Nexo Revista Científica
Vol. 34, No. 02, pp. 596-607/Junio 2021

ISSN-E 1995-9516
Universidad Nacional de Ingeniería

http://revistas.uni.edu.ni/index.php/Nexo
https://doi.org/10.5377/nexo.v34i02.11545

# Emoji captcha; una novedosa opción para proteger sitios web

# Emoji captcha; a novel option for protect web pages

Manuel Oswaldo López Marín[1,*], Marlon David González Ramírez[1], Rodolfo Romero Herrera[2], José Félix Serrano Talamantes[1]

[1] Instituto Politécnico Nacional. CIDETEC, Maestría en tecnología de cómputo. Ciudad de México, México.
[2] Instituto Politécnico Nacional. Escuela Superior de cómputo. Ciudad de México, México.

[*]mlopezm1809@alumno.ipn.mx

*(recibido/received: 12-enero-2021; aceptado/accepted: 17-abril-2021)*

## RESUMEN

En el presente trabajo se presenta un desarrollo de una variante de captcha con el uso de una imagen gif, compuesta por 6 fotogramas; cada fotograma está formado por 9 imágenes ordenadas en una matriz de 3 por 3; cada imagen utilizada expresa una emoción de un conjunto de 5 emociones básicas. Cada uno de los 9 sectores en los que se divide el gif, tiene asignado una marca dígito, con el propósito de que el usuario reconozca una emoción dentro del gif y utilizando sus habilidades cognitivas relacione esta emoción con un número y, de esta forma identifique la respuesta correcta. Se propone una alternativa simple y segura para la protección de sitios web, ideal para un amplio rango de usuarios, sin importar su edad o conocimientos informáticos, esto se debe al uso de emociones que son reconocidas por todo ser humano. Los desarrollos actuales realizan análisis de trafico de red y tiempo de respuesta para identificar si el usuario es humano o un programa malicioso, permitiendo a los atacantes acceder a otro tipo de información de usuario de una manera más simple, la ventaja de esta propuesta proviene del hecho de la regeneración del captcha y la redistribución de los números identificadores cada 2 minutos, reforzados por una serie de distorsiones aplicadas, de esta forma los atacantes no pueden acceder a información extra del usuario y debido al tiempo de regeneración lo hace inviable para él.

**Palabras claves:** Emoji; GIF; Seguridad.

## ABSTRACT

In this work, a development of a captcha variant is presented with the use of a gif image, composed of 6 frames; each frame is made up of 9 images arranged in a 3 by 3 matrix; Each image used expresses an emotion from a set of 5 basic emotions. Each of the 9 sectors into which the gif is divided is assigned a digit mark, in order for the user to recognize an emotion within the gif and using their cognitive skills to relate this emotion to a number and, in this way, identify the right answer. A simple and safe alternative is proposed for the protection of websites, ideal for a wide range of users, regardless of their age or computer knowledge, this is due to the use of emotions that are recognized by every human being. Current

developments perform network traffic analysis and response time to identify if the user is human or a malicious program, allowing attackers to access other types of user information in a simpler way, the advantage of this proposal comes from fact of the regeneration of the captcha and the redistribution of the identification numbers every 2 minutes, reinforced by a series of applied distortions, in this way the attackers cannot access extra information from the user and due to the regeneration time makes it unfeasible for him.

**Keywords:** Emoji; GIF; Security.

## 1. INTRODUCCIÓN

La constante interacción del ser humano con internet ha evolucionado a tal grado que se ha generado una industria de miles de millones de dólares, la cual es un blanco atractivo para los ciber delincuentes, no sólo por el beneficio monetario que se obtiene sino por la información que se puede obtener. Para conseguir su objetivo los atacantes hacen uso de diferentes métodos, que tienden a ser automatizados. Esta situación ha impulsado el desarrollo de distintas técnicas y procedimientos para ralentizar y en el mejor de los casos evitar el robo de información.

