Diploma Project

PERSONALIZED IMAGE RECOGNITION CAPTCHA SCHEMES BASED ON HUMAN COGNITIVE FACTORS

Pantelitsa Leonidou

University of Cyprus

Computer Science Department

May 2019

I

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

PERSONALIZED IMAGE RECOGNITION CAPTCHA SCHEMES BASED ON HUMAN COGNITIVE FACTORS

Pantelitsa Leonidou

Supervisor

Professor Antonis Kakas

Co-Supervisor

Dr. Marios Belk

The individual thesis submitted for partial fulfillment of the requirements for obtaining
Computer Science's Undergraduate degree, Department of Computer Science,
University of Cyprus

May 2019

Acknowledgements

Firstly, I would like to express my respect and my special thanks to Professor George Samaras, who although is no longer with us, has inspired and encouraged me to follow this field of studies for my thesis.

I would like to express my sincere thanks to Professor Antonis Kakas, the supervisor of my dissertation, who did not hesitate to take over my supervision and gave me the opportunity to undertake this project. By giving me this opportunity, during the course of the dissertation, I was able to study in-depth, fields that I am interested in and acquire knowledge that is essential for my academic and professional career.

I would also like to express my deep gratitude to Dr. Marios Belk, the co-supervisor of my dissertation, for his guidance and support during this whole year. His ideas and knowledge about this field motivated me to bring this thesis to an end and gain a lot of knowledge and experience.

Furthermore, I am also grateful to Argyris Constantinides, for his technical support and assistance during the development of the dissertation project.

It would be my omission not to express from the depths of my heart a great thank you to my beloved family and special friends who are always by my side offering me their generous help and support in every step of my life and strongly believe in me.

Περίληψη

Τα CAPTCHA - Completely Automated Public Turing Test to tell Computers and Humans Apart είναι μια μέθοδος που χρησιμοποιείται ευρέως ως μηχανισμός ανίχνευσης ανθρώπινης αλληλεπίδρασης σε διαδικτυακές υπηρεσίες με σκοπό να προφυλάσσονται από κακόβουλους αυτοματοποιημένους πράκτορες λογισμικού.

Το αμφιλεγόμενο ζήτημα στο σχεδιασμό των συστημάτων CAPTCHA είναι να βρεθεί μια ισορροπία μεταξύ χρηστικότητας και ασφάλειας. Τα συστήματα CAPTCHA πρέπει να είναι αρκετά περίπλοκα ώστε να είναι δύσκολο για τους υπολογιστές να τα επιλύσουν, αλλά αρκετά απλά για να μην υποβαθμίσουν την εμπειρία των χρηστών στις διαδικτυακές υπηρεσίες.

Με γνώμονα την ιδέα της ανάπτυξης εξατομικευμένων προκλήσεων CAPTCHA έχοντας ως σκοπό τη βελτίωση της χρηστικότητας και της εμπειρίας των χρηστών, στα πλαίσια αυτής της πτυχιακής μελετάται η κατηγορία CAPTCHA βασισμένη στην αναγνώριση εικόνας (Image Recognition Captcha Schemes) για να προταθούν νέοι παράγοντες που μπορούν να ληφθούν υπόψη για την εφαρμογή της εξατομίκευσης στις δοκιμασίες CAPTCHA.. Πιο συγκεκριμένα, διεξήχθη μια μελέτη χρήστη για να εξεταστεί η επίδραση στην απόδοση, στην οπτική συμπεριφορά, στην εμπειρία - προτίμηση του χρήστη κατά την επίλυση δοκιμασιών CAPTCHA (βασισμένων στην αναγνώριση εικόνας), αν παρουσιάζεται στον χρήστη εικόνα με οικείο περιεχόμενο. Πιο συγκεκριμένα, μελετάται η διαφορά στη επίδραση των πιο πάνω παραγόντων όσο αφορά χρήστες με διαφορές στο γνωστικό στυλ και ικανότητες. Η θεωρία Ολιστή/Αναλυτή, η χωρητικότητα της μνήμης εργασίας και η ταχύτητα επεξεργασίας διακρίνουν τους συμμετέχοντες σε διαφορετικές ομάδες γνωστικού στυλ και ικανοτήτων.

Τα αποτελέσματα της πειραματικής μελέτης αποδεικνύουν πως η χρήση εικόνων με οικείο περιεχόμενο προς τον χρήστη μπορεί να συμπεριληφθεί σαν παράγοντας για την υιοθέτηση της εξατομίκευσης στα σχήματα CAPTCHA μόνο σε συνδυασμό με το γνωστικό στυλ του χρήστη. Οι χρήστες με διαφορετικό γνωστικό στυλ παρουσίασαν διαφορές στην προτίμηση τους ως προς το περιεχόμενο της εικόνας όπως και διαφορές στην οπτική τους συμπεριφορά ενώ η απόδοση τους δεν φάνηκε να επηρεάζεται. Επίσης φάνηκε ότι η διαφορά των χρηστών στο επίπεδο χωρητικότητας της μνήμης

εργασίας και της ταχύτητας επεξεργασίας δεν επηρεάζουν την απόδοση τους στις δοκιμασίες IRCS.

Abstract

A CAPTCHA(Completely Automated Public Turing Test to tell Computers and Humans Apart) scheme is a common and a widely-used method in on-line services and acts as a Human Interaction Proof (HIP) mechanism in order to keep the services to be protected from malicious automated software agents. So a CAPTCHA is a challenge where users must prove that they are human beings and not robots.

The controversial issue in CAPTCHA schemes design is to find a fair trade-off between usability and security. CAPTCHA schemes must be complicated enough in order to be difficult for computers to solve but simple enough to not degrade user experience in online-services.

Motivated by the idea of delivering personalized CAPTCHA challenges in order to improve usability and user experience, Image Recognition Captcha Schemes are studied to introduce new factors that can be taken into consideration to achieve generating challenges that are customized on user's individual characteristics. More specifically, a user study was conducted to examine if displaying an image in Image Recognition Captcha Schemes (IRCS) challenges, with content familiar to the user affects the performance or the preference of the user. Additionally, it is studied if the results in user's performance and preference differ in users with different cognitive styles and skills. Field dependency, working memory capacity and speed of processing are used to distinguish the participants in cognitive style and abilities groups.

The results of the study show that users with different cognitive styles have differences in preference and in performance towards IRCS challenges with familiar content images. Additionally, users with differences in cognitive abilities are shown to have similar performance when displaying familiar or generic content image in IRCS challenges. Displaying familiar content images in IRCS challenges can be applied as a factor in the adaptation of personalized CAPTCHA schemes but only if it is used alongside with the cognitive style (FI/FD) of the users.

Contents

Figures

VIII

Chapter 1

Introduction

This chapter aims to discuss the main problem of CAPTCHA schemes that this thesis attempts to address, its field area and the motivation behind this study. Then the scope of the thesis is determined by presenting the idea of the solution proposed for the problem stated. At the end of this chapter a roadmap of the upcoming chapters is given.

1.1. Problem Statement and Motivation

Nowadays, web requires a defending mechanism to protect online services from automated malicious software agents. CAPTCHA is the mostly known and used Human Interaction Proof mechanism. The problem is that CAPTCHA schemes should not interrupt the user from executing his/her primary task. The challenges must be as unobtrusive and transparent as possible to the user in order not to affect the user's experience in online services and their usability. The current method of delivering CAPTCHA challenges follows the "one-size-fits-all" approach where all individuals need to solve common challenges despite the difference in their individual characteristics. Since personalization plays a main role in the web world, CAPTCHA schemes adapting personalization seems to be a promising approach that can improve user experience and leads to the desired results.

1.2. Scope of the Thesis

Trying to solve the problem mentioned above, this thesis studies the alternative approach of adapting personalization in CAPTCHA systems in order to increase their

usability and improve user's experience. A list of factors must be created to be taken into consideration to apply personalization in CAPTCHA schemes. For example user's device is an important factor in CAPTCHA personalization since different types of challenges can be used based on the device type. Specifically, this study is focused in Image Recognition CAPTCHA schemes (IRCS) and introduces a factor that can get involved in the personalization mechanism of CAPTCHA systems. The idea of this study is to examine if the content type of the image that is displayed in IRCS affects the user's performance or preference. Additionally, it is examined whether individuals with different cognitive styles and abilities have differences in performance and preference or not by giving images with different content type. The type of image's content is distinguished in familiar to the user content or a generic content. Providing challenges with familiar content images to the user leads to personalization since users with different context will receive different images. A user study with 46 participants has been conducted to investigate if this factor can be involved in the personalization mechanism in order to extend the idea of personalization in CAPTCHA schemes.

1.3.   Thesis Overview

Following the problem's definition and the thesis' scope, a brief overview is given for the study's structure.

Chapter 2 is providing the background knowledge on CAPTCHA schemes that is required, for the reader, to have a better understanding along the study. The definition of CAPTCHA is given, followed by explaining CAPTCHA as a security mechanism. Afterwards, applications of CAPTCHA are explained and different categories of CAPTCHA schemes are presented.

In Chapter 3, a more detailed analysis on Image Recognition Captcha Scheme (IRCS) is given since this thesis is focused in IRCS. The idea behind IRCS and the argument that motivated researchers to introduce this category of CAPTCHA challenge are described. Additionally, the image displaying and selecting methods that are used in existing IRCS are presented.

In Chapter 4, the background theory in cognitive skills is available to provide the knowledge around the cognitive styles and abilities that are used in this study and help

the reader to understand how CAPTCHA can be related with individual cognition styles.

Chapter 5 is composed by the previous work and researches related with this thesis' scope. Existing IRCS are analyzed by describing their implementation and their pros and cons. Recommendations in usability, security and accessibility aspect are mentioned and the article about personalized CAPTCHA schemes which motivated this thesis is discussed.

In Chapter 6 the technical aspect of the study is covered. The software technologies that are used for designing and developing the user study are presented accompanied by the reasons of their selection. Then, the implementation of the CAPTCHA challenge that is used in the user study is analyzed.

In Chapter 7, the user study conducted within the thesis scope is analyzed. The idea and the hypotheses of the study, the procedure of the Lab Experiment, the collection and analysis on the data retrieved from the lab experiment, the analysis of the evaluation questionnaire and the results of the study are presented in details.

In the last chapter the conclusions of the thesis are summarized and the limitations of the thesis are presented. Then future work based on the results and the thesis' scope is annotated.

Chapter 2

Background Theory in CAPTCHA

2.1 Introduction of Captcha as a Human Interaction Proof Mechanism

2.2 Security Aspects of Captcha

2.3 Applications of CAPTCHA in online-services

2.4 Variation of Captcha Schemes:

      2.4.1 Text Recognition Captcha

      2.4.2 Audio Recognition Captcha

      2.4.3 Mathematical Captcha

      2.4.4 Graphics Captcha

      2.4.5 Transparent Captcha

This is an introductory chapter about CAPTCHA schemes. A short introduction about CAPTCHA's origin and its creators' motivation is presented. Then the security features of CAPCTHA schemes are explained and some applications' examples of CAPTCHA in online-services are given to show the importance of such challenges in nowadays life. In the end of this chapter, the different types of CAPTCHA schemes are presented accompanied by their pros and cons.

2.1. Introduction on CAPTCHA Schemes

CAPTCHA was first introduced by AltaVista in 1997 when a text-based scheme with random and distorted characters was developed to prevent offensive submission of URLs to their search engines by software robots. The term coined in 2000 by Luis von Ahn, Manuel Blum and Nicholas J. Hopper of Carnegie Mellon University and John Langford of IBM. From then CAPTCHA schemes become very popular and had been established as the most common HIP (Human Interaction Proof) mechanism in online services. CAPTCHA act as a reverse Turing Test since an automated program has to

decide if the user is a human or a bot. The argument of CAPTCHA challenges security is that the task that the user needs to solve is something that a human can solve easily but for automated software is impossible or too costly in resources to solve.

2.2. The security features of CAPTCHA Schemes

There are many different types of online services security. CAPTCHA is a front-end security mechanism and follows the negative policy. Front-end security means that the mechanism runs on client side of a service. The state that CAPTCHA follows negative policy describes the assumption it does that all the users are computers unless proved otherwise. Additionally, it is used as a preventive method of security that is in charge of keeping systems safe by making attacks/intrusion as hard as possible as it is used to prevent attacks. The security features of CAPTCHA are shown in Figure 2.1.
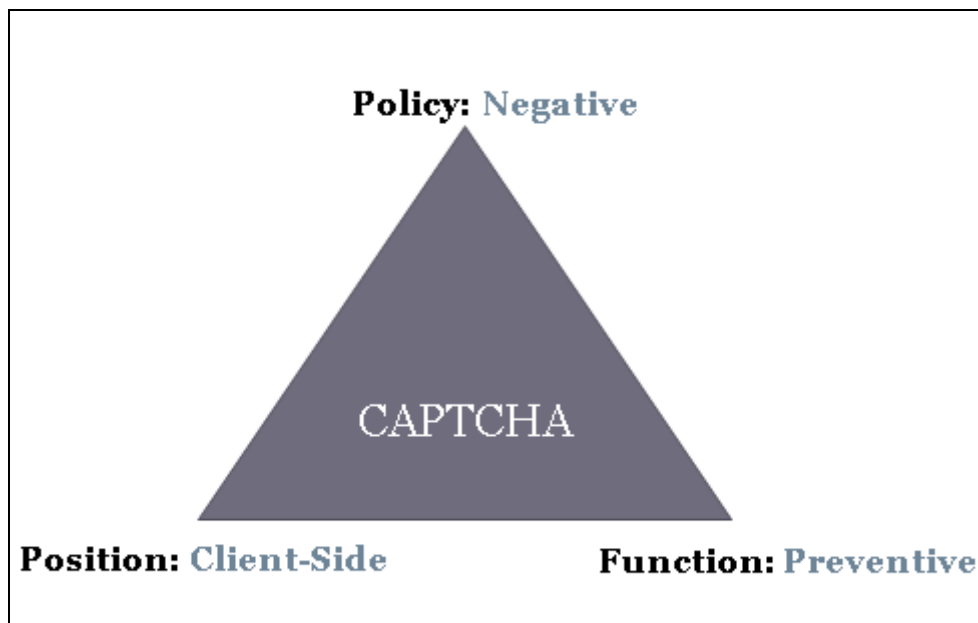
Figure 2. 1: Security Features of CAPTCHA

A CAPTCHA can also be considered as a two rounded authentication protocol.

Round 1: Service ⟶ Client: a CAPTCHA challenge

Round 2: Client ⟶ Service: client response.

Initially CAPTCHAs were employed to protect web forms which were the most common way that users interact with a service. Nowadays, as the interactions between users and services are multiple CAPTCHAs found a lot of applications.

5

2.3. Applications of CAPTCHA in online-services

Many websites use CAPTCHAs, in an attempt to block automated interactions with their sites. These efforts may be crucial to the success of these sites in various ways. Generally, they have several applications for practical security, which include (but are not limited to), the following [5]:

• Preventing comment spam: There are some programs that submit comments in order to raising search engine ranks of some websites or advertisements. Such comments are called comment spam. With the use of CAPTCHAs only humans can post comments in blogs without the need to sign up/in and no legitimate comments are lost.

• Protecting website registration: most of the websites, which have free registration such as email provider services, are the target of bots' attacks that sign up for thousands of email accounts in a minute. One of the effective solutions of this problem is to use CAPTCHAs for ensuring that only humans will have free accounts. In general, free services should be protected by a CAPTCHA in order to prevent abuses by automated scripts. For example, Facebook limits creation of fraudulent profiles used to spam honest users or cheat at games.

• Protecting email addresses: To protect the email addresses posted in clear text from spammers (and screen scraper programs), an effective mechanism is to use CAPTCHAs, specifically reCAPTCHA service, named Mailhide, which helps individuals to protect their email addresses by asking people to solve a reCAPTCHA before viewing the address.

• Online polls: using CAPTCHA is a useful means for holding safe and protected online polls and surveys. The classic example of CAPTCHA's application in this area Slashdot.com's poll in 1999 [8] clearly illustrates threats of this kind. Also, there are other examples in which results of (probably unprotected) polls are influenced by massive automated voting.

• Preventing dictionary attacks: CAPTCHAs can be also used to prevent dictionary attacks in password systems. The idea is to prevent a computer from being able to iterate via the entire space of passwords by requiring it to solve a CAPTCHA after a certain number of unsuccessful logins.

• Securing E-commerce: security is important, but will be crucial when it comes to monetary transactions such as payment processes in E-commerce activities. To provide safety of these processes, users are asked to solve a CAPTCHA prior to clicking the

submit button in payment gateway forms and thus protect their credit cards (accounts) against abuses of bots.

• Interactions of social networks: because of the increasing popularity of social networks (or better to say, social networking sites) among different people, they are turning into potential targets of attackers. Thus, as a preventive strategy, using CAPTCHAs may be advantageous to secure some actions that could be automated such as sending private messages.

2.4. Variation of CAPTCHA Schemes

Since the first introduction of CAPTCHA schemes, many researchers and developers, who adopted the idea, designed and developed many different challenges adding on the initial idea. This caused in having a variation of CAPTCHA scheme types in existing challenges on the web. A presentation of the most known CAPTCHA types is following in this chapter [12].

2.4.1. Text Recognition CAPTCHA

Text Recognition CAPTCHA was the first type introduced and was mostly used in earlier times.

In text-based CAPTCHA Schemes the user needs to recognize the distorted characters represented in a picture and type the characters in an input text box.
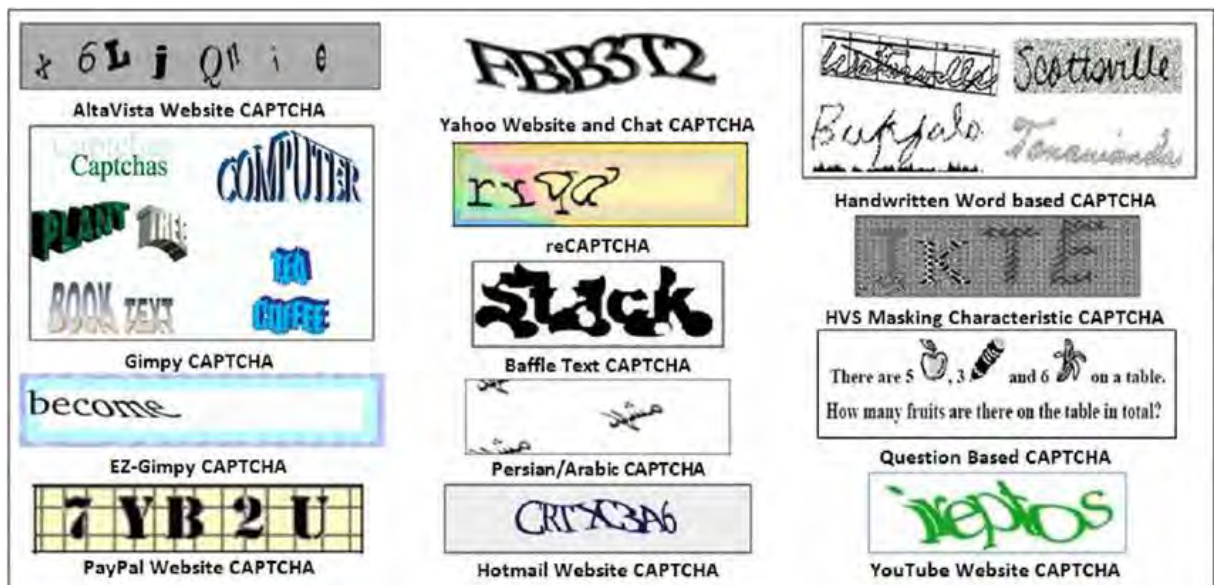
Figure 3. 1: Text-based CAPTCHA Schemes used from well-known online services

Although the characters are distorted enough, making it difficult, not only for automated software but also for humans to recognize, machine learning algorithms (OCR-Optical Character Recognition) have become accurate enough and can easily breaks text-based CAPTCHAs. Many researches took place in order to increase the security and defend machine learning attacks. Some studies' proposals to increase security are the following:

- Random length and font size of text
- Rotate characters in a wave fashion
- Use lines in same width and color as characters
- Collapse the characters
- Use multiple fonts
- Noisy Background
- 3D characters

By adding those security meters in text-based CAPTCHA the task become less vulnerable to attacks. But what happens with task's usability and user experience?

