



UNIVERSITY OF PADOVA
ENGINEERING DEPARTEMENT

Computer Engineering Master Degree

INVISIBLE CAPTCHA

Candidate

Di Nardo Di Maio Raffaele

Supervisor

Prof. Migliardi Mauro

Co-Supervisors

Guerar Meriem

DD-MM-YYYY

ACCADEMIC YEAR 2020-2021

To my parents, that always help
me to be happy doing what I love
and support me reaching my goals.

Most people assume that once security software is installed, they're protected. This isn't the case. It's critical that companies be proactive in thinking about security on a long-term basis.

Kevin Mitnick

Devi imparare le regole del gioco. E poi devi giocare meglio di chiunque altro.

Albert Einstein

Si come il ferro s'arrugginisce senza esercizio, e l'acqua si putrefà o nel freddo s'addiaccia, così lo 'ngegno senza esercizio si guasta.

Leonardo da Vinci

Contents

1	Introduction	1
2	State of Art	3
2.1	Design of CAPTCHA	3
2.2	Traditional CAPTCHA	5
2.3	Alternatives	11

Chapter 1

Introduction

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is a program used to distinguish human users from bots. A bot is a malicious application that automates a task, gathering useful information about user credentials or pretending to be a human interaction with Web application. Hence the term "*bot*" is an abbreviation of the words "software robot".

The CAPTCHAs are traditionally used in Web applications for[4]:

- **Online Polls**
CAPTCHAs prevent the creation and the submission of a large number of votes, favouring a party.
- **Protecting Web Registration**
CAPTCHAs prevent the creation of free mail account to bot instead of human users. The goal of the use of CAPTCHAs is to remove the possibility that the hacker could take advantages from the large amount of registrations.
- **Preventing comment spam**
CAPTCHAs prevent the insertion of a large amount of posts made by bot on pages of social platforms or blogs.
- **Search engine bots**
CAPTCHAs are used to guarantee that a website should be unindexed to prevent the reading of the page through search engine bots. The CAPTCHAs are added because the html tag, used to unindex the web page, doesn't guarantee unindexing.
- **E-Ticketing**
CAPTCHAs prevent that a big events would sell out minutes after

tickets become available. In fact ticket scalpers that make large number of ticket purchases for big events.

- **Email spam**

CAPTCHAs are used to verify that a human has sent the email.

- **Preventing Dictionary Attacks**

CAPTCHAs prevent bot to guess the password of a specific user. The hacker could guess the password, taking it from a dictionary of passwords. The use of the CAPTCHA challenge prevents the iteration of the login phase made by the bot using all the words of the dictionary. After a certain number of failures POST requests, the CAPTCHA challenge is shown to the user.

- **Verifying digitized books**

ReCAPTCHA can verify the contents of a scanned piece of paper analysing responses in CAPTCHA fields. A computer cannot identify all the words from a digital scan.

The application submits two words to the user in the CAPTCHA challenge: the first one that the machine has already recognized and the other for which it can correctly associate a word. If the user types the two words and the first one was correctly detected, it assumes that also the second one is correct.

In this case the second word is added to a set of words that are going to be added to other users' challenges. If the application receives enough responses with the same typed word related to the unknown word, the program establishes that typed word is the CAPTCHA is related only to the first word and the challenge related to the second word is exploited by the application to scan digitally the paper.

Another useful application of CAPTCHA is the support to the authentication process. This application is going to be analysed in details in the next chapters, looking at the authentication from smartphone.

In Chapter 2 there is a description of the state of art of CAPTCHA, looking at types of CAPTCHA and the related tests from which this challenge is born.

DESCRIPTION OF THE CONTENT OF THE CHAPTERS

Chapter 2

State of Art

2.1 Design of CAPTCHA

CAPTCHA takes inspiration and is related to three main elements[5]:

1. **Turing test**

it's used to determine how much a machine can think like a human. The test is made by three figures: a human examiner, an human and a machine. The examiner asks some questions to both other two figures and, after a fixed amount of time, evaluates if the two answers are different or not.

If they are similar w.r.t. the point of view of the examiner, the machine is an AI (Artificial Intelligence) similar to an human. The test is very important if the answers have many possibilities.

