TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

DESARROLLO DE UNA API PARA AUTENTICACIÓN GRÁFICA BASADA EN PASSPOINTS

Alex Sánchez Saez[1], Evaristo José Madarro Capó[2], Joaquín A. Herrera Macías[3], Lisset Suárez Plasencia[4]

[1] Universidad de La Habana, Facultad de Matemática y Computación, Cuba, [2,3,4]Universidad de La Habana, Facultad de Matemática y Computación, Instituto de Criptografía, Cuba,
[1]e-mail: alex.sanchez@estudiantes.matcom.uh.cu
[2]e-mail: evaristo.madarro@matcom.uh.cu
[3]e-mail: joaquin.herrera@matcom.uh.cu
[4]e-mail: lisset.suarez@matcom.uh.cu

RESUMEN

La autenticación es crucial para la protección de los usuarios y sus datos. Debido a las debilidades que aparecen en las contraseñas alfanuméricas por la acción de los usuarios, se han desarrollado nuevos enfoques como son los basados en autenticación gráfica. Uno de estos sistemas es el Passpoints que se destaca por su seguridad y facilidad de uso. En este artículo se presenta una implementación propia de dicho sistema, resultado de un exhaustivo estudio del sistema en cuestión. Dicho estudio abordó tanto el funcionamiento como la seguridad del sistema Passpoints, identificando sus debilidades y explorando las propuestas existentes para mitigarlas. Para la implementación principal de este sistema, se llevaron a cabo otras implementaciones intermedias esenciales para su desarrollo completo. Para ello se realizó un análisis exhaustivo de los métodos de discretización disponibles con el fin de seleccionar el más efectivo y eficiente para su posterior traducción a código de programación, así como una investigación referente a la adaptación de este sistema a la variedad de resoluciones de pantalla y tamaños de imagen actuales, permitiendo la adaptación de esta implementación a cualquier tipo de dispositivo. Este proceso es fundamental para convertir el sistema en un producto real que pueda ser evaluado por usuarios reales en diferentes medios.

PALABRAS CLAVES: Passpoints, autenticación gráfica, métodos de discretización, API.

DEVELOPMENT OF AN API FOR GRAPHICAL AUTHENTICATION BASED ON PASSPOINTS

ABSTRACT

Authentication is crucial for protecting users and their data. Due to the weaknesses that appear in alphanumeric passwords as a result of user actions, new approaches have been developed, such as those based on graphical authentication. One of these systems is Passpoints, which stands out for its security and ease of use. This article presents our own implementation of this system, the result of an exhaustive study of the system in question. This study addressed both the functioning and security of the Passpoints system, identifying its weaknesses and exploring existing proposals to mitigate them. For the main implementation of this system, other essential intermediate implementations were carried out for its complete development. To achieve this, a comprehensive analysis of available discretization methods was conducted to select the most effective and efficient for subsequent translation into programming code, as well as research regarding the adaptation of this system to the variety of current screen resolutions and image sizes, allowing the adaptation of this implementation to any type of device. This process is fundamental to turning the system into a real product that can be evaluated by real users across different media.

INDEX TERMS: Passpoints, graphical authentication, discretization methods, API.

1. INTRODUCCIÓN

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

En el mundo moderno es creciente la tendencia a acumular datos de toda índole en los diferentes servicios y medios digitales, por lo que es común depositar información sensible que puede ser utilizada contra los usuarios. En este escenario se ve necesaria la tarea de incrementar la seguridad de dicha información, una de las formas de llevar a cabo esta tarea es teniendo buenos mecanismos de autenticación que permitan dar acceso a la información solo al usuario legítimo [1]. Existen 3 tipos de autenticación [2]: la basada en Tokens (¿qué tienes?), la basada en datos biométricos (¿quién eres?) y la basada en conocimiento (¿qué sabes?). El método de autenticación más usado en la actualidad es el basado en contraseñas alfanuméricas, estas tienen una gran contradicción entre su seguridad y su usabilidad [3] ya que para ser segura una contraseña alfanumérica debe tener una gran longitud y un alto nivel de entropía, lo cual la hace extremadamente difícil de recordar para el usuario; por otra parte para ser sencillas de memorizar deben ser predecibles y cortas, características que afectan a su seguridad, permitiendo la autenticación de falsos usuarios. Recientemente una aplicación haciendo uso de técnicas de inteligencia artificial reafirma aún más la necesidad de emplear métodos alternativos de autenticación [4].
Las contraseñas gráficas se erigen como una buena alternativa y una solución a los problemas presentes en las contraseñas alfanuméricas. Entre los diferentes tipos de autenticación gráfica destaca el Passpoints, por su seguridad y usabilidad [5]. El sistema Passpoints está basado en el modelo *Cued-Recall* [5],[6], el cual aprovecha la capacidad humana de reconocer patrones en imágenes. En términos más simples, consiste en sustituir las tradicionales contraseñas alfanuméricas por contraseñas gráficas, consistentes en una selección de 5 puntos en una imagen.
Este trabajo tiene como objetivo presentar una implementación propia del sistema Passpoints, con la intención de contar con una alternativa práctica a las contraseñas alfanuméricas. Para llevar a cabo dicha implementación fue necesaria la solución de varios problemas, uno de ellos fue la implementación de uno de los métodos de discretización encontrados en la bibliografía, los cuales son empleados por este sistema durante la fase de autenticación, esto por la baja probabilidad para un usuario de seleccionar exactamente los mismos puntos en ambas fases, registro y autenticación. Otros problemas tratados fueron los de mejorar la adaptabilidad de este sistema a diferentes tamaños de imagen y pantalla en su uso y convertir la implementación en una API (*Aplication Program Interface*) que permite su utilización en diferentes entornos y dispositivos.

2. PRELIMINARES

2.1 ¿Por qué usar Passpoints?

