of type. The analysis results from Table 21 and Table 22 show that *F* is equal to 106.049 and Sig. p= 0.000< 0.05 (α), and F is equal to 6.076 and Sig. is 0.014< 0.05 (α) respectively. So, these results clarify that the time spent has influence on the correctness of typing CAPTCHA in the third and the fourth position.

4.3 Analysis of Weka

Classification by decision tree are used to predict membership of cases or objects in the class

In this research, the classification tree was performed using Weka 3.6.10. The analysis based on J48graft decision tree classifier. The data set that use 17 attributes as UserID, Position1, Position2, Position3, Position4, CAPTCHA1, CAPTCHA2, CAPTCHA3, CAPTCHA4, Key number1, Key number2, Key number3, Key number4, Period of time, Character Color, background color and Final status. This analysis uses pair of 100 User's ID to 50 pairs. The pairs of user's ID are as shows on Table A16.

From the result, there are 45,318 instants with total instants 34,549 of correct and total instants 10,769 incorrect. Table 4.2 shows the accuracy of the classification of J48graft as the columns Correctly, Incorrectly, True Positive Rate (TP Rate), False Positive (FT Rate) and Precision. The average accuracy shows in Table 4.2, the correctly classified instances at 64.43%, using 7 attributes as User ID, Character Color, Background Color, Correctness, CAPTCHA Key, CAPTCHA was presented and Position.

Table 4.2 Average of accuracy of 7 attributes

No.	correctly	incorrectly	TP Rate	Ft Rate	Precision
Total	64.43%	21.57%	0.76%	0.26%	0.63%

The results from Table 4.3 shows the average accuracy of 8 attributes as User ID, Character Color, Background Color, Correctness, CAPTCHA Key, CAPTCHA was presented, Position and period of time, so the correctly classified instances at 64.43%,

Table 4.3 Average of accuracy of 8 attributes

No.	correctly	incorrectly	TP Rate	Ft Rate	Precision
Total	81.83%	4.17%	0.76%	0.04%	0.82%

Another result from different attributes as User ID, Character Color, Background Color, Correctness, CAPTCHA Key, CAPTCHA was presented, Position, period of time, age, gender and occupation, The average accuracy shows in Table 4.4, the correctly classified instances at 75.85%.

Table 4.4 Average of accuracy of 11 attributes

No.	correctly	incorrectly	TP Rate	Ft Rate	Precision
Total	75.85%	10.14%	0.76%	0.11%	0.76%

On the other hand, if reducing the attributes into 9 attributes as User ID, Character Color, Background Color, Correctness, CAPTCHA Key, CAPTCHA presented, Position, age, gender and occupation, the average accuracy showed in Table 4.5 is 78.89%. So, the correctness does not rely on the number of attributes to be used.

Table 4.5 Average of accuracy of 10 attributes

No.	correctly	incorrectly	TP Rate	Ft Rate	Precision
Total	78.89%	7.11%	0.02%	0.02%	0.97%

Furthermore, when use only biometrics from each participant as soft-biometrics and interleave time, the average accuracy shows the correctly classified instances at 78.89%, in Table 4.6. So, the using biometrics can classify users from intruders, the average accuracy is highest from other attributes.

Table 4.6 Average of accuracy of only biometrics

No.	correctly	incorrectly	TP Rate	Ft Rate	Precision
Total	98.33%	1.67%	0.017%	0.017%	0.97%

CHAPTER 5
DISCUSSION AND CONCLUSION

In this chapter, the discussion will be discussed in Section 5.1, limitation of the experiment is stated in Section 5.2, and finally conclusion will be drawn in Section 5.3.

5.1 Discussion

Since security issues are very important role for users and systems over the Internet, many techniques have been proposed and implemented, including CAPTCHA. Currently, there are three mains CAPTCHA mechanisms but the most implemented CAPCHA is Text-based CAPTCHA.

Although CAPTCHA are applied to various systems in order to proof human's access from bots, not many CAPTCHA systems have applied biometrics of human to protect bots. Thus, the BDF of each person is able to classify when using CAPTCHA on the authentication systems.

In additional, some research defined, human spend time when use CAPTCHA mechanism is faster than bots, and the timeout mechanism was used to protect bots [26]. This technique is one part of human's behavior to against bots. This technique can apply Image-based CAPTCHA. So, the timeout value is the key point of this method. Therefore, there is a possibility that bots simulate perform tasks slow than human user. So, the timeout mechanism cannot be applied in such case.

This paper proposes factors that are able to consider and deploy when implement Text-based CAPTCHA, such as age, gender, occupations, access times, foreground and background color, and eye vision perception.

Since characteristics of each demographic data that provide different typing results, so applying the users' profile with the CAPTCHA mechanism should be able to increase the correctness of human's authentication process. Moreover, the characters on each position and different time typing are significant that must to consider. As well as, the important significantly is eye detection based on shapes and position of display of numbers.

These differences character of human can distinguish not only between human and bots, but also distinguish between right users and intruders, the 3rd party human attack, according to the keystroke times. Therefore, the proposed factors are much flexible and realistic than other CAPTCHA techniques. Table 7 demonstrates the comparisons between the proposed mechanism and the existing techniques.

Table 5.1 Pros and Cons of the CAPTCHA system

Pros & Cons	Proposed Technique	Existing Techniques
Pros	- This proposed technique using unique of each human to against legitimate user - Bio-detection function was used to protect human intruders	- iCAPTCHA using time out to distinguish legitimate user from human user[26] -GeoCAPTCHA use geographic information to prevent the 3rd party human attack [25]attacks [26]
Cons	- time to solve this CAPTCHA technique cannot be considered in this proposed technique	- Users with eye problem may have a slow response time, so iCAPTCHA technique must reject their response [26]

Referring to Table 5.1, it is clear that the proposed method is better than the existing mechanisms mentioned previously.

5.2 Limitation of the experiment

There are many styles of the Text-based CAPTCHA, but in this research use simple the Text-based CAPTCHA with only numbers, and no noise and neither any distortion.

5.3 Conclusion

Text-based CAPTCHA is the most widely used security technology that is used on web pages. This protects automatic malicious program to access the system. Many researchers have tried to implement many styles of Text-based CAPTCHA for a high level of protection, such as adding more noise and distortion that is hard to be solved by bots. Unfortunately, it is also hard for human users as well as bots. Especially, it cannot protect the 3rd human users. Therefore, in order to increase the solving capability of human towards Text-based CAPTCHA, this research suggests factors to be included in the BDF of Text-based CAPTCHA, such as human's demographic information, set of displayed characters in each position, and color of foreground and background. The biometrics are suggested in this research can easily protect bots from entering to the required system. As a consequence, these factors can be applied to the authentication process since the ability of owners will be different from ability of intruders, based on keystroke dynamics assumption.

The result of this research that uses a simple text-based CAPTCHA that combine with color foreground and background. Which effect to the BDF of user vision while the numbers and position are another affect that have typing correctness. As well as, spend time to read CAPTCHAs is important factor to user typing correctness.

Nevertheless, the all factors that mention before, use to consider when implements CAPTCHA to protect the 3rd party human users. For the next generation of CAPTCHA must be use timeout mechanism for protect all bots and human attack.