Increasing security decreases task's transparency towards the user. The task might be obtrusive and frustrate the user, whose primary task wasn't to solve CAPTCHA challenges.

In order to combine security and usability in a balanced way some usability meters need to be introduced also.

Results of usability studies proposed:

- Addition of Reload button
- Text characters used in task are from user's tongue language alphabet
- Add audio CAPTCHA for users with disabilities

Furthermore, usability issues still occur and researchers introduced many alternative types of CAPTCHA Schemes that provide a better balance between security and usability.

2.4.2. Audio Recognition CAPTCHA

To overcome the accessibility problems of text recognition CAPTCHA, audio recognition based CAPTCHA schemes were introduced as an alternative for those

unable to use the more common visual CAPTCHAs. In Audio Recognition CAPTCHA Schemes users are asked to listen to an audio and then type the words that they have listened or a word to describe the context of the audio. Some text-recognition CAPTCHA schemes have adopted the option to give audio recognition CAPTCHA for user with disabilities (ex. people with vision impairments) and for those who prefer to solve audio instead of text CAPTCHA tasks.
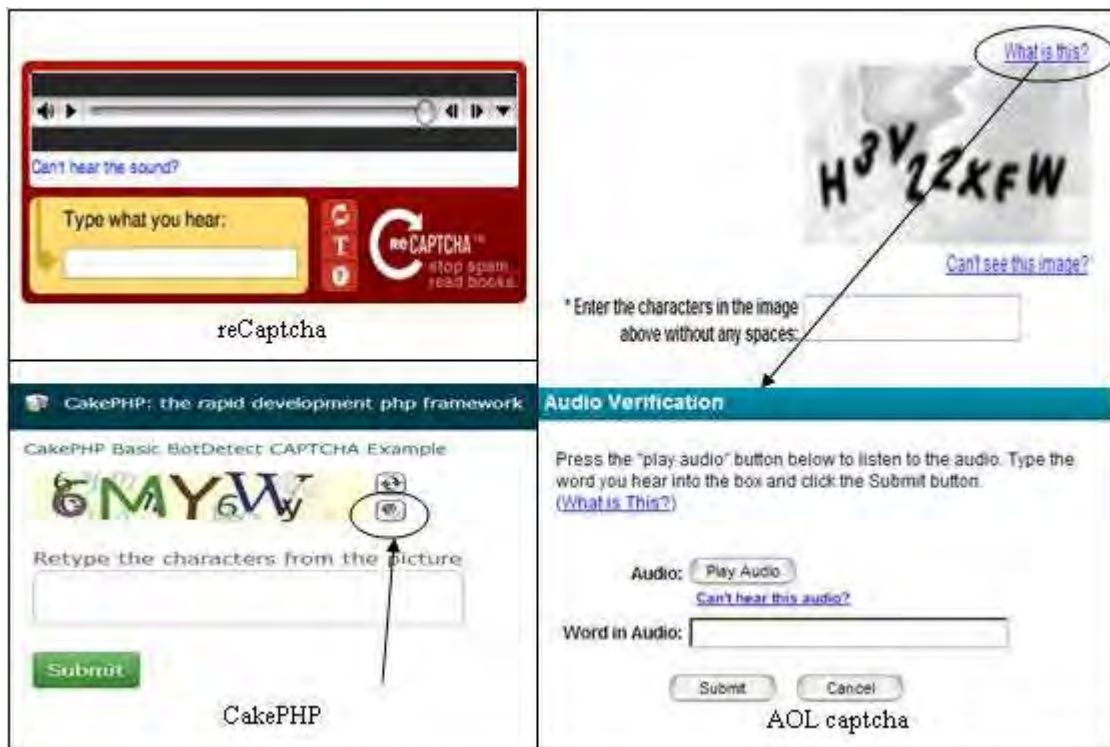
Figure 3. 2: Audio Recognition CAPTCHA Examples

The audio is distorted by adding background noise so machine learning algorithms for audio/speech recognition cannot solve the tasks. The security of such CAPTCHAs depends on the weakness of current audio recognition algorithms to accurately recognize audio when noise is added and the ability of users to do so. The increased distortion of the audio has a negative impact to user performance also, as users cannot easily understand the text and should replay the full audio to understand the previously misunderstood part of it.

2.4.3. Mathematical CAPTCHA

The CAPTCHA task in this category ask user to solve a simple mathematical problem. As for humans, it is really easy to solve the problem a bot is difficult to recognize the

characters and then understand the mathematical equation that needs to be solved and give the solution. Distortion is also added in order to make it even more difficult for bots to recognize the numbers and the symbols. In some systems there were also trials to add more complicated math problems to the task but usability and user performance while solving the problem were badly affected.
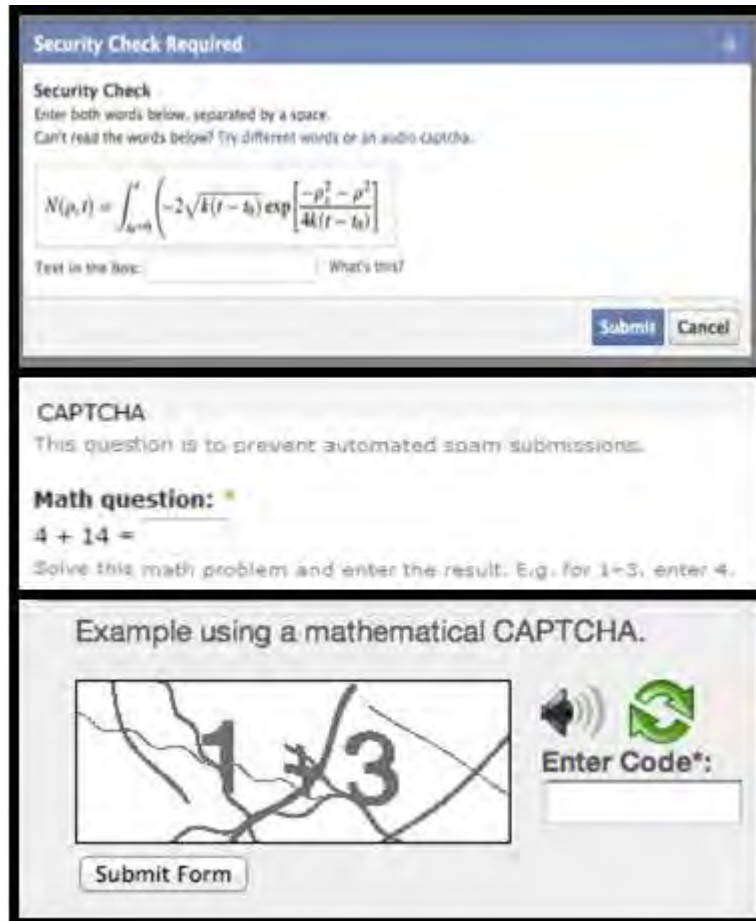
Figure 3. 3: Mathematical CAPTCHA Schemes Examples

The addition of the problem solving and security to the scheme but also the transparency of the CAPTCHA is degraded as the user might be frustrated in solving math problems in order to be able to register to an online-service.

2.4.4. Graphics CAPTCHA:

a) Game Activities CAPTCHA

Since high level of transparency, in CAPTCHA tasks, is difficult to be accomplished researchers invested in making CAPTCHA tasks as enjoyable and unobtrusive as

possible for users. The idea of the implementation of small games and activities in CAPTCHA schemes was introduced. Some existing schemes inspired from this idea are the following:

i. Bongo CAPTCHA:

Bongo is a program that asks the user to solve a visual pattern recognition problem. In particular, Bongo displays two series of blocks, the left and the right series. The blocks in the left series differ from those in the right, and the user must find the characteristic that sets the two series apart. An example is shown below:
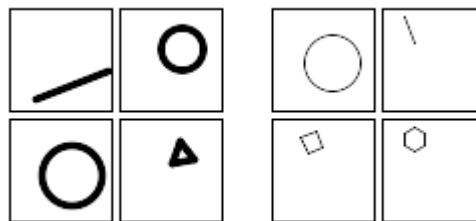
Figure 3. 4: Bongo CAPTCHA: These two series are different because everything in the left is drawn with thick lines, while everything in the right is drawn with thin lines.

After looking the two series of blocks, the user is presented with four single blocks and is asked to determine whether each block belongs to the right series or to the left. The user passes the test if he or she correctly determines the side to which all the four blocks belong.

ii. Are you Human:

Test whether you are human or not by playing games. This is one of the innovative CAPTCHA that uses a game of picking up objects and putting them in right position by dragging and dropping the items.

Figure 3. 5: Are you a Human CAPTCHA

iii. Motion CAPTCHA:

This is an innovative CAPTCHA. MotionCAPTCHA is a jQuery CAPTCHA plugin, based on the HTML5 Canvas Harmony procedural drawing tool by Mr Doob and the $1 Unistroke Gesture Regonizer algorithm (and the more recent Protractor algorithm improvement), requiring users to sketch the shape they see in the canvas in order to submit a form.
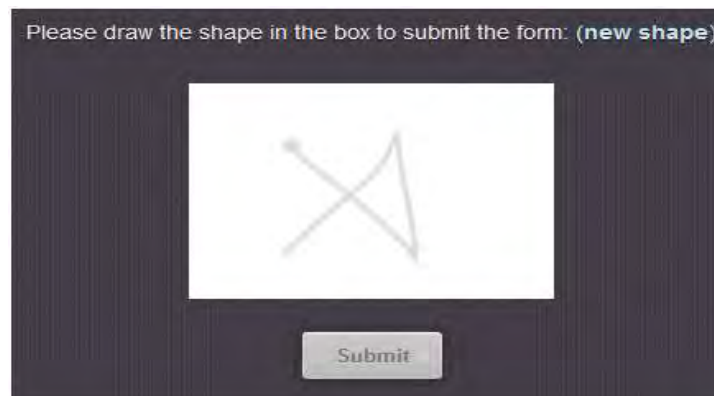
Figure 3. 6: MotionCAPTCHA Scheme Example

iv. Tic Tac Toe CAPTCHA

A very common game "Tic Ta.c Toe" is used in the CAPTCHA task. The user is asked to add a "X" to make three "X" in a row. This CAPTCHA which involve gamification was design for a fun and easy way to prove that the user is human. As the user gives the correct answer the system confirms that the user is not a bot. Being such an easy CAPTCHA to be solved security issues appear. As you can see the possible solutions given by the user are four, an automated software has a possibility of 0.25 to randomly

select the correct solution. Tic Tac Toe CAPTCHA is a glaring example that usability and security must equally co-exist in CAPTCHA design.
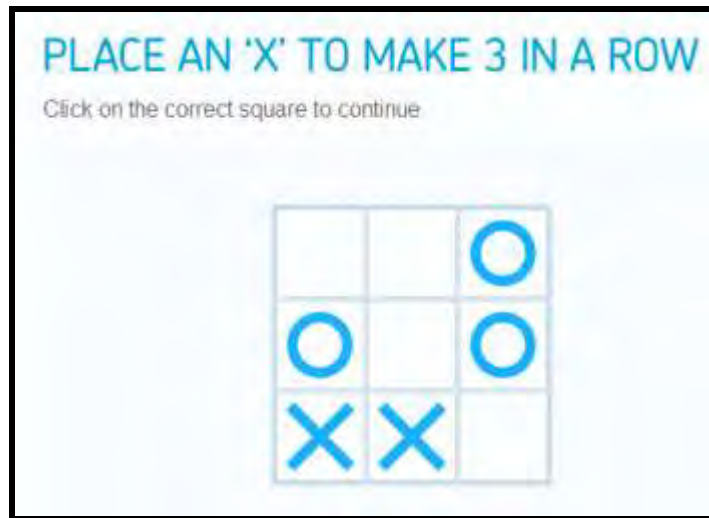
Figure 3. 7: Zero CAPTCHA Task example

v.Sweet CAPTCHA

Sweet CAPTCHA involves asking the user to perform some kind of task where they are moving and matching items to one another. An example is shown in Figure 4.5 where the user should move the worm image to the apple image to verify his/her human identity.

Figure 3. 8: Sweet CAPTCHA Task example

These types of tasks are not something a robot can perform accurately, so it is very efficient at determining a human identity. The con to this type of CAPTCHA might be that it can interfere with user experience. If the user makes a mistake, they will have to perform the task again. This can become frustrating for the user.

b) Image Recognition CAPTCHA

In this type of CAPTCHA the task the user is asked to do is image-based. A number of images are represented to the user and he/she need to follow the instruction to solve the CAPTCHA task. An example of Image Recognition CAPTCHA Scheme is showed in Figure 6. A more detailed analysis on Image Recognition CAPTCHA Schemes follows in Chapter 3.

Figure 3. 9: Google reCAPTCHA Image Recognition task example

2.4.5. Transparent CAPTCHA

(a) Social Media Sign In:

Signing in or signing up to the user' social account (Facebook, Instagram, Google etc.) is used by CAPTCHA as a foolproof way to defend bots to act illegally in online-services. In that way, the only task the user is asked to complete is sign in or sign up with no need of playing games or recognize text, audio or images. Users might be more familiar to sign in to their account than completing all the CAPTCHA Tasks that are mentioned above. Additionally, the security level of the CAPTCHA type is high enough since bots are unable to sign in because they do not have social accounts to use. However promising this CAPTCHA type looks like, it has a major drawback. Users nowadays are hesitant to have all their information linked because of personal

information and security. So the users might be unwilling to sign in or register to an account and just quit on using the online-service. Such an action will harm the online-service provider.

(b) <u>Time-Based:</u>

This type of CAPTCHA records the amount of time it takes a user to fill out their information on a form. If it is a human, it will probably take a bit of time to fill out a form. Bots, on the other hand, will fill out a form almost instantaneously. The advantage is that it is pretty easy to determine whether or not it is a human user or a bot. The downside is that having someone fill out a form every time they want to make a comment, post a message, or perform a task, the user might find this frustrating and time-consuming.

(c) <u>Honeypot:</u>

This type of CAPTCHA involves a bunch of hidden fields on a screen. The interesting part about Honeypot is that it is not the human that is tricked, but the robot. Bots are able to see these fields on the websites, but humans are not. In essence, it tricks the bot into filling out these fields that humans are not able to see. When the bot fills it out, the website knows it is not a true human user. One of the greatest benefits of this type of CAPTCHA is that it is unknown to humans, meaning the user experience is not affected by annoying games or having to input lots of information. There is always the possibility that it won't work with some Bots who are smart enough to know they are being tricked. For example, Safari autofills forms, so the Bots are more likely to get around this. When creating a website, all the developer has to do is add the hidden field, give it any kind of name and use CSS to make a rule "display: none" which will hide it from the human users who are filling out the given form.

(d) <u>No CAPTCHA reCAPTCHA:</u>

The "No CAPTCHA reCAPTCHA" method is a type of CAPTCHA that has been introduced by Google in 2014 and has already made its place on the internet. This

method asks the user to click on a check box indicating "I am not a robot". The CAPTCHA tracks the movement and figures that if the box is clicked directly in the middle, it is a robot.
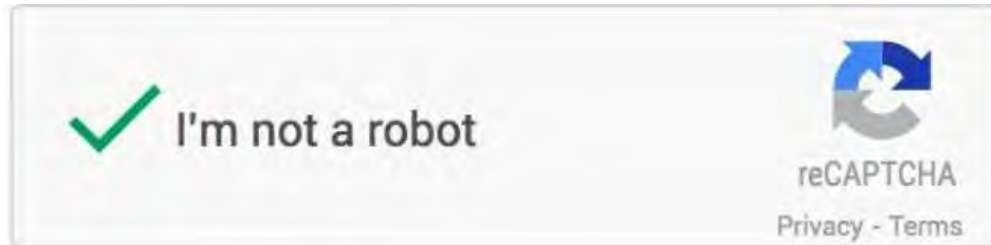
Figure 3. 10: No CAPTCHA reCAPTCHA task

Bots are very methodical, so it is quite easy to determine their behavior. Humans would most likely not click directly in the middle but in some other area of the box. This method has been incredibly accurate. In case this first test fails, there is a backup CAPTCHA task where the user will be asked to solve. The downside is that it can create a frustrating experience for the user if they have to do the test twice.

(e) Invisible reCAPTCHA:

Invisible reCAPTCHA is the new version of No CAPTCHA reCAPTCHA introduced in 2017. To improve the user experience invisible CAPTCHA there is no text or numbers to enter or box to be checked but it does use a method of monitoring user's behavior while they are on the site. The company said that reCAPTCHA works thanks to a combination of machine learning and advanced risk analysis that adapt to new and emerging threats. Google didn't offer more information about how Invisible reCAPTCHA works. But the system probably analyzes things like typing speed, cursor movements, and rate of scrolling to determine whether a visitor is a human or a bot. People type relatively slowly, they rarely move their cursors in straight lines, and usually take their time scrolling through a website. Bots often do the opposite--they look for certain elements and work as quickly as possible. The user is no more frustrated by solving CAPTCHA Task.While it seems to be successful as of now, there is always the chance that robots will eventually adopt humanize behavior and be able to

outsmart it. Moreover, in cases the test isn't sure if the user is a human or a bot it asks user to solve a different type of CAPTCHA to make it sure.

    (f) <u>Biometrics and the future of CAPTCHA:</u>

In our modern era, almost everyone owns a smartphone. New models of smartphones support biometrics such as face recognition, iris scanner, and fingerprint scanner. You can use biometrics as another kind of security feature. While this isn't yet an actual CAPTCHA, it is a very important security feature that could be the future of CAPTCHA. It allows for complete security because everyone has unique fingerprints, iris etc. By using your fingerprint to sign into your phone or an app, it ensures that you are the only one who can get the information needed. This could be something that websites require in the future to complete tasks like sign up for an account, post messages, or making a purchase. It could certainly be beneficial because it would prove a user's identity. A downside could be that users might not be willing to give their biometrics to access an online-service. Although using biometrics as a human proof mechanism looks promising. Accessibility issues still occur for people with disabilities.
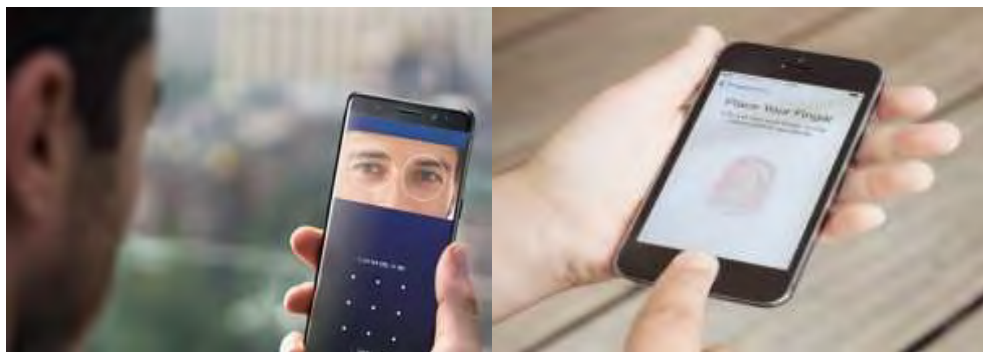
Figure 3. 11: Iris and fingerprint scanners on mobile phone devices

Chapter 3

Background Theory in Image Recognition CAPTCHA Schemes (IRCS)

3.1 Introduction of IRCS

3.2 Methods in selecting and displaying images in IRCS

    3.2.1 Methods in selecting images

    3.2.2 Methods in displaying images

This chapter aims to give a more detailed analysis of Image Recognition CAPTCHA Schemes (IRCS). An introduction about how and why IRCS were first developed and why can act as a Human Proof Mechanism. Furthermore, the different methods of selecting and displaying images are described and existing IRCS are analyzed.