La notoria falta de seguridad de las contraseñas alfanuméricas debido a la contradicción que presentan las mismas [3] es una señal de que se requieren alternativas más seguras y sencillas de usar. En este escenario es donde el Passpoints se erige como una buena alternativa a las tradicionales contraseñas alfanuméricas, lo que hace tan seguro a este método de autenticación gráfica es su espacio de contraseñas Q^L, donde Q es el tamaño del alfabeto y L la longitud de la contraseña [7]. Mientras que en el caso de las alfanuméricas este consiste en la cantidad de cadenas que se pueden formar con un alfabeto específico, en el Passpoints será la cantidad de combinaciones de puntos (píxeles) de la imagen que se utilice. En la actualidad los tamaños de imágenes que se manejan rondan los cientos de miles de píxeles, esto incrementa aún más el espacio de contraseñas del Passpoints, teniendo un impacto positivo en su nivel de seguridad y resistencia a ataques de fuerza bruta. Al ser muy novedoso y poco conocido, no existen grandes bases de datos de contraseñas Passpoints, a diferencia de la enorme cantidad de información y recopilaciones de contraseñas alfanuméricas que se pueden encontrar en internet, esto le da mucha más resistencia al Passpoints ante los ataques de Diccionario [8]. Al explotar la capacidad humana de reconocer patrones en imágenes hace que recordar las contraseñas sea muy sencillo para cualquier tipo de persona desde niños y adolescentes, hasta personas de la tercera edad, a diferencia de las contraseñas alfanuméricas donde se hace necesario para garantizar la seguridad de las personas que estas memoricen largas cadenas con altos niveles de aleatoriedad. En [9] se ratifica la posición del Passpoints como el método de autenticación gráfica más conveniente, a través de una comparación y evaluación crítica de los diferentes métodos de este tipo existentes.

2.2 Passpoints

El sistema Passpoints [5], fue diseñado en el 2005 por Susan Wiedenbeck, basa su funcionamiento en que un usuario seleccione un conjunto ordenado de 5 puntos en una imagen como su contraseña en la fase de registro. En la fase de autenticación tendrá que seleccionar los mismos puntos con un margen de error o región de tolerancia de aproximadamente $0.25cm$ y en el mismo orden que en la fase de registro.

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

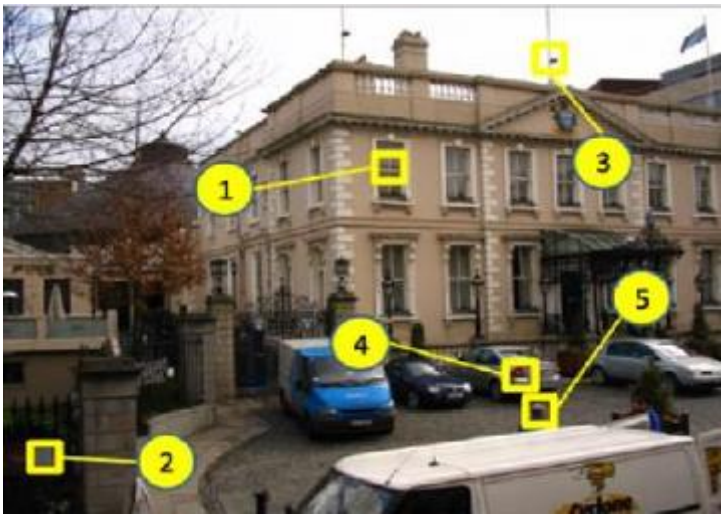


Figura 1: Funcionamiento del Passpoints, tomada de [5].

En este sistema cualquier imagen puede ser utilizada (pinturas, fotos naturales, fotos familiares, etc), y puede ser seleccionada por el usuario o proveídas por el sistema. La imagen debe tener cientos de puntos probables de ser seleccionados y deben estar diseminados de forma homogénea para mayor seguridad. Por motivos de seguridad, el sistema no almacena de forma explícita la contraseña, sino un hash de la misma, esto trae consigo el problema de identificar el usuario legítimo, ya que es muy poco probable que se digiten exactamente los mismos puntos durante las fases de registro y autenticación, haciendo que los hashes sean diferentes si esto no ocurriese. Para solventar este problema es necesario agregar un margen de error para la selección de los puntos; una región de tolerancia. Para lograr esto se utiliza una discretización de la imagen, lo que reduce el espacio de contraseñas y aporta información relevante para llevar a cabo ataques de diccionario [10], además permite la aparición de falsos positivos y negativos en la autenticación debido a la forma de las regiones calculadas utilizando la discretización. Una discusión acerca de la importancia del mecanismo de discretización en los esquemas de contraseñas gráficas y de los diferentes métodos de discretización conocidos hasta el momento puede verse en [11], [12], [13], [14]. Otros aspectos negativos a destacar en este sistema son: algunas regiones en la imagen son más propensas a ser seleccionadas por el usuario para formar su contraseña [15]. Dado que este sistema basa su funcionamiento en la selección de 5 puntos en la imagen, la fase de registro y de autenticación pueden extenderse lo que conlleva a que sean vulnerables ante ataques de tipo Shoulder-Surfing [8]. Si el conjunto de puntos seleccionados por el usuario no sigue un patrón aleatorio es considerada débil y es susceptible a ataques de diccionarios [8]. En varios artículos publicados recientemente [16], [17], [18], [19], [20], [21], [22] se proponen tests para evitar el registro de contraseñas gráficas no aleatorias. Estos resultados unidos a la propuesta en [7] de un modelo probabilístico capaz de medir el nivel de autenticidad de un usuario, conllevan a un aumento significativo en la seguridad de este sistema y por consiguiente lo convierten en una de las alternativas más prometedoras ante las contraseñas alfanuméricas.

2.3 Discretización

Es sencillo percatarse de la baja probabilidad de que un usuario seleccione siempre exactamente el mismo pixel en las fases de registro y autenticación, situación que se agrava aún más en escenarios como el de los teléfonos móviles, cajeros y otras situaciones donde el usuario no posee un puntero digital. Es por esto que se hace necesario dar un margen de error a cada punto de la contraseña Passpoints, a la región definida por el punto y su margen de error se le conoce como región de tolerancia. Una forma eficiente y segura de introducir esta región de tolerancia en un sistema de autenticación gráfica Passpoints es utilizando una discretización.

