Graphic Method for Human Validation of Web Users

Jose A. Noh[1], Cinhtia M. González[2], Michel García[3]

Facultad de Matemáticas, Universidad Autónoma de Yucatán, Tizimín, México[1, 2, 3]

Abstract: This paper presents an alternative to traditional CAPTCHA methods used on the Web. The CAPTCHA methods allow differentiating between human users and automated algorithms, as a security service for information websites. The traditional CAPTCHA methods use some type of Optical Character Recognitions (OCR) on images. In this work some concepts related to interactive human testing are presented, subsequently developing and proposing a new CAPTCHA method, based on the identification of sectioned graphic images. The new method is compared with the traditional one based on OCR and a comparative analysis of the two methods is presented. A group of users assess the usability of the new method after interacting with a system incorporating a traditional OCR CAPTCHA method and other with the new method not based on OCR. The results show that the proposed method is more pleasant for users; besides, this new method has been made available for public use.

Keywords: CAPTCHA, OCR, Graphics, Usability.

I. INTRODUCTION

The web sites that contains registration forms for users to access certain services are a common target for malicious attacks. These attacks are often carried out automatically using some software that tries to send large amount of data to serve multiple purposes, causing problems ranging from the removal of pages to identity theft or denial of service (saturation of the server), the last one due to the automatic conduct of the same request to the server several times.

The above gives rise to the methods of user authentication, which consists of incorporating in web forms a little security lock whose opening is easy to achieve for a human being, but hard for an automated program or robot-spammer, thus achieving to regulate the access to certain services on the web.

Such methods come from techniques that has been denominated HIP (Human Interactive Proofs), which enable a person to authenticate through a challenge offered by the computer, which should be easy to overcome for a human, but difficult for who is not [1]. In other words, the human user proves to be so through a challenge/answer that usually consists of a problem compound of graphic elements (words, images and even videos) [2].

Since its beginnings, the authentication methods of users cost time and effort, which led them to turn into a complicated and tedious task for users. Thus, web designers and programmers gave themselves the task of improving the methods of user authentication, coming to what today is known as CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), one of the more popular authentication methods nowadays.

The CAPTCHA term started to be used in the year 2000 at Carnegie Mellon University, and responds to a play of words, since the pronunciation of the word reminds of "catch ya", an informal version of "I catch you" [4].

The CAPTCHA methods are based on artificial intelligence [2] and are oriented to benefit the owner of a web site since they filter the unwanted spammer robots, and provide enhanced user security perception [3].

The application of one of the most popular CAPTCHA methods of the present day, consists of displaying several characters distorted in an image whose pictorial effects hinder slightly the identification of the code that the human user must enter and that cannot be easily recognized by a malicious bot.

Algorithms inspired by the CAPTCHA method are classified primarily as based and not based on OCR (Optical Character Recognition) methods [2]. OCR based methods are the most known and used nowadays, they consist of displaying the image of a word distorted with several effects, which must be typed by the user and, due to the pictorial effects and the restricted time to transcribe the presented characters, can hardly be deciphered by a spammer robot. For its implementation, usually a general procedure is followed, in which the methods of generation are differentiated by means of the algorithms to choose words/dictionaries, the format applied to characters, and the degradations performed on the images.

This paper presents a new algorithm developed as a method not based on OCR, in which users must identify which are the inconsistent parts of an image that has been partitioned in a grid of puzzle type where two random pieces have been incorrectly positioned. In this way the user will be able to validate his or her human identity by clicking on the inconsistent parts of the image.

Subsequently to implementation, several tests were performed comparing the new implemented method with an OCR based method, with the purpose of comparing the usability and to analyse its degree of acceptance among users.

Table 1 presents some CAPTCHA generation techniques classified in two groups: those based on text and those based on images.

Table 1. Generation techniques, classified as: based on text and based on image. Classification taken from [5].

Type	Generation Technique
Text-based techniques; Techniques based on character recognition (OCR).	Gimpy
	Pessimal Print
	MSN CAPTCHA
	Baffle Text
	Scatter Type
Image-based techniques; Techniques non-oriented to character recognition (No OCR).	Bongo
	PIX
	IMAGINATION
	Simplified 3D to 2D

These methods accessibility is sustained in the principles of inclusive design or universal design, which consists of a series of premises which aims to verify that products and environments are designed to be easy to use for the greatest possible number of people, without the need to adapt them or to redesign them in a special way [6].