2. **Human-Computer Interaction (HCI)**

according to cognitive psychology studies, a human process data in a specific way and this test evaluates the interaction between humans and machines. The HCI model is divided into five levels:

- task level
- semantic level
- syntactic level
- interactive level
- a level of physical devices

Then the obtained information is processed by:

- reasoning

- problem solving
- skill acquisition
- error

3. **Human Interactive Proof (HIP)**

it's used to make differentiation between machine and human users and computer user programs. The test require a type of interaction, that is simple to be done by human instead of bot. The main goals of this type of test are:

- To differentiate the humans from the computers
- To differentiate a category of the humans
- To differentiate a specific human from the category of humans

HIP has the test program that is subjected to the human and the computer. As a result, only a specific group of humans can positively solve the test and then the test results can be validated by the computer.

In order to guarantee a good level of security, a CAPTCHA has to satisfy the following requirements:

- The solution to the CAPTCHA isn't conditional and shouldn't depend on the user's language and/or age.
- The solution of the CAPTCHA must be easy for the humans and hard for the bots. Hence, humans in no longer than 30 seconds with very high success rate
- The creation of the CAPTCHA must not disturb the user privacy (not linked to the user).

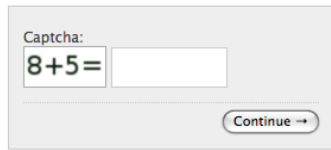
2.2 Traditional CAPTCHA

The traditional CAPTCHAs are based on the knowledge and correct insertion of solution by the user. The main types of this CAPTCHAs are:

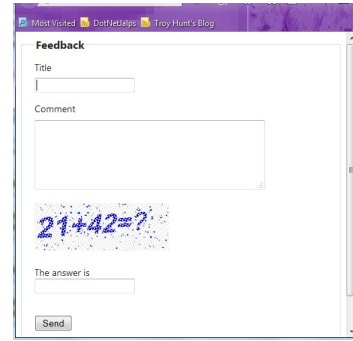
- **Arithmetic (Math)**

Looking to an operation specified in a frame, the user needs to insert the result in a text field. The operation is written in plain text or, to improve the security of this challenge, it's warped like text-based CAPTCHAs (Figure 2.1). These classical math-CAPTCHAs, also known as *arithmetic CAPTCHAs*, are vulnerable to OCR (Optical Character Recognition) techniques.

An advanced version of this CAPTCHA is used in the Quantum Ran-



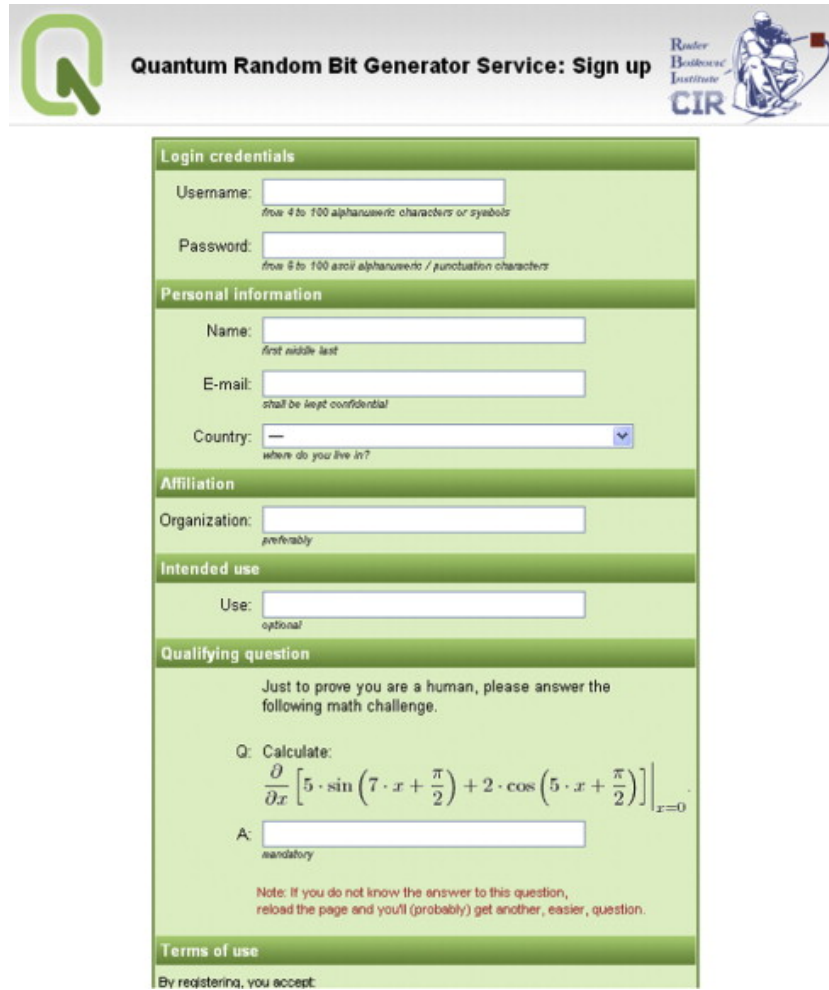
(a) With plain text.