Lo anterior dio origen a que el informático guatemalteco Luis Von Ahn (Elizondo, 2008) desarrollara el captcha, el cual es una imagen conformada por caracteres distorsionados, dichas imágenes tienen que ser identificadas por el usuario. La idea central de este método es que una computadora no puede identificar de manera correcta los caracteres. El captcha debe de ser fácil de resolver para los humanos además de ser complejo para las computadoras sin dejar de lado su fácil generación y simple evaluación de la solución proporcionada, tomando en cuenta estas prerrogativas se han desarrollado varias propuestas, no solo con caracteres, si no empleando sonidos, videos. imágenes, etc. Se han diseñado una alta cantidad de propuestas que ocupan el texto como su principal componente, empleando variaciones en su presentación, como invertir la orientación de las letras, presentarlas de manera cruzada con otras palabras, variación del idioma, mostrar los caracteres en tercera dimensión, todo esto con el objetivo de dificultar al máximo la posible identificación de los caracteres por parte de atacantes. Otras investigaciones proponen usar video para solicitar al usuario que proporcione etiquetas que lo describan, esta técnica se ha empleado para presentar letras e imágenes.

El uso de imágenes en los captchas es extendido, empleando imágenes especializadas aprovechando que se requiere conocimiento especializado para identificarlas como las más simples, los rostros, con los cuales se obtiene una identificación natural por parte de los humanos, ya que todos tienen rostro y sumamente compleja para las maquinas, ya que implica recursos especializados para cada diferente tipo de rostro que se presente.

Todos los tipos de captcha mencionados conllevan técnicas de distorsión variadas y especificas para cada uno de los mismos.

Tomando como base las propuestas existentes este trabajo describirá, diseñará e implementará una variante de captcha, que sea de tipo video, empleando emociones mezclándolas con distintas distorsiones.

Las ventajas que esto provee es que el tipo de captcha video es el que menos uso ha tenido, logrando así que las herramientas utilizadas para atacarlos sean pocas, dicho captcha al estar conformado por imágenes que muestren emociones aprovechara la facilidad por parte de los humanos para identificar estas imágenes y la dificultad inherente de las computadoras para no reconocerlas. Como todo captcha contará con

diferentes tipos de distorsión que abonarán a fortalecer la seguridad y dificultar su solución por parte del atacante.

## 2. MARCO TEÓRICO

### 2.1 Máquina de Turing

Descrita por el científico ingles Alan Turing en 1936, la máquina de Turing es un programa con instrucciones y ciclos estructurados (Rocha, 2005) , caracterizado por su simplicidad y que cuenta con la habilidad hipotética de simular la lógica de cualquier algoritmo de un computador. Esto da origen al Test de Turing , el cual es un método para recabar evidencia que indique la existencia de mentalidad en computadoras, y el método escogido para realizarlo es el denominado juego de la imitación, que consiste en que un computador induce a interrogadores a creer que es una persona. Según Turing, si la máquina logra convencer a los jueces humanos, resulta justificado creer que es inteligente y pensante, pues es capaz de suplantar a humanos mediante comportamiento lingüística (González, 2007).

Al reorientar la prueba de Turing planteando que los seres humanos son el objeto de estudio y probar si son o no indistinguibles de las máquinas. Las preguntas más importantes para considerar son si, cuándo y cómo se pueden construir los seres humanos a través de la tecnología, el contexto social y el entorno en el que vivimos y a través del cual se forman nuestras preferencias y creencias para que no se puedan distinguir de las máquinas, esto se le conoce como prueba de Turing inversa (Frischmann, 2014). En otras palabras, un ser humano puede contar con características de una máquina y al mismo tiempo mentir en cuestiones en las que las máquinas aun no logran imitar al ser humano. La prueba inversa puede describirse de la siguiente manera:

- Cálculos matemáticos.- Las máquinas son más eficientes y precisas que el ser humano, por lo cual es necesario flexibilizar el tiempo de respuesta o limitar el tipo de operaciones.
- Generación de números aleatorios.- Los humanos no son eficientes generando números aleatorios de manera consciente, basta con un poco de repeticiones para que el humano termine delatándose.
- Sentido común.- La capacidad del ser humano de dar por sentado gran cantidad de detalles sobre el mundo que nos rodea a pesar de que no se mencione explícitamente en ciertas preguntas o escenarios, capacidad de la que carece una máquina.
- Racionalidad.- Las máquinas son racionales y ante dilemas morales, los cuales conllevan una gran cantidad de juicios humanos, las simulaciones que llevan a cabo las máquinas se complican. Dichas simulaciones tienden a ser equilibradas y con un enfoque matemático, lo que las hace diferenciables.

Dado que este tipo de prueba es controlada por una máquina, en lugar de un humano, con el objetivo de determinar cuando el usuario es o no humano, surge como una variante de esta prueba el captcha.