Since its inception, user authentication methods cost time and effort, becoming a complicated and tedious task for users [7]. Thus, programmers and web designers embarked upon the task of improving the users authentication, arriving at what today is known as CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), one of the most popular authentication methods.

According to [9], for a human being, average resolution time for an OCR-based authentication method is 16 seconds, in comparison, the average time that a bot takes to obtain an attempt of solution, which could be wrong or right, is of approximately 6 seconds, regardless of the method used [10].

However, the existing popular CAPTCHA methods currently require the user to invest a significant amount of time, what is desirable to reduce. According to [4], it is possible to solve these problems, what led to the creation of new CAPTCHA, some of them as effective as the traditional image-based but presenting greater accessibility for people with disabilities.

Besides, as is the case with any type of application used to prevent the illicit use of a service, the CAPTCHA are susceptible to attacks, and given that its main use is the protection of the mail registration through forms, the largest number of attacks comes from the spammers, who maintain a constant search for free registration and use of multiple email accounts. It is important to note that these are in constant development, as well as the efforts to prevent them, so that "actually it has always been clear to the CAPTCHAs creators that these will have a useful life determined and only a high percentage (expected to be very high) of effectiveness" [8].

This paper presents a tool created for the authentication of users who wants to access a web service using a CAPTCHA graphical method not oriented to character recognition for the validation of some human user who wishes to access certain web system. The purpose of this new method is to decrease the access time, improving usability and accessibility, through a method that seeks to be easy to solve for a human and difficult for a computer. This validation method will be available to be used in services that need of human validation, offering a quick, safe, and visually attractive option.

II. DEVELOPMENT

It has been developed a web system in which are implemented two authentication methods: the first based on the optical recognition of characters (OCR), and the other not based on OCR. In the Non-OCR-based proposed method, the user must identify the inconsistent parts of an image that the algorithm has partitioned obtaining a partitioning matrix from which two parts are randomly selected and their positions interchanged. At each attempt the image is renewed, is randomly obtained from a database located in the web. To solve this new authentication method, the user has a limited amount of time in which he or she must choose which are the parts that are out of their original position in the image. This approach pretends that the user can validate his human identity while is managed to restrict the automated access of spammer robots to the web systems.

Upon completion of the algorithm design, development and implementation, a comparative analysis was carried out between the Non-OCR-based proposed method and an OCR-based one obtained from a web service. To perform an accurate analysis, it was implemented an online system that shows to users both types of authentication, one after another, to then gather information from the user, to finally show them the minutes and seconds that were necessary to invest to pass every method. This was done in order to compare the efficiency between both methods and gather information to improve the proposed one.

Subsequently to the performed tests, the recommendations made by the users were attended, and the new developed method was made publicly available to users.

The OCR-based method used in the comparison was obtained from the site http://www.phpCAPTCHA.org (Fig 1), a replica was created and adapted to include in the system and perform the corresponding tests.

Fig 1. Logo from the web of Securimage

With the demo tab of the previous mentioned site is possible to visualize the three alternatives that the method has. By default, the package offered to download is the first option, which is one of the most used and that is

commonly found in web sites that contains registration forms. It is also possible to listen the audio of the displayed characters. Fig. 2 shows the method that offers a traditional interface of distorted alphanumeric characters that users must recognize and transcribe accurately (case sensitive) to validate their human identity.

Fig. 2. OCR-based method obtained and adapted to the test site.

In the second algorithm (Non-OCR method), it is displayed an image randomly selected from a database, which simulates to be a puzzle in which exists two pieces incorrectly positioned, which the user must identify, and by clicking on these pieces he or she is granted access.

The implemented system to perform the comparison measures the time that takes for each user to solve each method, considering that if a user requests to change the image, the stopwatch is restarted too.

For testing, initially 30 royalty-free images randomly chosen were used, obtained from the website of Gimp (http://www.gimp.org.es/), in the section of royalty-free images to download for free. To obtain the optimal features required by the images to be solved by users, some lines were traced using the editing tools of the software Gimp. At the end all the images were stored in an online server, from where the tests were performed with the users.

An example of this method would be the division of an image in four divisions by side, generating, an image with 16 pieces of the same size, each piece is stored in an array, using a random function, two different numbers are chosen according to the array size, and the corresponding pieces are interchanged, being stored in a new array with the new order, then the new image corresponding to the new arrangement is shown, with the two interchanged pieces. Specifically exists one solution, and it is clicking the two interchanged pieces, in this test it is possible to select other pieces, but it would not be a solution and this would lead the user to be delayed in accessing the protected information.