(b) With wrapped text.

Figure 2.1: Example of arithmetic CAPTCHAs.

dom Bit Generator Service (QRBGS) sign-up Web Page[10] (see Figure 2.2). This type of CAPTCHA asks user to solve an advanced math expression. It prevents the use of free or commercial OCRs because many mathematical symbols are not considered in their detection algorithm. Hence many math symbols are wrongly translated by bot programs and the challenge is very secure. The only problem is that this CAPTCHA is very complex for normal users and many of them could not solve the challenge correctly.



Quantum Random Bit Generator Service: Sign up

Login credentials


Username:
from 4 to 100 alphanumeric characters or symbols

Password:
from 6 to 100 ascii alphanumeric / punctuation characters

Personal information

Name:
first middle last

E-mail:
shall be kept confidential

Country: 
where do you live in?

Affiliation

Organization:
preferably

Intended use

Use:
optional

Qualifying question

Just to prove you are a human, please answer the following math challenge.

Q: Calculate:

$$\left. \frac{\partial}{\partial x} \left[5 \cdot \sin \left(7 \cdot x + \frac{\pi}{2} \right) + 2 \cdot \cos \left(5 \cdot x + \frac{\pi}{2} \right) \right] \right|_{x=0}$$

A:
mandatory

Note: If you do not know the answer to this question, reload the page and you'll (probably) get another, easier, question.

Terms of use

By registering, you accept:

Figure 2.2: Example of Quantum Random Bit Generator Service (QRBGS) sign-up Web Page [10].

- **Audio-based**

this type of CAPTCHAs asks the user to type the words listened by an audio file (see Figure 2.7). It's developed for vision-impaired users. It usually has problems related to the language dictionary, from which words are taken, and the similarity of the sound between several words. This type of CAPTCHAs is vulnerable to many Automatic Speech Recognition (ASR) programs[3].

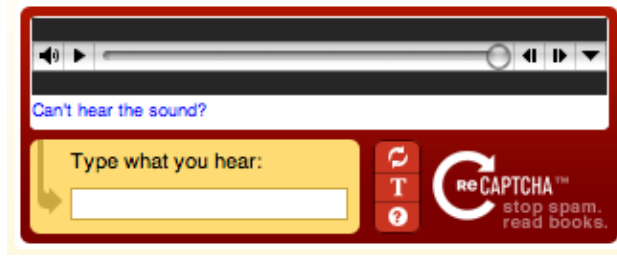


Figure 2.3: Example of audio-based CAPTCHA.

- **Game-based**

This type of CAPTCHAs performs the verification of the user nature through a set of several kind of games (see Figure 2.4). This type of CAPTCHAs is called *Dynamic Cognitive Game (DCG)* is usually developed using Flash and HTML5 with JavaScript. These technologies download the game code to the client and execute it locally. The only difficult for the bot to attack the challenge is the encryption/obfuscation of the code. This strategy prevent the store of the code onto different internet domains. However for example, there exists a bot attack, called *Stream Relay Attack*, that obtains good results bypassing these challenges [11].



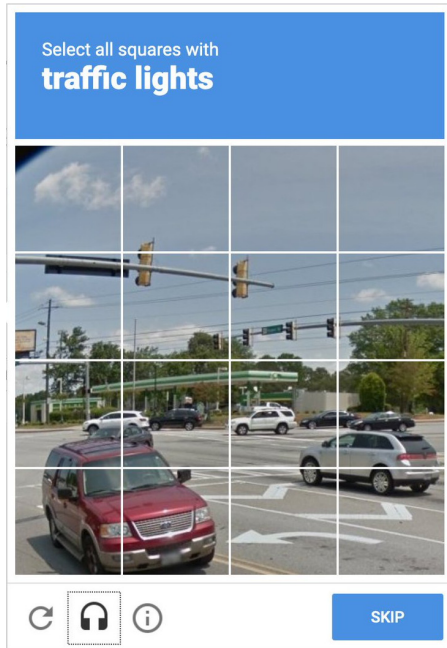
Figure 2.4: Examples of game-based CAPTCHAs.