El captcha es una prueba tipo desafío-respuesta usada en computación para determinar cuándo el usuario es o no humano. Descritos por primera vez por Luis Von Ahn en el año 2000 (Elizondo, 2008).. En sus inicios el comportamiento de estos consistía en solicitar al usuario introducir correctamente una serie de caracteres alfanuméricos contenidos en una imagen distorsionada, este procedimiento se basa en que una máquina no es capaz de comprender y capturar la secuencia de forma correcta, acción que un humano puede resolver con facilidad (Elizondo, 2008).

### 2.2 Emociones

El psicólogo estadounidense Paul Ekman, realizó varios estudios en una tribu de Papúa, Nueva Guinea, los integrantes de esta tribu se encontraban aislados y por consiguiente no conocían la radio, el cine, ni la lectura. Durante un tiempo determinado Ekman les presentó diferentes experimentos con tal de identificar sus reacciones. Al termino de dichos experimentos Ekman concluyó que las emociones no son determinadas por la cultura, si no que son universales, por consecuencia tienen un origen biológico como lo planteó Darwin (Ekman, Emotions Revealed, 2003).

Ekman identificó 6 emociones básicas o como él las describió biológicamente universales, las cuales son:

- Alegría
- Tristeza
- Miedo
- Ira
- Asco
- Sorpresa

## 3. TRABAJOS PREVIOS

Los ataques cada vez más complejos incrementan el riesgo de vulnerar los sistemas, lo cual ha impulsado el desarrollo de distintas propuestas de captcha. Para contextualizar la propuesta descrita en este trabajo, se describen a continuación algunas propuestas, los captchas de video son los menos empleados, entre las propuestas que se han implementado, existe una en donde el usuario proporciona tres etiquetas que identifiquen el video presentado, el reto es contestado correctamente si las etiquetas proporcionadas pertenecen a un conjunto generado automáticamente (Kluever, 2008).

Los captcha de texto son ampliamente utilizados y cuentas con varias propuestas, algunas de ellas consideran variar la orientación de una imagen, tiene como ventaja la independencia del idioma no requiere el ingreso de texto ni el empleo de distorsión de caracteres (R. Gossweiler, 2009), considerando esta y otras propuestas se planteo la creación de captchas tridimensionales en el que se muestran imágenes con texto. Su objetivo es complicar las técnicas de reconocimiento de caracteres que son eficaces para la mayoría de los captchas. La forma de resolverlo es mediante la rotación de la imagen para la identificación de caracteres, aprovechando la dificultad de los computadores para rotar una imagen y establecer un punto base para la identificación (Woo, 2018), tomando en cuenta las ventajas de estos se planteo una propuesta de captchas cognitivos, en los que su resolución se basa en tener conocimientos especiales y habilidades perceptivas (M. Ogiela, 2018).

Los captchas de imágenes tienen varias propuestas, una de ellas emplea el reconocimiento de rostros, en donde el usuario debe de reconocer un par de rostros que pertenezcan al mismo sujeto. Para poder lograr esto el usuario deberá de ser capaz de distinguir los rostros de entre imágenes no humanas, fondos oscuros, distorsiones y otros rostros. La ventaja de esta propuesta se basa en ofrecer una mejor precisión para los humanos y una menor tasa de ataques (G. Goswami, 2012). Tomando como base esta propuesta se presentó una variante que utiliza rostros en donde el usuario debe de seleccionar caras humanas de una imagen que presenta múltiples distorsiones y así evitar seleccionar una cara no-humana, esta propuesta ofrece mayor éxito en su resolución y bajos índices de ataques automáticos (G. Goswami B. M., 2012). Considerando las ventajas de estos diseños pero partiendo de las debilidades de los captcha de tipo texto se creo un captcha en el que en una imagen se tiene que encontrar un par de rostros humanos en un conjunto de fondos e imágenes distorsionados, partiendo del principio de que todos los captchas basados en texto tienen problemas con las distorsiones haciéndolos complejos para los usuarios (G. Goswami B. M., 2014). Empleando imágenes diferentes a rostros se ha propuesto unir dos imágenes tridimensionales formando una tercera llamada quimera, cada imagen es diferente en tipo y tema, el reto para el humano es

identificar una imagen individual. Su efectividad gira entorno a que las imágenes fusionadas no son fáciles de identificar para los humanos usando el sentido común pero complicado para otros entes (Fujita, Ikeya, Kani, & Nishigaki, 2015).