REFERENCES

1. Ahn, L.v., M. Blum, and J. Langford, Telling humans and computers apart automatically. Commun. ACM, 2004. 47(2): p. 56-60.
2. Ahn, L.V., et al., CAPTCHA: using hard AI problems for security, in Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques. 2003, Springer-Verlag: Warsaw, Poland. p. 294-311.
3. Chandavale, A. and A. Sapkal. An Improved Adaptive Noise Reduction for Secured CAPTCHA. in Emerging Trends in Engineering and Technology (ICETET), 2011 4th International Conference on. 2011.
4. Chellapilla, K., et al., Designing human friendly human interaction proofs (HIPs), in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2005, ACM: Portland, Oregon, USA. p. 711-720.
5. Fidas, C.A., A.G. Voyiatzis, and N.M. Avouris, On the necessity of user-friendly CAPTCHA, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2011, ACM: Vancouver, BC, Canada. p. 2623-2626.
6. Ferzli, R., R. Bazzi, and L.J. Karam. A Captcha Based on the Human Visual Systems Masking Characteristics. in Multimedia and Expo, 2006 IEEE International Conference on. 2006.
7. Motoyama, M., et al., Re: CAPTCHAs: understanding CAPTCHA-solving services in an economic context, in Proceedings of the 19th USENIX conference on Security. 2010, USENIX Association: Washington, DC. p. 28-28.
8. Hajjdiab, H. and A. Khalil. Image Matching CAPTCHAs. in Computer Modelling and Simulation (UKSim), 2012 UKSim 14th International Conference on. 2012.
9. Nayeem, M.T., et al. Use of Human Cognition in HIP Design Via EmotIcons to Defend BOT Attacks. in Computational Science and Engineering (CSE), 2012 IEEE 15th International Conference on. 2012.
10. Rui, Y. and Z. Liu, Excuse me, but are you human?, in Proceedings of the eleventh ACM international conference on Multimedia. 2003, ACM: Berkeley, CA, USA. p. 462-463.
11. Turing, A.M., Computing machinery and intelligence, in Computers &amp; thought, A.F. Edward and F. Julian, Editors. 1995, MIT Press. p. 11-35.
12. Yan, J. and A.S.E. Ahmad, Usability of CAPTCHAs or usability issues in CAPTCHA design, in Proceedings of the 4th symposium on Usable privacy and security. 2008, ACM: Pittsburgh, Pennsylvania. p. 44-52.

13.Haichang, G., et al. A Novel Image Based CAPTCHA Using Jigsaw Puzzle. in Computational Science and Engineering (CSE), 2010 IEEE 13th International Conference on. 2010.

14.Bursztein, E., M. Martin, and J. Mitchell, Text-based CAPTCHA strengths and weaknesses, in Proceedings of the 18th ACM conference on Computer and communications security. 2011, ACM: Chicago, Illinois, USA. p. 125-138.

15.Aadhirai, R., P.J.S. Kumar, and S. Vishnupriya. Image CAPTCHA: Based on human understanding of real world distances. in Intelligent Human Computer Interaction (IHCI), 2012 4th International Conference on. 2012.

16.Gossweiler, R., M. Kamvar, and S. Baluja, What's up CAPTCHA?: a CAPTCHA based on image orientation, in Proceedings of the 18th international conference on World wide web. 2009, ACM: Madrid, Spain. p. 841-850.

17.Shirali-Shahreza, M. and S. Shirali-Shahreza. Advanced Collage CAPTCHA. in Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on. 2008.

18.Haichang, G., et al. An Audio CAPTCHA to Distinguish Humans from Computers. in Electronic Commerce and Security (ISECS), 2010 Third International Symposium on. 2010.

19.Gupta, A., et al. Sequenced Tagged Captcha: Generation and its Analysis. in Advance Computing Conference, 2009. IACC 2009. IEEE International. 2009.

20.Tam, J., et al., Breaking Audio CAPTCHAs, in Proceedings of the Twenty-Second Annual Conference on Neural Information Processing Systems. 2008. p. 1625-1632.

21.Shirali-Shahreza, M. and S. Shirali-Shahreza. CAPTCHA for Blind People. in Signal Processing and Information Technology, 2007 IEEE International Symposium on. 2007.

22.Google, Telling Humans and Computers Apart Automatically. 2014.

23.Confident Technologies, I., Confident CAPTCHA. 2010 - 2013.

24.Ltd., M., Magnetic CAPTCHA. 2010-2014.

25.Te-En, W., A.B. Jeng, and L. Hahn-Ming. GeoCAPTCHA &#x2014; A novel personalized CAPTCHA using geographic concept to defend against 3<sup>rd</sup> Party Human Attack. in Performance Computing and Communications Conference (IPCCC), 2012 IEEE 31st International. 2012.

26.Truong, H.D., C.F. Turner, and C.C. Zou. iCAPTCHA: The Next Generation of CAPTCHA Designed to Defend against 3rd Party Human Attacks. in Communications (ICC), 2011 IEEE International Conference on. 2011.

27.Tamang, T. and P. Bhattarakosol. Uncover impact factors of text-based CAPTCHA identification. in Computing and Convergence Technology (ICCCT), 2012 7th International Conference on. 2012.

28.Nanglae, N. and P. Bhattarakosol. A Study of Human Bio-detection Function under Text-Based CAPTCHA System. in Computer and Information Science (ICIS), 2012 IEEE/ACIS 11th International Conference on. 2012.

29.Nanglae, N. and P. Bhattarakosol, Authentication Indicators Based Bio-Detection Function with Text-based CAPTCHA. International Journal of Digital Content Technology and its Applications (JDCTA), 2014. 8(1): p. 10-18.

30.Saito, D., et al. The effect of Age on Web-safe Color Visibility for a White Background. in Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE. 2006.

31.Zhenhua, W. Biometrics Authentication System on Open Network and Security Analysis. in Electronic Commerce and Security, 2008 International Symposium on. 2008.

32.Monrose, F. and A.D. Rubin, Keystroke dynamics as a biometric for authentication. Future Gener. Comput. Syst., 2000. 16(4): p. 351-359.

33.Malinka, K. Usability of Visual Evoked Potentials as Behavioral Characteristics for Biometric Authentication. in Internet Monitoring and Protection, 2009. ICIMP '09. Fourth International Conference on. 2009.

34.Buhan, I., E. Kelkboom, and K. Simoens. A Survey of the Security and Privacy Measures for Anonymous Biometric Authentication Systems. in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on. 2010.

35.Bhattacharyya, D., et al., Biometric Authentication: A Review International Journal of u- and e- Service, Science and Technology 2009. 2(3).

36.Teh, P.S., A.B.J. Teoh, and S. Yue, A Survey of Keystroke Dynamics Biometrics. The Scientific World Journal, 2013. 2013: p. 24.

37.Arvindhanp. Captcha. July 20, 2010; Available from: http://hadeswork.wordpress.com/2010/07/20/captcha/.

38.Bursuc, F.A.F.G. CAPTCHA: Telling Humans and Computers Apart. What is CAPTCHA ? 2011 13 IANUARIE 2011; Available from: http://captcha4web.blogspot.com/.

39.Taylor, D., WHAT IS A CAPTCHA ANTI-SPAM SYSTEM? 2009, March 10, 2009: www.askdavetaylor.com.

40.Jisong, Z. and W. Xingfen. Breaking Internet Banking CAPTCHA Based on Instance Learning. in Computational Intelligence and Design (ISCID), 2010 International Symposium on. 2010.

41.ur Rahman, R., D.S. Tomar, and S. Das. Dynamic Image Based CAPTCHA. in Communication Systems and Network Technologies (CSNT), 2012 International Conference on. 2012.

42.Bigham, J.P. and A.C. Cavender, Evaluating existing audio CAPTCHAs and an interface optimized for non-visual use, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2009, ACM: Boston, MA, USA. p. 1829-1838.

43.Polakis, I., G. Kontaxis, and S. Ioannidis. CAPTCHuring Automated (Smart) Phone Attacks. in SysSec Workshop (SysSec), 2011 First. 2011.

44.Li, S., et al., Breaking e-banking CAPTCHAs, in Proceedings of the 26th Annual Computer Security Applications Conference. 2010, ACM: Austin, Texas. p. 171-180.

45.Yan, J. and A.S. El Ahmad, Captcha Robustness: A Security Engineering Perspective. Computer, 2011. 44(2): p. 54-60.

46.Lampson, B.W., Computer security in the real world. Computer, 2004. 37(6): p. 37-46.

47.Walsh, T.R. Protecting information assets through effective computer security training. in Security Technology, 1994. Proceedings. Institute of Electrical and Electronics Engineers 28th Annual 1994 International Carnahan Conference on. 1994.