2.4 Región de Tolerancia

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

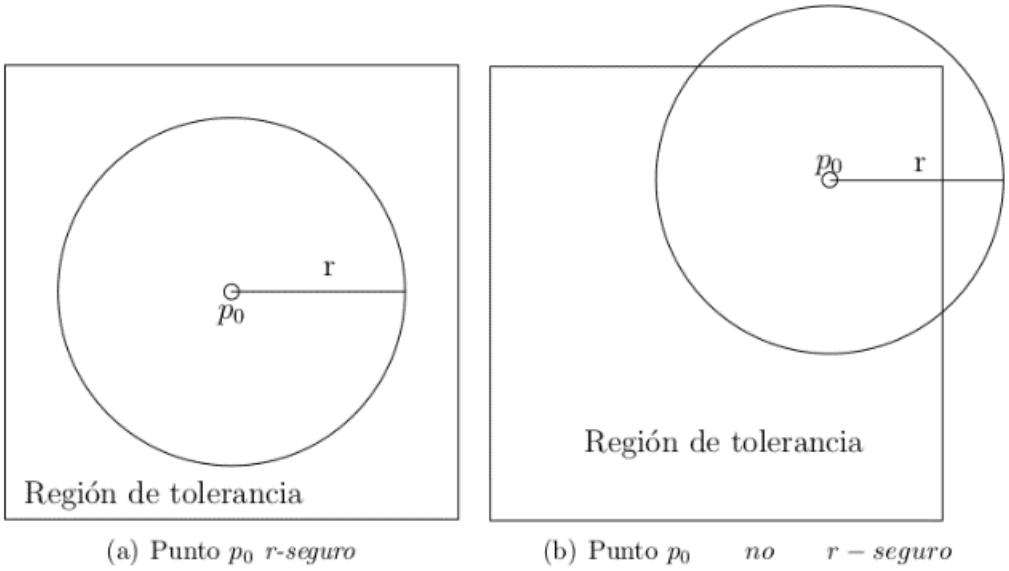
La región de tolerancia [7], [23] de un punto p se define como el conjunto de puntos de la imagen tal que son aceptados como válidos durante la autenticación para el punto original p_0, se denota como RT. Sea I el conjunto de píxeles de la imagen, f una función tal que para todo punto de la imagen devuelve 1 si es aceptado y 0 en caso contrario, entonces RT quedaría definido como:

$$RT = p, p \in I \cap f(p) = 1 \quad (1)$$

Puede interpretarse la región de tolerancia como el error permitido al usuario en el momento de seleccionar su contraseña.

Un punto es considerado r-seguro [7], [23] para un radio r si y solo si todo punto que está a una distancia r de él se incluye en la región de tolerancia, sea I el conjunto de píxeles de una imagen, p_0 un punto de la imagen y RT la región de tolerancia, se dice que p_0 es r-seguro si y solo si:

$$\forall p \in I: d(p_0, p) < r \Rightarrow p \in RT \quad (2)$$



(a) Punto p_0 *r-seguro* (b) Punto p_0 *no* $r-$*seguro*

Figura 2: Punto r-seguro (a), punto no r-seguro (b)

2.5 Problema del Vértice

Este problema surge durante la fase de registro [7], [11], [23], cuando el usuario puede seleccionar un punto que no es r-seguro. Hay dos casos posibles seleccionar un punto localizado exactamente en los vértices o aristas de la región de la partición, o seleccionar un punto que está situado a una distancia $d < r$ de los mismos. El primer caso plantea un problema de decisión para determinar la región de tolerancia de punto. Es necesario discretizar las imágenes de tal manera que cada punto pertenezca a una región de tolerancia.

2.6 Problema del Hash

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

Por temas de seguridad las contraseñas no pueden almacenarse en texto claro, es necesaria una forma segura de representarlas tal que para cada contraseña exista un identificador único y que estas no sean recuperables desde dicho identificador, las funciones hash [7], [23] encajan perfecto con esta definición por lo que son un buen recurso a utilizar para almacenar las contraseñas. Usando un hash surge la problemática de que cada punto de la región de tolerancia tendrá un hash diferente, impidiendo así que guardar el hash de los puntos seleccionados sea una buena opción. Utilizando como parámetro de la función hash no solo un punto, sino toda su región de tolerancia, haciendo esto no solo se garantiza que se puedan guardar los hashes de las contraseñas, también aumenta la cardinalidad del espacio de entrada de la función hash lo que dificulta los ataques de fuerza bruta.

Métodos de Discretización

2.5 Discretización Robusta

Para evitar el problema del vértice [11], se utiliza un conjunto de tres particiones diferentes de la imagen, esto garantiza que cada punto es r-seguro en al menos una de dichas particiones. Esto se logra asegurando una separación de al menos r-píxeles entre el punto y el borde de alguna de las 3 particiones [10], [12].
Se toman cuadrículas de dimensiones $6r \times 6r$ y cada partición debe estar separada una distancia $2r$ del resto. Durante la fase de autenticación, debido a la construcción de las particiones, cualquier punto a una distancia $d \leq r$ del punto original pertenecerá al mismo cuadrante, lo que garantiza la autenticación del usuario ya que la salida de la función hash será la misma. Por otro lado, cualquier punto a una distancia mayor a $5\sqrt{2}$ pertenecerá a otro cuadrante, lo que garantiza la no autenticación del usuario ilegítimo.

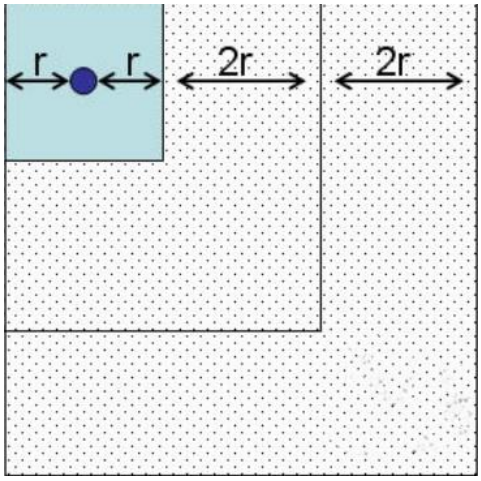


Figura 3: Cálculo de las particiones tomada de [11].

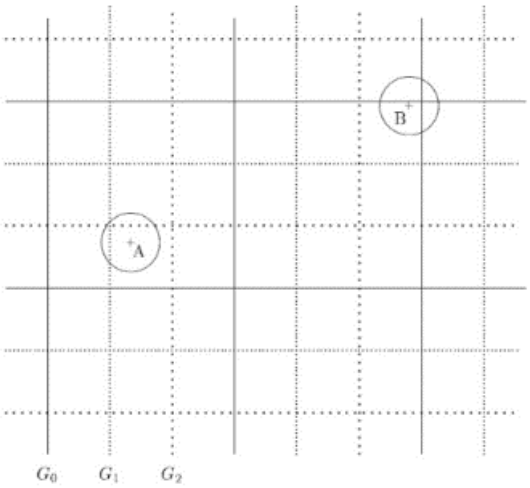


Figura 4: Puntos dentro de la discretización, tomada de [11].

