Universidad de la Habana

Facultad de Matemática y Computación

Test para la detección de patrones DIAG y LINE en las contraseñas gráficas de PassPoint, basada en la cantidad de triángulos de Delaunay

Autor: Ovidio Navarro Pazos

Tutor(es): MrS.Lisset Suárez Plasencia
MrS.Joaquín A. Herrera Macías

La Habana, Cuba
15 de diciembre de 2024

Índice general

Índice de figuras

Índice de Tablas

Introducción

En la actualidad, una gran mayoría de los usuarios tiende a ignorar las recomendaciones de seguridad al momento de crear contraseñas alfanuméricas. Es común observar el uso de contraseñas cortas y cargadas de información personal, lo cual facilita su memorización, pero también aumenta significativamente su vulnerabilidad frente a ataques de fuerza bruta o de diccionario [[1,4,5,6]].

Para abordar estas debilidades, se han desarrollado nuevas alternativas, entre las cuales destacan las contraseñas gráficas. Este enfoque se basa en la capacidad humana de recordar patrones visuales en una imagen con mayor facilidad que largas cadenas de caracteres alfanuméricos. En este tipo de contraseñas, el usuario debe recordar una imagen o partes específicas de ella mediante la selección de determinados puntos, imágenes que dadas sus características posean un amplio espacio para la construcción de sus contraseñas y de este modo ser más resistentes a los ataques de diccionarios, obteniendo un espacio de búsqueda mucho más amplio y resistente a los ataques comunes.

En este trabajo, específicamente, vamos a trabajar sobre el PassPoint[1], una técnica de autenticación gráfica que en su fase de registro consiste en seleccionar cinco puntos de una imagen elegida por el usuario. Durante la autenticación, el usuario debe hacer clic en una determinada vecindad y en el mismo orden de los puntos registrados. Entre las debilidades de esta técnica se encuentran los Hotspots[6](puntos más probables a seleccionar por el usuario), además diversos patrones predefinidos que los usuarios tienden a seguir durante el registro para facilitar la memorización. Estos patrones incluyen formas específicas como Z, W, C, V, patrones agrupados o regulares, y patrones LOD, DIAG o LINE (formas de línea o diagonales).

La tendencia de los usuarios a crear patrones entre los puntos seleccionados, ya sea de manera independiente o en combinación con Hotspots, constituye una debilidad importante. Esto hace que las contraseñas generadas sean menos aleatorias y más susceptibles a ataques basados en diccionarios específicos. Por ello, resulta fundamental desarrollar pruebas que detecten la existencia de estos patrones en las contraseñas antes de su uso, ya que contribuirían significativamente a mejorar la seguridad de la técnica PassPoint.

A lo largo de los últimos años, se han realizado pocas investigaciones enfocadas en este tema. Entre los métodos más comunes para evaluar la Aleatoriedad Espacial Completa se encuentran: el test de la función K-Ripley, el test de la función G, que analiza la distancia al vecino más cercano, y el test de la función F, que se centra en la distancia de espacio vacío. Sin embargo, en [9-10 sensor] se demuestra que, en el contexto de PassPoint, dos de estos métodos son ineficaces para detectar contraseñas gráficas compuestas por patrones agrupados. Por otro lado, en [15, 16] se evidencia que los tres tests no logran identificar ni el agrupamiento ni la regularidad en las contraseñas de este escenario. Hasta ahora, en la bibliografía revisada, se han encontrado dos tests efectivos (tesis de Liset y Joakin) para identificar contraseñas no aleatorias que presentan patrones agrupados o regulares en el contexto de PassPoint. Estos métodos se basan, en el caso de (Liset), en la distancia

promedio de los perímetros de los triángulos de Delaunay, y, en el caso de (Joakin), en la distancia media entre cinco puntos.