48.Yassin, Y. and Z. Yunos, ETHICS IN INFORMATION SECURITY NST Tech & U, 2006: p. 1-4.

49.Masrom, M. and Z. Ismail. Computer security and computer ethics awareness: A component of management information system. in Information Technology, 2008. ITSim 2008. International Symposium on. 2008.

50.Wen-Yuan, L., L. Yong-An, and S. Ya-Li. A Security Multi-Bank E-cash Protocol Based on Smart Card. in Machine Learning and Cybernetics, 2007 International Conference on. 2007.

51.Aloul, F., S. Zahidi, and W. El-Hajj. Two factor authentication using mobile phones. in Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on. 2009.

52.Yampolskiy, R.V. User Authentication via Behavior Based Passwords. in Systems, Applications and Technology Conference, 2007. LISAT 2007. IEEE Long Island. 2007.

53.More, S.B., A.B. Ubale, and K.C. Jondhale, Biometric Security, in Proceedings of the 2008 First International Conference on Emerging Trends in Engineering and Technology. 2008, IEEE Computer Society. p. 701-704.

54.Ivanov, V.I. and J.S. Baras. Authentication of fingerprint scanners. in Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on. 2011.

55.Zhou, H.-l. and M. Xie. Iris Biometic Processor Enhanced Module FPGA-Based Design. in Computer Modeling and Simulation, 2010. ICCMS '10. Second International Conference on. 2010.

56.FUJITSU. Biometric Products. [cited 2014 March 14]; Available from: http://www.fujitsu.com/us/services/biometrics/.

57.Xue, Y. Biometric verification using hand vein-patterns. in Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on. 2010.

58.Ahn, L.v. and L. Dabbish, Labeling images with a computer game, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2004, ACM: Vienna, Austria. p. 319-326.

59.Shirali-Shahreza, S. and A. Movaghar. A New Anti-Spam Protocol Using CAPTCHA. in Networking, Sensing and Control, 2007 IEEE International Conference on. 2007.

60.Sheng, L., W. Xing-yu, and Y. Xiao-ming, Implementation of OpenGL 3D animation simulation and scene walkthrough based on VC++. Computer Engineering and Design, 2006(17): p. 3235-3238

61.Carr, M., Visualization with OpenGL: 3D made easy. Antennas and Propagation Magazine, IEEE, 1997. 39(4): p. 116-120.

62.JingSong, C., et al. CAPTCHA design based on moving object recognition problem. in Information Sciences and Interaction Sciences (ICIS), 2010 3rd International Conference on. 2010.

63.Almazyad, A.S., Y. Ahmad, and S.A. Kouchay. Multi-Modal CAPTCHA: A User Verification Scheme. in Information Science and Applications (ICISA), 2011 International Conference on. 2011.

64.Rusu, A. and R. Docimo. Securing the Web Using Human Perception and Visual Object Interpretation. in Information Visualisation, 2009 13th International Conference. 2009.

65.Chew, M. and J.D. Tygar, Image Recognition CAPTCHAs, in Information Security, K. Zhang and Y. Zheng, Editors. 2004, Springer Berlin Heidelberg. p. 268-279.

66.El Ahmad, A.S., J. Yan, and N. Wai-Yin, CAPTCHA Design: Color, Usability, and Security. Internet Computing, IEEE, 2012. 16(2): p. 44-51.

67.University, C.M. CAPTCHA: Telling Humans and Computers Apart Automatically. [cited 2014 March 14]; Available from: http://www.captcha.net/.

68.Jain, A., S. Dass, and K. Nandakumar, Soft Biometric Traits for Personal Recognition Systems, in Biometric Authentication, D. Zhang and A. Jain, Editors. 2004, Springer Berlin Heidelberg. p. 731-738.

69.Givens, G., et al. A Statistical Assessment of Subject Factors in the PCA Recognition of Human Faces. in Computer Vision and Pattern Recognition Workshop, 2003. CVPRW '03. Conference on. 2003.

70.Jain, A.K., S.C. Dass, and K. Nandakumar. Can soft biometric traits assist user recognition? 2004.

APPENDIX

EXPERIMENTAL RESULTS

Table A1 The correctness by period of time with age

Age			Final status		Total
			Incorrect	Correct	
10-25	Period Time	06.01am-08.00am	0.54	7.85	8.39
		08.01am-12.00pm	0.84	12.40	13.24
		12.01pm-01.00pm	0.48	8.19	8.66
		01.01pm-04.00pm	1.01	13.05	14.06
		04.01pm-08.00pm	0.98	17.31	18.28
		08.01pm-06.00am	1.92	35.44	37.36
	Total		5.76	94.24	100.00
26-40	Period Time	06.01am-08.00am	0.76	12.63	13.38
		08.01am-12.00pm	1.16	24.50	25.65
		12.01pm-01.00pm	0.09	3.91	4.01
		01.01pm-04.00pm	1.20	21.93	23.12
		04.01pm-08.00pm	1.18	18.47	19.65
		08.01pm-06.00am	0.52	13.66	14.19
	Total		4.90	95.10	100.00
41-60	Period Time	06.01am-08.00am	0.55	12.94	13.49
		08.01am-12.00pm	1.12	27.94	29.06
		12.01pm-01.00pm	0.40	8.68	9.09
		01.01pm-04.00pm	0.48	10.11	10.59
		04.01pm-08.00pm	1.12	12.57	13.69
		08.01pm-06.00am	0.99	23.09	24.08
	Total		4.66	95.34	100.00

Table A2 The result of Chi-Square Tests by the correctness of period of time with age

Age		Value	df	Asymp. Sig. (2-sided)
10-25	Pearson Chi-Square	28.195a	5	.000
26-40	Pearson Chi-Square	22.090b	5	.001
41-60	Pearson Chi-Square	24.585c	5	.000

Table A3 The correctness by period of time with genders

Gender			Final status		Total
			Incorrect	Correct	
Male	Period Time	06.01am-08.00am	0.77	10.16	10.93
		08.01am-12.00pm	0.81	14.97	15.78
		12.01pm-01.00pm	0.48	9.26	9.74
		01.01pm-04.00pm	1.15	13.05	14.21
		04.01pm-08.00pm	0.90	14.36	15.26
		08.01pm-06.00am	1.90	32.18	34.08
	Total		6.01	93.99	100.00
Female	Period Time	06.01am-08.00am	0.57	11.52	12.09
		08.01am-12.00pm	1.32	23.97	25.29
		12.01pm-01.00pm	0.33	6.60	6.94
		01.01pm-04.00pm	1.07	20.50	21.56
		04.01pm-08.00pm	1.43	23.65	25.08
		08.01pm-06.00am	1.31	30.66	31.97
	Total		6.03	116.91	122.94

Table A4 The result of Chi-Square Tests by the correctness of period of time with gender

Gender		Value	df	Asymp. Sig. (2-sided)
Male	Pearson Chi-Square	37.674a	5	.000
Female	Pearson Chi-Square	17.572b	5	.004

Table A5 The correctness by period of time with occupation

Do you work in field computer?	Occupation			Final status		Total
				Incorrect	Correct	
Do	Student	Period Time	06.01am-08.00am	0.35	7.32	7.67
			08.01am-12.00pm	0.76	13.45	14.21
			12.01pm-01.00pm	0.42	8.50	8.92
			01.01pm-04.00pm	0.97	13.28	14.25
			04.01pm-08.00pm	0.97	16.30	17.28
			08.01pm-06.00am	1.79	35.89	37.68
		Total		5.25	94.75	100.00
	Private staff	Period Time	06.01am-08.00am	2.23	44.64	46.88
			08.01am-12.00pm	0.00	6.70	6.70
			12.01pm-01.00pm	0.00	6.70	6.70
			01.01pm-04.00pm	0.89	32.14	33.04
			04.01pm-08.00pm	0.00	6.70	6.70
		Total		3.13	96.88	100.00
	Government officer	Period Time	06.01am-08.00am	1.14	20.57	21.71
			08.01am-12.00pm	1.58	25.62	27.20
			12.01pm-01.00pm	0.43	8.09	8.52
			01.01pm-04.00pm	0.71	19.24	19.95
			04.01pm-08.00pm	0.82	14.36	15.18
			08.01pm-06.00am	0.34	7.11	7.45
		Total		5.01	94.99	100.00

Table A5 The correctness by period of time with occupation (cont.)