3.1. Introduction of IRCS

As the text-based CAPTCHA schemes were vulnerable to OCR attacks, researchers introduced Image Recognition CAPTCHA Schemes with the argument of the weakness of Computer Vision and Pattern Recognition algorithms in that period of time. Although nowadays these algorithms had been really improved, image recognition CAPTCHA schemes are less vulnerable to machine learning attacks than text based CAPTCHA tasks, especially if the design of the schemes follows specific guidelines which will be analyzed further in this chapter.

Instead of increasing security, studies on IRCS showed to improve user experience as less failed attempts had been recorded in such schemes. Users find solving IRCS more enjoyable and less obtrusive than recognizing distorted characters and typing them afterwards. Also, it looks like is a more friendly mobile-screen mechanism for human interaction proof (HIP).

However, IRCS does not overcome accessibility issues that appear also in text-based CAPTCHA tasks. People with vision problems (e.g. blind people, people with colorblindness etc.) cannot complete the tasks as they are not able to see or recognize the objects and they use screen readers to access the web. IRCS must provide alternative schemes for users with disabilities, such as audio recognition CAPTCHA, in order to be accessible by everyone.

In Image Recognition CAPTCHA Schemes, a number of images are represented to the user and then the user is asked to do a specific task based on these images. The typical task that was first introduced was to choose the images that represent a specific object. In the progress of time, new types of tasks were introduced as more and more researchers and developers got interested in the new category of Human Interaction Proof.

3.2. Methods in selecting and displaying images in IRCS

(a) Methods in selecting images

The selection of the images to be displayed in the task is done by using one of the following models:

- Database Model:

In this model, a huge number of images are collected from the internet and other sources. To display the CAPTCHA task, a number of images are selected randomly

This model's pros are that the images can be selected beforehand, carefully to be high quality images so the content can be clear for the user to identify. So, possible problems like mislabeling and low quality images are eliminated. Furthermore, as the images are chosen and stored beforehand this model is time efficient in CAPTCHA generation. It doesn't require long time to retrieve and load the images from the database as suitably designed hashing functions could be employed. By decreasing the load time of images the user-friendliness of the task is increased. In the other hand, this model suffers from the high cost of updating that huge database. Updating such a big database can be a time consuming process since its picture need to be labeled manually or in an automated mean. Additionally, the maintenance's cost of that type of databases may become too high and unacceptable.

- On-the-fly Model:

In this model, there is no database to store the images but for a selected name of object, images are searched and selected from the Internet using standard search engines like Google. A number of images that are in search results are selected and displayed in the CAPTCHA.

The dynamically obtained images from the web eliminate the costs associated with the storage and maintenance of a database. Moreover, since the web content is updated and changed dynamically so the images are used in the task are not constant but new images might been displayed. This act as a defense to Pictionary Attacks that will be defined later in this chapter, but if the website attracts high amount of traffic, pictures may start repeating themselves. This is because search engines only provide limited search results (1000 for Google). This may assist the hacker in breaking the picture CAPTCHA. However, this model also has its drawbacks. Since the images are searched and then selected from online resources, the loading time of the images is increased and that has a negative effect in user experience. Also, images that are searched and chosen from the web might not match completely with their object. This is the problem of Internet's mislabeled images and this might ends up in user confusion while solving CAPTCHA tasks. Users in that occasion can be frustrated and give up on using the online-service.

(b) Methods in displaying images in IRCS:

Existing IRCS differs in the method that the images are been displayed. Some of the methods that are used are:

- One Segmented Image:

By using this method, the CAPTCHA challenge displays just one image segmented in equal smaller pieces. Each piece of image is located in a grid in the right sequence in order to make the user see the initial image but each piece is in a different block. Usually in this method the user must choose all the blocks that contain a certain object. In the design of such tasks the space between the blocks must be quite small so the user can see the image as it is not segmented. Users sometimes are confused because a small part of the object that need to be identified might located also in the next block and that makes users not being sure if the next block need to be selected or not.

- A grid of several images:

This is a very common method used in existing IRCS. A grid of several different images is displayed in the task. Each image represents a different object and the user

need to select the object the task asks for. Most of the times the content of the image is clear and easy for the user to identify making this method to be considered as a user friendly method, but also Image Recognition Algorithms can identify more easily the content which making this method attack prone. Many image transformations are introduced to harden Image Recognition Attacks.

- A collage of several images:

This method is not used very often as the process to prepare the image must cost in time terms. An automated tool chooses several images from a database or with the on-fly method. Afterwards, it makes a collage of those images and optionally transforms or edits them. This method is introduced to improve the security aspect of IRCS, but studies showed poor performance in usability as the image is getting more complex and is obtrusive against user.

Chapter 4

Background Theory in Cognitive Skills and Styles

4.1 Introduction in Cognitive Skills and Styles

4.2 Cognitive Skills and Styles analyzed and used in this thesis

    4.2.1 Field Dependent/Independent

    4.2.2 Processing Speed Ability

    4.2.3 Visual Working Memory Capacity

4.3 Cognitive Skills and CAPTCHA

In this chapter, a short overview about the background theory in cognitive skills is given in order to understand the related terms that are used in this thesis. The three cognitive skills that have been examined in the scope of the thesis are explained and the

corresponded tests to measure these skills are presented. In the end of this chapter, it is explained how cognitive skills can be used in the context of CAPTCHAs.

4.1. Introduction in Cognitive Skills and Styles

Cognition is "the mental action or process of acquiring knowledge and understanding through thought, experience and the senses" based on the English definition of the word in Oxford Dictionary. This term includes many intellectual functions or processes such as attention, the formation of knowledge, memory and working memory, judgment and evaluation, reasoning and "computation", problem solving and decision making, comprehension and production of language.

Cognitive skills refer to mental activities that an individual performs associated with learning and problem solving. Some examples are verbal ability, processing-speed ability, working memory capacity. Each person develops cognitive skills in different levels, since each person get educated and brought up in a different environment. Additionally, cognitive skills are also affected by biological factors such as human's genome and everyone has a capacity for cognitive function since born in order to be able to think and remember.

A combination of different levels of cognitive skills and characteristics identifies several different cognitive styles. A cognitive style characterizes a group of people with similarities in the way of processing, transforming incoming information and categorizing the new knowledge within the memory structure. To define the cognitive style of an individual, psychologists have developed psychometric tests. Those psychometric tests categorize the individuals in different cognitive styles by analyzing the score of the tests.

4.2. Cognitive Skills and Styles analyzed and used in this thesis

In the context of this dissertation Field Dependent-Independent (FD-I) cognitive style, Visual Working Memory Capacity and Processing-speed ability are used to create the cognitive profile of the users of CAPTCHA schemes.

4.2.1. Field Dependence-Independence (FD-I)

A cognitive theory interrelated with the visual behavior is the Field Dependence-Independence (FD-I) theory [3]. In this theory is suggested that individuals have different approaches in recalling, retrieving, processing and storing visual information. Individuals are categorized either as Field Dependent (FD) or Field Independent (FI).

Field Dependent individuals tend to have a more holistic approach to process visual information and find it difficult to identify details in a more complex background. Additionally, FDs rely on the surrounding perceptual field and experience the environment in a relatively global fashion by conforming to the effects of the context. FD can be also called Holists or Global.

Field Independent (FI) individuals, on the other hand, follows a more analytical approach to process visual information and find no difficulties in separating simple structures from a complex background as they pay a lot of attention to details. Furthermore, FIs can abstract an item from the surrounding field and solve problems that are presented and reorganized in different fields. An FI individual can also be called Analyst.

FI and FD individuals are shown to have differences in visual behavior. A metric that is used to observe visual behavior is fixation number and fixation duration in a certain AOI (Area of Interest). Fixations are one of the basic eye-movements, and they occur while individuals' eyes are kept aligned with the target for certain duration, allowing for the visual scene details to be processed. The number of fixations metric is the total number of fixations of an individual within each AOI, considering visits and revisits to the AOI.

Group Embedded Figures Test (GEFT):

To differentiate an individual in FD-I cognitive style Group Embedded Figures Test (GEFT) was constructed by Herman A Witkin, Philip K. Oltman, Evelyn Raskin, and Stephen A. Karp. GEFT is the original classification FD-I tool and a "paper and pencil" instrument, which measures the ability of individuals to separate an outline figure in a more complex figure. The test consists three sections; the first section is a 3 minute practice in order to make the user familiar with the task and its results are not included in the final score. The second and the third part are the actual tasks that are included in

the score and each one takes 5 minutes to complete. The individual needs to detect as much figures as he/she is able to, in the given amount of time. The correct answers of the second and third sections are summed up to provide a raw score in a range of 0-18. Individuals are classified as FD or FI by using a cut-off score.

4.2.2. Processing-Speed Ability

The speed of processing is a cognitive ability that refers to the efficiency of an individual's maximum speed in executing a given mental act. It is also related to the speed in which a person can understand and react to given information. Literally, processing speed is the time between receiving and responding to a stimulus. Some people have enhanced processing-speed that means that they can react to mental activities faster than people with moderate or low processing speed.

Μπλέ
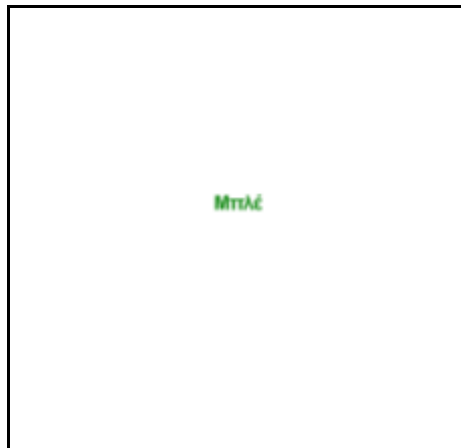
Figure 4. 1: SCWT capture: the individual needs to answer "green"

Stroop Color and Word Test (SCWT):

A psychological test that is commonly used to measure the processing-ability is the Stroop Color and Word Test (SCWT) introduced by Stroop J.R. (1935). This test consists of 18 words, one word appears each time. The word can be either the word "green", "red" or "blue" but colored in a different color form the following colors {green, red, blue}. The user who is taking the test must pay attention to the color of the words ink and not in the color written in the word. For example, if the word "red" is written in blue ink the user must answer "blue". It is important for the user to answer as fast as possible because the test wants to capture how quickly and correctly the user reacts and gives the answer.

4.2.3. Visual Working Memory Capacity (VWMC)

Visual Working Memory Capacity defines the maximum amount of visual information the mind can efficiently activate during information processing. When human brain is exposed to visual information each individual has a limited capacity of the information she/he can store while processing this visual information. Some people can keep more visual information than others.
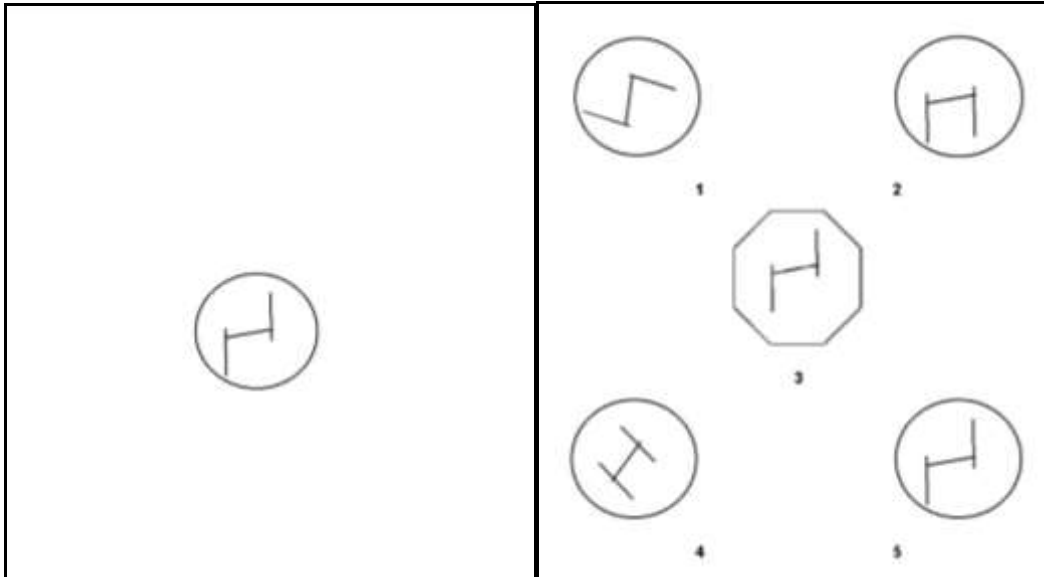
Figure 4. 2: A capture of VWM test: the individual needs to select figure 5

Visual Working Memory Capacity Elicitation Test:

To measure VWMC the following psychometric test is used. A geometrical figure is illustrated on the screen for some seconds and then disappears. At this time five different geometrical figures are appeared on screen labeled with a number. The participant must give the number (through the keyboard) of the figure that was initially illustrated on the screen. Total 21 figures are showed, seven levels of three trials each. As the participant gives right answers, the test provides more complex figures indicating enhanced working memory capacity. If the participant gives continuously wrong answer the test stops.

4.3. Cognitive Skills and CAPTCHA

Taking into consideration human cognitive skills can be a fruitful addition in CAPTCHA schemes' design and development. There are two dimensions of CAPTCHA schemes where cognitive skills can be applied. The first one is to improve

the security aspect of the scheme. Designing and developing challenges which requires human cognitive abilities to find a solution increase the security of such schemes since automated software programs are not able yet to mimic human cognitive behavior. Secondly, the CAPTCHA schemes can get personalized and be adaptive based on the user's cognitive styles and skills. By following this approach, CAPTCHA challenges 'usability is expected to get improved as the users will deal with challenges related to their skills and abilities. The user experience and the user preference are also expected to be improved. In this thesis the second dimension is going to be studied further.

Chapter 5

Related Work

5.1 Analysis of existing IRCS

5.2 Design and Implementation Recommendations for IRCS

     5.2.1 Recommendations in usability aspect

     5.2.2 Recommendations in security aspect

     5.2.3 Recommendations in accessibility aspect

5.3 Personalization and CAPTCHAs

In this chapter prior work in IRCS is presented by presenting and analyzing existing IRCS. Then, design and implementation recommendations extracted from the analysis of IRCS and other sources are given in the aspect of usability, security and accessibility. In the end of Chapter 5, it is explained how personalization can be adapted in CAPTCHA schemes and prior studies in that field.

5.1.   Analysis of existing IRCS

There are several existing Image Recognition CAPTCHA Schemes. A brief presentation of IRCS is following in this sub-chapter [1]:

a) KittenAuth

KittenAuth is a very common IRCS which present to the user a number of animal pictures and ask him/her to select all pictures of a specific animal species. An example is shown in figure 4.3.1.

A very small image database is used, which contains only 84 images. A simple random guess has 1 chance of succeeding out of 84. If enough time is provided, an automated software can easily pass the challenge by executing random guess attack. To increase security, the number of valid images must increase and also the number of images in database should increase. However, if the database is not large enough and dynamic, the attacker can build an identical copy of the database and manually classify the images and so KittenAuth can be attacked. Even after enlarging and dynamically change the database, the lack of image transformation (by distorting the image) decreases the security of this scheme.
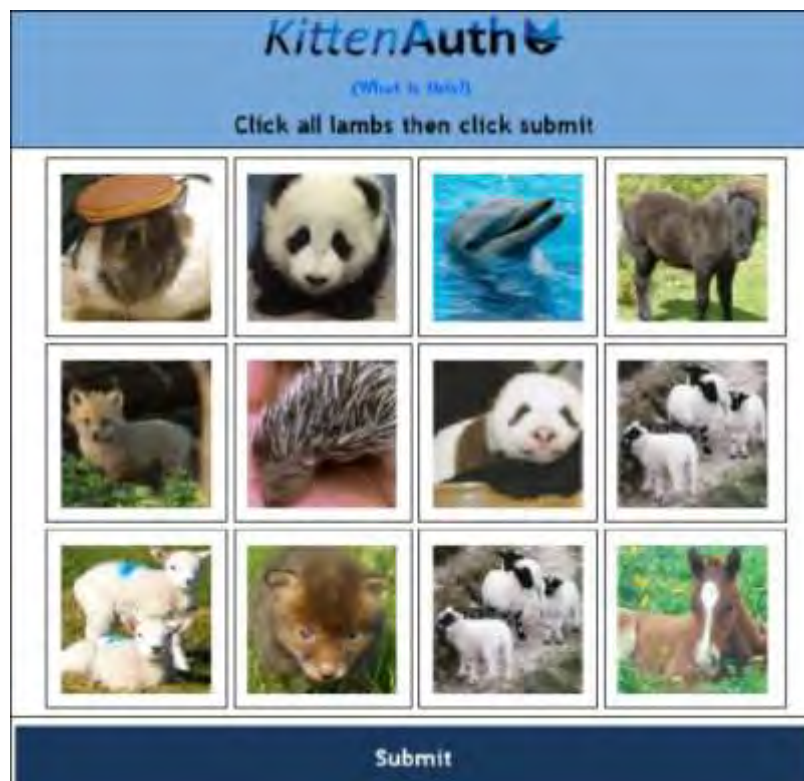
Figure 5. 1: Kitten Auth example the user must select all images with lambs in order to solve the CAPTCHA

a) ESP-PIX

27

Von Ahn et al, initially proposed a HIP test called "PIX" on the original CAPTCHA Project's Web site but it is known as "ESP-PIX". This challenge is randomly selecting four images from a specific category from a large database of labelled pictures. The four images are randomly distorted and presented to the user and ask "What are these pictures of?" offering multiple options to choose from a drop down list. The crucial step in ESP-PIX is the distortion of the images. The database is publicly available and attackers are a step away of solving the challenge by a simple search in database for the images that are shown to reveal the label. The benefit of the distortion is that it makes it difficult for malware to find a match searching the database.

Figure 5. 2: An example of ESP-PIX CAPTCHA .Four pictures showing cats are displayed and, to pass the test, a user has to select the option "cat" from the drop-down menu.

b) Asirra

ASIRRA was introduced by Microsoft and its acronym stands for "Animal Species Image Recognition for Restricting Access". It uses a similar approach with KittenAuth but using a giant database of more than 3 million photos which is obtained through a partnership with Petfinder.com, a website devoted to finding homes for homeless pets, with a daily addition of around 10,000 more pics. The database is not fully public, since only 10% of it is openly accessible through Petfinder's public interface. Asirra displays 12 images from the database (mostly composed of dogs or cats images) and asks the user to select the cats in it. As it is using Petfinder.com web service, it provides a link for adopting each pet, promoting the aim of Petfinder.com of finding new pet owners. An example of Asirra test is shown in Figure 5.3.

The argument of Microsoft for the security of Assira was that it is difficult to achieve classification accuracy better than 60% in recognizing cats from dogs, without a significant advance in the state of the art of current computer vision techniques. Under this assumption, the probability to solve an Asirra HIP with the random guess attack is 0.2%.

However, a recent study on the security of Asirra pointed out that an improved classifier, with an accuracy of 82.7%, can solve the HIP with a probability of 10.3% .Such a value is considerably higher than the probability estimated when the random guess attack is executed and can pose a serious threat to Asirra.

Also the lack of distorting images is affecting the security of Asirra but increase its usability. In order to achieve a better user experience, PCA (Partial Credit Algorithm) is introduced. PCA give a second chance to users that have correctly selected 11 of the 12 images, to solve another Asirra test. If the user solve the second test, then the user is verified as a human. On the other hand, while CPA makes the scheme more usable for humans to solve Asirra, it also considerably increases the probability of success of the classifier presented in to 38%. This fact discourages the use of PCA, since it considerably weakens Asirra. Despite such issues, Asirra can be considered relatively effective in performing human–machine discrimination.

Figure 5. 3: Asirra's example test, the user should choose all images that contains cats

c) IMAGINATION

This is another image recognition CAPTCHA task that was developed to defend the vulnerabilities of the existing IRCS. The name was generated from the following phrase "IMAge Generation for INternet AuthenticaTION".It is an interesting image-based CAPTCHA that breaks the test into two parts. The CAPTCHA challenge system uses a database of simple images and a user interface which generates the test for the user. The first part of the test presents a composite picture that contains a sequence of 8 sub-images different in size, as it is showed in Figure 5.4. Then the user must click in the center of a specific image.