Teniendo en consideración que las propiedades de una triangulación de Delaunay brindan la capacidad de obtener información acerca de la interrelación entre puntos, se ha empleado como una herramienta en la mitad de la década de 1980 para identificar configuraciones de puntos. En el estudio realizado por Chiu [22], se emplearon varias de estas propiedades para reconocer la agrupación y la regularidad entre los puntos. Específicamente, la característica del“ ángulo máximo de un triángulo de Delaunay”, según la literatura revisada, nunca había sido utilizada previamente para identificar otro tipo de configuraciones además de las agrupadas o regulares. No obstante, dado que los patrones DIAG y LINE se distinguen por presentar un ángulo cercano a 0° entre dos segmentos consecutivos, en [sensor] se propuso y demostró que la media de los ángulos máximos de los triángulos de Delaunay generados a partir de los puntos de las contraseñas gráficas de PassPoint es un estadígrafo eficaz para detectar la presencia de patrones DAIG y LINE, incluso con un número limitado de puntos. En [15] se entendía como el ángulo formado entre dos segmentos consecutivos ,el menor de los dos ángulos que forman la intersección de la prolongación de los segmentos de una contraseña.Nos referiremos al mayor de estos dos ángulos como el ángulo adyacente entre dos segmentos .

Según los resultados obtenidos en (sensor) se sugiere investigar la eficacia de un test de detección de los patrones DIAG y LINE utilizando como estadígrafo el promedio de los ángulos máximos de los triángulos de Delaunay pero realizando análisis independientes según la cantidad de triángulos en su triangulación (3,4,5) y realizar un análisis comparativo respecto a los resultados obtenidos en (sensor).

Problema de investigación:

Detectión contraseñas que sigan los patrones suaves DIAG y LINE en PassPoint, basada en la cantidad de triángulos de Delaunay.

Objetivo de estudio:

Comprobar si el estadígrafo “promedio de los ángulos máximos de las triangulaciones de Delaunay ”, es más eficaz si se trabaja individualmente sobre las distintas cantidades de triángulos existentes en las triangulaciones.

Campo de acción:

Detección de contraseñas gráficas no aleatorias en el escenario PassPoint utilizando las triangulaciones de Delaunay.

Hipótesis:

Es posible que utilizar el estadígrafo “promedio de los ángulos máximos de las triangulaciones de Delaunay”de manera individual sobre las distintas cantidades de triángulos existentes en las triangulaciones es mas eficaz que trabajarlo de manera general.

Idea de la solución:

Para cada cantidad de triángulos en las triangulaciones de Delaunay para 5 puntos:

- Encontrar como distribuyen las contraseñas aleatorias
- Realizar un análisis estadístico obteniendo los errores tipo I y II

- Realizar una comparación con los resultados obtenidos en (SENSOR).

Objetivos

Objetivos generales:Detectar[1] la no aleatoriedad en las contraseñas gráficas que siguen patrones DIAG o LINE en PassPoint para cada número de triángulos en una triangulación de Delaunay

Objetivos específicos:

- Crear un criterio de desición basados en el promedio de los ángulos máximos de los triángulos de Delaunay para cada posible cantidad de triángulos en su triangulación.
- Para cada cantidad de triángulos, obtener estimaciones teóricas del número esperado de fallos en la detección de contraseñas gráficas débiles.

1. Marco Teórico

Incluye el marco teórico, revisiones de la literatura y conceptos clave relacionados con tu trabajo. En esta sección se definen los conceptos clave que son relevantes para este trabajo.

1.1. PassPoint

La técnica PassPoint diseñada por Wiedenbeck(77 osviel) destaca entre los sistemas de autenticación gráfica del tipo cued-recall por su usabilidad y seguridad(rodrigez et al..2018 comparacion pag3) . Esta técnica consiste en que en su fase de registro el usuario debe seleccionar 5 puntos(pixeles) de una imagen ya sea seleccionada por el o dada por el sistema y en el proceso de autentificación este debe hacer click en el mismo orden y en determinada vecindad o región de tolerancia de los puntos escogidos en la fase de registro. Wiedenbeck su investigación (77 osviel) asegura que las imágenes más deseadas para el proceso debían tener contenido que tuviera significado para el usuario por lo que debían tener escenas concretas, otro requisito es que la imagen seleccionada posean cientos de HOTSPOST(puntos más probables a seleccionar por el usuario o mejor llamados puntos calientes) diseminados de forma homogenea ,pero existe el problema de que en el momento de autentificación el usuario no seleccione exactamente el mismo punto y a esto se le llaman errores de discretización, la discretización se encarga de establecer una tolerancia alrededor de cada punto por tanto esto disminuye el espacio de contraseñas y aumenta información relevante a la hora de los ataques de diccionarios. Se puede encontrar un análisis sobre la relevancia del mecanismo de discretización en los sistemas de contraseñas gráficas en [75, 76, 77 Lisset]. Por otro lado, en [75, 76, 77, 78 Liset] se describen los distintos métodos de discretización que se han desarrollado hasta ahora.