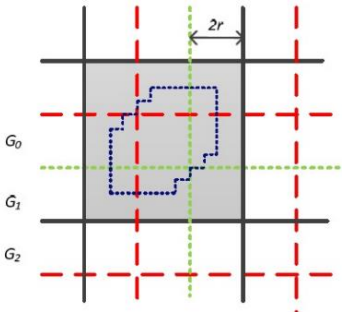


Figura 5: Regiones G_0, G_1, G_2; tomada de [11].

2.6 Discretización Centrada

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

La Discretización Centrada [12] ofrece mejoras en usabilidad y seguridad en comparación con la discretización robusta. Esta técnica garantiza que la región de tolerancia esté centrada en el punto seleccionado para la contraseña, resolviendo así el problema del vértice. Al determinar una región de dimensiones $2r \times 2r$ centrada en el punto. Este método funciona encontrando, en cada dimensión de la imagen (x, y), un segmento de longitud $2r$ en el cual el centro sea el punto originalmente seleccionado en el registro. Sea x un punto en la semirrecta numérica que comprende los valores entre 0 y m, donde m es el ancho o largo de la imagen, dependiendo de la dimensión que se quiera calcular. A partir de ese segmento, se divide el resto del intervalo $[0, m]$ en subintervalos de igual longitud. En la mayoría de los casos, habrá sobrantes de tamaño d, donde d pertenece al intervalo $[0,2r]$, por lo que si se almacena el valor de d es posible reconstruir la partición realizada comenzando en d, donde uno de estos subintervalos estará centrado en x. Una vez establecido el radio r y el punto de la contraseña x, se puede calcular la región de tolerancia.
Se calcula el sobrante d que se utilizará luego en la fase de autenticación

$$d = (x - r) mod 2r. \quad (3)$$

Determinar el intervalo exacto i donde se encuentra x

$$i = \lfloor \frac{x-r}{2} \rfloor \quad (4)$$

Una vez seleccionado el punto x'durante la fase de autenticación se halla el intervalo i' donde este se encuentra

$$i' = \lfloor \frac{x'-r}{2} \rfloor \quad (5)$$

Nótese que i no está centrado en x', pero

$$|x - x'| < r \rightarrow i = i' \quad (6)$$

Por tanto se utiliza i como componente de la contraseña

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

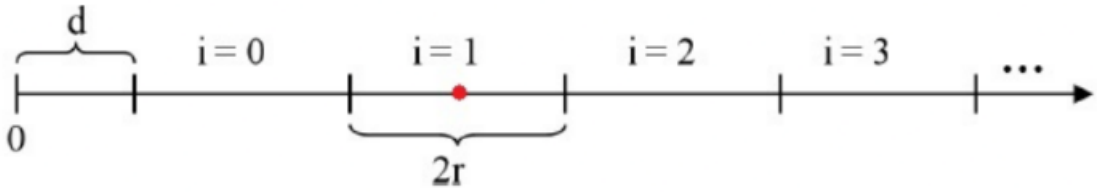


Figura 6: Ejemplo de recta numérica discretizada centradamente, tomado de [12].

Este método de autenticación supone una mejora sustancial en cuanto a su complejidad de implementación, ya que elimina la necesidad de crear varias particiones en la imagen. Sin embargo, este método introduce un nuevo problema, es la necesidad de almacenar el valor d en texto claro para poder efectuar la autenticación correctamente. Una posible solución a este problema sería encriptar este valor de forma reversible y almacenarlo junto al hash de la contraseña concatenándolo al mismo. Esto permitiría al sistema, durante la fase de autenticación, recuperar estos datos y determinar si los puntos seleccionados son válidos o no.

2.7 Discretización Optimal

Este método mantiene la filosofía de particionar la imagen generando una región centrada en el punto original de la contraseña, pero utiliza propiedades de la aritmética modular para construirla [13].
Sean r el radio de tolerancia y X el punto seleccionado por el usuario, se calcula

$$\begin{aligned} Xmod2r \geq r \rightarrow \phi = Xmodr \\ Xmod2r < r \rightarrow \phi = (Xmod2r) - r \end{aligned} \tag{7}$$

De forma análoga se calcula

$$\begin{aligned} Ymod2r \geq r \rightarrow \varphi = Ymodr \\ Ymod2r < r \rightarrow \varphi = (Ymod2r) - r \end{aligned} \tag{8}$$

Estos valores (ϕ) y (φ) se almacenan en claro en el sistema junto a los hashes

$$S_X = \frac{X-\phi}{2r}, S_Y = \frac{Y-\varphi}{2r} \tag{9}$$

Durante la fase de autenticación, el usuario selecciona el píxel (X', Y'), utilizando los valores de (ϕ) y (φ) almacenados para ese usuario se calculan los hashes $S_{X'}$ y $S_{Y'}$ cumpliéndose lo que se garantiza la autenticación.

$$\|(X,Y) - (X' - Y')\| < r \rightarrow S_{X'} = S_X \wedge S_{Y'} = S_Y \tag{10}$$

Este método es más eficiente que los descritos anteriormente, ya que su implementación a nivel computacional tiene una menor complejidad. Al tomar como base la aritmética modular se reduce la complejidad de los cálculos necesarios. No soluciona el problema de la discretización optimal debido a que mantiene la necesidad de guardar texto claro junto

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

con las contraseñas, en este caso son los valores (ϕ) y (φ). Aunque este sistema tiene una solución rápida que comparte con la discretización centrada.

2.8 Discretización mediante Polígonos de Voronoi

Otras propuestas de discretización encontrada en la bibliografía es la hecha por Kirovski et.al. [14], donde proponen utilizar diagramas de Voronoi. partiendo de los puntos más probables de ser seleccionados en la imagen (conocidos como *Hotspots* en la literatura), propone aplicar una discretización de Voronoi ponderada usando una heurística para maximizar la entropía $H(P_w)$, tratando de obtener polígonos equiprobables. Su ventaja principal es que todos los polígonos de la partición obtenida poseen aproximadamente la misma probabilidad a priori de que el usuario escoja un punto de ese polígono, esta propiedad parece ofrecer mejor resistencia a los ataques de diccionario basados en *Hotspots*. Sin embargo, en [10] se afirma que la propuesta de [14] sigue dejando información en claro, útil para ataques de diccionario.