Do you work in field computer?	Occupation			Final status		Total
				Incorrect	Correct	
Do	Other	Period Time	06.01am-08.00am	1.18	4.40	5.58
			08.01am-12.00pm	2.36	17.99	20.35
			12.01pm-01.00pm	0.62	12.10	12.72
			01.01pm-04.00pm	3.66	13.03	16.69
			04.01pm-08.00pm	0.74	10.42	11.17
			08.01pm-06.00am	3.60	29.90	33.50
		Total		12.16	87.84	100.00
Don't	Student	Period Time	06.01am-08.00am	0.76	10.87	11.63
			08.01am-12.00pm	0.65	11.43	12.08
			12.01pm-01.00pm	0.51	6.55	7.06
			01.01pm-04.00pm	0.65	13.12	13.76
			04.01pm-08.00pm	1.00	18.91	19.91
			08.01pm-06.00am	1.76	33.80	35.55
		Total		5.32	94.68	100.00
	Private staff	Period Time	06.01am-08.00am	1.04	15.65	16.69
			08.01am-12.00pm	0.90	26.22	27.12
			12.01pm-01.00pm	0.42	5.84	6.26
			01.01pm-04.00pm	1.18	23.85	25.03
			04.01pm-08.00pm	1.32	19.40	20.72
			08.01pm-06.00am	0.07	4.10	4.17
		Total		4.94	95.06	100.00
	Government officer	Period Time	06.01am-08.00am	0.18	4.04	4.22
			08.01am-12.00pm	1.29	29.78	31.07
			12.01pm-01.00pm	0.03	3.80	3.83
			01.01pm-04.00pm	1.32	18.10	19.43
			04.01pm-08.00pm	1.50	17.38	18.88
			08.01pm-06.00am	0.91	21.67	22.58
		Total		5.23	94.77	100.00

Table A5 The correctness by period of time with occupation (cont.)

Do you work in field computer?	Occupation			Final status		Total
				Incorrect	Correct	
Don't	Unemployed	Period Time	06.01am-08.00am	2.16	21.37	23.53
			01.01pm-04.00pm	1.96	9.80	11.76
			04.01pm-08.00pm	4.90	36.27	41.18
			08.01pm-06.00am	3.73	19.80	23.53
		Total		12.75	87.25	100.00
	Other	Period Time	08.01am-12.00pm	0.70	19.03	19.74
			12.01pm-01.00pm	0.05	7.00	7.05
			01.01pm-04.00pm	0.47	10.81	11.28
			04.01pm-08.00pm	0.38	19.27	19.64
			08.01pm-06.00am	0.80	41.49	42.29
		Total		2.40	97.60	100.00

Table A6 The results of Chi-Square Tests by the correctness of period of time with occupation

Do you work in field computer?	Occupation		Value	df	Asymp. Sig. (2-sided)
Do	Student	Pearson Chi-Square	16.170a	5	.006
	Private staff	Pearson Chi-Square	4.849b	4	.303
	Government officer	Pearson Chi-Square	7.602c	5	.180
	Other	Pearson Chi-Square	47.191d	5	.000
Don't	Student	Pearson Chi-Square	12.433e	5	.029
	Private staff	Pearson Chi-Square	6.309f	5	.277
	Government officer	Pearson Chi-Square	45.773g	5	.000
	Unemployed	Pearson Chi-Square	3.374h	3	.337
	Other	Pearson Chi-Square	9.020i	4	.061

Table A7 The correctness by period of time with occupation in computer field

If work in field computer what part do you work?	Occupation			Final status		Total
				Incorrect	Correct	
Computer	Student	Period Time	06.01am-08.00am	0.5	5.2	5.7
			08.01am-12.00pm	0.5	6.0	6.5
			12.01pm-01.00pm	0.7	16.1	16.8
			01.01pm-04.00pm	0.5	5.5	5.9
			04.01pm-08.00pm	1.6	25.2	26.8
			08.01pm-06.00am	1.9	36.3	38.2
		Total		5.7	94.3	100.0
	Government officer	Period Time	06.01am-08.00am	0.0	0.8	0.8
			08.01am-12.00pm	1.4	10.0	11.4
			12.01pm-01.00pm	0.0	0.8	0.8
			01.01pm-04.00pm	0.5	10.4	11.0
			04.01pm-08.00pm	0.7	10.2	10.9
			08.01pm-06.00am	0.0	1.6	1.6
		Total		2.6	33.9	36.5
IT	Student	Period Time	08.01am-12.00pm	0.3	2.1	2.4
			12.01pm-01.00pm	0.0	0.8	0.8
			01.01pm-04.00pm	0.2	2.3	2.4
			04.01pm-08.00pm	0.1	2.3	2.4
			08.01pm-06.00am	0.1	3.1	3.3
		Total		0.8	10.6	11.3
	Government officer	Period Time	08.01am-12.00pm	0.1	5.7	5.7
			01.01pm-04.00pm	0.1	6.4	6.5
		Total		0.1	12.1	12.2

Table A7 The correctness by period of time with occupation in computer field (cont.)

If work in field computer what part do you work?	Occupation			Final status		Total
				Incorrect	Correct	
IT	Student	Period Time	08.01am-12.00pm	0.3	2.1	2.4
			12.01pm-01.00pm	0.0	0.8	0.8
			01.01pm-04.00pm	0.2	2.3	2.4
			04.01pm-08.00pm	0.1	2.3	2.4
			08.01pm-06.00am	0.1	3.1	3.3
		Total		0.8	10.6	11.3
	Government officer	Period Time	08.01am-12.00pm	0.1	5.7	5.7
			01.01pm-04.00pm	0.1	6.4	6.5
		Total		0.1	12.1	12.2
Other	Student	Period Time	06.01am-08.00am	0.9	25.2	26.2
			08.01am-12.00pm	2.3	47.7	50.0
			12.01pm-01.00pm	1.0	18.4	19.4
			01.01pm-04.00pm	3.4	47.4	50.8
			04.01pm-08.00pm	2.3	40.2	42.5
			08.01pm-06.00am	5.4	109.5	114.9
		Total		15.4	288.5	303.9
	Private staff	Period Time	06.01am-08.00am	0.3	5.4	5.7
			08.01am-12.00pm	0.0	0.8	0.8
			12.01pm-01.00pm	0.0	0.8	0.8
			01.01pm-04.00pm	0.1	3.9	4.0
			04.01pm-08.00pm	0.0	0.8	0.8
		Total		0.4	11.8	12.2

Table A7 The correctness by period of time with occupation in computer field (cont.)