This part of the test is quite simple for a human to solve, but quite difficult for bots as special effects (e.g. Floyd-Steinberg dithering) are applied to the image with the purpose to soften images' boundaries.

In the second part, the image that the user was told to select before is displayed enlarged and distorted. The user is asked to choose from a drop down list a word that describes the image in a similar motion of ESP-PIX.

Figure 5. 4: An example of IMAGINATION images. On the left is the image for the first part of the test and on the right is the image for the second part of the test.

IMAGINATION has taken into consideration the security aspect and appears to be quite effective. But usability issues still occurs since the user need to solve two distinct challenges increasing the possibility of failing in correctly solving the CAPTCHA. Additionally the screen space that the CAPTCHA task covers to be displayed is quite large, a CAPTCHA task is not the main task that the user wants to reach in a service and must be as transparent as possible.

d) <u>ARTiFACIAL</u>

Another existing IRCS is ARTiFACIAL and its acronym stands for Automated Reverse Turing test using FACIAL features. The success on telling whether a user is a human or a computer depends on the superior ability of human being in recognizing human faces from images that has been edited and transformed. The transformation of the image is being achieved by applying extreme lighting conditions, shading, distortions, occlusions or cluttered background on image. This transformation makes it difficult for face recognition algorithms to solve the CAPTCHA.

Figure 5. 5: Example of an ARTiFACIAL challenge

This scheme, showed in Figure 5.5, challenge the user to click on 6 spots of an automatically synthesized and distorted image showing multiple human faces. More specifically it asks the user to click on 4 eyes' corners and 2 mouth corners of a human face.

Human faces that are shown in the image, are applied with several different transformations (e.g. translation, rotation, and scaling of the head) generated from a 3D wired model of a generic head.

A usability test conducted , claims that the 99.7% of users could complete the test in an average of 14 s. However, the requirement to identify 6 different points on the image contributes to increase the probability of failure.

<u>f)EasyPIC and MosaHIP</u>

"EasyPic" and "MosaHIP" are two HIPs based on the human ability to recognize a generic object displayed by a picture and were used in downloading resources services. EasyPic is using drag-and-drop approach. It asks the user to drag the resource he/she needs to download and drop it on a specific object-image from a number of different images. If the resource is dropped on the right image the challenge is solved and the resource can be downloaded. Otherwise a new challenge is generated with a double number of images (different from the previous).An example of EasyPic is shown in figure 5.6.

Figure 5. 6:

a. Example of EasyPic challenge with four images.

b. Example of EasyPic challenge with eight images, after incorrect solution given in (a).

After two failed attempts (where the number of images becomes 8) the test fails and the user is considered as a computer and cannot download the resources.

In order to harden the attempts of image matching algorithms to attack the scheme, transformations (as resize, rotation, flipping, controlled distortion, and dynamic shade modification of image pixels) take place on the images that are selected for the challenge.

MosaHIP, an acronym for Mosaic-based Human Interactive Proof, is an image-based CAPTCHA, which improves the EasyPIC scheme from the point of view of both security and usability. The fact that the image database of EasyPic, is public affects the

security of the scheme. MosaHIP uses virtually any large collection of images to create a database of pictures, without the need of executing a time-consuming and not often precise categorization process. MosaHIP exploits the current computer's difficulty in performing three specific vision-related activities: image segmentation in presence of complex background; recognition of specific concepts from background clutter; and shape-matching when specific transformations are applied to pictures. This CAPTCHA challenges the user with a single large image (mosaic image) composed by smaller and partially overlapping pictures.

Figure 5. 7:

a. MosaHIP's content based version example. The resource must be dragged and dropped on the pineapple image.

b.MosaHIP's "topmost" version example. The resource must be dragged and dropped on the scissors image.

To solve the challenge the user needs to use the drag and drop approach. The user must

identify an image, drag the resource that he/she wants to be downloaded and drop it on the image identified before. There are two different versions of this scheme.

One version is similar with the EasyPic, the user needs to identify an image that contains a specific object and it's called "content-based". This version is shown in figure 5.7.a.

The other version asks the user to identify the image that is lying upon all the other images and it is named "topmost". This version is shown in figure 5.7.b.

The difference of the two versions is that in the topmost version no image categorization needs to be done in the image-selection-database. The benefits of this version are that no time is wasted in image classification and also any existing virtually large image database can be used to generate the image needed for the task. MosaHIP topmost version introduced a new method which overcomes the problem of classification process of images, polysemy, mislabeling but studies showed that only 80% of participants solve the challenge correctly with the topmost version, whilst 98% of participants solve the challenge correctly in the content-based version, this makes topmost version to be poor in usability.

5.2.   Design and Implementation Recommendations for IRCS

When designing an IRCS there are a lot of factors that must be under consideration. The scheme should combine both usability and security. A scheme which suffers in usability is not going to be chosen from online-service providers since they are looking for a HIP mechanism that won't frustrate their clients. On the other hand, IRCS must insist on security, the schemes that do not use security mechanisms are not worthy of trust as they are vulnerable in attacks. Moreover, Web accessibility aims at enabling all users to have equal access to information and functionalities on the web. More specifically, Web accessibility means that people with all abilities and disabilities can perceive, understand, navigate, and interact with the Web. Since IRCS are used in web services must comply with accessibility rules. Recommendations in the design of IRCS that have been proposed in research studies or have been used in existing schemes are presented by categorizing them in the aspect of usability, security and accessibility.

5.2.1. Design and Implementation Recommendations in Usability aspect

a) Reload Button:

As the user is asked to solve an image-based CAPTCHA challenge, sometimes the images displayed or the guideline's caption given might not be clear and the user cannot solve it correctly. The user must have the choice to get another CAPTCHA by clicking a reload button. So the addition of a reload button on the CAPTCHA challenge is crucial for the user not to come to a dead-end when cannot understand a specific challenge which sometimes results in him/her leaving the online-service.

b) Selected Image must differs from an unselected image:

When the user selects an image as a part of the solution of the IRCS, there must be a mechanism to indicate that the image is selected. This can be done either by giving a colored frame or elevating the image that is selected. In this case the user doesn't have to remember what was selected by him before and prevents him from select an image twice.

c) Small space between images in the displaying method "One Segmented Image":

In "One Segmented Image" displaying method [4.2.2], one image is segmented in a number of smaller images. The smaller images must be displayed in a manner which makes the user see the initial image separated in parts but without losing the continuity of the image context. To achieve this, the space between the smaller parts of the image must be the least.

d) One-step challenges:

Many IRCS proposed to have more than one step challenges to increase the security of the schemes. As it mention before, the CAPTCHA challenges must be as transparent as possible to the user experience. By adding more steps in the challenges the time that is required by the user to solve the challenge is getting increased. So it is preferable to keep IRCS as a one-step challenge.

e) Challenge's caption must be explainable:

Physic Language suffers from the polysemy problem, where a word can have different meaning by changing the context that is used. The captions of the challenges must be as clear as possible in order to not lead to misunderstandings.

f) Challenge's caption must be in user's tongue language:

While users need to solve challenges in a foreign language there is always a possibility not to understand a certain word's meaning, resulting in user cannot provide a solution to the test. The usability of the IRCS will be improved if the language given in the caption is in user's tongue language.

5.2.2. Design and Implementation Recommendations in Security aspect

a) Number of images displayed:

In order to increase the security of IRCS towards Image Recognition Algorithms and Brute Force Attacks, the number of images displayed must be large enough to make the solution of the challenge to be computational hard for bots.

b) Image Transformation

As the Image Recognition Algorithms tend to get optimized and efficiently provide results in object detection, the IRCS need to embed image transformation mechanisms on the images displayed to the task. The images must be distorted using one or a combination of the following transformation techniques: translation, rotation, scaling, applying extreme lighting conditions, shading, distortions, occlusions or cluttered background on image, resize, rotation, flipping, controlled distortion, and dynamic shade modification of image pixels.

c) A large database of images:

In order to prevent Image Dictionary Attack the image database of IRCS must be large enough. Some schemes have their image databases public since they follow the

principle that even if someone has the algorithm and the images is still computational hard to solve the challenge. A large number of images in the database is crucial because it decrease the possibility to solve the challenge by using an Image Dictionary.

d) Update images in database:

By frequently updating the images used in the IRCS the possibility of Image Dictionary Attack is decreased. Moreover, using dynamic algorithm to display images in the scheme by using "On-the-fly" mode is a better method to increase security because new images are uploaded frequently.

e) Hide any information of the image in the source code:

Any name, category or else information about the images should not be accessible from the source code. The path of the images for example, cannot contain any information. This can be done manually while creating the image database, changing the path if it contains any information or by using cryptography to encrypt the path.

f) More than one step challenge:

A more than one-step challenge was proposed in many studies. Instead of give one challenge to the user you can give a number of challenges in order to make it more difficult for automated software to give a correctly solution.

g) Use humans cognitive abilities in the challenge and not only object detection:

By giving challenges that finding a solution for; demands the use of human cognitive skills, the bots are more unlikely to solve the challenge and pretend to be human. For example, in MosaHIP IRCS the "topmost" method requires the user to detect the image that is on the top of the rests and select it. This is a task that a human can easily bring to its end but an automated program finds it difficult. Also, a recommendation [6] for IRCS was to display images which follow a sequence and the user needs to select the images following the right sequence. This is a task that demands the use of human cognitive skills and increases the weakness of bots to correctly solve CAPTCHAs. Demanding human cognitive skills in CAPTCHA solutions require more effort from

automated programs, as Image Recognition Algorithms won't be enough to break an IRCS. Pattern Recognition Algorithms should also be used and optimized to break such schemes.

5.2.3. Design and Implementation Recommendations in Accessibility aspect

All the trials that have been in place to make IRCS accessible to people with vision problems or other disabilities drive the schemes to be vulnerable to attacks. The only secure method of IRCS to support accessibility is to give alternative challenges for people with disabilities. An alternative can be Audio Recognition CAPTCHA Mechanism or Social Media Account Log in.

There is a variation of recommendations to improve the usability or the security of IRCS. But the problem appears when recommendations that increase security come into conflict with usability and vice versa. Security and usability are both crucial in IRCS and none of them can be kept aside. The solution to this problem is to find a fair-trade off between security and usability and design and develop schemes that comply with the principles of CAPTCHA schemes.

5.3. Personalization and CAPTCHAs

In the modern word of technology, the term personalization is one of the main web services success' ingredients. "Personalization consists of tailoring a service or a product to accommodate specific individuals, sometimes tied to groups or segments of individuals" based on the term given in Wikipedia. Providing information or services in a way to meet individual's characteristics and context improves user satisfaction, experience and performance in online services. Personalization is mostly used in advertisement and marketing management of social media networks and in recommender systems. Several huge organizations such as Google, Amazon and others have adopted personalization in their services to benefit not only their users but also themselves.

Existing CAPTCHA challenges follow the "one-size-fits-all" approach where all users are provided more-or-less with common challenges, despite their individual characteristics. The idea of the iHIP (Individual Human Interaction Proof) framework proposed in [4], refers to deliver personalized CAPTCHAs challenges. Specifically three categories of factors are introduced to get involved to offer personalized CAPTCHA challenges. Those categories are Technology Factors, Captcha Design Factors and Human Factors.

In technology category, factors that have to do with the user device's type, software, state are involved in personalization mechanism. For example, if a user is using a mobile device is better to provide an image-based CAPTCHA than a text-based.

In CAPTCHA Design category, factors such as usability and security recommendations can be included. For example, for a specific service, a security recommendation might not be as important as in another service to implement.

In Human Factors' category, in which this study is concentrated, the idea is to involve human's characteristics in the design and development of CAPTCHA schemes. In [4], the proposed factors are lingual characteristics, accessibility problems and cognitive differences based on previous researches.

Extending the cognitive differences' factor, in [2] and [3], two studies were in place to determine whether human cognitive differences in information processing affect preferences and performance of CAPTCHA. The first experiment examined if the difference in users' cognitive style (Verbal/Imager) affects the users' performance and the preference towards image-based and text-based CAPTCHA challenges. The second experiment, examines if the level of cognitive abilities (speed of processing, controlled attention and working memory capacity) of an individual affects the performance in CAPTCHA challenges with different complexity levels. The two user studies' experiments conclude in cognitive styles and abilities affecting user's preferences and performance. So the factors examined within the study can get included in the Human Factor's category proposed in [4] to adopt personalization.

The conceptual design of iHIP is shown in Figure 5.8. The combination of Behavioral Interaction, User's Preference, Human, Technology, CAPTCHA Design and other factors consist the Individual Context Model. Based on the individual's characteristics and existing information a User model is built to define the user. This User or Context

39

Model with the Maintain Context Rules given from the provider will be processed in Adaptation Engine to deliver the personalized CAPTCHA challenge to the end user.
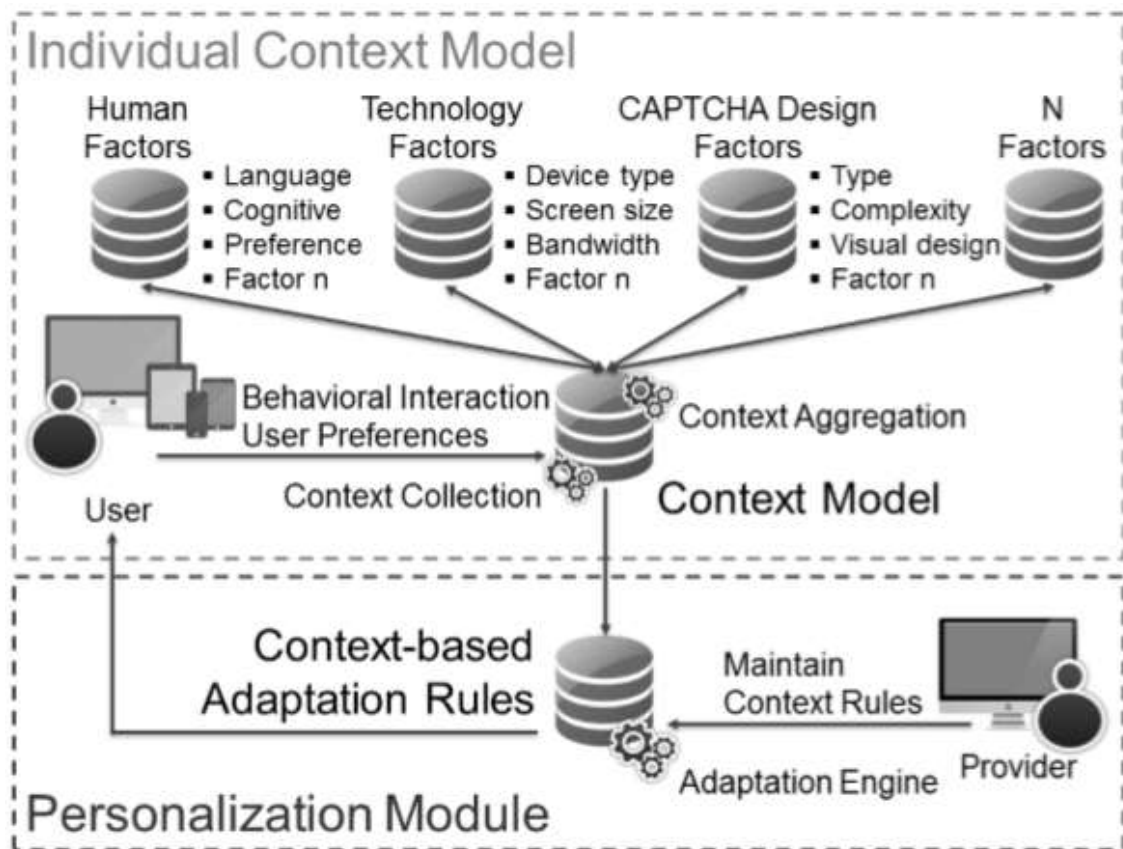
Figure 5. 8: Conceptual Design Scheme of iHIP[4]

In the context of this study, Human Factors and more specifically cognitive styles and abilities with the combination of the users' context and preference are analyzed to extend the Individual Context Model of iHIP to achieve personalization in Image Recognition CAPTCHA Schemes (IRCS).

Chapter 6

Design and Development of Image Recognition Captcha Challenge

---

6.1 Software Technologies:

      6.1.1 Back-end Technologies

      6.1.2 Front-end Technologies

      6.1.3 Gaze Point Eye tracking Software

6.2 Image-based CAPTCHA Challenge Implementation

In chapter 6 the technical aspect of the study is explained. Firstly, the technologies used for the implementation and the study are presented accompanied with the reasons behind choosing them. Then the method of the implementation of Image-based CAPTCHA challenge is described.

5.1. Software Technologies

The software technologies that were used to implement the IRCS challenge for the lab experiment are presented in this sub-chapter.

5.1.1. Back-end Technologies

- **Django Framework**

When it comes to choose a web-development framework there are a lot of things that must be taken into consideration. Each framework has its benefits or its problems. The IRCS challenge for this thesis was developed in Django Framework. Django is an open-source framework for backend-web applications based on Python. The principles of the framework are based on simplicity, flexibility, reliability and scalability. Additionally Django supports the MVC (Model-View-Controller) core architecture. It provides a

"fast and easy" way to develop small web applications as well as big ones. It also priorities security, it helps developers to avoid common security issues such as clickjacking, cross-site scripting and SQL injections as it obliges to take security meters against that problems (e.g. use of CSRF (Cross-Site Request Forgery) token in forms, use Prepared Statements for SQL queries). Moreover, it is a very well-established framework. Django is time and crowd-tested, it has a big and very helpful community and if a problem arises there is always help out here and a way to fix it. Also Django has great documentation [9]; it is maintained and updated on a high level. Many web application developed by huge companies are using Django and any knowledge in using it, is a very nice addition in a developer's CV.

- **Python:**

There is a variety of programming languages for backend in web applications. For the implementation of CAPTCHA challenge in this thesis, Python was selected. Python is a general purpose, interpreted and high-level Object-Oriented programming language. It has a very simple syntax that helps developers complete coding in fewer steps compared with other languages such as PHP. Additionally Python's libraries are so well developed and can be useful for a wide range of applications. Python is a very easy to learn programming language and widely used in development companies. Python's documentation is very well constructed and is getting updated in a frequent manner. As Python is used from a lot of people around the world, a support community is sustained and there is always willingness to provide help to beginners or developers that have problems while programming in Python.

- **PostgreSQL:**

PostgreSQL is a free and open source object-relational database system that uses and extends SQL language. The principles behind PostgreSQL are reliability, data integrity, robustness, extensibility. PostgreSQL runs on all majors operating systems. It is suitable to build either small or big databases with fault-tolerant environments. It tries to conform to the SQL standard by supporting 160 out of 179 mandatory features. The

syntax is quite similar with the SQL syntax and it is very easy to learn, especially when there is a basic knowledge in database systems. Additionally it is very well documented and there is a lot of support since many programmers use PostgreSQL. From administrator view, pgAdmin is an administration and development platform that provide graphical interface and makes it easier for the administrator to create and manage the database. PostgreSQL works well in web application projects developed with Django Framework, there are several tutorials and documentation to connect PostgreSQL database and Python in Django Framework.

5.1.2. Front-end Technologies

- **HTML, CSS , JAVASCRIPT:**

To develop the front-end of the web pages for the CAPTCHA Challenge, a combination of HTML, CSS and JAVASCRIPT was used. HTML (Hypertext Markup Language) is a mark-up language and is used to define the structure of the information in the web page built in a DOM tree. CSS (Cascading Style Sheet) is the language that describes the style of an HTML document; it describes how HTML elements are displayed in the browser. JAVASCRIPT is a run time, scripting language that runs on the client-side. It is mostly used for events handling to improve the interaction between the user and the web page.