2.9 Problemas de los Métodos de discretización

El uso de los métodos de discretización conlleva a ciertas limitaciones durante la autenticación. Una de estas es la falta de diferenciación entre los puntos que se encuentran dentro de la región de tolerancia. Todos los puntos reciben el mismo tratamiento, lo cual contradice el comportamiento esperado por parte del usuario legítimo, que debería seleccionar con mayor frecuencia los puntos más cercanos al punto original. Además, al representar la región de tolerancia como un polígono en lugar de un círculo, existe la posibilidad de obtener falsos positivos, es decir, puntos que se encuentran a una distancia mayor que el radio de tolerancia establecido pero que aún se consideran válidos como parte de la contraseña [6], [23].
Otro problema se presenta cuando existen puntos situados a la misma distancia del punto seleccionado como parte de la contraseña, siendo ambos válidos para el usuario legítimo. Sin embargo, uno de ellos puede quedar dentro de la región de tolerancia determinada por la discretización y el otro no, lo que genera falsos negativos. Además, al segmentar la imagen en cuadrículas, no se toman todos los puntos que deberían determinar la región de radio r alrededor del punto seleccionado como contraseña. Esto puede afectar la experiencia de usuario al utilizar el sistema [13], [23].

En general las limitaciones de los métodos de discretización radican en el hecho de que definen la región de tolerancia como un polígono, mientras que la distancia se plantea en términos de un círculo. Además, el criterio utilizado para determinar si un punto es válido o no se basa únicamente en la distancia. Otra debilidad de estos métodos es la necesidad de almacenar información adicional para garantizar la autenticación [23], esto podría ser explotado para aumentar la efectividad de ataques de tipo diccionario. Por lo tanto, es importante abordar en trabajos futuros estas limitaciones y buscar mejoras en los métodos de discretización para lograr una mayor precisión en la autenticación y brindar una mejor experiencia de uso al usuario.

3. CONTRIBUCIÓN DE ESTE ARTÍCULO: DESARROLLO DE UNA API PARA AUTENTICACIÓN GRÁFICA BASADA EN PASSPOINTS

La implementación realizada del sistema Passpoints consiste en una API, ejemplificada con una aplicación sencilla de notas privadas. Para obtener acceso al sistema el usuario debe registrarse introduciendo sus credenciales y su contraseña usando Passpoints, se le pedirá al usuario que seleccione 5 puntos de la imagen, esta puede ser la proveída por el sistema o una escogida por el usuario. En el servidor se calculará la discretización de la imagen y el hash de los puntos y se almacenará junto a todos los datos necesarios para la posterior fase de autenticación. Para llevar a cabo la discretización de la imagen se utilizó la discretización optimal, debido a los beneficios y ventajas previamente mencionados de su uso. Los datos de texto claro (ϕ) y (φ) necesarios para la autenticación son cifrados utilizando AES (*Advanced Encription Standard*) con tamaño de llave de 256 bits en modo de operación CBC (*Cipher Block Chaining*). Debido a la variabilidad de tamaños de imagen y densidad de píxeles de las mismas el radio de la región de tolerancia fue redefinido como un valor $0 < d < 1$ que representa el porcentaje de píxeles de la imagen que abarca dicha región, por lo que el tamaño en píxeles de la región de tolerancia es variable respecto a la imagen, esto abre la puerta a posteriores trabajos dando la posibilidad al usuario de seleccionar el tamaño de la región de tolerancia para su contraseña y simplifica el proceso de prueba de varios tamaños de la región de tolerancia. Para obtener el valor en píxeles del radio de la región de tolerancia se multiplica d por el mínimo entre el largo y ancho de la imagen, sea

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

d el valor porcentual del radio de la región de tolerancia, d' su valor en píxeles, a la altura en píxeles de la imagen y $b$el ancho en píxeles de la imagen, tenemos

$$d' = d \cdot min(a, b) \quad (11)$$

Las coordenadas de los puntos tomados, se dan en coordenadas de píxel de la imagen, haciendo que sea utilizable en cualquier tamaño de pantalla y cualquier densidad de imagen, sea (I_X, I_Y) las coordenadas de imagen del punto p_0 seleccionado por el usuario, (S_X, S_Y) sus coordenadas de ventana S_W el ancho de la ventana, S_h el alto de la ventana, I_W el ancho de la imagen, I_h el alto de la imagen entonces se calcula

$$I_X = \lfloor \frac{S_X}{S_W} \cdot I_W \rfloor$$
$$I_Y = \lfloor \frac{S_Y}{S_h} \cdot h \rfloor \quad (12)$$

Una vez verificada la autenticidad del usuario se calcula su token de acceso al sistema, en este caso se utilizó JWT (JSON web tokens) lo cual servirá para mantener la sesión del usuario. El código fuente de esta implementación puede encontrarse en https://github.com/AlexSanchez-bit/passpoint-beta

3.1 Pseudocódigo de la implementación

El pseudocódigo proporcionado muestra el algoritmo utilizado para la implementación del PassPoints utilizando la discretización optimal. El método "hashcode" calcula el hash de la contraseña proporcionada por el usuario dados los puntos y el resultado previo del cálculo de las variables ϕ y φ como se explicó anteriormente. Esto se hace en el código de "getVarphi" que calcula estos parámetros. Por último, "optimal_discretization" es la implementación de la discretización optimal donde para cada punto se calcula su hash. En todo el código se utiliza el parámetro "scale" que se usa para escalar los puntos a coordenadas de píxeles. Tanto la tolerancia como los puntos seleccionados por el usuario serán recolectados en la interfaz de usuario como valores reales x ∈ [0,1] que representarán en qué sección de la imagen estaba el punto. Luego, al multiplicar estos valores por el mínimo entre el largo y ancho de la imagen se obtendrá el píxel que se seleccionó originalmente, lo que permite utilizar el sistema en diferentes tamaños de imagen y pantallas, haciéndolo más accesible.