If work in field computer what part do you work?	Occupation			Final status		Total
				Incorrect	Correct	
other	Government officer	Period Time	06.01am-08.00am	1.7	30.6	32.3
			08.01am-12.00pm	1.0	23.4	24.4
			12.01pm-01.00pm	0.7	11.5	12.2
			01.01pm-04.00pm	0.5	12.5	13.0
			04.01pm-08.00pm	0.5	11.7	12.2
			08.01pm-06.00am	0.5	9.2	9.7
		Total		4.9	98.9	103.9
	Other	Period Time	06.01am-08.00am	0.5	1.9	2.4
			08.01am-12.00pm	1.0	7.9	8.9
			12.01pm-01.00pm	0.3	5.3	5.6
			01.01pm-04.00pm	1.6	5.7	7.3
			04.01pm-08.00pm	0.3	4.6	4.9
			08.01pm-06.00am	1.6	13.1	14.7
		Total		5.3	38.4	43.7

Table A8 The result of Chi-Square Tests by the correctness of period of time with occupation in computer field

If work in field computer what part do you work?	Occupation		Value	df	Asymp. Sig. (2-sided)
Computer	Student	Pearson Chi-Square	11.356a	5	.045
	Government officer	Pearson Chi-Square	25.908b	5	.000
IT	Student	Pearson Chi-Square	6.303c	4	.178
	Government officer	Pearson Chi-Square	.096d	1	.756
Other	Student	Pearson Chi-Square	16.470f	5	.006
	Private staff	Pearson Chi-Square	4.849g	4	.303
	Government officer	Pearson Chi-Square	3.303h	5	.653
	Other	Pearson Chi-Square	47.191i	5	.000

Table A9 The first position of CAPTCHA

1st CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
0	1	-.05	.093	.581	-.23	.13
	2	.06	.094	.509	-.12	.25
	3	.08	.094	.415	-.11	.26
	4	.05	.094	.573	-.13	.24
	5	.03	.095	.787	-.16	.21
	6	.13	.094	.176	-.06	.31
	7	.16	.095	.099	-.03	.34
	8	.12	.097	.204	-.07	.31
	9	.12	.094	.222	-.07	.30
1	0	.05	.093	.581	-.13	.23
	2	.11	.092	.218	-.07	.29
	3	.13	.092	.165	-.05	.31
	4	.10	.092	.257	-.08	.29
	5	.08	.093	.406	-.10	.26
	6	.18	.092	.052	.00	.36
	7	.21*	.093	.026	.03	.39
	8	.17	.095	.066	-.01	.36
	9	.17	.092	.071	-.01	.35
2	0	-.06	.094	.509	-.25	.12
	1	-.11	.092	.218	-.29	.07
	3	.01	.093	.876	-.17	.20
	4	-.01	.093	.923	-.19	.17
	5	-.04	.094	.696	-.22	.15
	6	.07	.093	.483	-.12	.25
	7	.10	.094	.313	-.09	.28
	8	.06	.096	.527	-.13	.25
	9	.05	.093	.570	-.13	.24

Table A9 The first position of CAPTCHA (cont.)

1st CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
3	0	-.08	.094	.415	-.26	.11
	1	-.13	.092	.165	-.31	.05
	2	-.01	.093	.876	-.20	.17
	4	-.02	.093	.800	-.21	.16
	5	-.05	.094	.585	-.23	.13
	6	.05	.093	.586	-.13	.23
	7	.08	.094	.394	-.10	.27
	8	.05	.096	.631	-.14	.23
	9	.04	.093	.681	-.14	.22
4	0	-.05	.094	.573	-.24	.13
	1	-.10	.092	.257	-.29	.08
	2	.01	.093	.923	-.17	.19
	3	.02	.093	.800	-.16	.21
	5	-.03	.094	.769	-.21	.16
	6	.07	.093	.425	-.11	.26
	7	.10	.095	.270	-.08	.29
	8	.07	.096	.468	-.12	.26
	9	.06	.093	.507	-.12	.25
5	0	-.03	.095	.787	-.21	.16
	1	-.08	.093	.406	-.26	.10
	2	.04	.094	.696	-.15	.22
	3	.05	.094	.585	-.13	.23
	4	.03	.094	.769	-.16	.21
	6	.10	.094	.276	-.08	.29
	7	.13	.095	.165	-.05	.32
	8	.10	.096	.312	-.09	.29
	9	.09	.094	.340	-.09	.27

Table A9 The first position of CAPTCHA (cont.)

1st CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
6	0	-.13	.094	.176	-.31	.06
	1	-.18	.092	.052	-.36	.00
	2	-.07	.093	.483	-.25	.12
	3	-.05	.093	.586	-.23	.13
	4	-.07	.093	.425	-.26	.11
	5	-.10	.094	.276	-.29	.08
	7	.03	.094	.753	-.16	.21
	8	.00	.096	.960	-.19	.18
	9	-.01	.093	.894	-.20	.17
7	0	-.16	.095	.099	-.34	.03
	1	-.21*	.093	.026	-.39	-.03
	2	-.10	.094	.313	-.28	.09
	3	-.08	.094	.394	-.27	.10
	4	-.10	.095	.270	-.29	.08
	5	-.13	.095	.165	-.32	.05
	6	-.03	.094	.753	-.21	.16
	8	-.03	.097	.721	-.22	.16
	9	-.04	.095	.656	-.23	.14
8	0	-.12	.097	.204	-.31	.07
	1	-.17	.095	.066	-.36	.01
	2	-.06	.096	.527	-.25	.13
	3	-.05	.096	.631	-.23	.14
	4	-.07	.096	.468	-.26	.12
	5	-.10	.096	.312	-.29	.09
	6	.00	.096	.960	-.18	.19
	7	.03	.097	.721	-.16	.22
	9	-.01	.096	.937	-.20	.18

Table A9 The first position of CAPTCHA (cont.)

1st CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
9	0	-.12	.094	.222	-.30	.07
	1	-.17	.092	.071	-.35	.01
	2	-.05	.093	.570	-.24	.13
	3	-.04	.093	.681	-.22	.14
	4	-.06	.093	.507	-.25	.12
	5	-.09	.094	.340	-.27	.09
	6	.01	.093	.894	-.17	.20
	7	.04	.095	.656	-.14	.23
	8	.01	.096	.937	-.18	.20

Table A10 The second position of CAPTCHA (cont.)

2nd CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
0	1	-.028698*	.0136636	.036	-.055485	-.001911
	2	-.010217	.0132641	.441	-.036221	.015787
	3	-.027420*	.0134327	.041	-.053754	-.001086
	4	-.011482	.0133017	.388	-.037559	.014596
	5	.012973	.0133207	.330	-.013142	.039088
	6	-.017219	.0132580	.194	-.043211	.008772
	7	-.014586	.0135303	.281	-.041111	.011940
	8	-.025260	.0133595	.059	-.051450	.000931
	9	.007971	.0132580	.548	-.018021	.033962
1	0	.028698*	.0136636	.036	.001911	.055485
	2	.018481	.0132877	.164	-.007569	.044531
	3	.001278	.0134559	.924	-.025102	.027657
	4	.017216	.0133251	.196	-.008907	.043339
	5	.041671*	.0133441	.002	.015510	.067831
	6	.011479	.0132815	.387	-.014559	.037516
	7	.014112	.0135533	.298	-.012459	.040683
	8	.003438	.0133828	.797	-.022798	.029675
	9	.036668*	.0132815	.006	.010631	.062706
2	0	.010217	.0132641	.441	-.015787	.036221
	1	-.018481	.0132877	.164	-.044531	.007569
	3	-.017203	.0130501	.187	-.042787	.008381
	4	-.001265	.0129152	.922	-.026584	.024055
	5	.023190	.0129348	.073	-.002168	.048548
	6	-.007002	.0128702	.586	-.032234	.018229
	7	-.004369	.0131505	.740	-.030150	.021412
	8	-.015043	.0129747	.246	-.040479	.010394
	9	.018187	.0128702	.158	-.007044	.043419

Table A10 The second position of CAPTCHA (cont.)