- **Image-based**

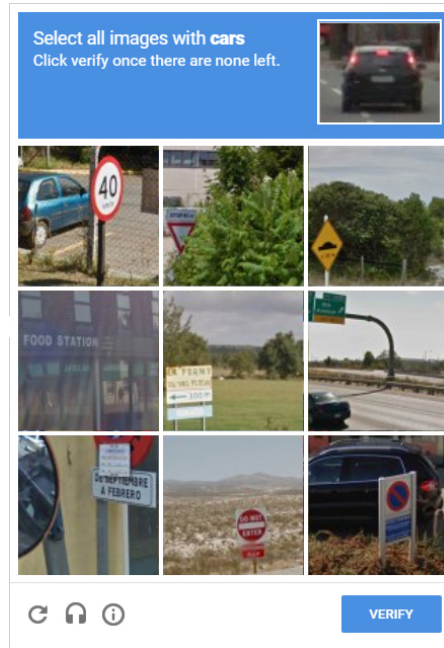
this type of CAPTCHAs asks to select the images that contain a requested subject. The set of images, on which the user needs to identify the subject, can be implemented in different ways, for example:

- An image is divided into a set of sub-squares and each of them is a candidate image 2.5a
- There are many images, each one with a unique different subject (see Figure 2.5b)

This type of CAPTCHAs is vulnerable to different Computer Vision techniques Object Recogni An extension of this type of CAPTCHAs, called *FaceDCAPTCHA*, has been introduced[?]. It incorporates elements of face detection. The human brain is very effective in the process of natural face segmentation even if there are complex backgrounds. This approach increases the security efficiency because the Computer Vision programs can easily detect if there is a face, e.g. Viola-Jones algorithm[9], but have many problems differentiating real and non-real photographs of faces.



(a) With an image divided in sub-squares.



(b) With several images.

Figure 2.5: Examples of image-based CAPTCHAs.

- **Puzzle-based**

this type of CAPTCHAs asks the user to complete a visual puzzle, created by dividing a given image in a set of pieces[6] (see Figure 2.6a). The task isn't easy for users because this type of CAPTCHAs takes more time to solve the puzzle but the security level is very high[6]. To improve the usability of the CAPTCHA, there exists a variant of the puzzle-based CAPTCHA in which needs to insert only some pieces of the puzzle instead of completing the whole puzzle (see Figure 2.6b).

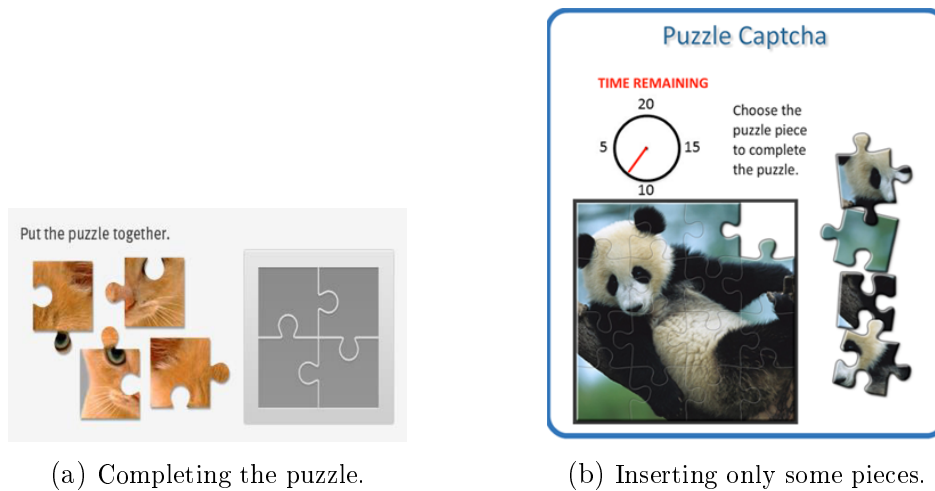


Figure 2.6: Examples of puzzle-based CAPTCHAs.