Entre las aplicaciones de los captchas se ha buscado utilizarlos de manera criptográfica al proponer la creación de un protocolo basándose en el proceso de resolución (A. Kumarasubramanian, 2013) o de manera biométrica (W. Lee, 2018). Además que en la búsqueda de crear propuestas más robustas y mejorar los diseños de los captchas, se ha utilizado técnicas de aprendizaje máquina, aprendizaje profundo para poder identificar vectores de ataque, al utilizar esta técnica de análisis los recursos necesarios para analizar las imágenes se reducen (C. J. Hernández-Castro, 2017), la viabilidad de introducir ruido de confrontación mutable e inmutable para lograr captchas resistentes a los intentos de eliminación de ruido (M. Osadchy, 2017), esto aunado con técnicas de procesamiento de imágenes, enfocadas en el reconocimiento de palabras en movimiento se han planteando contramedidas para fortalecer los captchas sacrificando la usabilidad (S. Gao, 2017).

## 4. PROPUESTA

A continuación se presenta la propuesta de solución mencionada en párrafos anteriores y que es aplicada a este trabajo, los parámetros que se utilizan en este trabajo son configurables, y los utilizados son aquellos que sirven para ejemplificar el proceso.

El proceso de generación de captcha, inicia con la solicitud de los datos del usuario, estos datos son almacenados para llevar un registro de las pruebas realizadas, realizado esto, se genera el captcha. El proceso de generación inicia con la selección de la emoción que fungirá como respuesta, la cual se realiza de manera aleatoria sobre el conjunto de emociones configuradas. A continuación, se crea un conjunto de imágenes, cada una de ellas es construida a partir de una emoción seleccionada de manera aleatoria, al tener este conjunto de imágenes, se toma un subconjunto, con el cual se crea una imagen que concentre 9 imágenes individuales ordenadas en renglones y columnas. Una vez que se tiene la imagen compuesta, se le aplica una serie de distorsiones y transformaciones geométricas para dificultar la identificación de patrones. Al termino de este proceso se crea una imagen gif conformada por 6 imágenes distorsionadas compuestas, la cual se presenta al usuario. Este proceso se representa en la Figura 1.

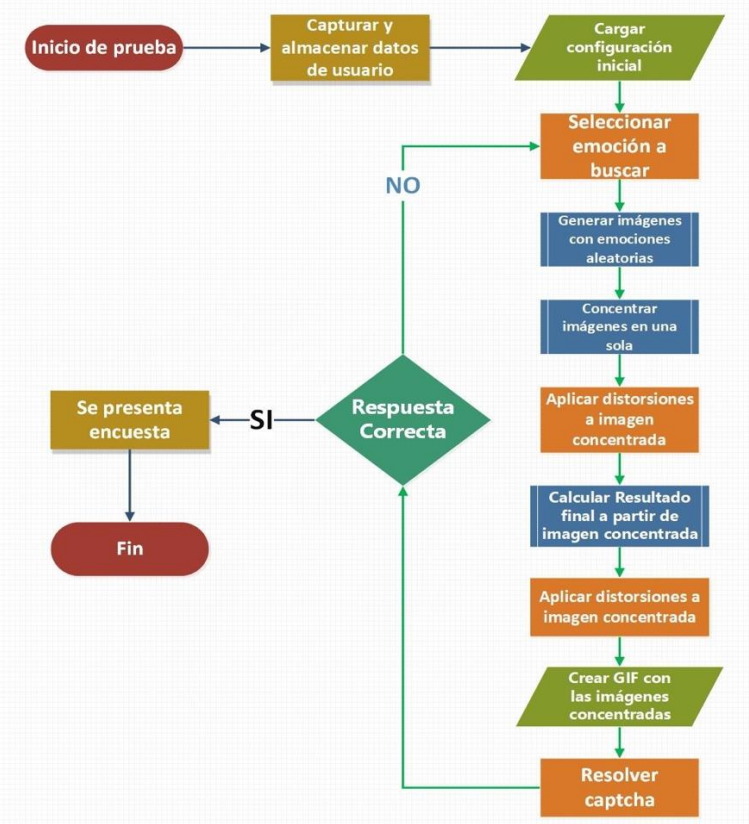


Figura 1. Diagrama de generación y resolución de captcha.
Fuente: (M.O. López Marín *et al*., 2020).