2nd CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
3	0	.027420*	.0134327	.041	.001086	.053754
	1	-.001278	.0134559	.924	-.027657	.025102
	2	.017203	.0130501	.187	-.008381	.042787
	4	.015938	.0130882	.223	-.009720	.041597
	5	.040393*	.0131076	.002	.014696	.066090
	6	.010201	.0130438	.434	-.015371	.035773
	7	.012835	.0133205	.335	-.013280	.038949
	8	.002161	.0131470	.869	-.023613	.027935
	9	.035391*	.0130438	.007	.009819	.060963
4	0	.011482	.0133017	.388	-.014596	.037559
	1	-.017216	.0133251	.196	-.043339	.008907
	2	.001265	.0129152	.922	-.024055	.026584
	3	-.015938	.0130882	.223	-.041597	.009720
	5	.024455	.0129733	.059	-.000979	.049888
	6	-.005737	.0129088	.657	-.031045	.019570
	7	-.003104	.0131884	.814	-.028959	.022751
	8	-.013778	.0130130	.290	-.039289	.011734
	9	.019452	.0129088	.132	-.005855	.044760
5	0	-.012973	.0133207	.330	-.039088	.013142
	1	-.041671*	.0133441	.002	-.067831	-.015510
	2	-.023190	.0129348	.073	-.048548	.002168
	3	-.040393*	.0131076	.002	-.066090	-.014696
	4	-.024455	.0129733	.059	-.049888	.000979
	6	-.030192*	.0129285	.020	-.055538	-.004847
	7	-.027559*	.0132076	.037	-.053452	-.001666
	8	-.038233*	.0130325	.003	-.063782	-.012683
	9	-.005003	.0129285	.699	-.030348	.020343

Table A10 The second position of CAPTCHA (cont.)

2nd CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
6	0	.017219	.0132580	.194	-.008772	.043211
	1	-.011479	.0132815	.387	-.037516	.014559
	2	.007002	.0128702	.586	-.018229	.032234
	3	-.010201	.0130438	.434	-.035773	.015371
	4	.005737	.0129088	.657	-.019570	.031045
	5	.030192*	.0129285	.020	.004847	.055538
	7	.002634	.0131443	.841	-.023135	.028402
	8	-.008040	.0129684	.535	-.033464	.017383
	9	.025190	.0128638	.050	-.000029	.050409
7	0	.014586	.0135303	.281	-.011940	.041111
	1	-.014112	.0135533	.298	-.040683	.012459
	2	.004369	.0131505	.740	-.021412	.030150
	3	-.012835	.0133205	.335	-.038949	.013280
	4	.003104	.0131884	.814	-.022751	.028959
	5	.027559*	.0132076	.037	.001666	.053452
	6	-.002634	.0131443	.841	-.028402	.023135
	8	-.010674	.0132467	.420	-.036643	.015296
	9	.022556	.0131443	.086	-.003213	.048325
8	0	.025260	.0133595	.059	-.000931	.051450
	1	-.003438	.0133828	.797	-.029675	.022798
	2	.015043	.0129747	.246	-.010394	.040479
	3	-.002161	.0131470	.869	-.027935	.023613
	4	.013778	.0130130	.290	-.011734	.039289
	5	.038233*	.0130325	.003	.012683	.063782
	6	.008040	.0129684	.535	-.017383	.033464
	7	.010674	.0132467	.420	-.015296	.036643
	9	.033230*	.0129684	.010	.007806	.058654

Table A10 The second position of CAPTCHA (cont.)

2nd CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
9	0	-.007971	.0132580	.548	-.033962	.018021
	1	-.036668*	.0132815	.006	-.062706	-.010631
	2	-.018187	.0128702	.158	-.043419	.007044
	3	-.035391*	.0130438	.007	-.060963	-.009819
	4	-.019452	.0129088	.132	-.044760	.005855
	5	.005003	.0129285	.699	-.020343	.030348
	6	-.025190	.0128638	.050	-.050409	.000029
	7	-.022556	.0131443	.086	-.048325	.003213
	8	-.033230*	.0129684	.010	-.058654	-.007806

Table A11 The third position of CAPTCHA

3rd CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
0	1	-.003872	.0194012	.842	-.041907	.034163
	2	-.041938*	.0196711	.033	-.080502	-.003373
	3	-.093461*	.0199560	.000	-.132584	-.054338
	4	-.045473*	.0193134	.019	-.083336	-.007610
	5	-.027054	.0193913	.163	-.065070	.010961
	6	-.079036*	.0196172	.000	-.117495	-.040578
	7	-.066037*	.0199921	.001	-.105231	-.026843
	8	-.093621*	.0197149	.000	-.132271	-.054970
	9	-.053026*	.0194714	.006	-.091199	-.014853
1	0	.003872	.0194012	.842	-.034163	.041907
	2	-.038065	.0198760	.056	-.077031	.000900
	3	-.089589*	.0201580	.000	-.129108	-.050070
	4	-.041601*	.0195220	.033	-.079873	-.003329
	5	-.023182	.0195991	.237	-.061605	.015241
	6	-.075164*	.0198227	.000	-.114025	-.036303
	7	-.062165*	.0201937	.002	-.101754	-.022576
	8	-.089749*	.0199193	.000	-.128800	-.050698
	9	-.049154*	.0196784	.013	-.087732	-.010575
2	0	.041938*	.0196711	.033	.003373	.080502
	1	.038065	.0198760	.056	-.000900	.077031
	3	-.051523*	.0204179	.012	-.091552	-.011495
	4	-.003535	.0197903	.858	-.042333	.035263
	5	.014883	.0198663	.454	-.024064	.053830
	6	-.037099	.0200869	.065	-.076478	.002281
	7	-.024099	.0204532	.239	-.064197	.015998
	8	-.051683*	.0201823	.010	-.091250	-.012117
	9	-.011088	.0199445	.578	-.050189	.028012

Table A11 The third position of CAPTCHA (cont.)

3rd CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
3	0	.093461*	.0199560	.000	.054338	.132584
	1	.089589*	.0201580	.000	.050070	.129108
	2	.051523*	.0204179	.012	.011495	.091552
	4	.047988*	.0200735	.017	.008635	.087341
	5	.066407*	.0201485	.001	.026906	.105907
	6	.014425	.0203660	.479	-.025502	.054352
	7	.027424	.0207274	.186	-.013211	.068059
	8	-.000160	.0204602	.994	-.040271	.039952
	9	.040435*	.0202256	.046	.000784	.080086
4	0	.045473*	.0193134	.019	.007610	.083336
	1	.041601*	.0195220	.033	.003329	.079873
	2	.003535	.0197903	.858	-.035263	.042333
	3	-.047988*	.0200735	.017	-.087341	-.008635
	5	.018418	.0195122	.345	-.019834	.056671
	6	-.033563	.0197367	.089	-.072256	.005130
	7	-.020564	.0201094	.307	-.059988	.018859
	8	-.048148*	.0198338	.015	-.087031	-.009264
	9	-.007553	.0195918	.700	-.045962	.030856
5	0	.027054	.0193913	.163	-.010961	.065070
	1	.023182	.0195991	.237	-.015241	.061605
	2	-.014883	.0198663	.454	-.053830	.024064
	3	-.066407*	.0201485	.001	-.105907	-.026906
	4	-.018418	.0195122	.345	-.056671	.019834
	6	-.051982*	.0198130	.009	-.090824	-.013139
	7	-.038982	.0201842	.054	-.078553	.000588
	8	-.066566*	.0199097	.001	-.105598	-.027534
	9	-.025972	.0196686	.187	-.064531	.012588

Table A11 The third position of CAPTCHA (cont.)

3rd CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
6	0	.079036*	.0196172	.000	.040578	.117495
	1	.075164*	.0198227	.000	.036303	.114025
	2	.037099	.0200869	.065	-.002281	.076478
	3	-.014425	.0203660	.479	-.054352	.025502
	4	.033563	.0197367	.089	-.005130	.072256
	5	.051982*	.0198130	.009	.013139	.090824
	7	.012999	.0204013	.524	-.026997	.052995
	8	-.014585	.0201298	.469	-.054048	.024879
	9	.026010	.0198914	.191	-.012986	.065006
7	0	.066037*	.0199921	.001	.026843	.105231
	1	.062165*	.0201937	.002	.022576	.101754
	2	.024099	.0204532	.239	-.015998	.064197
	3	-.027424	.0207274	.186	-.068059	.013211
	4	.020564	.0201094	.307	-.018859	.059988
	5	.038982	.0201842	.054	-.000588	.078553
	6	-.012999	.0204013	.524	-.052995	.026997
	8	-.027584	.0204953	.178	-.067764	.012596
	9	.013011	.0202612	.521	-.026710	.052732
8	0	.093621*	.0197149	.000	.054970	.132271
	1	.089749*	.0199193	.000	.050698	.128800
	2	.051683*	.0201823	.010	.012117	.091250
	3	.000160	.0204602	.994	-.039952	.040271
	4	.048148*	.0198338	.015	.009264	.087031
	5	.066566*	.0199097	.001	.027534	.105598
	6	.014585	.0201298	.469	-.024879	.054048
	7	.027584	.0204953	.178	-.012596	.067764
	9	.040595*	.0199878	.042	.001410	.079780

Table A11 The third position of CAPTCHA (cont.)