En el trabajo (3 sensor) se presenta un método que permite determinar si una imagen es adecuada para ser utilizada en esta técnica. Este método conduce al desarrollo de un modelo diseñado para identificar las regiones de una imagen que los usuarios tienen mayor probabilidad de elegir como parte de sus contraseñas. Según sus experimentos, el modelo puede predecir puntos de interés (hotspots) con una precisión de entre el 70 % y el 80 %, aunque el tamaño de la muestra utilizada es limitado. La aplicación de esta técnica en el sistema PassPoint sería especialmente útil para mejorar la confiabilidad en la asignación de imágenes. Por otro lado, en el estudio (4 sensor) se demostró que incluso un pequeño cambio en la imagen puede influir en la elección de contraseñas por parte del usuario durante la fase de registro, afectando así su nivel de seguridad.

En relación al espacio de contraseñas, según (77 Osviel), no sería necesario utilizar muchos puntos para crear una contraseña segura. Con solo 5 o 6 puntos (en una imagen de 1024x725), se podría lograr mayor seguridad que con contraseñas de 8 caracteres dentro de un alfabeto estándar de 64 símbolos. En la tabla (Graphical vs Alphanumeric), se muestra

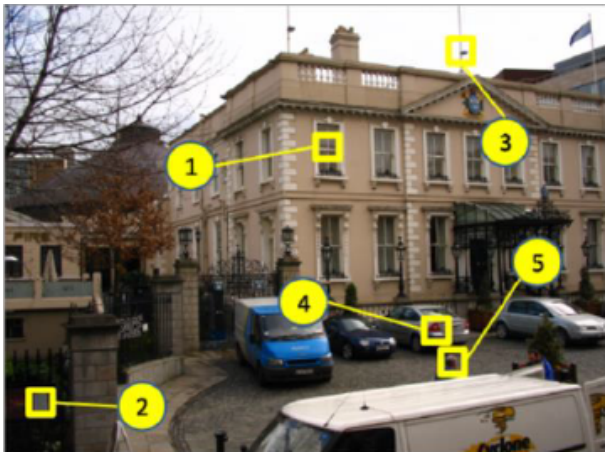

Figura 1.1: PassPoint.

una comparación entre los espacios de contraseñas gráficas y alfanuméricas, considerando factores como el alfabeto, la longitud de la contraseña, la tolerancia y el tamaño de la imagen. Se observa que, con 5 puntos y un tamaño de imagen razonable, las contraseñas gráficas mantienen un espacio de clave superior al de las contraseñas alfanuméricas.

	Image size	Grid square size(pixels)	Alphabet size/ No.squares	Lenght/No. click points	Password space size
Alfanumérica	N/A	N/A	64	8	2.8x
Alfanumérica	N/A	N/A	72	8	7.2x10
Alfanumérica	N/A	N/A	96	8	7.2x10
Gráficas	451x331	20x20	373	5	7.2x10
Gráficas	1024x752	20x20	1925	5	2.6x10
Gráficas	1024x752	14x14	3928	5	9.3x10
Gráficas(1/2 screen used)	1024x752	14x14	1964	5	2.9x10

Tabla 1.1: Alfanuméricas vs Gráficas

1.2. Patrones en contraseñas gráficas

Además de los Hotspots, las contraseñas graficas presentan otro tipo de debilidades como son leyes de percepcion, modelos de atención y distintos tipos de patrones, estas formas de seleccion son comunmente utlizadas por los usuarios para garantizar una mejor momorabilidad, lo que hace que sea mas facil contruir diccionarios de ataques estas contraseñas.