- **Image Picker:**

Image Picker is a simple jQuery plugin which upgrades a simple select HTML element into a more user friendly graphical interface. It is used in the development of the CAPTCHA challenge's grid of images. When the user need to solve an IRC challenge, a grid of images is displayed on the screen and he/she must select a number of images. When selecting an image the user must be able to see that this image is selected. This is what Image Picker jQuery plugin does; a colored frame is drawn around the image in order to show that this image is selected. Image Picker is used to improve the usability and the user experience of the user. It was very easy to embed the plugin in this project by following the instructions given in the documentation [11].

- **Material Design:**

Material Design is a visual language which was developed by Google in 2014. It was develop to synthesize the good, classical, designing principles that arise from the innovation in the world of science and design. Material is an adaptable system of guidelines, components, and tools that support the best practices of user interface design. Backed by open-source code, Material streamlines collaboration between designers and developers, and helps teams quickly build beautiful products. Each product that is proposed in Material Design is a result of a material study and the reasons for using a specific product are explained to the developer [10]. By using Material Design in this thesis project, it is claimed that web pages that are developed will provide a better user experience and usability level to the user.

5.1.3. Gaze Point Eye-tracking Technology

Gaze Point Eye-tracking Technology provides a high performance eye-tracking solution. It is affordable equipment for research or commerce purposes and provides high accuracy in data collection. The Gazepoint GP3 HD 150Hz Eye Tracker is used in the lab experiment within this study. Along with the Gaze Point hardware, Gazepoint Analysis UX Edition software, a software package designed for academic and usability research is used to manage data collection and data analysis.

Figure 6. 1: Gaze Point Device

The eye-tracking hardware is shown in Figure 6.1. It is a very easy to set and use equipment since the device is placed below the computer's screen and its orientation is adjusted to the participant's height of eyes. The device must be connected to a computer machine for power supplying and connection to the Gazepoint analysis Software.
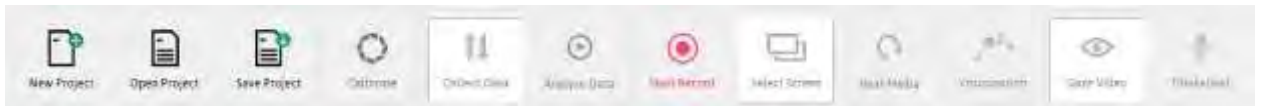
Figure 6. 2: Toolbar's option in data collection

Figure 6. 3: Toolbar's option in data analysis

Managing data collection and data analysis can be executed by using the Gaze Point Analysis Software. Firtstly, the callibration procedure is executed to identify participant's eyes and make sure that device 's mesaurements are right.The toolbar shown in Figure 6.2 represents the options when collecting the data. In collecting data there are two options of recording, the Gaze Video mode or the Thinkaloud mode. In Gaze Video mode,the software recording the computer screen and tracks and visualizes the spots that the participant is looking at within the screen (Figure 6.4), in Thinkaloud mode the voice of the participant is also recorded.
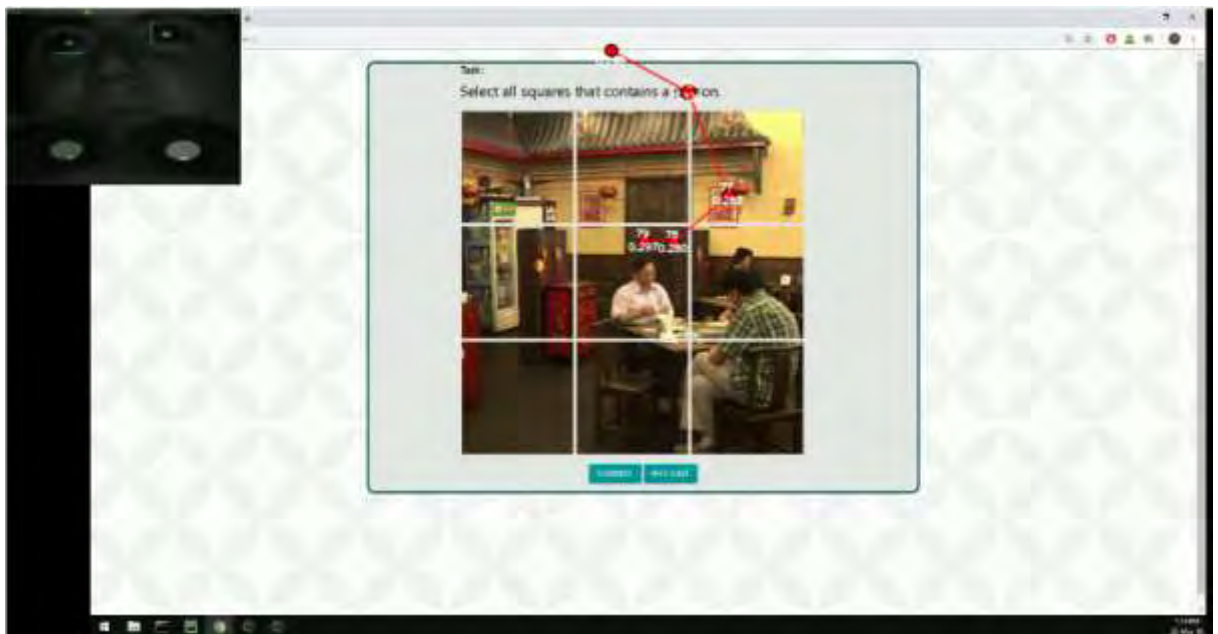
Figure 6. 4: Visualization of participant's gaze

Additionally, there is an option to select the screen that is recorded if an extended screen is connected to the computer machine. The toolbar shown in Figure 6..3

45

represents the options when analysing data. AOI option is the shortcut of Area Of Interest. To analyse a recorded session you can set AOIs. An AOI is a selected by the analyst area of the screen for a specific duration in the stimulus where the following information can be kept :

1. Name – The name you have given the AOI.

2. Viewers – The number of participants who viewed the AOI.

3. 1 st View – The time at which the participant first looked at the AOI.

4. View Time – How long the participant's fixation remained in the AOI.

5. Viewed Time (%) – The percentage of the stimulus duration spent in the AOI.

6. Revisitors – The number of viewers whose gaze revisited the AOI.

 7. Revisits – The total number of times the AOI was revisited.

The AOI list with the information mentioned above is shown in Figure 6.5.

AOI List						
Name	Viewers	1st View [s]	Viewed Tim...	Viewed Time [%]	Revisitors	Revisits
u1_g1	1 / 1	28.89	0.68	0.16	1 / 1	2.0
u1_g2	1 / 1	29.15	0.31	0.07	1 / 1	1.0
u1_g3	1 / 1	31.84	0.36	0.09	0 / 1	0.0
u1_g4	0 / 1	0.00	0.00	0.00	0 / 1	0.0
u1_g5	1 / 1	29.27	2.95	0.69	1 / 1	4.0
u1_g6	1 / 1	32.22	1.28	0.30	1 / 1	2.0
u1_g7	0 / 1	0.00	0.00	0.00	0 / 1	0.0
u1_g8	1 / 1	35.09	1.96	0.46	1 / 1	2.0
u1_g9	1 / 1	34.67	0.68	0.16	0 / 1	0.0

Figure 6. 5: An example of AOI's List

When data Gaze Point analysis is finished there is the option "Export" to export the collected data in .excel or .csv file.

5.2. Image–based CAPTCHA Challenge Implementation

For the purpose of this study an image recognition CAPTCHA challenge was designed and developed. The technologies used for the implementation are mentioned in Chapter 6.1.1, 6.1.2.

As image displaying method, "One segmented image" was selected. The decision to use this method was taken because web users are more likely to have already faced Google's image-based CAPTCHAs (shown in Figure 6.6) where this method is also

applied. In that manner the participants of the study would feel more confident solving the challenge within the lab experiment.

Furthermore, some of the designing and developing recommendations for increasing usability and security of the challenge mentioned in Chapter 5.2 are applied. Nevertheless, accessibility recommendations are not applied as accessibility issues of CAPTCHAs are not examined within this study.

An image is segmented in a grid of 3x3 smaller parts of the image as it is shown in Figure 6.6. Image picker jQuery plugin was used to provide a more user-friendly and interactive interface when selecting an image. The task's instruction is placed above the grid and the submit button is place below the grid.

The participant is asked to select all squares that contain a person in order to solve the challenge and afterwards the participant must click on the submit button to validate his/her solution. If the user gives an incorrect solution, a message is showed to instruct him/her to try again, which is placed near the task's instruction position, an example is shown in Figure 6.7.
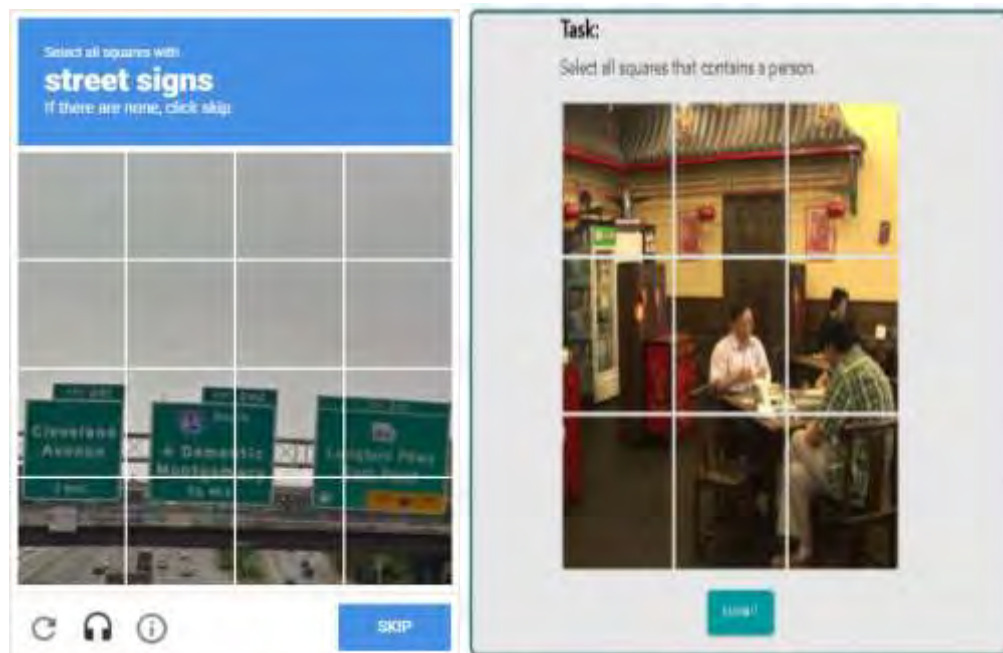
Figure 6. 6: Image recognition based challenge examples. On the right, Google's image-recognition based challenge and on the left the image-recognition based challenge implemented within this study.

Figure 6. 7: Example of challenge interface when user fails in solving the image-based CAPTCHA.

As image selecting method "Database Model" is used. The two images that are used in the challenge were first segmented using an online application that can be found in the following link: https://www.imgonline.com.ua/eng/cut-photo-into-pieces.php. The application accepts as input an image, the number of parts in width and height and the option to cut image into square parts. The output is a zipped file with .jpeg files which are the pieces of the initial image. After the segmentation of the images the .jpeg files are extracted and stored in separate folders. A table with the columns that are shown in Figure 6.8 was created in the database to store the images' information.

category	img_path	index	valid bit
familiar	\static\css\assets\category\familiar_image\image_part_001.jpg	1	0
familiar	\static\css\assets\category\familiar_image\image_part_002.jpg	2	0
familiar	\static\css\assets\category\familiar_image\image_part_003.jpg	3	0
familiar	\static\css\assets\category\familiar_image\image_part_004.jpg	4	0
familiar	\static\css\assets\category\familiar_image\image_part_005.jpg	5	0
familiar	\static\css\assets\category\familiar_image\image_part_006.jpg	6	1
familiar	\static\css\assets\category\familiar_image\image_part_007.jpg	7	1
familiar	\static\css\assets\category\familiar_image\image_part_008.jpg	8	1
familiar	\static\css\assets\category\familiar_image\image_part_009.jpg	9	1
unfamiliar	\static\css\assets\category\unfamiliar_image\image_part_001.jpg	1	0
unfamiliar	\static\css\assets\category\unfamiliar_image\image_part_002.jpg	2	0
unfamiliar	\static\css\assets\category\unfamiliar_image\image_part_003.jpg	3	0
unfamiliar	\static\css\assets\category\unfamiliar_image\image_part_004.jpg	4	0
unfamiliar	\static\css\assets\category\unfamiliar_image\image_part_005.jpg	5	1
unfamiliar	\static\css\assets\category\unfamiliar_image\image_part_006.jpg	6	1
unfamiliar	\static\css\assets\category\unfamiliar_image\image_part_007.jpg	7	0
unfamiliar	\static\css\assets\category\unfamiliar_image\image_part_008.jpg	8	1
unfamiliar	\static\css\assets\category\unfamiliar_image\image_part_009.jpg	9	1

Figure 6. 8:Database table of images that are selected and displayed in the IRCS challenge.

"Category" column contains the category of the image content that is used in the challenge, "img_path" column contains the path where the image is stored, "index" column contains an integer number that defines the order of the image in the grid and "valid_bit" column defines whether a square must be selected to correctly solve the challenge (1) or not (0).

To select the images to be displayed in each challenge the following query is executed in the database:

```
SELECT image_path FROM public.images WHERE category=%s ORDER BY index ASC;
```

Where "%s" is the category of image content that is used in the specific challenge, it can be either "familiar" or "unfamiliar".

To validate the user's solution the following query is executed in the database:

```
SELECT valid FROM public.images WHERE image_path= %s;
```

Where "%s" is the path of one of the selected images. If the returned list of valid bits contains only '1' the solution is considered as correct otherwise is considered as incorrect and the user should give a new solution.

The image recognition challenge that was implemented within this study follows the usability and security recommendations that could fit in it for the purpose of the lab experiment. The recommendation of adding a reload button was purposely not adopted since the images that were displayed in the experiment should be the same for all the users in order to set image as a dependent value in the statistical analysis.

Chapter 7

User Study

This Chapter presents the user study that was conducted within this thesis from its beginning to its end. At first, the idea and hypotheses behind the study are stated. Then the procedure of the lab experiment is explained in detail. How data was collected within the procedure and how the analysis of these data was performed is described to extract the quantitative results. Afterwards, the analysis of the evaluation questionnaire is given to extract the qualitative results. Closing this chapter, the results of the user study are presented.

7.1. Idea and Hypotheses of the study

Influenced by the idea of delivering personalized CAPTCHA schemes and more specifically Image Recognition CAPTCHA schemes, this user study examines the

affection of image content's type in the performance and preference of individuals with different cognitive styles and abilities.

Two different types of image content are used in this study, an image with familiar content and an image with generic content. Since the participants of the study are all Cypriot residents the image with the familiar content selected to be an image of a Cypriot style coffee shop(shown in Figure7.1) and the image with the generic content selected to be an image of a Chinese style coffee shop(shown in Figure 7.2).

Figure 7. 1: Image with familiar content to the participants

Figure 7. 2: Image with a non-familiar content to the participants

Giving an image with familiar content to the user in a CAPTCHA challenge is considered as personalization since different images are displayed for each individual based on what is familiar to the user. In the study the participants solves both of the two CAPTCHA challenges, one with the familiar content image and one with the generic content image.

For both of the challenges performance's metrics are collected and stored in database such as time to complete the task, number of failed attempts. Also Gazepoint Eye-tracking device is used to collect metrics such as total time the image was viewed, fixations' number, revisits' number, average fixations in an image's square. Additionally, the participant's preference on which type of image he/she prefers to be displayed in the challenge is recorded and stored in the database.
 To identify the cognitive styles of the participants 3 tests are used in the study GEFT, visual working memory capacity test and speed of processing test.

The following hypotheses were formulated for the purpose of this study:

H1. Web users would prefer familiar content images to be displayed in IRCS challenges.

H2. FD individuals prefer familiar content images to be displayed in IRCS challenges

H3. FI individuals don't show any preference towards familiar or generic content images that are displayed in IRCS

H4. FI individuals have more active Visual Behavior than FDs while solving IRCS challenges.

H5. Individuals with high working memory capacity have better performance than individuals with low working memory capacity while solving IRCS.

H6. Individuals with fast speed of processing have better performance than individuals with slow speed of processing while solving IRCS.

7.2. Lab Experiment Procedure

A lab experiment had been set up to study the hypotheses mentioned above. Totally 46 participants voluntarily participated in the experiment, 22 of them females and 24 of them males. The user's sample was composed from university students from different study's fields in a range of age between 19 and 27. All the individuals who participated in the experiment had at least the basic knowledge and experience in computer technology, 38 of the 46 participants had solved a CAPTCHA before and 37 of these 38 had solved Image Recognition CAPTCHA challenges before as shown in Figures 7.3 and 7.4. The participants were informed of the experiment's procedure and signed a consent form where they accepted the terms of the study.
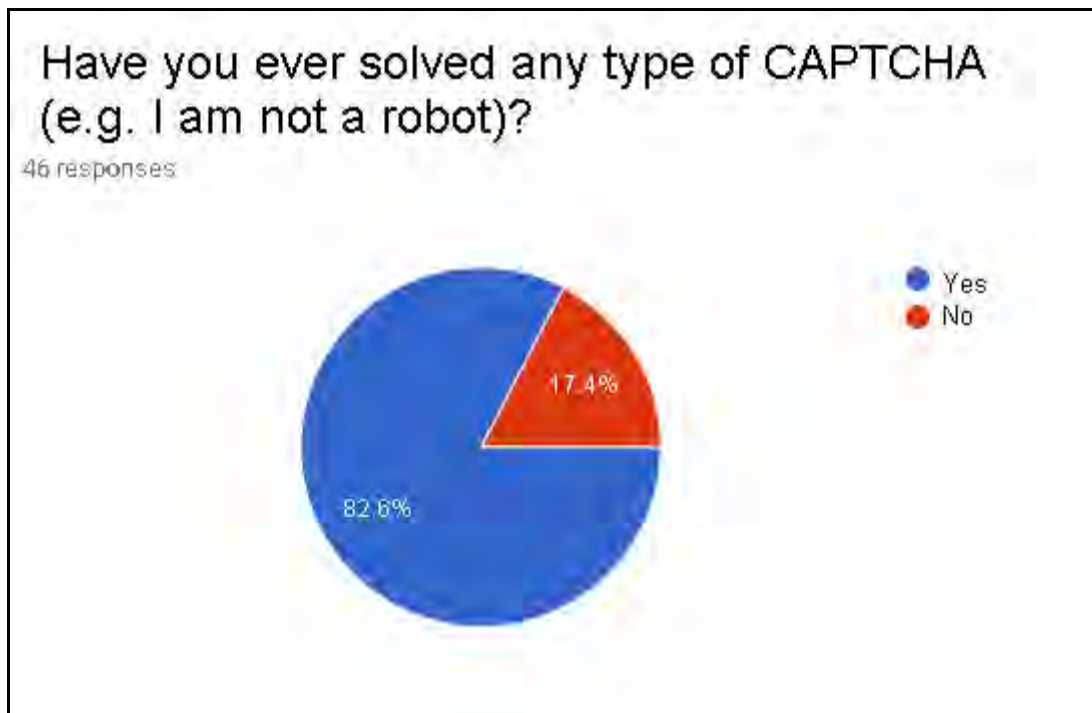
Figure 7. 3: Evaluation Questionnaire Response
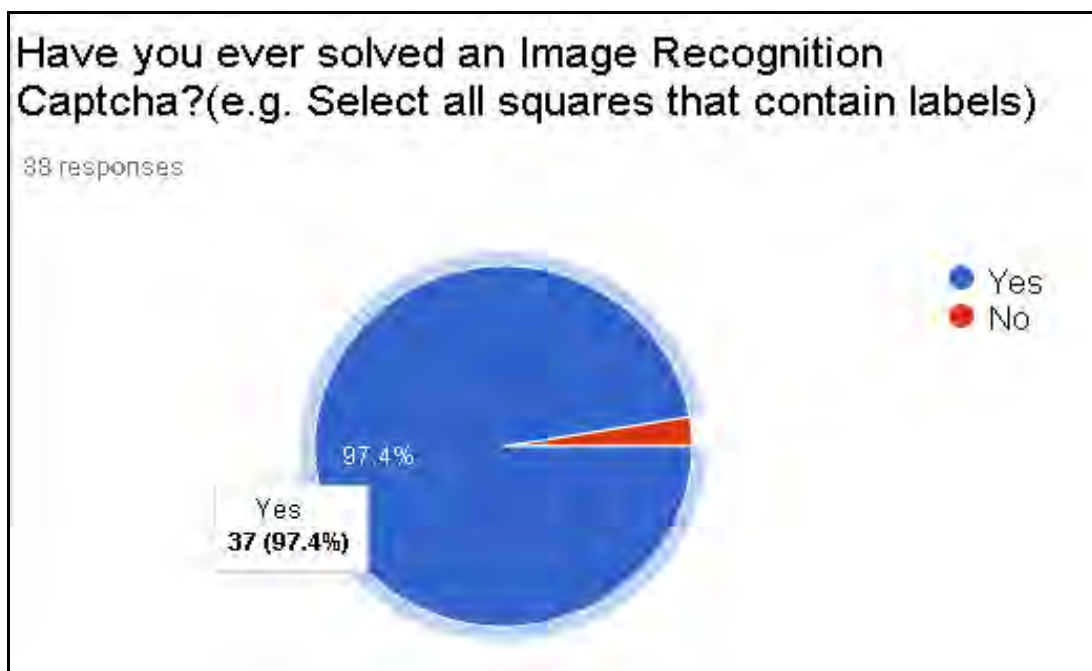

Figure 7. 4: Evaluation Questionnaire Response

The lab experiment duration was 35-40 minutes and was executed in one of Computer Science Department building's lab. The experiment can be divided in two sections. The first section of the experiment could be processed either individually or in a group of individuals, unlike the second part where only one individual could participate at time.