3rd CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
9	0	.053026*	.0194714	.006	.014853	.091199
	1	.049154*	.0196784	.013	.010575	.087732
	2	.011088	.0199445	.578	-.028012	.050189
	3	-.040435*	.0202256	.046	-.080086	-.000784
	4	.007553	.0195918	.700	-.030856	.045962
	5	.025972	.0196686	.187	-.012588	.064531
	6	-.026010	.0198914	.191	-.065006	.012986
	7	-.013011	.0202612	.521	-.052732	.026710
	8	-.040595*	.0199878	.042	-.079780	-.001410

Table A12 The forth position of CAPTCHA

4th CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
0	1	.009026	.0136642	.509	-.017762	.035814
	2	.011300	.0136772	.409	-.015514	.038114
	3	-.010986	.0138699	.428	-.038178	.016205
	4	.032791*	.0140752	.020	.005197	.060384
	5	.037589*	.0140278	.007	.010089	.065090
	6	.003812	.0139361	.784	-.023509	.031133
	7	.011766	.0139511	.399	-.015584	.039117
	8	.005713	.0140200	.684	-.021773	.033198
	9	.017912	.0136255	.189	-.008800	.044624
1	0	-.009026	.0136642	.509	-.035814	.017762
	2	.002274	.0135198	.866	-.024231	.028779
	3	-.020013	.0137147	.145	-.046900	.006874
	4	.023764	.0139223	.088	-.003530	.051058
	5	.028563*	.0138743	.040	.001363	.055763
	6	-.005214	.0137816	.705	-.032233	.021804
	7	.002740	.0137968	.843	-.024308	.029788
	8	-.003314	.0138664	.811	-.030498	.023871
	9	.008886	.0134675	.509	-.017517	.035288
2	0	-.011300	.0136772	.409	-.038114	.015514
	1	-.002274	.0135198	.866	-.028779	.024231
	3	-.022286	.0137277	.105	-.049199	.004626
	4	.021491	.0139351	.123	-.005829	.048810
	5	.026289	.0138872	.058	-.000936	.053515
	6	-.007488	.0137946	.587	-.034532	.019556
	7	.000466	.0138097	.973	-.026607	.027539
	8	-.005587	.0138793	.687	-.032797	.021622
	9	.006612	.0134807	.624	-.019816	.033040

Table A12 The forth position of CAPTCHA (cont.)

4th CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
3	0	.010986	.0138699	.428	-.016205	.038178
	1	.020013	.0137147	.145	-.006874	.046900
	2	.022286	.0137277	.105	-.004626	.049199
	4	.043777*	.0141243	.002	.016087	.071467
	5	.048576*	.0140770	.001	.020978	.076173
	6	.014798	.0139856	.290	-.012620	.042217
	7	.022753	.0140006	.104	-.004695	.050200
	8	.016699	.0140692	.235	-.010883	.044281
	9	.028898*	.0136762	.035	.002087	.055710
4	0	-.032791*	.0140752	.020	-.060384	-.005197
	1	-.023764	.0139223	.088	-.051058	.003530
	2	-.021491	.0139351	.123	-.048810	.005829
	3	-.043777*	.0141243	.002	-.071467	-.016087
	5	.004799	.0142793	.737	-.023195	.032793
	6	-.028979*	.0141892	.041	-.056796	-.001161
	7	-.021024	.0142040	.139	-.048871	.006822
	8	-.027078	.0142717	.058	-.055057	.000901
	9	-.014879	.0138844	.284	-.042098	.012341
5	0	-.037589*	.0140278	.007	-.065090	-.010089
	1	-.028563*	.0138743	.040	-.055763	-.001363
	2	-.026289	.0138872	.058	-.053515	.000936
	3	-.048576*	.0140770	.001	-.076173	-.020978
	4	-.004799	.0142793	.737	-.032793	.023195
	6	-.033777*	.0141422	.017	-.061503	-.006052
	7	-.025823	.0141570	.068	-.053577	.001931
	8	-.031877*	.0142249	.025	-.059764	-.003990
	9	-.019677	.0138363	.155	-.046803	.007448

Table A12 The forth position of CAPTCHA (cont.)

4th CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
6	0	-.003812	.0139361	.784	-.031133	.023509
	1	.005214	.0137816	.705	-.021804	.032233
	2	.007488	.0137946	.587	-.019556	.034532
	3	-.014798	.0139856	.290	-.042217	.012620
	4	.028979*	.0141892	.041	.001161	.056796
	5	.033777*	.0141422	.017	.006052	.061503
	7	.007954	.0140661	.572	-.019622	.035530
	8	.001901	.0141345	.893	-.025809	.029611
	9	.014100	.0137433	.305	-.012843	.041043
7	0	-.011766	.0139511	.399	-.039117	.015584
	1	-.002740	.0137968	.843	-.029788	.024308
	2	-.000466	.0138097	.973	-.027539	.026607
	3	-.022753	.0140006	.104	-.050200	.004695
	4	.021024	.0142040	.139	-.006822	.048871
	5	.025823	.0141570	.068	-.001931	.053577
	6	-.007954	.0140661	.572	-.035530	.019622
	8	-.006054	.0141493	.669	-.033793	.021685
	9	.006146	.0137585	.655	-.020827	.033119
8	0	-.005713	.0140200	.684	-.033198	.021773
	1	.003314	.0138664	.811	-.023871	.030498
	2	.005587	.0138793	.687	-.021622	.032797
	3	-.016699	.0140692	.235	-.044281	.010883
	4	.027078	.0142717	.058	-.000901	.055057
	5	.031877*	.0142249	.025	.003990	.059764
	6	-.001901	.0141345	.893	-.029611	.025809
	7	.006054	.0141493	.669	-.021685	.033793
	9	.012199	.0138284	.378	-.014910	.039309

Table A12 The forth position of CAPTCHA (cont.)

4th CAPTCHA		Mean Difference	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
9	0	-.017912	.0136255	.189	-.044624	.008800
	1	-.008886	.0134675	.509	-.035288	.017517
	2	-.006612	.0134807	.624	-.033040	.019816
	3	-.028898*	.0136762	.035	-.055710	-.002087
	4	.014879	.0138844	.284	-.012341	.042098
	5	.019677	.0138363	.155	-.007448	.046803
	6	-.014100	.0137433	.305	-.041043	.012843
	7	-.006146	.0137585	.655	-.033119	.020827
	8	-.012199	.0138284	.378	-.039309	.014910