1.2.1. Modelos de atención

Los Modelos Visuales De Atencion(MVA) estudian la forma en que las personas observan una imagen. Se estima que un grupo significativo de usuariios escoge los puntos siguiendo estos patrones (14). De esta manera se pueden construir dicccionarios con los grupos de puntos mas probables a seleccionar por el usuario. Los modelos computacionales de atencion Botton-Up, se definen normalmente por caracteristicas de las imagenes

digitales tales como: la intensidad, el color y la orientacion(9,12). Por otra partelos modelos computacionales TopDown, pueden ser definidos por entrenamiento. La dificultad de estos ultimos se basa en que la tarea Top-down debe ser predefinida(ej.encontrar personas en una imagen) en um grupo de imagenes que se etiquetan con areas que contienen a los sujetos (14). Nos enfocaremos en la la propuesta de Itti(8,9) ya que exsite evidencia empírica de que este captura la forma en que las persinas observan una imagen desde lo profundo hacia arriba(botton-up)(13). La idea principal de esta propuesta es que algunas areas de una imagen, son salientes o de alguna manera resaltan por que difieren del resto de su entorno. De esta manera dada una imagen ek modelo devuelve las localizzaciones y el orden en que el ser humano de forma insconciente y automatica la observa. El proceso se compone de dos etapas. En la primera se crea un mapa de salientes basados en las caracteristicas visuales. En la segunda etapa se usa una red neuronal 'winner-take-wall' con el objetivo de replicar la forma en que el usuario observaria la imagen. En(15) se desarrolla un ataque automatico de diccionario que se basaba solo en variaciones de la primera etapa donde utilizaba deteccion de esquinas para encontrar puntos referenciables, luego en (14) se describe como seria la segunda etapa del proceso. La idea principal (primera etapa) de esto metodo sirve de soporte para las tecnocas de analisis y procesamiento de imagenes. Estas se vasen en la deteccion de esquinas y centroides asi como la plicacion de herramientas y algoritmos de inteligencia artificial para detectar objetos en imagenes

1.3. Triangulaciones de Delaunay

Definición(Triángulación de Delaunay): Una triangulación del conjunto P de los puntos sobre el plano es de Delaunay,si y sólo si la circunferencia circunscrita de cualquier triángulo en la red no contiene un punto p en su interior,como muestra la figura(triangulacionnes). Esta condición es conocida como condición de Delaunay.[23,45,46 lisset].

Propiedades elementales de las triangulaciones de Delaunay

Una triangulación de Delaunay presenta las siguientes tres propiedades elementales:

1. La frontera externa de la triangulación de Delaunay forma la envoltura convexa del conjunto de puntos.

2. El ángulo mínimo dentro de todos los triangulos de Delaunay esta maximizado, es decir , se evita obtener resultados con angulos demasiados agudos. Como consecuencia de lo anterior, los Triangulos generados en una triangulacion tienden a ser lo mas equilatero posible. Esto es debido a que todo triangulo no equilatero siempre tine algun angulo menor que 60°.

3. La triangulacion es unica cuando ningun borde de la circunferencia circunferencia circunscrita contiene mas de tres vertices de la red

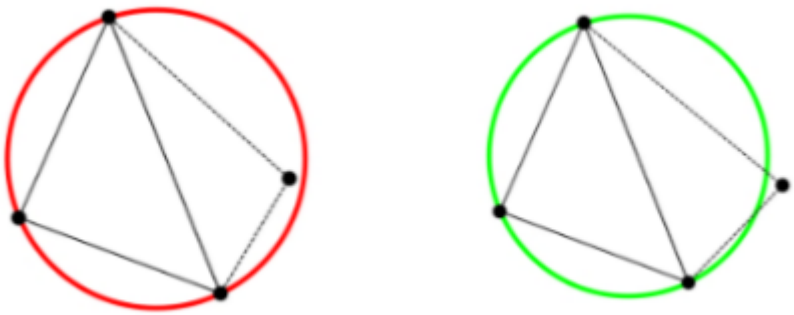

Figura 1.2: poner esta img como si fueran 2

2. Metodología

Describe la metodología utilizada en tu investigación, incluyendo los métodos, herramientas y procedimientos.

3. Resultados

Presenta los resultados obtenidos durante tu investigación.

4. Discusión

Analiza los resultados y compara con otros estudios o referencias relevantes.

5. Conclusiones y Recomendaciones

Resume los hallazgos principales y ofrece recomendaciones futuras.

Bibliografía

[1] Autor A, et al. Título del artículo. Revista, año.

A. Anexo A

Incluye aquí cualquier información adicional como encuestas, gráficos, o tablas complementarias.