In the first section of the experiment, the participants have the GEFT test mentioned in Chapter 4.2 to identify if the user is Field Dependent or Field Independent. Firstly, the participants get the instructions of how to answer the test and later they are having the test. The GEFT test; as it is composed of three parts of 3 minutes, 5 minutes and 5 minutes respectively and by adding 2-3 minutes for the instruction's time; takes totally 15-16 minutes to complete in case the participant is using all the available time for each part of the test. So in the first section, the task that the participant needs to do is on paper.

In the second section, the experiment is executed with the participant interacting with the computer. The participant takes a comfortably seat in front of the screen in order to be able to use the keyboard and mouse. Since eye-tracking data is collected while the participant is having the experiment, a calibration task must be executed in order to track the eyes of the participants and correctly collect the visual behavior's data. The calibration task takes 2-3 minutes. The participant needs to follow with their eye-gaze the circles that are displayed of the screen and focus in their center. After doing the calibration, the data collection process is started. Calibration task and data collection are done by using Gazepoint Analysis Software mention in Chapter 6.1.3.
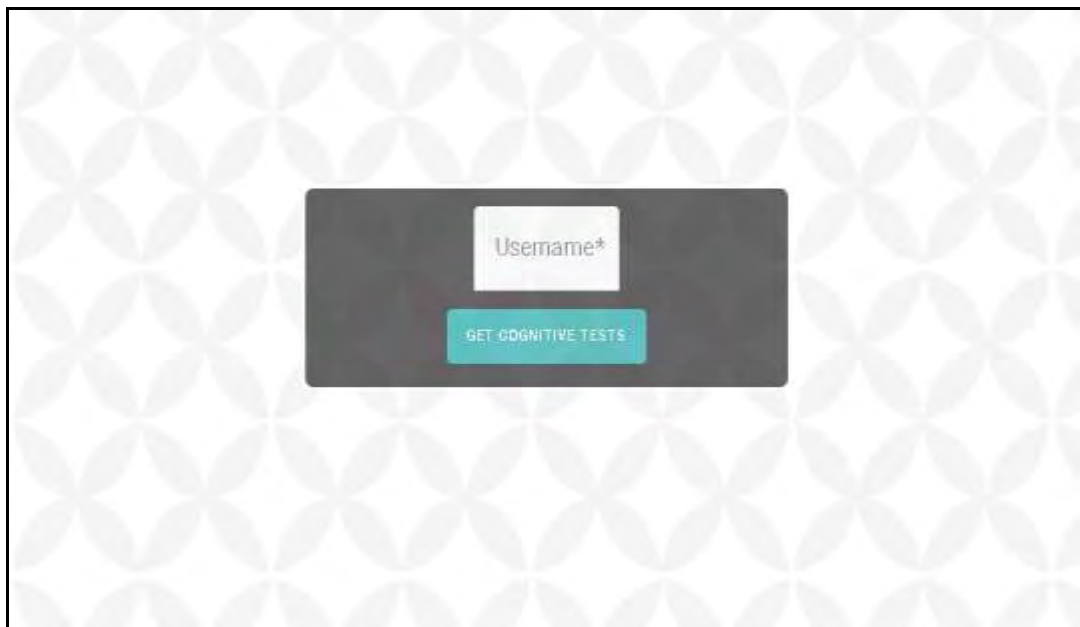

Figure 7. 5: Lab Experiment Login Page Screen

Then, the participant must log in to a webpage with a user name provided to him/her (e.g. "user1"), the login page screen is shown in Figure7.5. After logging in, the user has to choose which one of the two types of images he/she prefers to be used in the Image Recognition CAPTCHA challenge that must solve in the next step. The two options of types that are available are image with familiar content and image with unfamiliar content, the screen with the two options is shown in Figure 7.6.
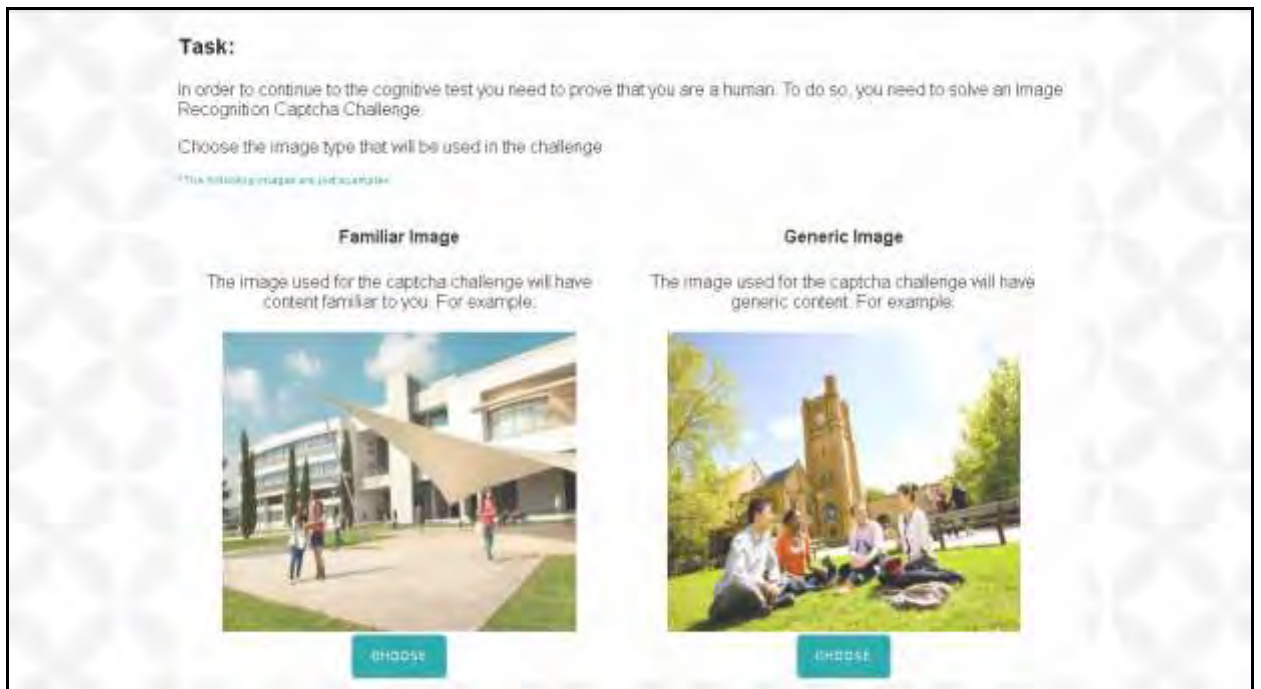
Figure 7. 6: Experiment's Screen of the two options of image's type given to the participant for Image Recognition CAPTCHA challenge

When the participant chooses one of the two types, he/she is led to a new page to solve the image recognition CAPTCHA with the image's type of his/her preference (the one selected before). The image recognition challenge that is used in the experiment is the one mentioned in Chapter 6.2 and its screen is showed in Figure7.7 and Figure7.8.

Figure 7. 7: Image Recognition CAPTCHA challenge with familiar content.

Figure 7. 8: Image Recognition CAPTCHA challenge with generic content.

After correctly solving the challenge the user is led to a web page where there are the instructions that must follow in the next step of the task. The instructions screen is shown in Figure7.9.

Figure 7. 9: Experiment's screen with the instruction to get the cognitive tests

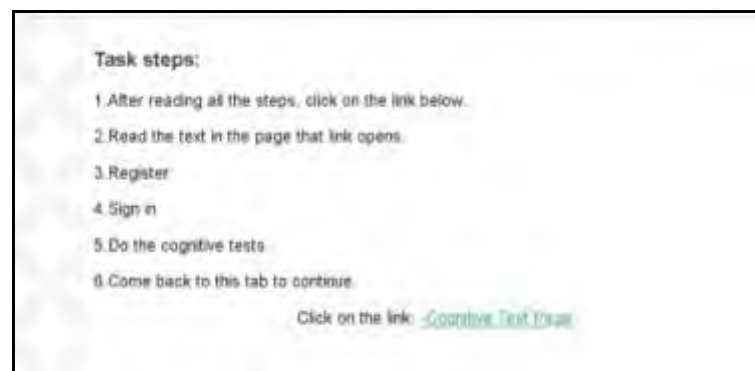When the participant clicks on the link to the "Cognitive Test Page" a new tab opens with the URL: "http://adaptiveweb.cs.ucy.ac.cy/profileConstruction/" which is a web system that provides to its users a number of tests to build their cognitive profile.

The participant must create an account in this system and then take the two tests that are necessary for this experiment. The two tests are the working memory capacity test and the speed of processing test that are described in Chapter 4.2. After completing the tests the user must go back to the previous tab and click continue to solve the image-recognition CAPTCHA challenge with the image's type that he/she hasn't selected before. By solving the second challenge the data collection stops and the user has to answer an online evaluation questionnaire to complete the process of the experiment.

7.3. Data Collection

During the study, the following data was collected: user's preference, user's performance and user's visual behavior metrics.

User's preference in image content type was collected while the participant was choosing familiar or generic image content within the second section of the lab experiment. His/her selection was stored in the database under a column with the name of "preference" after pushing the choose button below each option. User's preference could be either "familiar" or "generic". At the screen with the two options of image content type (shown in Figure 7.6), the order of displaying the two options were randomized to each participant in order not to get the participants to be biased and choose always the first or second option.

Metrics of user's performance were also collected while solving CAPTCHA challenges. The time to solve metric is considered to be the time between the time stamp of CAPTCHA page got loaded and the time stamp the participant click the "Submit" button. Attempt's number metric is the number of the current attempt to solve the challenge which is an increasing number which starts with the value of "1" and get increased after a wrong solution. Failed attempt metric gives the information if an attempt was failed (with the value of "1") or not (with the value of "0"). Captcha category indicates the type of image content of the challenge the metrics are for, as all

participants solve the challenge with both types of image content. In Figure 7.10, task's performance database scheme's table is shown. For each participant, number of failed attempts was calculated based on bigger attempt's number. The time to solve metric that is used in data analysis is the time to complete of the attempt with the correct solution (where "failed attempt" has the value of 0).

	attempt_number integer	time_to_complete character varying	session_id character varying	failed_attempt bit	captcha_category character varying	timestamp character varying	preference character varying
1	1	11.616	user1	0	unfamiliar	2019-03-26 13:13:49....	generic
2	1	8.111	user1	0	familiar	2019-03-26 13:20:05....	generic
3	1	9.699	user2	0	unfamiliar	2019-03-26 14:34:48....	generic
4	1	8.013	user2	0	familiar	2019-03-26 14:42:20....	generic
5	1	2.581	user3	1	familiar	2019-03-26 14:56:50....	familiar
6	2	7.364	user3	0	familiar	2019-03-26 14:56:58....	familiar
7	1	8.628	user3	1	unfamiliar	2019-03-26 15:01:33....	familiar
8	2	8.817	user3	0	unfamiliar	2019-03-26 15:01:43....	familiar

Figure 7. 10: Example of Task performance database scheme's table records.

Metrics of user's visual behavior were collected by using Gazepoint Technology described in Chapter 6.1.3. Each participant's second section of lab experiment was recorded by Gazepoint Analysis Software to track their gaze by using Video Gaze mode.

For study's purposes, focusing on the Image Recognition based CAPTCHA challenges and the image content type that is displayed to participants; AOIs(Area of Interest) were set only while the participants were solving the challenges. Each square of the initial image that was displayed in the challenges was set as an AOI. Totally, for each participant 18 AOIs were set, 9 for the challenge with the "familiar" content image and 9 for the challenge with the "generic". The AOIs that are set for generic content image is shown in Figure 7.11.
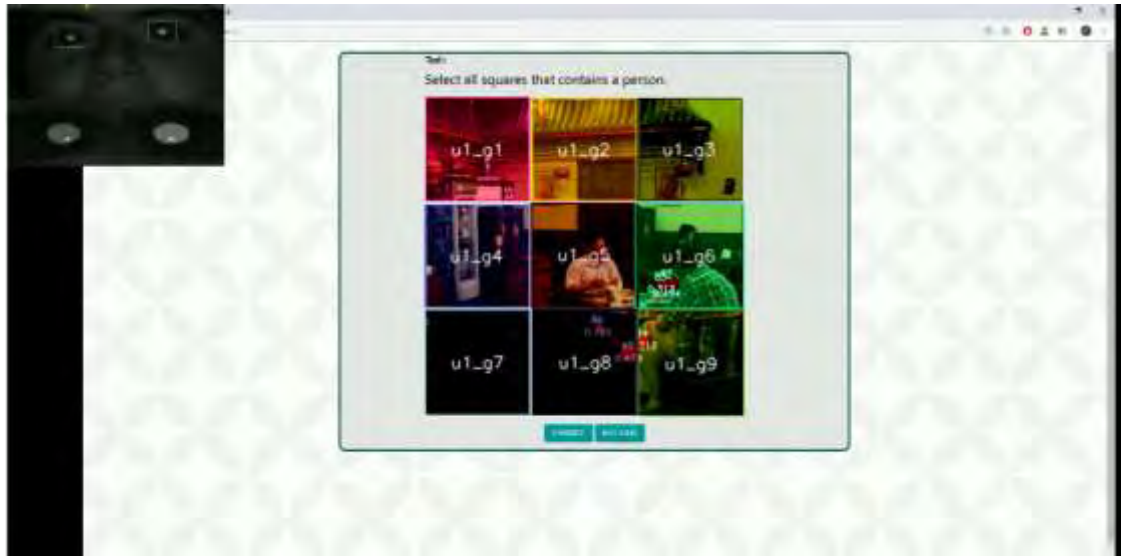
Figure 7. 11: AOIs that are set on generic content image.

After exporting the collected data in an .excel file in CSV format for each participant, the time viewed in seconds and in percentage, the number of fixations and the number of revisits were reported for each area of interest set for the participant.

7.4. Data Processing and Analysis

Processing the collected data:

Since all the data collected within the study wasn't stored in the same place, after completing the lab experiment with all the participants; the collected data needed to be processed before the analysis. User's preference and user's performance data were stored in the database while user's visual behavior data was stored in Excel files.

For each CAPTCHA challenge a participant solved, a record was stored in database. So all participants has the minimum of 2 records stored in the database. Participants who gave wrong solutions have more than 2 records. To run statistical analysis, the user's performance data should be processed and summarized in one record. For each participant of the lab experiment a new record is added in the "user_study_results". For each type of challenge (generic/familiar), the total number of failed attempts is measured, if there weren't failed attempts the value is set as "0". Also, the task duration

time that is recorded for each challenge is the duration of the attempt where the solution was correct. The preference of the user is also added.

The visual behavior data collected for each participant also needed to be processed. The collected metrics (number of fixation, fixation duration, revisits) that were exported from Gazepoint Analysis Software were taken for each AOI that was set. So the collected data needed to be processed to calculate the total number of fixations, the total fixation duration, the total revisits and the average number of fixations in a square for each type of challenge. Then the processed data was added in "user_study_results" Excel file.

The results of the cognitive tests for each participant are also included in each participant record.

Analyzing the processed data:

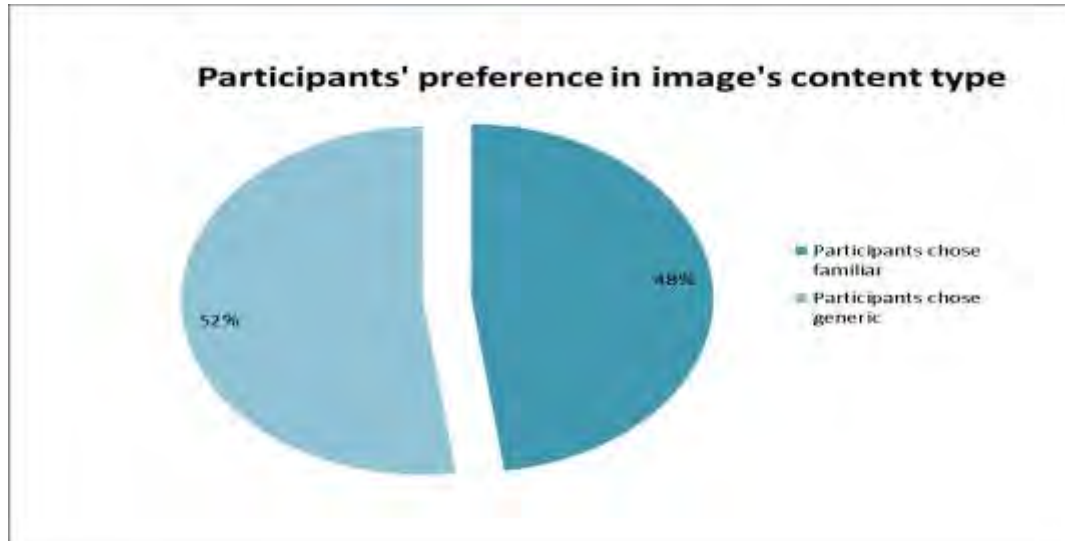*H1. Web users would prefer familiar content images to be displayed in IRCS challenges.*

Figure 7. 12: Pie Chart that represents participant's preference in image's content type

Within the lab experiment, 22 out of 46 participants (~48%) select familiar content image and 24 out of 46 participants (~52%) select generic content image to be displayed in the IRCS. These results reject H1 since participants haven't shown any special

preference towards familiar content image in IRCS challenge, but on the contrary with a small difference in percentage they showed greater preference in generic content image.