In the future, with the collected data will be provided a fixed number of pieces and changes of images when failing the selection, likewise, this method evaluates the time required by the user to solve the test, and the most common amount of pieces since this preliminary test shows 4, 5 or 6 divisions by side.
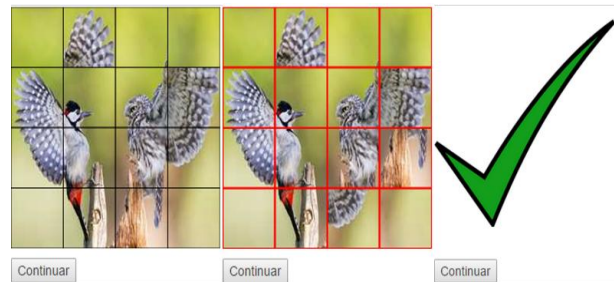

Fig. 3. Proposed method, Non-OCR.

Fig. 3 shows the sequence of actions that a user performs during the tests. Initially is presented an image with two parts placed incorrectly, the user must select these two pieces clicking on them. The user is then notified that the test has been correctly solved. As this is an initial test there is no error of solution, if the user fails, the method stops working, and the page must be restarted to get a new image.

Both methods were developed using HTML, PHP and JavaScript, as well as a web server Apache and an online server for Hosting. The complete interface consists of a sequence of forms that allow the users to interact with both methods consecutively and express their opinion regarding their experience. Thus, the novel proposed method will be able to be included in any web site in which is wished to be sure that visitors interacting with it are people and not spam robots trying to register on the website, post comments in blogs, etc. [3].

Once the system was published on an online server, the experiments were carried out spreading the address and inviting to participate through different digital media. 54 persons participated, who interacted with both methods and subsequently issued their opinion on the subject, of which 61.1% stated to possess an intermediate experience, and 38.8% manifested to have an advanced level in the use of systems.

Table 2 shows the information obtained from 15 of the total of participants in the test site for the comparison between the Non-OCR CAPTCHA method and the OCR-based one likewise is presented the preferred method selected by users.

Table 2 Information about the selection of the preferred method and the resolution time of 25 participants in the test.

# of participant	Preferred method	Time on Non-OCR method	Time on OCR method
1	Non-OCR	00:00:03	00:00:08
2	Non-OCR	00:00:03	00:00:07
3	Non-OCR	00:00:06	00:00:06
4	Non-OCR	00:00:14	00:00:12
5	Non-OCR	00:00:04	00:00:10
6	Non-OCR	00:00:06	00:00:09
7	Non-OCR	00:00:03	00:00:08
8	Non-OCR	00:00:06	00:00:11
9	Non-OCR	00:00:05	00:00:09

10	Non-OCR	00:00:03	00:00:08
11	Non-OCR	00:00:05	00:00:16
12	Non-OCR	00:00:09	00:00:16
13	Non-OCR	00:00:05	00:00:11
14	Non-OCR	00:00:04	00:00:13
15	Non-OCR	00:00:05	00:00:19

From the total of participants was obtained that altogether the resolution time for the provided OCR-based method was on average of 11 seconds, while for the second method, Non-OCR-based, on average was solved in 6 seconds.

Users were also asked about their opinion regarding both methods. All expressed opinions coincided in that the second method (Non-OCR) turns out to be more enjoyable than the first one (OCR-based).

With these results, is possible to conclude that the minimum resolution time is fulfilled so that the method's test could be solved in a time no longer than 6 seconds, on the contrary the user should repeat the authentication process with a new image and a new pair of pieces placed incorrectly.

On the other hand, as was observed in the comments and results provided by users during the preliminary tests, there were no problem in 4 and 5 divisions by side, so with the aim of increasing the method complexity for bots, it will be used a static amount of divisions which is of 5 by side, thus producing an image with 25 pieces.

III. IMPLEMENTATION

In order that all users can try the proposed CAPTCHA method, it was modularized, which consisted in to identify all components necessary for the correct operation of the method and making them available in an only web page so that any user (a web page developer) could take and use the method without great complexity, having as benefits:

- Is not needed to have a database of images in site, it would be remote, so it would not use space of the own server or hosting service.
- No worries about PHP versions, the server on which the method is hosted would run it.
- Reduced complexity for embedding some form, it would only need an "include" function from the standard of PHP.
- It avoids the need of downloading the method and embedding it in the user's site, and in some cases, that the user modifies the code according to the PHP version of his/her server.

Despite the method not being hosted in the server or hosting service of the user that intends to use the method, he or she will not notice the difference of a remote access because it will be the own server on use which will remotely access the server that hosts the CAPTCHA method for use.

For the method publication it was used a colorful and animated design with several .gif images, so that the users find it attractive, as Fig. 4 shows.
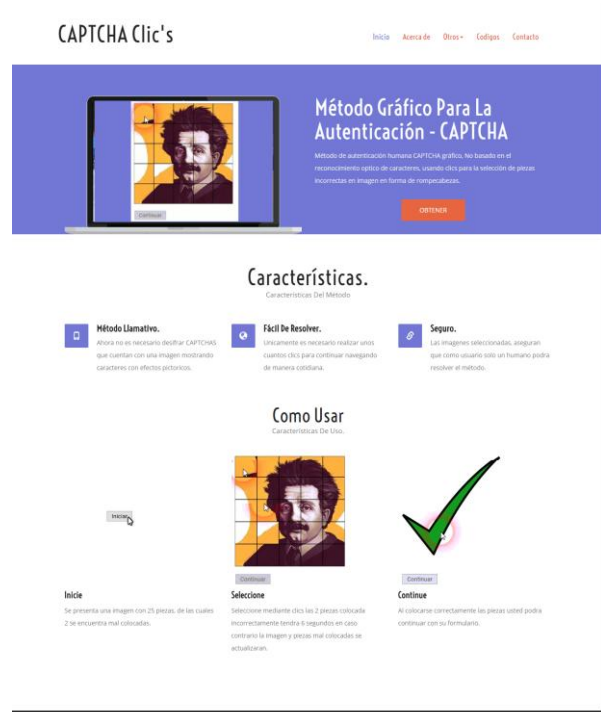

Fig. 4. Initial interface of the publication site of the method.

The web address of this site is: www.cclics.96.lt ; where the implementation of the method is already published, and is possible to obtain the instructions for embedding the method in most web pages.

While exploring the site the potential user will be able to notice at several points the text "OBTENER" ("GET"), even some images will be linked to this action, which consists of the instructions to embed the CAPTCHA method in the form in which the user wants it.

The same site, as part of the instructions to get the method, is explained the procedure to follow for embedding the method in many kinds of web pages, in order to see the procedure, the user must solve the method and validate his/her humanity, on success will be automatically deployed the steps that the user must follow for the correct operation of the CAPTCHA method in most kind of forms.

For the correct operation of the method in a form with its attributes defined, it is not necessary to place a "submit" option in the form in which the method is being used, this method provides, upon being correctly solved, a send button which performs the actions declared in the form where the CAPTCHA method is being used. It needs to be noted that the method has been developed in PHP7 and HTML5, compatible with the browsers FIREFOX, CHROME, OPERA, SAFARI; in their current versions.

The structures of the most common forms are:

Fig. 5. Example of a form structure using the attribute "action".

Fig. 6. Example of a form structure using the attribute "submit".

Fig. 5 presents the common structure of a form using the attribute "action" for the execution of external procedures or page redirection, similarly Fig. 6 presents the same structure but using the attribute "submit" of an HTLM form.

Now it will be embedded in the form the CAPTCHA method, which can be placed in any wanted position within the form, although is suggested to place it at the end to not interfere with the filling of data in the form. For using this tool, it is necessary to invoke the developed code, which can be done through the use of the sentence "include" of PHP, together with the address: http://goo.gl/KzlOry, concluding with a structure similar to what is shown in Fig. 7.

Fig. 7. Structure to embed the method in a form.

It is important to mention that the web file to include must contain a PHP method, since otherwise the tags " <?php … ?>" can not be used, and therefore the method will not be embedded.

IV. CONCLUSION

This paper presents the design and implementation of a new method for authenticating web users. The purpose of the work is to offer an alternative for human authentication in web forms, using a CAPTCHA method not oriented to Optical Character Recognition (Non-OCR). The new method is based on an image sectioned to look like a puzzle about to be resolved. This method sets off using a square image from which is obtained a partition of 25 pieces of equal size, shown in such way that is visually perceived the original image, except by two pieces incorrectly positioned. The user must identify which are those two misplaced pieces and click on them. This generates a challenge that the user must solve at a maximum time of 6 seconds. In case of exceeding this time, a new image is loaded and new pieces are misplaced, with which the method restarts.

Surveys conducted systematically during the implemented tests threw positive results for the use of this method. [11] suggests to conduct usability evaluations to ensure that individuals can solve the challenge on time and with reasonable success rate.

In order to obtain the results and characteristics of the method it was necessary to initially perform comparison tests with a CAPTCHA method based on the Optical Character Recognition (OCR) method, so it was created and disseminated an online web site (www.pruebacaptcha.esy.es) for the evaluation of both methods, obtaining as data the users' age, their expertise using systems, the amount of time needed to solve each method, and their comments about the evaluation, as well as an "id" containing the type of device used when participating in the evaluation. At the end 54 volunteers participated in the evaluation.

At this stage it was concluded that the developed Non-OCR method was successfully implemented, it was verified that it requires less time to solve for a human, and that users like more this new method than the traditional textual one that is commonly found in diverse web sites.

With the obtained results a new web site was created, located at the web address: www.cclics.96.lt, which contains the information obtained in the tests, besides from this site is possible to get structures to call the Non-OCR method, which permits to embed the method in any web form, as an authentication alternative, this published method has a database of 54 different images, which will be randomly selected, then divided into 25 pieces of which two will be misplaced, and the user must choose those misplaced in less than 6 seconds and more than one second. A variant of the presented method that could increase security, would be to misplace more than two pieces, although it would also increase the resolution time.

ACKNOWLEDGMENT

REFERENCES

[1] J. Areitio Bertolín y T. Areitio Bertolín, «Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación,» Revista española de electronica, pp. 52-67, 2007.

[2] M. Shirali-Shahreza y S. Shirali-Shahreza, «Encouraging Persons with Hearing Problem to Learn Sign Language by Internet Websites,» de Eighth IEEE International Conference on Advanced Learning Technologies, ICALT '08 , IEEE , Tehran, Iran, 2008.

[3] V. Cabezas Mena, A. Sabaté Mojica, A. Vendrell Villafruela y M.-C. Marcos, «Experiencia de usurio y captchas, explorando la semiótica visual,» no solo usabilidad, 2014.

[4]   O. Prieto Gordo y D. Martínez Ávila, «Servicios Accesibles de Acceso Esclusivamente Humano,» de Segunda Conferencia Internacional sobre brecha digital e inclusión social, Leganés, Madrid, España, 2009.

[5]   A. M. Vazquez, «Diseño e implementación de un protocolo seguro de intercambiode mensajes con un dispositivo seguro,» Universidad Carlos III de Madrid, Madrid, España., 2010.

[6]   EIDD, «dfaeurope.eu,» 9 Mayo 2004. [En línea]. Available: http://dfaeurope.eu/what-is-dfa/dfa-documents/the-eidd-stockholm-declaration-2004/.

[7]   S. Jain y B. Sivaselvan, «Usability Aspects of HCI in the Desing of CAPTCHAs,» International Conference on Computational Intelligence and Computing Research, pp. 1-4, 2012.

[8]   F. J. Elizondo, «Enredándose, CAPTCHA,» Ingenierias, pp. 74-78, 2008.

[9]   A. Y. López Sánchez, N. U. López Flores y A. L. González Lara, «COMPARACIÓN DE USABILIDAD ENTRE CAPTCHA BASADO EN TEXTO Y CAPTCHA BASADO EN IMÁGENES,» de Memorias Arbitradas Del VIII Congreso De Ingeniería Industrial Y De Sistemas, San Nicolas de los Garza, Nuevo Leon, Mexico, 2013.

[10] C. Hadiwijaya Saputra, E. Adi y S. Revina, «Comparison of Classification Algorithms to tell Bots and Humans Apart,» Journal Of Next Generation Information Technology [serial online], pp. 23-32, 2013.

[11] R. Gossweiler, M. Kamvar y S. Baluja, «What's Up CAPTCHA? A CAPTCHA Based On Image Orientation,» de 18th international conference on World wide web, Nueva York, NY, EE.UU, 2009.

BIOGRAPHIES

Jose Alberto Noh Student of eighth semester of a degree in computer science at the Autonomous University of Yucatan. His research interests include artificial intelligence, software development and web applications.

Cinhtia Maribel Gonzalez Segura Master in Computer Sciences for the Institute Technology of Monterrey in México, is professor of the Autonomous University of Yucatán. Responsible of the Intelligents Systems lab. His researcher lines: Optimization, Artificial Intelligence, Mobile Robots

Michel Garcia García Master in Computer Sciences for the Institute Technology of Monterrey in México, is professor of the Autonomous University of Yucatán, actually collaborate in the Intelligent Systems Lab. His researcher lines: Machine Learning, Artificial Intelligence, Mobile Robots.