Algoritmo 1: Ejemplo de tolerancia utilizada

```
1 Constante tolerance = 0.1;
2 //corresponde a un cuadrado cuyo tamaño es el 10% del mínimo entre el largo y ancho de la imagen.
```

Algoritmo 2: Pseudocódigo para hashcode

```
Data: points, _varphi, scale
Result: total_hash
1 total_hash = 0;
2 para i = 0 hasta points.length - 1 haga
3   total_hash += optimal_discretization(points[i][0], points[i][1], _varphi[i][0], _varphi[i][1], scale);
4 fin
5 Devolver total_hash;
```

Algoritmo 3: Pseudocódigo para getVarphi

```
Data: points, scale
```

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

```
Result: return_array
1 return_array = Nuevo Arreglo;
2 const _tolerance = Truncar(tolerance * scale);
3 para i = 0 hasta points.length - 1 haga
4   x = points[i][0];
5   y = points[i][1];
6   fi = Si (x % (2 * _tolerance)) >= (_tolerance) Entonces x % _tolerance Sino (x % (2 * _tolerance)) - _tolerance;
7   Fin Si;
8   fiy = Si (y % (2 * _tolerance)) >= (_tolerance) Entonces y % _tolerance Sino (y % (2 * _tolerance)) - _tolerance;
9   Fin Si;
10  return_array.Agregar([fi, fiy]);
11 fin
12 Devolver return_array;
```

Algoritmo 4: Pseudocódigo para optimal_discretization

```
Data: x, y, fi, fiy, scale
Result: hash
1 const _tolerance = Truncar(tolerance * scale);
2 hash = Truncar((x - fi) / (2 * _tolerance)).ConvertirAString();
3 hash += Truncar((y - fiy) / (2 * _tolerance)).ConvertirAString();
4 Devolver hash;
```

La complejidad algorítmica de este código es sencilla de calcular, al ser la cantidad de puntos constantes (5 puntos) y solo iterarse a través de estos se puede llegar a la conclusión de que la complejidad es constante o en notación Big O, $O(1)$. En [11] se muestra el tamaño del espacio de contraseñas que se obtiene al utilizar la discretización optimal:

$$P = \left(\frac{a^6}{r} \cdot \frac{b^6}{r}\right) \quad (13)$$

donde:
$a \cdot b$: dimensión de la imagen,
c: cantidad de puntos seleccionados, y
r: radio de la región de tolerancia.

3.2 Pruebas e interfaz

Para llevar a cabo el proceso de prueba de la presente implementación propuesta, se construyó una interfaz gráfica consistente en una aplicación sencilla de notas, con una vista de inicio de sesión y registro, donde el usuario puede tanto crear una cuenta como iniciar su sesión. Se probaron diferentes tipos de pantalla, tanto móvil con resoluciones de 390x844, 360x740, y 375x667 como escritorio con 1920x1080, para probar que la misma contraseña funcionara correctamente en diferentes pantallas con distintas dimensiones y resoluciones. Como parte del proceso se crearon contraseñas desde las pantallas escritorio y se validó que en las móviles se mantuviera consistente dicha contraseña. Para el ingreso y validación de estas contraseñas se tiene en cuenta el orden en que se incluyen los puntos a la contraseña y que los puntos seleccionados en la fase de autenticación se encuentren en la región de tolerancia de los insertados durante la fase de registro.