- **Text-based**

this type of CAPTCHAs shows a series of wrapped characters and/or numbers on the screen. The users needs to understand which are the characters that composes the shown sequence and then type them inside a text-field. This type of CAPTCHAs is vulnerable to several type of attacks, related to Computer Vision techniques, that are:

- OCR techniques[2]
- Segmentation techniques (e.g. DECAPTCHA[1])
- Machine Learning and Deep Learning techniques

In the design phase of a text-based CAPTCHA there are many issues, related to Computer Vision techniques, to be considered. For each of them, there is usually a solution in the design phase of the CAPTCHA that reduces the possibility that the challenge would be broken by a bot[1].

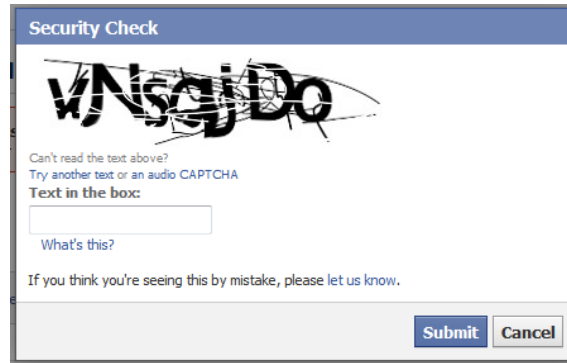
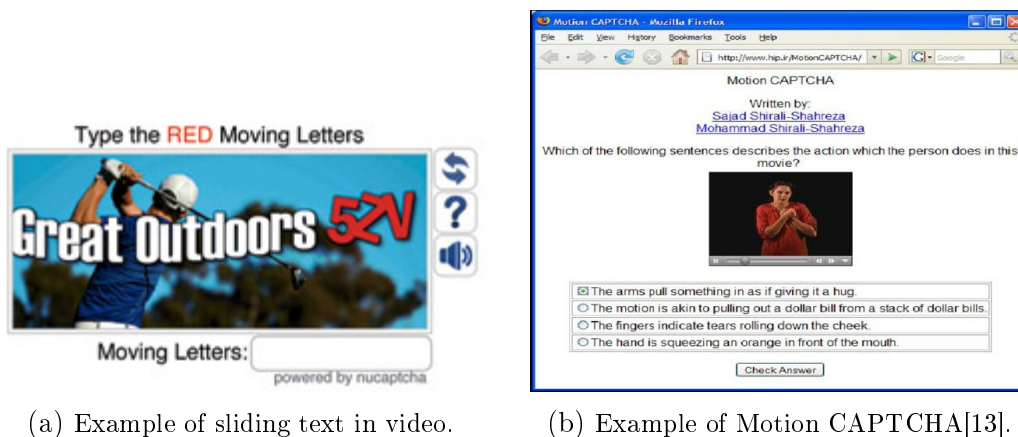


Figure 2.7: Example of text-based CAPTCHA.

- **Video-based**

this type of CAPTCHA is not very common because of the weight of the file to be downloaded[7]. The traditional video-based CAPTCHA is composed by a video in which a sliding text is shown (see Figure 2.8a). The user needs to type this message in a text field to pass the challenge. Some implementations of this type of CAPTCHAs are vulnerable to machine learning attacks.

Another similar and interesting variant of this CAPTCHA is the *Motion CAPTCHA*[13], developed by M. Shirali-shahreza and S. Shirali-shahreza, in which the user needs to watch a video. Then he needs to select which action was performed in the played file, choosing it from multiple answers (see Figure 2.8b). The strength of these implementations of CAPTCHAs depends on the relationship between the multiple choices submitted to the user[14].



(a) Example of sliding text in video.

(b) Example of Motion CAPTCHA[13].

Figure 2.8: Examples of video-based CAPTCHAs.

Some types of CAPTCHA don't destroy a session, after the correct answer is inserted by the user[4]. Hence, the hacker can crack following accesses using the same session id with the related solution of the challenge, after connecting to the web page of CAPTCHA. In this way the attacker can make hundreds of requests before the session expires and the previous operation must be computed again.

More details about the particular implementations of many of previously mentioned CAPCTHAs types are explained in the article of Walid Khalifa Abdullah Hasan[7]. With respect to user experience, the most enjoyable CAPTCHAs are usually the game-based and image-based ones but the most frustrating CAPTCHA is the text-based one[12]. A summary of usability and security issues is shown in Table 2.2.