Como resultado del proceso anterior, el captcha propuesto puede verse en la figura 2, la cual se muestra a continuación:


Figura 2. Imagen de captcha generado.
Fuente: (M.O. López Marín *et al*., 2020).

Si bien existen una cantidad variada de emociones (Ekman, Emotions Revealed, 2003), aquellas contempladas para la creación de este captcha se pueden ver en la figura 3.

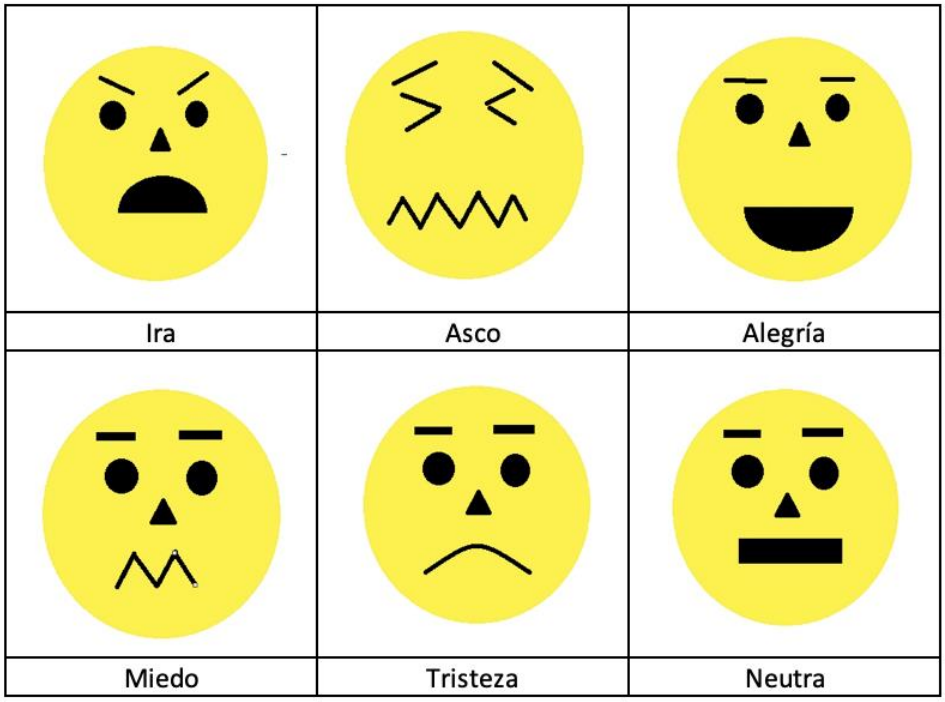


Figura 3. Emociones empleadas en la creación del captcha
Fuente: (M.O. López Marín *et al*., 2020).

4.2. Resolución

Para resolver el captcha, el usuario cuenta con 2 minutos para introducir la respuesta en un campo de texto, dicha respuesta debe de proporcionarse al sistema mediante un teclado numérico, donde los dígitos son acomodados aleatoriamente, véase la figura 4. Al término del periodo de tiempo y si el captcha no ha sido resuelto correctamente, un nuevo captcha es generado al igual que se cambia el orden del teclado con el que se introduce la respuesta, concluyendo el ciclo al introducir la respuesta correcta antes de que se cumpla el tiempo.


Figura 4. Método de captura de para solucionar el captcha.
Fuente: (M.O. López Marín *et al*., 2020).

En la figura 5, se describe el proceso general de resolución de captcha:

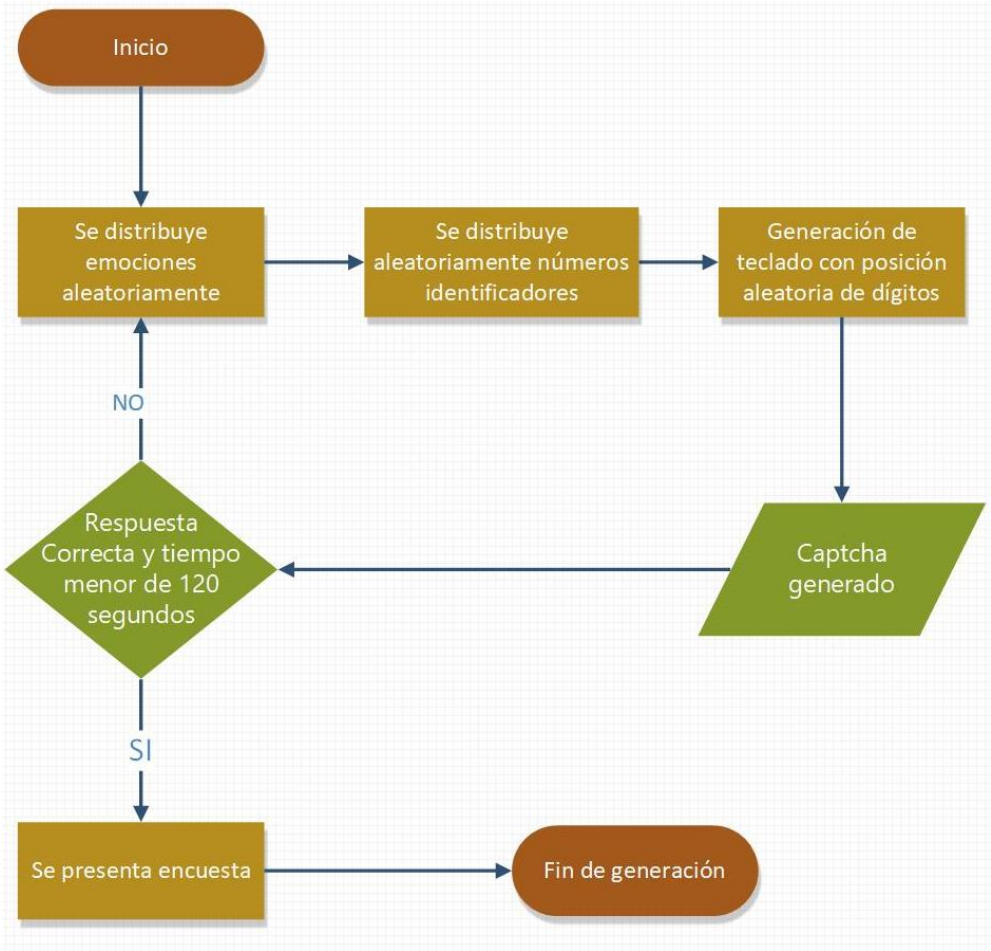


Figura 5. Flujo de resolución de captcha.
Fuente: (M.O. López Marín *et al*., 2020).

4.3. Pruebas de rendimiento

Las pruebas de rendimiento realizados sobre computadoras, redes, software u otros dispositivos, son utilizados para determinar la velocidad y eficiencia de estos. Este procedimiento puede involucrar tanto pruebas cuantitativas, por ejemplo, medir tiempos de respuesta o cantidad en millones de líneas de código, como pruebas cualitativas, en los cuales se evalúa fiabilidad, escalabilidad e interoperabilidad. Estas pruebas de rendimiento pueden ser realizadas a través de herramientas que proveen pruebas de estrés, que permiten determinar la estabilidad del sistema (F. J. Diaz, 2008), la herramienta utilizada para la realización de estas pruebas es JMeter (APACHE, 2020).

Tabla 1.Tabla de tiempos para 1000 usuarios recurrentes.

| | # muestras | Media | Mediana | Línea de 90% | Min. | Máx. | % Error | Rendimiento | kb/seg |
|---|---|---|---|---|---|---|---|---|---|
| Total | 41020 | 3366 | 53 | 5327 | 0 | 704944 | 0 | 4.1 seg | 362.91 |

Fuente: (M.O. López Marín *et al*., 2020).

Como puede verse, el tiempo promedio para acceder a una página es 3366 segundos, realizándose un total de 41020 requerimientos al servidor.

El tiempo total utilizado para los 100 hilos se puede calcular con la siguiente fórmula:

Tiempo Total = #Muestras * Media = 41020 * 3366 = 138073320 milisegundos

El tiempo promedio total requerido por cada hilo, se puede calcular de la siguiente manera:

((Tiempo Total /1000)/60)/cantidad de hilos = ((138073320/1000)/60)/1000= 2.301222 minutos

4.3. Pruebas de usabilidad

La propuesta de captcha se sometió a pruebas con 100 personas, al finalizar la misma se les aplico dos preguntas, con el objetivo de saber su experiencia de uso: De la primera pregunta, la cual se puede observar en la gráfica de la figura 6, el 48% le resulta fácil usar la aplicación y solo un 7% le resulto difícil.

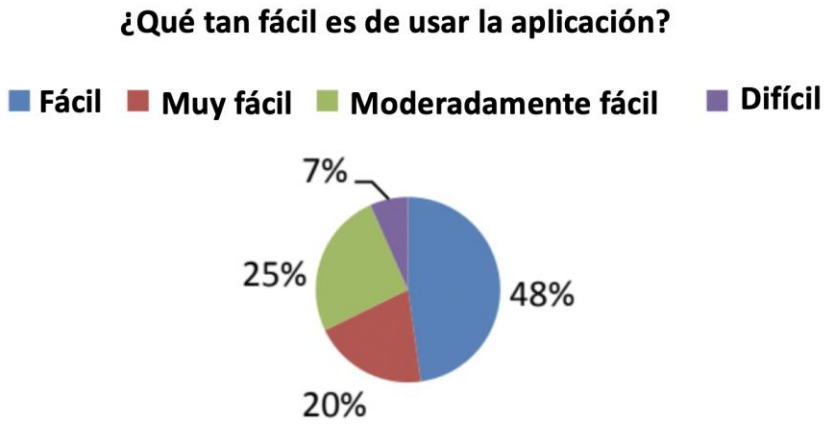


Figura 6.Porcentaje de uso de la aplicación.
Fuente: (M.O. López Marín *et al*., 2020).

En la figura 7 se responde a la pregunta de identificación de expresiones faciales. Se puede observar que el 43% pudo identificar fácilmente los iconos de rostros, mientras solo el 10% le resulto difícil reconocerlas.


Figura 7.Porcentaje de identificación de expresiones faciales.
Fuente: (M.O. López Marín *et al*., 2020).

4.4. Complejidad

En los artículos referenciados no se hacen análisis de complejidad, sin embargo se hizo una medición del autómata propuesto con base en las permutaciones que se realizan. Esto esta definido por la ecuación para un frame de 3 x 3:

$$\theta(n_i!)$$

Donde:
n = emociones
i = cualquiera de 1 a 5 emociones diferentes

## 5. CONCLUSIONES

Con base en las pruebas de usabilidad se concluye que el captcha propuesto es fácil de usar, debido principalmente a lo sencillo que es identificar la emoción en la imagen. Entre las ventajas de esta propuesta se encuentra la de no ocupar una alta cantidad de recursos de cómputo, gracias a que es una imagen GIF, además es importante señalar que la imagen es generada en tiempo real, esto implica que no se tiene un patrón predecible para la generación de un captcha, en otra palabras si se tuviera una base de datos de combinaciones, estas serian limitadas coadyuvando a que sistemas automatizados de ataque puedan identificar y por lo tanto resolver con cierta facilidad el captcha propuesto.

Si bien el captcha propuesto representa una opción relativamente fácil para cualquier tipo de usuario, cuenta con una desventaja en comparación con algunas opciones actuales, una de ellas es la necesidad de la interacción con el usuario, esto se debe a que para resolver esta propuesta el usuario tiene que dar una cantidad de pulsaciones de teclas que van de 0 a n, siendo n la cantidad de imágenes individuales que conforman al captcha final, mientras que las variantes actuales basta con al menos un pulso de tecla, ya que el análisis para identificar si el usuario es una maquina o no, se basa en un análisis de la interacción del usuario con el sitio web que consulta (Google, 2020).

Para evitar que el sistema que implemente el captcha pueda ser vulnerado, se emplea la cognición y la dificultad inherente que tiene una máquina para emplearla, como se mencionó en el marco teórico, se verifica la prueba inversa de Turing.

## REFERENCIAS

C. J. Hernández-Castro, M. d.-M. (2017). Using machine learning to identify common flaws in CAPTCHA design: FunCAPTCHA case analysis. omputers & Security, 744-756.

Lawan, T. (2018). Application of Pattern for New CAPTCHA Generation Idea. Springer International Publishing AG, part of Springer Nature, 257-264.

A. Kumarasubramanian, R. O. (2013). Cryptography Using Captcha Puzzles. International Association for Cryptologic Research, 89-106.

APACHE. (14 de 07 de 2020). APACHE. (APACHE) Recuperado el 14 de 07 de 2020, de https://jmeter.apache.org/

D. Lin, F. L. (2018). Chinese Character CAPTCHA Recognition and performance estimation via deep neural network. Elsevier, 11-19.

Diaz, F. J., Tzancoff Banchoff, C. M., S. Rodríguez, A., & Soria, V. (2008). Usando Jmeter para pruebas de rendimiento. XIV Congreso Argentino de Ciencias de la Computación.

Elizondo, F. J. (2008). Enredándose. CAPTCHA. Ingenierías.

Ekman, P. (2003). Emotions Revealed. New York: Times Books.

F. J. Diaz, C. M. (2008). Usando Jmeter para pruebas de rendimiento. XIV Congreso Argentino de Ciencias de la Computación.

Frischmann, B. M. (2014). Human-Focused Turing Tests: A Framework for Judging Nudging and Techno-Social Engineering of Human Beings. Faculty Research Paper, 1-57.

Fujita, M., Ikeya, Y., Kani, J., & Nishigaki, M. (2015). himera CAPTCHA: A Proposal of CAPTCHA Using Strangeness in Merged Objects. 48-58.

G. Goswami, B. M. (2012). Face Recognition CAPTCHA. Future Generation Computer Systems, 59-68.

G. Goswami, B. M. (2012). FaceDCAPTCHA: Face detection based color image CAPTCHA. Elsevier, 59-68.

G. Goswami, B. M. (2014). FR-CAPTCHA: CAPTCHA Based on Recognizing Human Faces. PLoS ONE.

González, R. (2007). El test de Turing: dos mitos, un dogma. Revista de filosofía, 37-53.

Google. (24 de 11 de 2020). Obtenido de https://developers.google.com/recaptcha/docs/v3

Kluever, B. K. (2008). Evaluating the Usability and Security of a Video CAPTCHA. Rochester.

M. Fujita, Y. I. (2015). Chimera CAPTCHA: A Proposal of CAPTCHA Using Strangeness in Merged Objects. T. Tryfonas and I. Askoxylakis, 48-58, 2015.

M. Ogiela, N. K. (2018). pplication of knowledge-based cognitive CAPTCHA in Cloud of Things security. Concurrency Computat Pract Exper.

M. Osadchy, J. H.-C.-C. (2017). o Bot Expects the DeepCAPTCHA! Introducing Immutable Adversarial Examples, With Applications to CAPTCHA Generation. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.

R. Gossweiler, M. K. (2009). What´s Up CAPTCHA? A CAPTCHA Based on Image Orientation. In Proceedings of the 18th International conference on World wide web, 841-850.

Rocha, J. (2005). Autómatas de Pila y Máquinas de Turing Estructurados. Fundamentos teóricos de la informática, 331-338.

S. Gao, M. M. (2017). Emerging-image Motion CAPTCHAs: Vulnearabilities of Existing Designs, and Countermeasures. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING.

W. Lee, E. U. (2018). Captcha check could boost phone security. Biometric Technology Today.

Woo, S. S. (2018). Design and evaluation of 3D CAPTCHAs. Elsevier, 49-67.

## SEMBLANZA DE LOS AUTORES

**Manuel Oswaldo López Marín:** Obtuvo el grado de Ingeniero en Computación en la Universidad Nacional Autónoma de México, México. Desarrolló sus estudios de maestría en el Instituto Politécnico Nacional, México.

**Marlon David González Ramírez** es Ingeniero en Sistemas Computacionales y Especialista en Redes de Computadora por la Universidad Tecnológica de México (México, 2004), es Maestro en Tecnología de Cómputo por el Instituto Politécnico Nacional (México, 2007). Actualmente estudia su Doctorado en Ingeniería de Sistemas en el Instituto Politécnico Nacional. Es profesor de tiempo completo en el CIDETEC-IPN. Sus áreas de interés son la seguridad informática, criptografía, redes y sus aplicaciones.

**Rodolfo Romero Herrera:** Egresado de la ESIME (Escuela Superior de Ingeniería Mecánica y Eléctrica) del IPN ( Instituto Politécnico Nacional) donde se realizaron estudios en Ingeniería en Comunicaciones y Electrónica. Autor de 5 libros en el área de la electrónica y cómputo. Con diversos artículos en Procesamiento digital de señales publicados en revistas y congresos nacionales e internacionales.

**José Félix Serrano Talamantes:** Recibió su grado de Dr en Ciencias de la Computación en El Centro de Investigación en Computación del Instituto Politécnico Nacional (CIC-IPN) en el año 2011. Sus Líneas de Investigación son: Visión por Computadora, Inteligencia Artificial, Procesamiento de patrones, y el Cómputo inteligente.