	Task Duration (in sec)		#Failed Attempts	
	Average	σ	Average	Σ
Familiar	10.270587	4.2654552	0.10869565	0.31469639
Generic	9.08719565	4.26549468	0.32608696	0.66847581

Figure 7. 13: Table of User's Performance Metrics for familiar and generic content images.
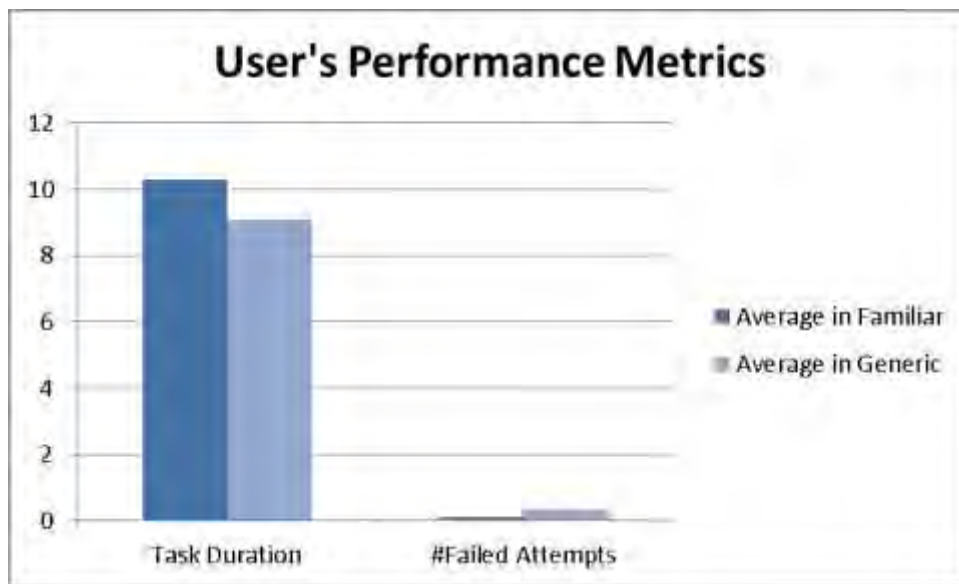

Figure 7. 14: User's Performance Metrics Chart

Figure 7.13 and Figure 7.14 show that there is no significant difference in task duration for familiar content and generic content images. In the challenge with the familiar the task duration is a bit greater but the difference is less than 1 second. The failed attempts averages are both in very low since very few participants had failed attempts. In the challenge with the generic image content the failed attempts average is greater than in the challenge with the familiar content image, but there isn't any significant difference.

	#Fixations		Time Viewed (in sec)	
	Average	Σ	Average	σ
Familiar	24.6521739	12.8395524	6.6746087	3.32819884
Generic	22.1086957	11.3553282	5.97834783	3.14074164
	#Revisits		#Fixations in a square	
	Average	Σ	Average	σ
Familiar	13.9347826	9.95412181	2.73913043	1.42661694
Generic	12.7608696	8.77416608	2.45652174	1.26170313

Figure 7. 15: Table with Visual Behavior Metrics for familiar and generic content images.
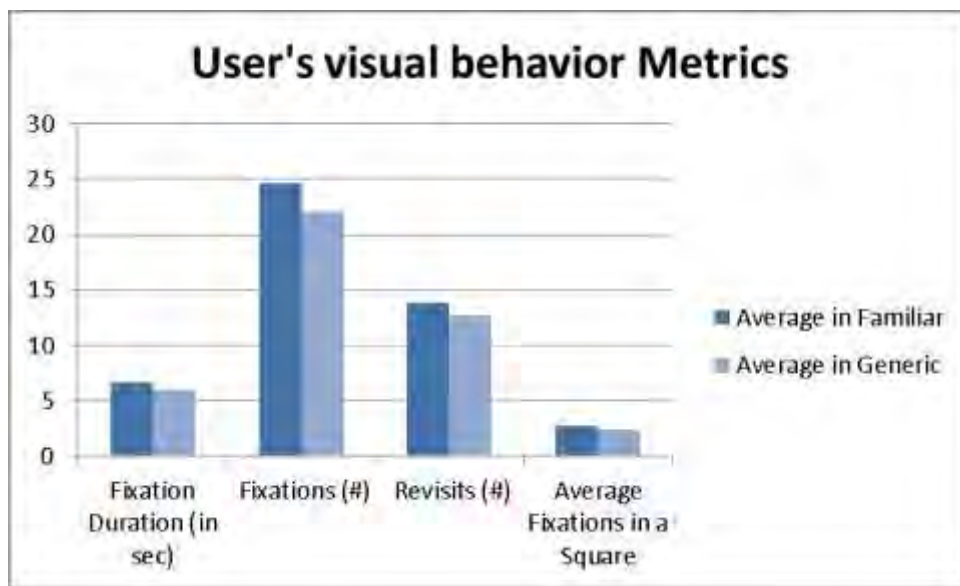

Figure 7. 16: Chart of Average User's Visual Behavior Metrics

As shown in Figure 7.15 and Figure 7.16 there is no significant difference in user's visual behavior metrics in the familiar and the generic content image. Familiar content image's metrics appears to be a bit greater than generic content image's metrics. Otherwise, since the values of the metrics are very similar the H2 is verified.

After scoring the GEFT test of each participant, 25 out of 46 participants are shown to be FDs and 21 out of 46 participants are shown to be FIs. The percentage of each cognitive style's group is shown in Figure 7.17.
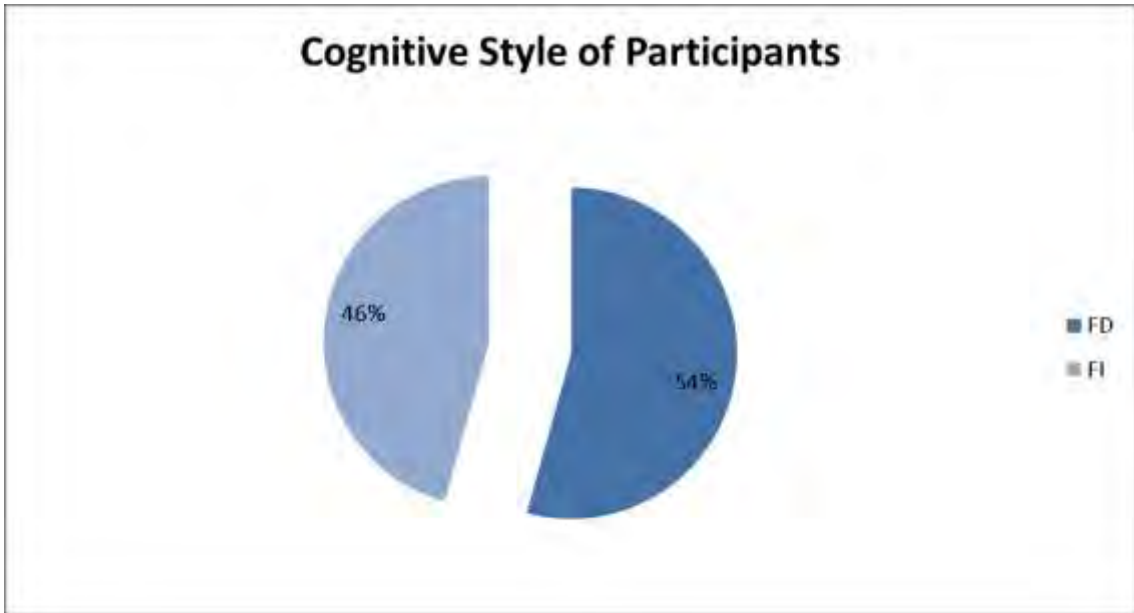
Figure **7. 17: Cognitive Style of Participants Chart**

H3. FD individuals prefer familiar content images to be displayed in IRCS challenges
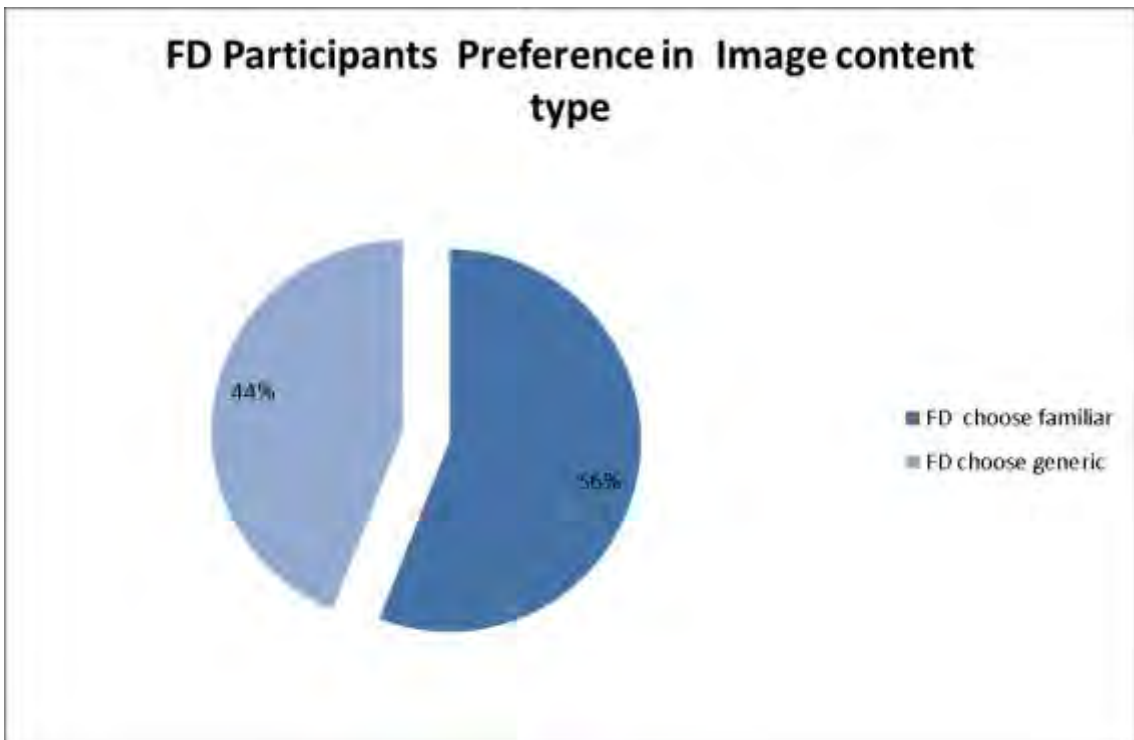

Figure 7. 18: FD participants' preference in image content type

Figure 7.18 is showing the percentage of FD individuals who choose familiar content image and the percentage of FD individuals who choose generic content. A number of 14 out of 25 FDs chose familiar content image and 11 out of 25 FDs chose generic. Since, the percentage of the FDs who chose familiar content image (56%) is greater than the percentage of the FDs who chose generic (44%) H3 can be verified.

H4. FI individuals don't show increased preference towards familiar content images that are displayed in IRCS.
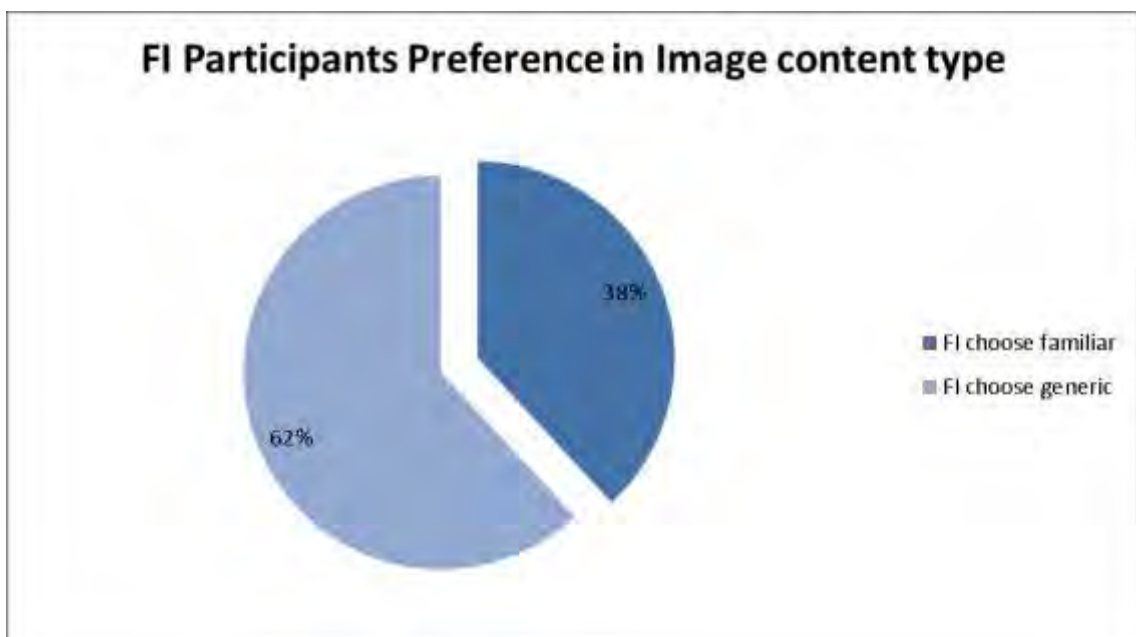
Figure 7. 19: FI participants' preference in image content type

The results that are shown in Figure 7.19 reject H5 since the percentage of FI individuals who chose the generic content image (~62%) to be displayed in IRCS challenge was significantly greater than the percentage of those who chose familiar content image (~38%). Based on the preference that FI individuals show towards image content type, we can conclude that FI individuals prefer IRCS challenge to display generic content images and they are not interested in displaying familiar content image. H4 can be verified.

	Familiar Content Image			
	FD		FI	
	Average	Σ	Average	Σ
Task Duration	9.40724	4.241704525	11.29838095	4.15997426
#Failed Attempts	0.12	0.331662479	0.095238095	0.3007926
	Generic Content Image			
	FD		FI	
	Average	Σ	Average	Σ
Task Duration	8.67684	5.182879313	9.575714286	2.87084354
#Failed Attempts	0.56	0.820568908	0.047619048	0.21821789

Figure 7. 20: Table of User's Performance Metrics of FD/FI participants in the different image content types.
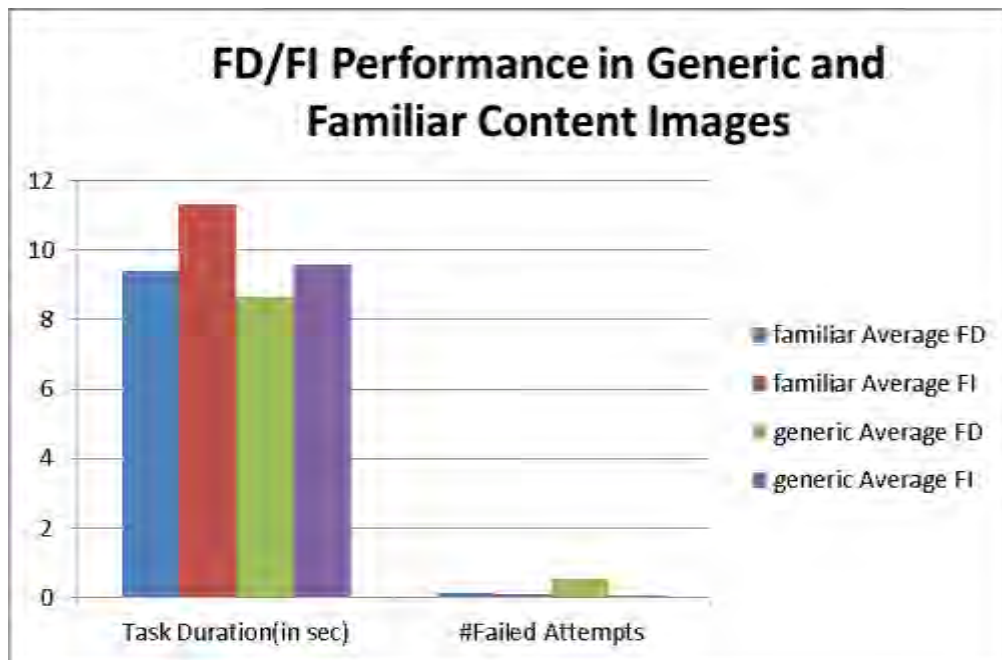

Figure 7. 21: Chart of User's Performance Metrics of FI/FD participants in the different image content types.

Figure 7.20 and 7.21 show that FD individuals have slightly better performance than FI individuals in both of the challenges since FDs solved the challenge in a shorter duration than FIs. Otherwise the difference does not look significant (~1-2 seconds).

The results shown in Figure 7.20 and 7.21 shows FIs have a better performance in generic content image than in familiar content image. But the difference between the task duration in the two challenges are not significant (~1-3 seconds.)

The results shown in Figure 7.20 and 7.21 shows that FI participants have better performance in generic content image than in familiar content image. But the difference between the task duration in the two challenges are not significant (~1-2 seconds.)

H4. FIs have more active Visual Behavior than FDs while solving IRCS challenges.

| | Familiar Content Image | | | |
| | FD | | FI | |
	Average	σ	Average	Σ
Fixation Duration(sec)	5.68892	2.816678983	7.848047619	3.569642
Fixations (#)	20.76	10.58017013	29.28571429	13.96833
Revisits (#)	11	8.490190418	17.42857143	10.62342
Average Fixations in a Square	2.306666667	1.175574459	3.253968254	1.552037
	Generic Content Image			
	FD		FI	
	Average	σ	Average	Σ
Fixation Duration(sec)	5.6022	3.678099237	6.426142857	2.360737
Fixations (#)	19.84	12.83445883	24.80952381	8.852226
Revisits (#)	11.6	10.24288371	14.14285714	6.605193
Average Fixations in a Square	2.204444444	1.426050981	2.756613757	0.983581

Figure 7. 22: Table of Visual Behavior Metrics of FD/FI participants in different image content type.
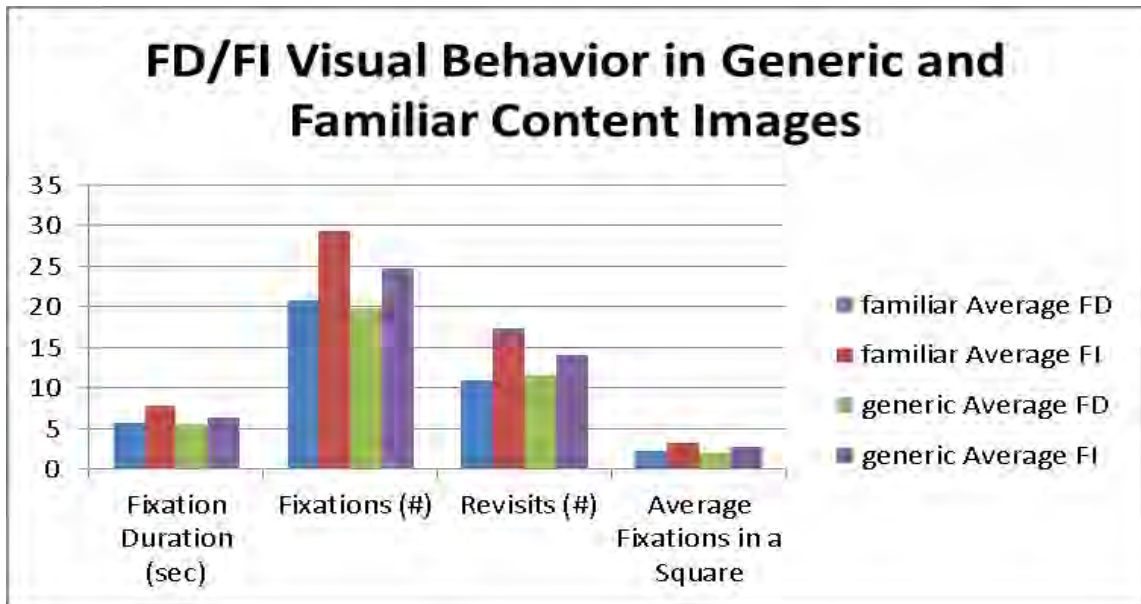
Figure 7. 23: Chart of Visual Behavior Metrics of FD/FI participants in different image content type.

Figures 7.22 and 7.23 show the results of Visual Behavior Metrics for each cognitive style group (FD/FI) while solving IRCS challenges with the two different image content type (familiar/generic). FD individuals records less fixation duration, less number of fixations, less revisits and less average fixations in a square than FI individuals. FIs have more active Visual Behavior than FDs so H5 is verified.

In Figures 7.22 and 7.23, it is shown that the visual behavior of FDs is not affected by the image content type since the metrics are quite similar in the two different types.

In Figures 7.22 and 7.23, it is shown that the visual behavior of FIs is affected by the image content type since the metrics while solving the IRCS challenge with the familiar content image shows more active visual behavior than in the challenge with the generic content image.