2.3 Alternatives

This types of CAPTCHA and authentication mechanisms are far from traditional CAPTCHAs and aren't based on cognitive knowledge of the human user but on other parameters:

- **Biometrics-based**
- **Behavioural-based**
- **Social media sign-in**

CAPTCHA type	Usability issues	Security
<i>Arithmetic (Math)</i>	To be more effective, it requires advanced math knowledge.	Vulnerable to OCR techniques.
<i>Audio-based</i>	Issues of recognition: <ul style="list-style-type: none">• Previous knowledge of English dictionary by the user.• Some character sounds very similar to others.	It's vulnerable to ASR programs.
<i>Game-based</i>	No problem	Vulnerable to Stream Relay Attack
<i>Image-based</i>	Difficulty of identification of images caused by: <ul style="list-style-type: none">• Blur of images.• Low vision condition.	
<i>Puzzle-based</i>	Too much time to solve the puzzle	No significant issues
<i>Text-based</i>	Many problems have to be solved by user: <ul style="list-style-type: none">• Multiple fonts.• Font size.• Blurred Letters• Wave Motion.	It can be identified by: <ul style="list-style-type: none">• OCR technique• Segmentation techniques• Machine Learning and Deep Learning techniques
<i>Video-based</i>	Heavy file to be downloaded	

Table 2.1: Survey of main types of traditional CAPTCHAs[6].

Alternative	Type	Name of implementation	Usability issues	Security
-------------	------	------------------------	------------------	----------

Table 2.2: Survey of main types of alternatives of CAPTCHAs[6].

Bibliography

- [1] E. Bursztein, M. Martin, and J. Mitchell, "Text-based CAPTCHA strengths and weaknesses" in *Proc. 18th ACM Conference on Computer and Communications Security (CCS)*, 2011, pp. 125–138.
- [2] Silky Azad, Kiran Jain, "Captcha: Attacks and weaknesses against OCR technology" in *Global Journal of Computer Science and Technology*, 2013.
- [3] Jennifer Tam, Jiri Simsa, David Huggins-Daines, Luis von Ahn, and Manuel Blum, "Improving Audio CAPTCHAs" in *Symposium On Usable Privacy and Security (SOUPS)*, 2008.
- [4] Sarika Choudhary, Ritika Saroha, Yatan Dahiya, and Sachin Choudhary, "Understanding CAPTCHA: Text and Audio Based Captcha with its Applications" in *International Journal of Advanced Research in Computer Science and Software Engineering*, 2013, vol. 3(6), pp. 106-115.
- [5] Darko Brodić, Alessia Amelio, Radmila Janković, "Exploring the influence of CAPTCHA types to the users response time by statistical analysis" in *Multimedia Tools and Applications*, vol. 77, pp. 12293–12329, 2017.
- [6] Ved Prakash Singh, Preet Pal, "Survey of Different Types of CAPTCHA" in *International Journal of Computer Science and Information Technologies (IJCSIT)*, vol. 5(2), 2014.
- [7] Walid Khalifa Abdullah Hasan, "A Survey of Current Research on Captcha" in *International Journal of Computer Science Education in Schools (IJCES)*, vol. 7, pp. 141–157, 2016.
- [8] Goswami G, Powell BM, Vatsa M, Singh R, Noore A, "FaceDCAPTCHA: face detection based color image CAPTCHA" in *Future Generation Computer Systems*, vol. 31(2), pp. 59–69, 2014.

- [9] Wen-yao Lu and Ming Yang, "Face Detection Based on Viola-Jones Algorithm Applying Composite Features" in *International Conference on Robots & Intelligent System (ICRIS)*, pp. 82-85, 2019.
- [10] Carlos Javier Hernandez-Castro, Arturo Ribagorda, "Pitfalls in CAPTCHA design and implementation: The Math CAPTCHA, a case study" in *Computers & Security*, vol. 29(1), pp. 141-157, 2010.
- [11] Manar Mohamed, Song Gao, Nitesh Saxena, Chengcui Zhang, "Dynamic cognitive game captcha usability and detection of streaming-based farming" in *The Workshop on Usable Security (USEC), co-located with NDSS*, 2014.
- [12] Ruti Gafni, Idan Nagar, "CAPTCHA – Security affecting user experience" in *Issues in Informing Science and Information Technology*, vol. 13, pp. 63-77, 2016.
- [13] M. Shirali-Shahreza and S. Shirali-Shahreza, "Motion CAPTCHA" in *2008 Conference on Human System Interactions, Krakow*, pp. 1042-1044, 2008.
- [14] Kameswara Rao Kavya Sri, Gnana Sai, "A Novel Video CAPTCHA Technique to Prevent BOT Attacks" *International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science*, vol. 85, pp. 236-240, 2016.