Table A13 Color by Correctness of the Test-based CAPTCHA identification

Status			Background Color									Total
			Red	Yellow	Green	Cyan	Blue	Magenta	Gray	Black	White	
Incorrect	Character Color	Red	4.28	1.67	4.16	1.22	3.55	4.57	0.94	0.41	0.08	20.88
		Yellow	1.39	0.29	1.47	0.77	1.51	1.67	0.41	0.00	0.08	7.59
		Green	5.42	2.28	8.69	1.88	4.36	3.26	1.35	0.16	0.33	27.73
		Cyan	1.14	0.33	2.08	0.24	1.06	1.67	0.33	0.00	0.08	6.93
		Blue	3.38	0.98	3.71	1.22	1.75	2.77	0.77	0.08	0.08	14.76
		Magenta	3.47	1.26	2.94	1.14	3.34	2.04	0.86	0.08	0.33	15.46
		Gray	0.82	0.41	1.10	0.45	0.90	0.86	0.00	0.00	0.00	4.53
		Black	0.24	0.04	0.24	0.20	0.16	0.33	0.00	0.00	0.00	1.22
		White	0.16	0.12	0.12	0.12	0.08	0.16	0.12	0.00	0.00	0.90
	Total		20.31	7.38	24.51	7.26	16.72	17.33	4.77	0.73	0.98	100.00
Correct	Character Color	Red	3.00	1.56	4.72	1.55	3.41	3.68	1.02	0.20	0.16	19.29
		Yellow	1.68	0.27	1.91	0.61	1.29	1.37	0.37	0.07	0.06	7.62
		Green	5.29	2.21	4.84	1.73	3.92	4.20	1.15	0.21	0.24	23.78
		Cyan	1.63	0.54	2.17	0.26	1.22	1.31	0.34	0.08	0.05	7.60
		Blue	3.34	1.13	4.64	1.48	1.88	3.17	0.69	0.16	0.17	16.66
		Magenta	3.72	1.32	4.21	1.46	3.68	2.35	1.02	0.22	0.18	18.17
		Gray	0.97	0.37	1.17	0.38	0.74	1.09	0.06	0.02	0.04	4.83
		Black	0.20	0.10	0.23	0.07	0.20	0.21	0.01	0.00	0.01	1.02
		White	0.18	0.09	0.24	0.07	0.17	0.22	0.03	0.01	0.00	1.01
	Total		20.01	7.59	24.12	7.60	16.50	17.60	4.69	0.98	0.91	100.00

Table A14 Position and CAPTCHA

Final status			CAPTCHA										Total
			0	1	2	3	4	5	6	7	8	9	
Incorrect	Position	1	1.78	1.81	2.23	2.62	1.97	2.20	1.99	1.76	2.62	3.04	22.02
		2	2.41	2.73	2.44	2.39	2.44	2.28	2.67	1.94	2.07	2.10	23.46
		3	2.75	3.09	2.80	2.75	2.75	2.88	2.70	2.15	2.15	2.70	26.74
		4	2.15	2.57	3.49	2.49	2.91	2.94	2.96	2.46	2.88	2.94	27.79
	Total		9.10	10.20	10.96	10.25	10.07	10.30	10.33	8.31	9.72	10.77	100.00
Correct	Position	1	2.48	2.47	2.54	2.50	2.49	2.55	2.54	2.53	2.56	2.41	25.06
		2	2.44	2.49	2.47	2.55	2.50	2.51	2.50	2.50	2.49	2.58	25.03
		3	2.47	2.50	2.57	2.47	2.52	2.49	2.52	2.44	2.49	2.50	24.96
		4	2.50	2.43	2.50	2.52	2.49	2.52	2.51	2.46	2.51	2.50	24.94
	Total		9.89	9.89	10.07	10.04	10.00	10.07	10.08	9.93	10.04	10.00	100.00

Table A15 Position and Key the numbers

		Key										Total
		0	1	2	3	4	5	6	7	8	9	
CAPTCHA	0	9.682	0.048	0.030	0.021	0.014	0.013	0.012	0.004	0.009	0.039	9.873
	1	0.039	9.680	0.036	0.009	0.061	0.010	0.009	0.033	0.008	0.008	9.894
	2	0.030	0.044	9.863	0.048	0.017	0.043	0.013	0.013	0.015	0.007	10.093
	3	0.020	0.025	0.048	9.830	0.014	0.016	0.039	0.011	0.015	0.026	10.045
	4	0.012	0.039	0.017	0.021	9.794	0.055	0.017	0.034	0.008	0.010	10.005
	5	0.021	0.019	0.023	0.010	0.045	9.854	0.042	0.004	0.039	0.012	10.071
	6	0.024	0.015	0.010	0.034	0.017	0.045	9.864	0.010	0.024	0.039	10.081
	7	0.020	0.024	0.008	0.009	0.037	0.006	0.010	9.717	0.035	0.025	9.891
	8	0.020	0.017	0.019	0.017	0.010	0.046	0.019	0.020	9.826	0.035	10.030
	9	0.033	0.011	0.015	0.032	0.011	0.019	0.041	0.014	0.049	9.791	10.017
Total		9.901	9.922	10.070	10.033	10.021	10.107	10.065	9.861	10.028	9.992	100.000

Table A16 Pair of User ID

No.	User ID	User ID	No.	User ID	User ID
1	30	212	26	144	58
2	213	22	27	148	59
3	214	23	28	153	60
4	215	24	29	155	61
5	216	25	30	165	62
6	217	26	31	18	67
7	218	35	32	181	68
8	219	31	33	182	70
9	220	32	34	184	71
10	999	33	35	19	73
11	101	34	36	193	79
12	101	28	37	194	81
13	103	36	38	198	82
14	104	37	39	199	86
15	107	38	40	20	88
16	110	39	41	200	89
17	112	40	42	202	90
18	114	41	43	203	92
19	115	42	44	204	93
20	116	44	45	207	94
21	119	45	46	208	95
22	129	46	47	209	96
23	135	49	48	21	97
24	138	54	49	210	98
25	140	56	50	211	99

Table A17 Effects of Time spent and Key CAPTCHA on the Third position

Dependent Variable:3rd Time					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	42.194a	9	4.688	23.563	.000
Intercept	11596.885	1	11596.885	58285.596	.000
Key3	42.194	9	4.688	23.563	.000
Error	9010.002	45284	.199		
Total	20648.906	45294			
Corrected Total	9052.196	45293			

Table A18 Effects of Time spent and Period of time on the Third position

Dependent Variable:3rd Time					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	132.634a	5	26.527	134.687	.000
Intercept	9107.578	1	9107.578	46242.629	.000
PeriodTime	132.634	5	26.527	134.687	.000
Error	8919.562	45288	.197		
Total	20648.906	45294			
Corrected Total	9052.196	45293			

Table A19 Effects of Time spent and Eyesight problem on the third position

Dependent Variable:3rd Time					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	396.182a	5	79.236	414.562	.000
Intercept	3591.766	1	3591.766	18792.007	.000
Problem Eye	396.182	5	79.236	414.562	.000
Error	8656.014	45288	.191		
Total	20648.906	45294			
Corrected Total	9052.196	45293			

Table A20 Effects of Time spent and Eyes sight problem on the forth position

Dependent Variable:4th Time					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	11257.688a	5	2251.538	3.935	.001
Intercept	510.428	1	510.428	.892	.345
Problem Eye	11257.688	5	2251.538	3.935	.001
Error	25909820.612	45288	572.112		
Total	25922772.505	45294			
Corrected Total	25921078.300	45293			

Table A21 Effects of Time spent and Typing correctness on the third position

Dependent Variable:3rd Time					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	21.146a	1	21.146	106.049	.000
Intercept	2717.904	1	2717.904	13630.673	.000
Correct	21.146	1	21.146	106.049	.000
Error	9031.051	45292	.199		
Total	20648.906	45294			
Corrected Total	9052.196	45293			

Table A22 Effects of Time spent and Typing correctness on the forth position

Dependent Variable:4th Time					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	3476.683a	1	3476.683	6.076	.014
Intercept	1185.007	1	1185.007	2.071	.150
Correct	3476.683	1	3476.683	6.076	.014
Error	25917601.617	45292	572.234		
Total	25922772.505	45294			
Corrected Total	25921078.300	45293			

VITA

Nilobon Nanglae graduated a bachelor of Arts in English from Mae Fah Luang University. Currently, doing Master in Computer Science and Information Technology, from Chulalongkorn University, Bangkok, in 2014. My journal was Authentication Indicators Based Bio-Detection Function with Text-based CAPTCHA, have been published in JDCTA (International Journal of Digital Content Technology and its Applications) in 2014.