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

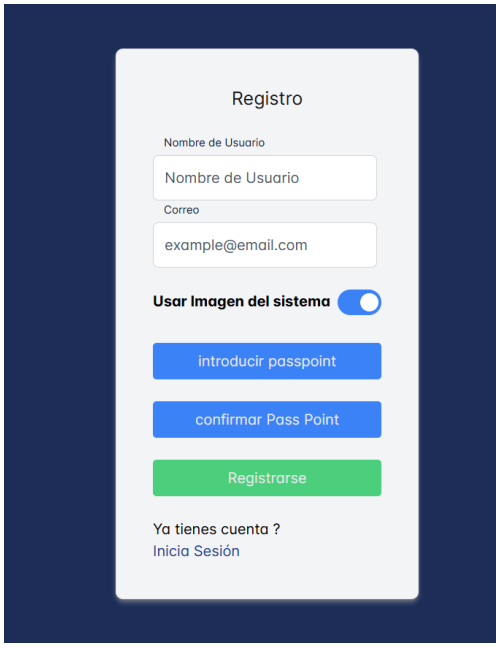


Figura 7: Interfaz de la aplicación

Figura 8: Ingresando contraseña en pantalla móvil (390x844) tolerancia: 0.03

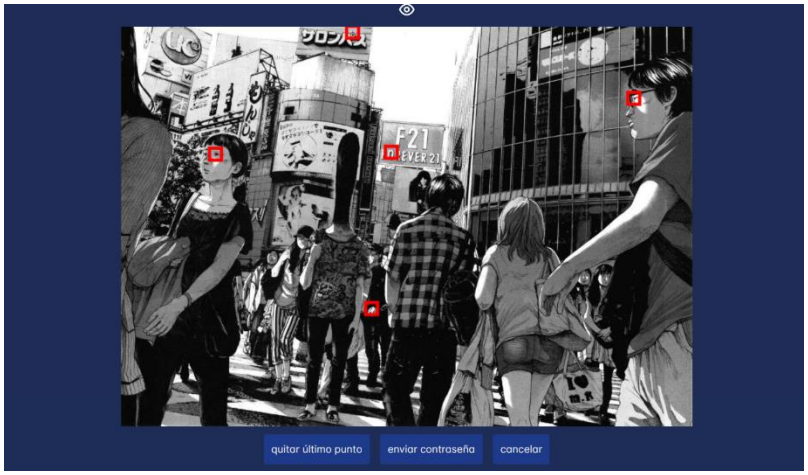


Figura 9: Autenticando la contraseña en (1920x1080) tolerancia:0.03

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

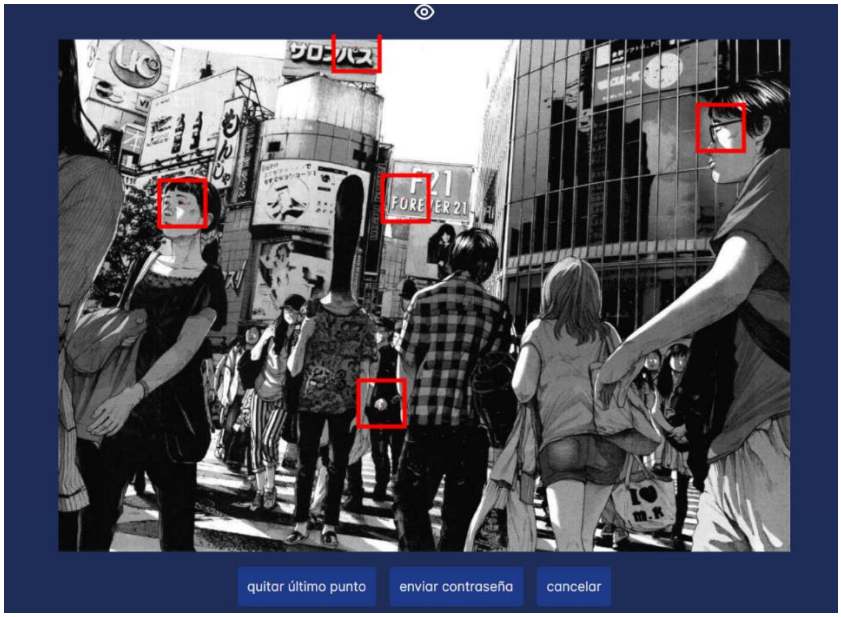


Figura 10: Registrando la contraseña en (1920x1080) tolerancia 0.06

Figura 11: Autenticando en (375x667) Tolerancia 0.06

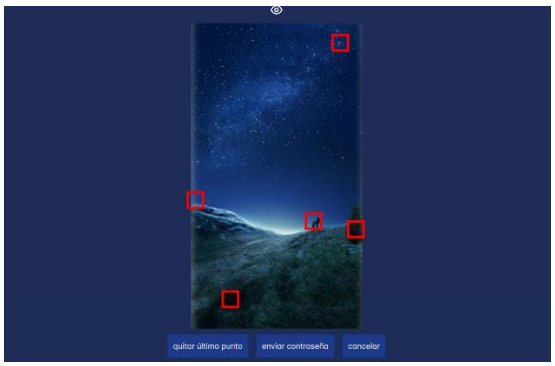


Figura 12: Utilizando imagen de resolución(243x432)

Figura 13: variando el tamaño de pantalla (390x844)

Figura 14: variando el tamaño de pantalla(375x667)

CONCLUSIONES

En este trabajo se presentó una implementación propia del sistema Passpoints, con la intención de contar con una alternativa práctica a las tradicionales contraseñas alfanuméricas. Se mostró por qué constituye un método novedoso superior en cuanto a seguridad y usabilidad con respecto a los sistemas actuales basados en contraseñas alfanuméricas. Se realizó un estudio riguroso de este sistema, por lo que fueron definidas sus características, funcionamiento y

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

seguridad. Se analizaron y compararon los distintos métodos de discretización existentes, seleccionando la discretización optimal por presentar la menor complejidad algorítmica y por ser una de las dos discretizaciones que ofrecen mayor seguridad. Una de las ventajas de contar con esta implementación propia será poder realizar experimentos empleando datos y usuarios reales, y no simulaciones como se había hecho hasta el momento en la mayoría de los antecedentes que hacían uso del Passpoints.

En trabajos futuros se continuará trabajando en la implementación del Passpoints, se incorporarán al sistema una cantidad significativa de imágenes y los test de aleatoriedad espacial encontrados en la bibliografía capaces de detectar contraseñas gráficas no aleatorias, con el objetivo de aumentar su seguridad en la fase de registro.

RECONOCIMIENTOS

Esta investigación se desarrolló en el marco del proyecto de investigación "Pruebas estadísticas de aleatoriedad aplicadas a la seguridad de sistemas de información" del Programa Nacional de Ciencias Básicas de la Academia de Ciencias de Cuba. Código del proyecto: PN223LH010-048.

REFERENCIAS

[1] R.W. Proctor, M.C. Lien, K.P.L. Vu, E.E. Schultz y G. Salvendy, «Improving computer security for authentication of users: Influence of proactive password restrictions», *Behavior Research Methods, Instruments & Computers*, Vol.34, No.2, pp. 163–169, 2002.

[2] P.P. Ray, «Rays Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices», *Journal of Information Engineering and Applications*, Vol. 2, 2012.

[3] V. Zimmermanna y N. Gerberb, «The password is dead, long live the password - A laboratory study on user perceptions of authentication schemes», *International Journal of Human Computer Studies*, 133, pp. 26-44, 2020.

[4] J. Rando, F. Pérez-Cruz y B. Hitaj, «PassGPT: Password Modeling and (Guided) Generation with Large Language Models», arXiv:2306.01545, 2023. https://doi.org/10.48550/arXiv:2306.01545

[5] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy y N. Memon, «PassPoints: Design and longitudinal evaluation of a graphical password system», *International Journal of Human Computer Studies*, Vol. 63(1-2), pp. 102-127, 2005.

[6] G. E. Blonder, «Graphical password», US Patent No. 5559961, 1996 (Sept. 24).

[7] C.M. Legón, R. Socorro, P. Navarro, O. Rodríguez y E. Borrego, «Nuevo modelo probabilístico en autenticación gráfica», *Ingeniería Electrónica, Automática y Comunicaciones*, Vol.40, No.3, pp. 92-104. Epub 08 de septiembre de 2019.

[8] O. Rodriguez, «Algoritmo para la detección de claves débiles en la técnica de autenticación gráfica passpoints», M.Sc. tesis, Universidad de la Habana, Facultad de Matemática y Computación, Instituto de Criptografía, 2019.

[9] O. Rodriguez, C. M. Legón y R. Socorro, «Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica», *Revista Cubana de Ciencias Informáticas*, vol. 12, no. Especial UCIENCIA, pp. 13-27, 2018.

[10] Bi.B. Zhu, D. Wei, M. Yang y J. Yan, «Security Implications of Password Discretization for Click-based Graphical Passwords», *Proceedings of the 22Nd International Conference on World Wide Web*, New York, USA: ACM, pp. 1581–1591, 2013.

[11] J.C. Birget, D. Hong y N. Memon, «Graphical Passwords Based on Robust Discretization», *IEEE Transactions on Information Forensics and Security*, Vol.1, No.3, 2006b.

[12] S. Chiasson, J. Srinivasan, R. Biddle y P.C. van Oorschot, «Centered Discretization with Application to Graphical Passwords», *In: UPSEC*. Citeseer. 2008b.

[13] K. Bicakci, «Optimal Discretization for High-Entropy Graphical Passwords», Ph.D. thesis, OBB University of Economics and Technology, Ankara, Turkey, 2007.

[14] D. Kirovski, N. Jogic y P. Roberts, «Click Passwords». *Microsoft Research*, One Microsoft Way, Redmond, WA 98052, USA, 2007.

[15] K. Renaud y A.D. Angeli, «My password is here! an investigation into visio-spatial authentication mechanisms», *Interacting with Computers 16*, pp. 1017-1041, 2004.