H5. Individuals with high working memory capacity have better performance than individuals with low working memory capacity while solving IRCS.

	Low Working Memory Capacity		High Working Memory Capacity	
	Average Task Duration	σ	Average Task Duration	Σ
Familiar	10.4967	3.878579028	10.52790476	4.815859154
Generic	8.9305	5.355780532	9.450761905	3.232845881

Figure 7. 24: Table of User'Performance based on Working Memory Capacity
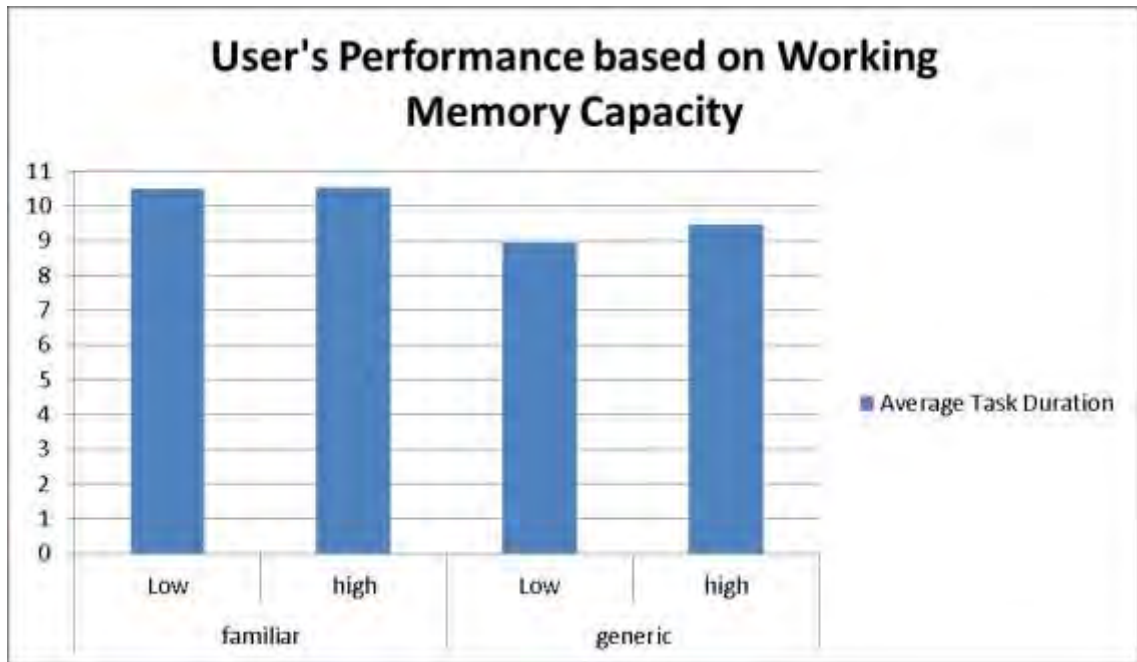
Figure 7. 25: Chart of User's Performance based on Working Memory Capacity

Figures 7.24 and 7.25 shows that the user's performance is not affected from working memory capacity of the participants since for each challenge the average task duration is similar for participants with low and participant with high memory capacity. H5 is rejected.

H6. Individuals with fast speed of processing have better performance than individuals with slow speed of processing while solving IRCS.

	Slow Speed of Processing		Fast Speed of Processing	
	Average Task Duration	**Σ**	**Average Task Duration**	**σ**
Familiar	10.36524	4.265455196	10.1579	4.223089958
Generic	8.76664	5.323077665	9.46881	4.265494676

Figure 7. 26: Table of User's Performance based on speed of processing of participants
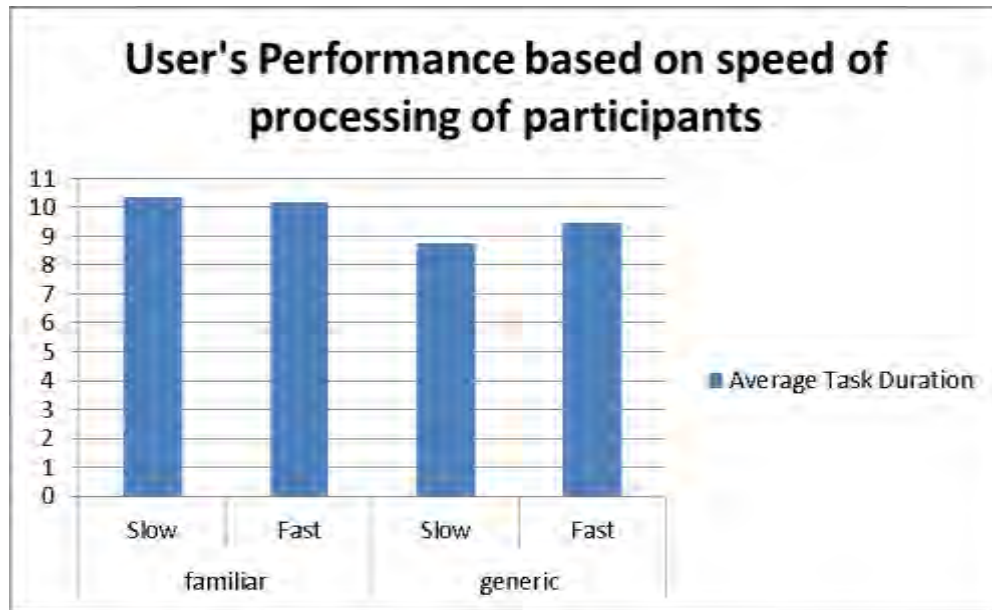

Figure 7. 27: Chart of User's Performance based on speed of processing of participants

The results represented in Figures 7.26 and 7.27 show that the user's performance is not affected by the level of participant's processing speed since the task duration in each challenge are very similar between users with low and user with fast speed of processing. H6 can be rejected since there is no difference in performance associated with speed of processing.

7.5. Analysis of Evaluation Questionnaire

The results of the evaluation questionnaire that users completed about the lab experiment, they have participated in, are shown in the following figures.
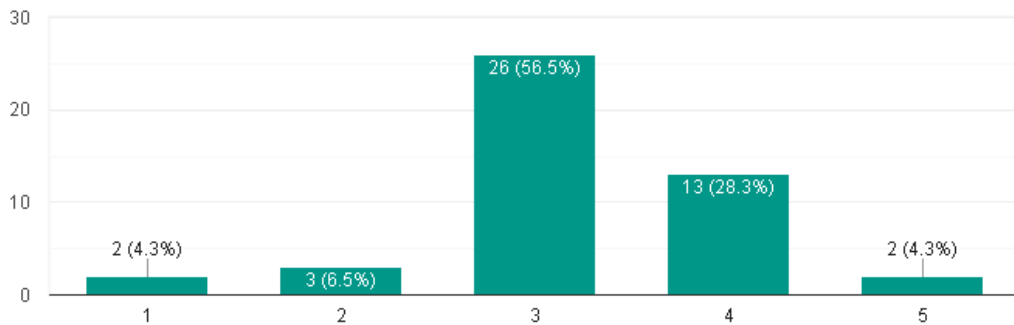
Figure 7. 28: Results about generic content images in Image Recognition Captcha participant solved in lab experiment

In Figure 7.28, it is shown that 26 participants answered with the degree of 3 (enough) and 13 participants answered with the degree of 4 (very) in the question "In what degree would you prefer the images that are displayed in Image Recognition CAPTCHA to have a generic content to you?". Only a few participants answer with 1, 2 and 5. That leads to the conclusion that users are not bothered with generic-content images and they are slightly more positive against them.
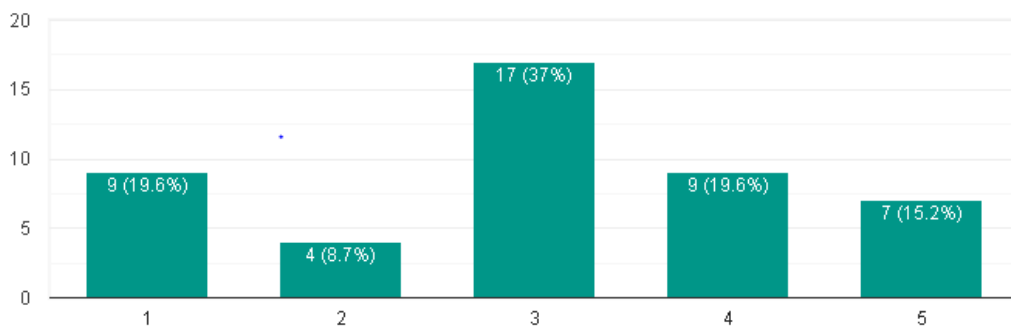

Figure 7. 29: Results about familiar content images in Image Recognition Captcha participant solved in lab experiment

In Figure 7.29, it is shown that 17 participants answered with the degree of 3 (enough) and 9 participants answered with the degree of 4 (very) in the question "In what degree

would you prefer the images that are displayed in Image Recognition CAPTCHA to have content familiar to you?" .The interesting observation here is that a great number of participants answered with 1 and 5 which shows that there are participants that are negative in familiar content and other participants that are positive in it.

If it taken into consideration that in the lab experiment, 22 participants choose to solve the familiar content image recognition CAPTCHA and 24 choose the generic content that are very similar numbers, it can be concluded that in general the image content type does not affect the user preference.
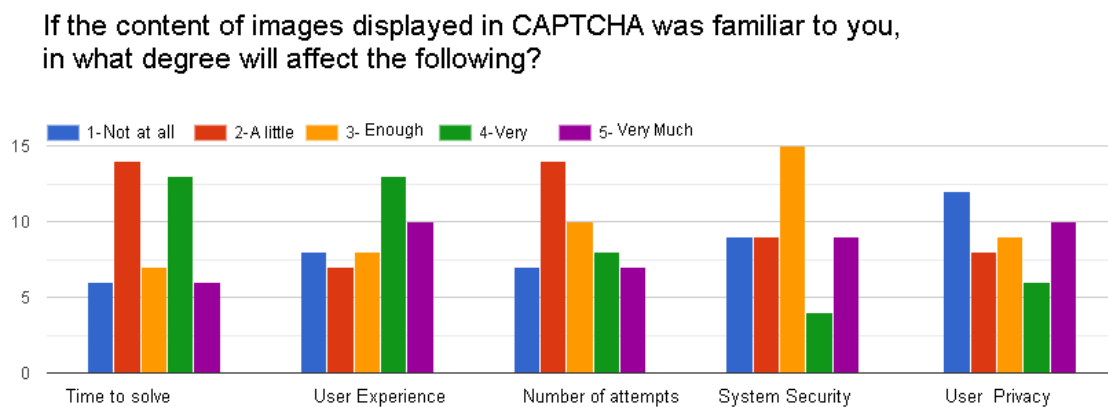
Figure 7. 30: Results about the factors that are affected by using familiar content images in Image Recognition Captcha

In Figure 7.30, it is shown in what degree having a familiar content Image Recognition CAPTCHA affects the time to solve the CAPTCHA, the user experience, the number of attempts, the system security and the user privacy.

In time to solve factor, a similar number of users answered 2(little) and 4(very) which shows that the content type of the image affects that factor in participants opinion.

In user experience factor, there is a variety of answers in similar numbers but with 4,5 answers to be greater than the others, which shows that user experience is affected by giving a familiar content image.

In number of attempts, the majority of the users answered with the degree of 2, which concludes in that image content type does not affect this factor.

In system security factor, the majority answered with a degree of 3 which shows that participants believes that by giving familiar content images the security of the system is affected.

72

In user privacy factor, the answers vary in all degrees but the degree of 1 has the greatest number of answers. The user privacy of the users seems like is not affected in a high degree in participants opinion. This is a crucial factor in all personalized systems, since the users should not be afraid that their privacy is diminished while interacting with them.

7.6.   User Study's Results

Processing and analyzing the data collected within the user study lab experiment led to the following results:

- In general, users don't show preference in familiar content image to be displayed in IRCS instead of generic content image. The fact that the percentage of the participants who chose familiar and the percentage of those who chose generic content image were very similar can lead to the conclusion that user's preference is not affected by providing different image content type to IRCS.
- The performance and the visual behavior of the participants is also not affected in a major way by providing IRCS challenges with familiar content instead of generic content images.
- FD participants show preference in familiar content images to be displayed in the IRCS challenged while FI participants show preference in generic content images.
- FD participants show slightly better performance in the terms of task duration than FI participants in IRCS challenges.
- The visual behavior of FIs while solving both of the challenges is more active than the visual behavior of FDs.
- FIs' visual behavior is affected by providing a familiar content image in IRCS challenge since the visual behavior is more active than in challenge with generic content images.
- FDs' visual behavior is not affected by providing a familiar content image.
- User's performance in familiar and generic content images is not depended on user's level of working memory capacity and speed of processing

Chapter 8

Conclusions and Future Work

This is the concluding chapter of the study where the results of the study and general conclusions are presented and summarized. The limitations of this study and the solution proposed for the problem stated are annotated. Afterwards, the future work that must be done to extend and complete this study is stated.

8.1.   Conclusions

This study was conducted with the purpose to introduce displaying familiar content images in IRCS challenges as a factor to be considered in the context of adapting personalization in CAPTCHA schemes. Since CAPTCHA schemes need to be as transparent and as unobtrusive as possible to the user's experience in online services, the factor introduced is needed to be evaluated in order to study how user's experience would be affected.

A lab experiment has been in placed to research the user's performance and preference towards IRCS challenges with familiar and generic content images. Additionally, the visual behavior of the participants was also recorded as a measure of user's performance. Moreover, it was examined if the differences in cognitive style (FI/FD) of the participants and their cognitive abilities (working memory capacity, speed of processing) had any impact on user's preference and performance towards image content type.

The results of the user study show that providing IRCS challenges with image content familiar to the users, can be considered as a factor of personalization in CAPTCHA schemes but only if it is used alongside with the cognitive style (FI/FD) of the users. FD

users showed increased preference towards IRCS challenges with familiar content type while their performance and visual behavior was similar in both challenges. FI users, in contrary, showed increased preference towards IRCS challenges with generic content type. The performance of FIs in both of the IRCS challenges was similar, but the visual behavior of FIs was quite more active while solving the challenge with the familiar content image. If the image content type will be considered as a factor in personalization of CAPTCHA schemes, images with familiar content in IRCS challenges looks to be beneficial for FD users in their experience while can be constructive for FI users 'experience.

The differences in working memory capacity and speed of processing of the user's don't seem to affect the user's performance while solving the IRCS challenges with different image content types.

Concluding, the importance to increase the usability and to improve the user's experience while solving CAPTCHA challenges in online services results in the idea of adapting personalization of CAPTCHA schemes. In order to achieve this, a group of factors must be considered to build the personalization mechanism of CAPTCHA schemes. This study can be a guideline for future studies that are seeking for factors that can be introduced in the context of adapting personalization in CAPTCHA schemes.

8.2.   Limitations

The limitations of the reported study are related to the participant's sample of the lab experiment. Despite the effort to keep the sample representative towards population, the sample is consisted only from University of Cyprus students with an age between 19 and 27. Having participants from different age groups would be the ideal sample but the time schedule of the study was narrow so it was quite difficult to find volunteers that weren't students. Otherwise, students from several disciplines participated in the study and the majority of them were familiar with the concept of CAPTCHA challenges.

Lab experiments are quite efficient in collecting complex data while special equipment can be used (e.g. eye-tracking device). Also the fact that the experimenter is present and can have a better understanding of the user's behavior and quality of experience is a gain since this knowledge can be taken into consideration in the process of data analysis. However, since the participants are aware of the experiment procedure and

they know that their visual behavior and performance is tracked they might interact with the computer in a non-natural way. This is because they might get stressed or they are affected by the presence of the experimenter. An unrealistic performance during the experiment might affect the results of the study in some degree.

On the other hand, there has been an effort to increase ecological and internal validity of the research. This was achieved by asking participants to perform a specific task where the two CAPTCHA challenges where embedded in a way that users would not pay all their attention in solving the challenges, which is similar to the concept that users are familiar in online services. The presence of the experimenter was discreet, since in the second section of the experiment all the instructions were described on the computer and so only if the participant was facing a problem the experimenter intervened.

Another aspect of the study that can be considered as limitation is the subjectivity in what a participant perceives as "familiar content" and how this information can be extracted. An idea is to use the user's location by translating his/her IP address into a physical address and provide images that are related to this address. This would either require an on-the-fly database model which suffers from image's mislabeling problems or a huge database with images related to each geographical area around the world. An idea could be to use cookies to extract the information and give an image related on previous visited sites' content.

The fact that 3 cognitive tests should be answered by the participants within the study in order to make their cognitive profile shows that it is difficult to retrieve such information without interrupting the user. In personalized systems the collection of user's data is the most important and difficult task in general. However, since the technology evolves it is expected that automated software is going to be developed to identify these cognitive characteristics by tracking user and computer interaction.

8.3. Future Work

Since this study examines just a specific factor that can be considered in the adaptation of personalization in CAPTCHA schemes, future studies can be conducted to explore and analyze new and alternative factors.

As an extension of the current analysis of the lab experiment's results, the creation of 8 different groups of user models (by combining their FI-D cognitive style, low/high processing speed and low/high working memory capacity) can be done. The 8 different groups are shown in Figure 8.1. With the categorization of the users under these 8 groups, a more specific analysis can be done to examine whether displaying of a familiar content image in IRCS affect there visual behavior, performance and preference.

Group ID	Field Dependency	Speed of processing	Visual Working Memory Capacity
1	FD	Low	Low
2	FD	Low	High
3	FD	High	Low
4	FD	High	High
5	FI	Low	Low
6	FI	Low	High
7	FI	High	Low
8	FI	High	High

Figure 8. 1: Groups with the combination of the different cognitive styles and skills

Extending this study, methods of extracting the user's information to deliver a familiar content image in CAPTCHA challenges need to be introduced and implemented. A feasibility study must also be conducted to evaluate the easiness of using familiar content images as a factor in adapting personalization.

As a great number of factors that can be used to adapt personalization in CAPTCHA schemes are known and introduced in [4] so as future work a first attempt to implement a personalized CAPTCHA system can be considered.

In a more abstract concept as future work, automated software tools to identify user cognitive styles and abilities could be studied and implemented in order to make web able to adapt personalization in a cognitive level without the need of the having user to complete questionnaires and tests.

References

[1] A. Basso and F. Bergadano, "Anti-bot strategies based on human interactive proofs," in *Handbook of Information and Communication Security*Anonymous 2010, .

[2] M. Belk *et al*, "Do human cognitive differences in information processing affect preference and performance of CAPTCHA?" *International Journal of Human-Computer Studies,* vol. 84, pp. 1-18, 2015.

[3] M. Belk *et al*, "Studying the effect of human cognition on text and image recognition CAPTCHA mechanisms," in *International Conference on Human Aspects of Information Security, Privacy, and Trust,* 2013, .

[4] C. Fidas *et al*, "iHIP: Towards a user centric individual human interaction proof framework," in *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems,* 2015, .

[5] M. Moradi and M. Keyvanpour, "CAPTCHA and its Alternatives: A Review," *Security and Communication Networks,* vol. 8, *(12),* pp. 2135-2156, 2015.

[6] A. Raj *et al*, "Picture captchas with sequencing: Their types and analysis," *International Journal of Digital Society,* vol. 1, *(3),* pp. 208-220, 2010.

[7] O. N. Saracho, "Cognitive style: individual differences," *Early Child Development and Care,* vol. 53, *(1),* pp. 75-81, 1989.

[8] L. Von Ahn *et al*, "CAPTCHA: Using hard AI problems for security," in *International Conference on the Theory and Applications of Cryptographic Techniques,* 2003.

[9]*Django Framework Documentation*. Available: https://docs.djangoproject.com/en/2.2/.

[10] *Material Design Documentation*. Available: https://material.io/design/.

[11] *Image Picker Documentation*. Available: https://rvera.github.io/image-picker/.

[12] Categories of CAPTCHA schemes. Available: https://dynomapper.com/blog/514-online-captcha-solving-services-and-available-captcha-types.