Capítulo 3

DISEÑO E IMPLEMENTACIÓN DE UN CAPTCHA PARA BRINDAR SEGURIDAD EN SITIOS WEB MEDIANTE RECONOCIMIENTO DE IMÁGENES

Manuel Oswaldo López Marín, Marlon David González Ramírez, José Félix Serrano Talamantes, Eduardo Vega Alvarado

Instituto Politécnico Nacional, México

mlopezm1809@ipn.mx, dgonzlaezr@ipn.mx, jfserrano@ipn.mx, evega@ipn.mx

https://doi.org/10.3926/oms.411.3

López Marín, M. O., González Ramírez, M. D., Serrano Talamantes, J. F., & Vega Alvarado, E. (2022). Diseño e implementación de un captcha para brindar seguridad en sitios web mediante reconocimiento de imágenes. En M. A. Ramírez Salinas, L. N. Oliva Moreno, L. I. Garay Jimenez y P. Gomez Miranda (Ed.), *Avances 2022: Red de Investigación Computación del Instituto Politécnico Nacional, México* (pp. 49-60). Barcelona, España: OmniaScience.

Resumen

Actualmente hay una creciente necesidad de evitar generar o difundir información falsa en el internet, lo que obliga a los proveedores de servicios a proporcionar ciertas medidas de seguridad a sus posibles clientes. En este contexto, el presente trabajo tiene como objetivo primordial desarrollar una opción simple, segura y eficiente para la validación de un usuario al momento de interactuar ya sea con otros usuarios o con diferentes tipos de sistemas. Para ello se propone un esquema basado en imágenes que incluyen expresiones; su finalidad es utilizarlo en las validaciones del tipo desafío-respuesta conocido como prueba de Turing Pública y automática (*captcha*), para poder diferenciar a las máquinas (*bots*) de los seres humanos cuando se registra un intento de ingreso a un sitio web. La solución del captcha implica la identificación de una emoción aleatoria dentro de una imagen tipo GIF, la cual a su vez está conformada por nueve imágenes del mismo tipo. Dicha imagen cuenta con diferentes niveles de distorsión gráfica, lo que dificulta la identificación de la emoción en un grado mínimo para el usuario humano promedio, pero suficientemente compleja para una máquina. Esta propuesta fue programada en los lenguajes Java y HTML5. El desarrollo se validó con ayuda de un grupo de 90 individuos con personalidades diversas, para efecto de las pruebas de usabilidad. Los resultados muestran que una mayoría de usuarios calificaron al sistema como de fácil uso, indicando adicionalmente que la identificación de las emociones también fue lo suficientemente simple para recomendar su empleo para control de acceso a sistemas reales.

Keywords

Captcha, imagen GIF, Test de Turing, bots, expresión facial.

1. Introducción

Las pruebas de Turing proponen un método para indicar la existencia de mentalidad en las computadoras, y consisten en que una computadora puede inducir a sus interrogadores a creer que es una persona. La prueba de Turing inversa es una reorientación de la prueba de Turing, en la que se plantea que los seres humanos son el objeto de estudio y se prueba sí son o no distinguibles de las máquinas [1].

Una c*aptcha* (*Completely Automated Public Turing test to tell Computers and Humans Apart*: prueba pública de Turing completamente automatizada para distinguir a las computadoras de los humanos), es una medida de seguridad que se aplica comúnmente en páginas Web, de tal manera que ayude a proteger del Spam (Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales), o para evitar el descifrado de contraseñas, efectuando una serie de pruebas para verificar que es un humano y no una computadora quien quiere acceder a la cuenta, tal como lo intentan los hoy conocidos como *hackers*, quienes son expertos en descubrir vulnerabilidades en sistemas. En la Figura 1 se muestran algunos captchas, indicándose la página Web donde se utilizan:

La prueba de un captcha consta de dos etapas, mismas que se muestran en la Figura 2: 1) Se genera aleatoriamente una serie de letras o números que comúnmente aparecen en imágenes ligeramente distorsionadas, 2) el usuario humano debe identificar estas letras o números y escribirlos en un cuadro de texto.

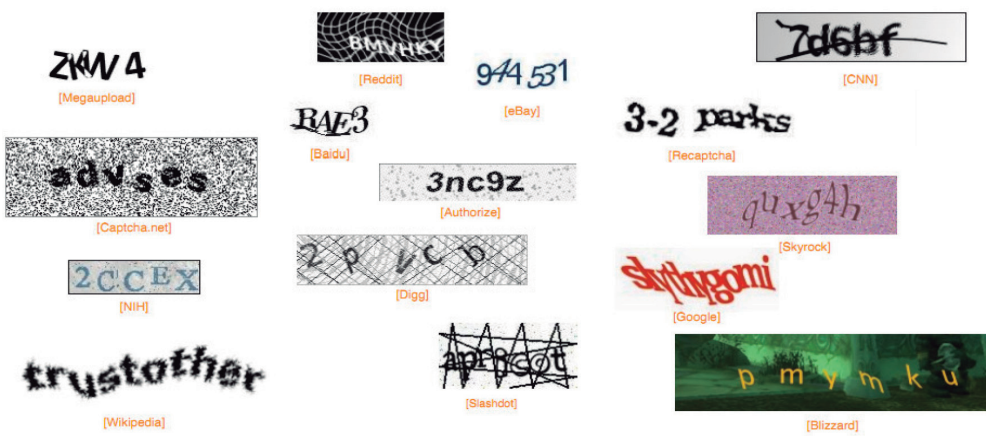

Figura 1. Ejemplos de las partes del Captcha

Figura 2. Generación de un captcha e ingreso de las letras y números correspondientes[8]

El usar un captcha ofrece protección contra entradas digitales remotas, ya que un ser humano con el conocimiento de su información y apoyo de un sistema de cómputo puede acceder a su cuenta. Actualmente se puede ver el uso de captchas en varias páginas Web de renombre, como lo son: Facebook, YouTube, Amazon, Google, etc. Estas páginas, al ser muy grandes y con un compromiso social, deben salvaguardar los datos personales de sus usuarios, como lo son: direcciones, contraseñas, datos de tarjetas de crédito o débito, etc.

Los captchas se pueden usar en las siguientes situaciones:

- registrándote para un nuevo servicio (Gmail, Facebook o YouTube),
- registrándote en cualquier edición de una cuenta
- cambiando una contraseña en una cuenta ya existente,
- configurando servicios a otro dispositivo o aplicación (como iPhone, Outlook, ActiveSync, etc.).

Existe un nuevo término para identificar al complemento de algunas acciones de un captcha, denominado *ReCaptcha*. Este sistema mantiene la idea usada por muchos captchas de obligar al usuario a reconocer una palabra, pero en este caso se añade una segunda palabra que el sistema de reconocimiento de imagen es incapaz de descifrar. Si un número suficiente de usuarios introducen de forma correcta la palabra conocida y transcriben la desconocida de forma similar, se considera que esta es la forma correcta [1].

Respecto al desarrollo de diversas variantes de captchas destacan los siguientes trabajos: En B. Kurt Alfred Kluever [2] se plantea un captcha de video en donde el usuario proporciona tres etiquetas que identifiquen un video presentado. Por su parte en R. Gossweiler, M. Kamvar y S. Baluja [3] presentaron un captcha

tipo texto que se basa en la orientación vertical de una imagen. En G. Goswami, B. M. Powell, M. Vatsa, R. Singh y A. Noore [4] propusieron un captcha basado en el reconocimiento de rostros de un mismo sujeto, donde el usuario distingue los rostros de entre imágenes no humanas, fondos, distorsiones y caras. Ellos implementaron un captcha donde el usuario selecciona rostros humanos dentro de una imagen con distorsiones, además propusieron un captcha en el que en una imagen se tiene que encontrar un par de caras humanas en un conjunto de fondos e imágenes distorsionados. En A. Kumarasubramanian, R. Ostrovsky, O. Pandey y A. Wadia [5] exploraron la manera de utilizar los captchas de manera criptográfica al proponer la creación de un protocolo basándose en el proceso de resolución. En M. Fujita, Y. Ikeya, J. Kani y M. Nishigaki [6] crearon un captcha en el que se mezclan dos imágenes tridimensionales formando una tercera, y el reto es identificar una imagen individual. En C. J. Hernández-Castro, M. d. R-Moreno, D. F. Barrero y S. Gibson [7] crearon un captcha para resolverse mediante el uso de *machine learning* teniendo por objetivo identificar vectores de ataque. En S. Gao, M. Mohamed, N. Saxena y C. Zhang [8] diseñaron un catpcha tipo video, e implementaron un marco de ataque automatizado para vencer este diseño usando procesamiento de imágenes. En M. Osadchy, J. Hernandez-Castro, S. Gibson, O. Dunkelman y D. Perez-Cabo [9] identificaron los principales problemas de seguridad en los captchas, apoyándose de técnicas de *deep learning*. En D. Lin, F. Lin, Y. Lv, F. Cai y D. Cao [10] presentaron un desarrollo con el objetivo de resolver captchas de tipo texto basados en el lenguaje chino. En 2018, investigadores del Instituto de Tecnología de Georgia crearon un captcha basado en reconocimiento de rostros específico para dispositivos móviles. En M. Ogiela, N. Krzyworzeka y L. Ogiela [11] plantearon una propuesta de captchas cognitivos, en los que su resolución se basa en tener conocimientos especiales y habilidades perceptivas. Finalmente, en T. Lawan [12] propone tres diferentes tipos de captcha, diferenciando cuáles son los patrones idóneos de usabilidad para la creación de un captcha, resultando que los captchas con imágenes son los más simples de resolver por usuarios.

2. Metodología

Para el desarrollo de este sistema se utilizaron las siguientes aplicaciones:

- CentOs 7,
- WildFly 14,

- MariaDB,
- JavaScript,
- JavaServer Faces (JSP) y
- Html5.

El primero de ellos, CentOs 7, es un sistema operativo con núcleo Linux con la ventaja de ser una distribución libre estable y con documentación disponible. Por su parte, WildFly 14 es un servidor de aplicaciones flexible en el desarrollo de interacciones y una comunicación cliente-servidor confiable; además, cuenta con una variada compatibilidad con diversas herramientas de desarrollo y *frameworks*. Finalmente, MariaDB es un repositorio y manejador de bases de datos, escalable y de mediano alcance de distribución libre, compatible con las plataformas antes mencionadas.

Como herramientas de desarrollo se contó con el lenguaje Java y JavaScript; el primero de ellos se utilizó para desarrollar la imagen dinámica de nueve emociones utilizando el *framework* de JSP por medio del Modelo Vista Controlador (MVC) y, el segundo es una tecnología para desarrollar páginas Web que solamente se ejecutan con el explorador, que en conjunto con la herramienta JQuerry facilita el funcionamiento y manipulación de documentos HTML (*HyperText Markup Language*). HTML 5, es la versión del lenguaje HTML que define la estructura de un documento web.

En este trabajo se desarrolló un captcha animado tipo GIF para un servidor en red, como método de acceso a páginas web. En este caso el captcha manifiesta siete emociones, aunque se pueden adaptar más gestos. Se proporciona un tiempo de espera para que el usuario identifique las emociones. En caso de fallo se proporciona un segundo intento; si esta falla, el ingreso a la página web se descarta para evitar diversos intentos de acceso por parte de robots informáticos.

3. Pruebas y resultados

Con todo lo mencionado, se desarrolló un captcha dinámico en una matriz de 3×3 contenido en una arquitectura de red por medio de un servidor, como se muestra en la Figura 3. Dicha aplicación tiene la funcionalidad de generar aleatoriamente imágenes de emociones (alegría, tristeza, miedo, ira, asco, sorpresa y neutra) con una complejidad computacional de $\theta(n_i!)$, donde n es el número de emociones.

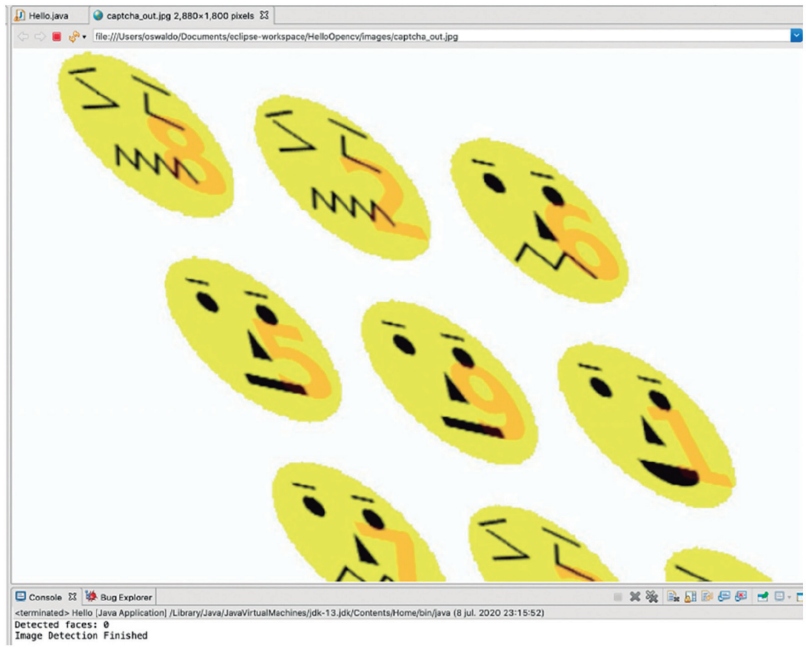

Figura 3. Captcha generado por emociones en una matriz de 3 × 3

Las pruebas de código realizadas a esta aplicación se implementaron con el objetivo de detectar los defectos en la codificación; para realizar este proceso se utilizó la herramienta FindBugs, la cual es un *plug-in* del entorno de desarrollo eclipse. Como resultado de las pruebas se obtuvo un código sin defectos. Con el objetivo de fortalecer el captcha implementado en esta propuesta, una imagen de prueba fue sometida a dos programas de identificación de rostros: OpenCV y MATLAB, como resultado dicho programa no pudo detectar rostros en dicha imagen por medio de la distorsión, es decir, el desarrollo es único (ver Figura 4). La propuesta de captcha se sometió a la validación de un grupo formado por 100 personas de diferentes entornos. Los individuos participantes en esta prueba cuentan con las características mostradas en la Tabla 1.

Al finalizar la prueba se aplicaron dos preguntas al grupo de validación, con el objetivo de conocer su experiencia de uso. De la primera pregunta, la cual se puede observar en la gráfica de la Figura 5, al 48 % le resulta fácil usar la aplicación y solo un 7 % lo consideró difícil.

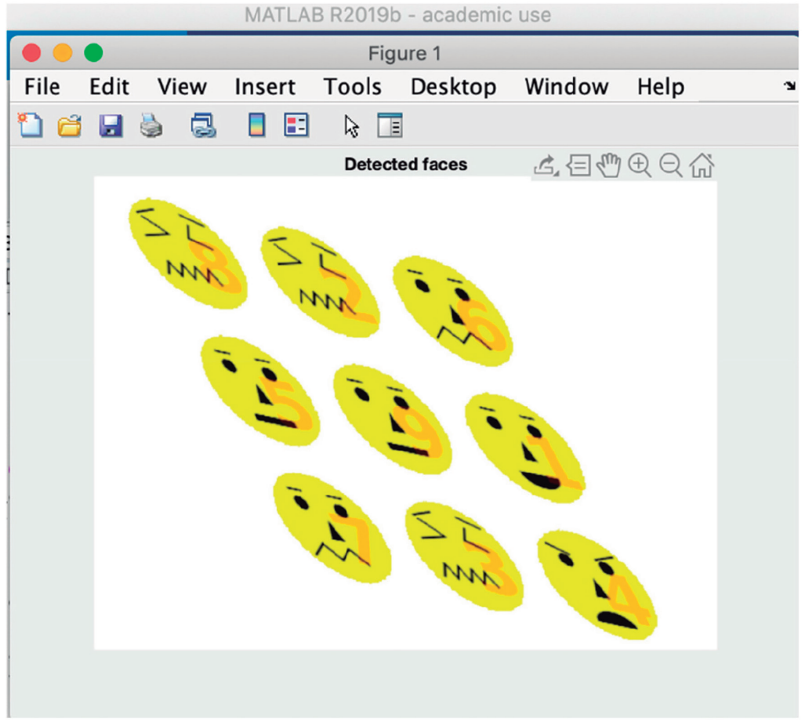

Figura 4. Rostros no identificados en MATLAB

Rango de edad	Individuos	Escolaridad mínima	Escolaridad máxima	# Hombres	# Mujeres
11 a 20	10	Primaria	Preparatoria	10	0
21 a 30	20	Licenciatura	Maestría	15	5
31 a 40	30	Licenciatura	Maestría	20	10
41 a 50	15	Maestría	Maestría	10	5
51 a 60	10	Maestría	Maestría	10	0
61 a 63	15	Preparatoria	Doctorado	15	0

Tabla 1. Características de las personas que utilizaron el captcha

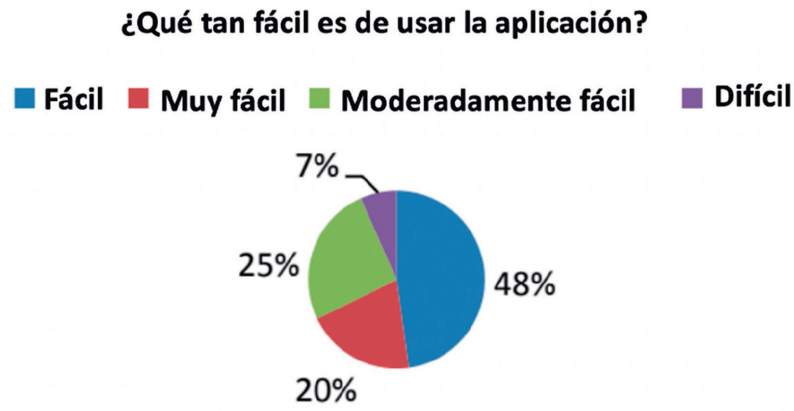

Figura 5. Usabilidad de la aplicación

Figura 6. Facilidad en la identificación de emociones

La Figura 6 visualiza la identificación de expresiones en las imágenes GIF. Se observa que el 43 % identificó sin problema alguno las expresiones representadas, mientras sólo al 10 % le resulto difícil reconocerlas.

4. Discusión y conclusiones

Se desarrolló un captcha animado tipo GIF para un servidor en red como método de acceso a páginas Web. En este caso, el captcha presenta cinco emociones,

aunque se pueden adaptar más de ellas. Las emociones se interpretaron por los usuarios de una manera media, es decir, no cualquier individuo puede identificarlas (43 %), por lo tanto, cumple con el objetivo de ser un control de acceso limitado y para usuarios específicos. Por otra parte, este sistema es flexible para integrar sentimientos y expresiones en imágenes GIF. Adicionalmente, se proporciona un tiempo de cinco segundos para la identificación de las emociones; si no hay identificación, se permite un segundo intento. Si la segunda oportunidad es fallida, se impide el ingreso a la página web como candado para evitar el acceso de robots informáticos.

La utilización de lenguaje Java y JavaScript proporcionó flexibilidad al desarrollo del proyecto, incluso por la parte gráfica del mismo, además de otorgar gran contenido de documentación. El uso de la biblioteca de visión artificial OpenCV sirvió para generar distorsiones a la imagen producida de manera aleatoria, incrementando así la complejidad del reconocimiento de las emociones.

El captcha desarrollado conllevó un trabajo de investigación, iniciando con el entendimiento de emociones universales, hasta la aplicación de distorsionas en imágenes tipo gif y su despliegue en un contexto web. Los entornos de desarrollo y las bibliotecas de procesamiento gráfico representaron una gran ayuda para culminar este proyecto; si bien existieron complicaciones, todas fueron sorteadas de tal manera que coadyuvaron en el desarrollo de esta nueva propuesta de captcha. De los resultados obtenidos en las diferentes pruebas realizadas se puede concluir que el captcha es fácil de usar, así como es sencillo identificar la expresión facial marcada en la imagen. El software tiene la ventaja de no ocupar una alta cantidad de recursos de cómputo, esto se debe que es un GIF animado, lo que le permite conservar la dificultad cognitiva que evita que pueda ser hackeado y por lo tanto se verifica la prueba inversa de Turing.

Financiamiento

Esta propuesta se deriva del proyecto de investigación *Metodología funcional de captchas basado en procesamiento de imágenes*, apoyado por la Secretaría de Investigación y Posgrado del IPN mediante el registro SIP20201616.

Referencias

[1] Antonio Vega Omar, Vinasco Salazar Ronald Eduardo, Captcha: ¿Una solución para la seguridad informática o problema para la accesibilidad/usabilidad Web? *Revista E-Ciencias de la información* Volumen 4, número 2, Ensayo 1 Julio-diciembre 2014. https://doi.org/10.15517/eci.v4i2.15125

[2] B. Kurt Alfred Kluever, Evaluating the Usability and Security of a Video CAPTCHA, Thesis. Rochester Institute of Technology, 2008. https://scholarworks.rit.edu/theses/163

[3] R. Gossweiler, M. Kamvar y S. Baluja, «What's Up CAPTCHA? A CAPTCHA Based on Image Orientation,» *In Proceedings of the 18th international conference on World wide web,* pp. 841-850, 2009. https://doi.org/10.1145/1526709.1526822

[4] G. Goswami, B. M. Powell, M. Vatsa, R. Singh y A. Noore, «FR-CAPTCHA: CAPTCHA Based on Recognizing Human Faces,» *PLoS ONE,* vol. 9, nº 4, 2014. https://doi.org/10.1371/journal.pone.0091708

[5] A. Kumarasubramanian, R. Ostrovsky, O. Pandey y A. Wadia, «Cryptography Using Captcha Puzzles,» *International Association for Cryptologic Research,* pp. 89-106, 2013. https://doi.org/10.1007/978-3-642-36362-7_7

[6] M. Fujita, Y. Ikeya, J. Kani y M. Nishigaki, «Chimera CAPTCHA: A Proposal of CAPTCHA Using Strangeness in Merged Objects,» *T. Tryfonas and I. Askoxylakis,* pp. 48-58, 2015. https://doi.org/10.1007/978-3-319-20376-8_5

[7] C. J. Hernández-Castro, M. d. R-Moreno, D. F. Barrero y S. Gibson, «Using machine learning to identify common flaws in CAPTCHA design: FunCAPTCHA case analysis,» *Computers & Security,* nº 70, pp. 744-756, 2017. https://doi.org/10.1016/j.cose.2017.05.005

[8] S. Gao, M. Mohamed, N. Saxena y C. Zhang, «Emerging-image Motion CAPTCHAs: Vulnearabilities of Existing Designs, and Countermeasures,» *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING,* 2017.

[9] M. Osadchy, J. Hernandez-Castro, S. Gibson, O. Dunkelman y D. Perez-Cabo, «No Bot Expects the DeepCAPTCHA! Introducing Immutable Adversarial

Examples, With Applications to CAPTCHA Generation,» *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,* vol. 12, nº 11, 2017. https://doi.org/10.1109/TIFS.2017.2718479

[10] D. Lin, F. Lin, Y. Lv, F. Cai y D. Cao, «Chinese Character CAPTCHA Recognition and performance estimation via deep neural network,» *Elsevier,* pp. 11-19, 2018. https://doi.org/10.1016/j.neucom.2017.02.105

[11] M. Ogiela, N. Krzyworzeka y L. Ogiela, «Application of knowledge-based cognitive CAPTCHA in Cloud of Things security,» *Concurrency Computat Pract Exper,* nº 30, 2018.

[12] T. Lawan, «Application of Pattern for New CAPTCHA Generation Idea,» *Springer International Publishing AG, part of Springer Nature,* p. 257-264, 2018. https://doi.org/10.1007/978-3-319-76451-1_24