[16] J.A. Herrera, C.M. Legón, L. Suárez, L.R. Piñeiro, O. Rojas y G. Sosa, «Test for Detection of Weak Graphic Passwords in Passpoint Based on the Mean Distance between Points», *Symmetry* 2021, 13, 777.

[17] L. Suárez, C.M. Legón, J.A. Herrera, R. Socorro, O. Rojas y G. Sosa, «Weak PassPoint Passwords Detected by the Perimeter of Delaunay Triangles», *Security and Communication Networks*, 2022.

[18] L. Suárez, J.A. Herrera, C.M. Legón, G. Sosa y O. Rojas, «Detection of DIAG and LINE patterns in PassPoints graphical passwords based on the maximum angles of their Delaunay triangles», 22(5):1987, DOI: 10.3390/s22051987, *Sensors*, March 2022. https://doi.org/10.3390/s22051987

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

[19] J.A. Herrera, L. Suárez, C.M. Legón y G. Sosa, «Comparación y combinación de dos test efectivos en la detección de contraseñas gráficas no aleatorias en Passpoints», *Revista Cubana de Ciencias Informáticas*, Vol.17, No.1, feb. 2023. ISSN 2227-1899. https://rcci.uci.cu/?journal=rcci$\&$page=article$\&$op=view$\&$path$\%$5B$\%$5D=2584
[20] J.A. Herrera, L. Suárez y C.M. Legón, «Nuevo test para detectar contraseñas gráficas agrupadas en Passpoints», *Congreso Internacional Matemático COMPUMAT 2023*, La Habana, Cuba. ISBN 978-959-16-4930-0.
[21] J.A. Herrera, L. Suárez y C.M. Legón, «Nuevo test para detectar contraseñas gráficas regulares en Passpoints», *Congreso Internacional Matemático COMPUMAT 2023*, La Habana, Cuba. ISBN 978-959-16-4930-0.
[22] J. A. Herrera-Macías, L. Suárez-Plasencia, C. M. Legón-Pérez, G. Sosa-Gómez y O. Rojas, «New test to detect clustered graphical passwords in Passpoints based on the perimeter of the convex hull», *Information*, vol. 15, no. 8, p. 447, 2024. DOI: https://doi.org/10.3390/info1508044.
[23] E.A. Borrego, P.E. Navarro y C.M. Legón, «Debilidades de los métodos de discretización para contraseñas gráfica», In: de Criptografía. Sociedad Cubana de Matemática y Computación, Instituto (ed), *IV Seminario Científico Nacional de Criptografía*. Universidad de la Habana. 2018.

SOBRE LOS AUTORES

Alex Sánchez Saez: Estudiante de cuarto año de licenciatura en Ciencias de la Computación en la Facultad de Matemática y Computación de la Universidad de La Habana (UH), Cuba. Ganador del tercer lugar en el Evento Académico “Matemática” dentro de la Jornada Científica Estudiantil 2023 de su facultad. Participante del XVIII Congreso Internacional de Matemática y Computación (COMPUMAT 2023), y del Evento INFORMÁTICA 2024 en el programa científico “XVI Seminario Iberoamericano de Seguridad en las Tecnologías de la Información” en el área de Ciberseguridad. Orcid: https://orcid.org/0009-0009-1672-0583 .

Evaristo José Madarro Capó: Graduado en el 2010 de Ingeniero en Ciencias Informáticas en la Universidad de Ciencias Informáticas (UCI). Culminó en el 2012 la Especialidad en Aplicaciones Criptográficas en la Universidad Tecnológica de La Habana (CUJAE). En el 2017, terminó la Maestría en Ciencia de la Computación (3 años) en la Universidad Central "Marta Abreu" de Las Villas (UCLV). Trabaja actualmente en su doctorado en el Instituto de Criptografía en la Facultad de Matemática y Computación de la Universidad de La Habana. Las áreas de interés están relacionadas a la aplicación de algoritmos matemáticos-computacionales a la Criptografía y la seguridad en el desarrollo de software. Pertenece, desde el 2022, a la red “New cryptographic tools for the e-community” (522RT0131) del programa iberoamericano de ciencia y tecnología para el desarrollo (CYTED). Orcid: http://orcid.org/000-0002-5226-5946X .

Joaquín Alberto Herrera Macías: Graduado de Licenciatura en Matemática en la UH en el 2017, y Máster en Ciencias Matemáticas en la misma universidad en el 2021. Es profesor instructor de la Facultad de Matemática y Computación, UH, donde ha impartido cursos de pregrado y posgrado. Ha participado tanto en eventos nacionales como internacionales. Ha publicado varios artículos en Cuba y en el extranjero. Miembro desde el año 2022 de la Red Iberoamericana de Ciencia y Tecnología para el Desarrollo (CYTED). Fue premiado con el Premio Anual de la Academia de Ciencias de Cuba 2022, por ser uno de los autores de los resultados de investigación “Pruebas estadísticas de aleatoriedad aplicadas a la seguridad de sistemas de información”. Orcid: https://orcid.org/0000-0001-8940-050X .

Lisset Suárez Plasencia: Graduada de Licenciatura en Matemática en la UH en el 2017, y Máster en Ciencias Matemáticas en la misma universidad en el 2021. Es profesora instructor de la Facultad de Matemática y Computación, UH, donde ha impartido cursos de pregrado y posgrado. Ha participado tanto en eventos nacionales como internacionales. Ha publicado varios artículos en Cuba y en el extranjero. Miembro desde el año 2022 de la Red Iberoamericana de Ciencia y Tecnología para el Desarrollo (CYTED). Fue premiada con el Premio Anual de la Academia de Ciencias de Cuba 2022, por ser uno de los autores de los resultados de investigación “Pruebas estadísticas de aleatoriedad aplicadas a la seguridad de sistemas de información”. Poseedora del premio Sofia Kovalevskaya en la mención Tesis de Maestría del 2023 que otorga la Sociedad Cubana de Matemática y Computación con el auspicio de la Fundación Kovalevskaya. Orcid: https://orcid.org/0000-0001-5344-667X .

CONFLICTO DE INTERESES

Los autores declaran no tener conflictos de intereses.

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.22, 2023, p.133-147 ISSN 1729-3804

CONTRIBUCIONES DE LOS AUTORES

Todos los autores contribuyeron en igual medida a este artículo.

Manuscrito recibido: 10-7-2024, aceptado: 11-9-2024
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele