Universidad de la Habana

Facultad de Matemática y Computación

Test para detectar patrones DIAG y LINE en las contraseñas gráficas de PassPoint, basado en el promedio de los ángulos máximos de los triángulos de Delaunay, condicionado al número de triángulos

Trabajo de Diploma presentado en opción al título
de Licenciado en Ciencias de la Computación

Autor: Ovidio Navarro Pazos

Tutores: M.Sc. Lisset Suárez Plasencia
Dr.C. Carlos Miguel Legón Pérez
M.Sc. Joaquín A. Herrera Macías

La Habana, Cuba
22 de enero de 2025

Resumen

Un método de autenticación que difiere de las contraseñas alfanuméricas tradicionales es la autenticación gráfica. Una de las técnicas más valiosas dentro de este campo es PassPoint, conocida por su equilibrio entre seguridad y usabilidad. Sin embargo, esta técnica puede ser vulnerada si el usuario sigue patrones predefinidos al seleccionar los cinco puntos en la imagen, como los patrones DIAG y LINE. Investigaciones previas han destacado la utilidad de las características de las triangulaciones de Delaunay para extraer información de estos puntos que constituyen la contraseña, siendo el AMADT (promedio de los ángulos máximos de los triángulos de Delaunay) una de estas características relevantes.

En este estudio, se comparan contraseñas gráficas generadas por la elección aleatoria de cinco puntos en una imagen con contraseñas que siguen patrones específicos del tipo DIAG y LINE. La comparativa se basa en segmentar las contraseñas que siguen estos patrones, considerando el número de triángulos en sus triangulaciones de Delaunay (3, 4 o 5). Experimentalmente se demuestra que, para cada número de triángulos, las contraseñas con patrones DIAG y LINE tienen un AMADT más alto que aquellas generadas con puntos aleatorios. Estudios previos respaldan este resultado y sugieren la viabilidad de un *test* de aleatoriedad espacial para identificar contraseñas gráficas débiles que sigan los patrones DIAG y LINE, utilizando el AMADT como estadígrafo. Se estiman las distribuciones más adecuadas para cada número de triángulos, se implementa un *test* de hipótesis y se valida mediante la estimación de los errores de tipo I y II. La relevancia de este *test* radica en la similitud de los resultados con pruebas previas. Sería crucial determinar si estos hallazgos son redundantes o complementarios para mejorar la seguridad del sistema de autenticación gráfica PassPoint.

Abstract

One authentication method that differs from traditional alphanumeric passwords is graphical authentication. One of the most valuable techniques within this field is PassPoint, known for its balance between security and usability. However, this technique can be breached if the user follows predefined patterns when selecting the five dots in the image, such as the DIAG and LINE patterns. Previous research has highlighted the usefulness of Delaunay triangulation features to extract information from these points that constitute the password, with AMADT (average of the maximum angles of the Delaunay triangles) being one of these relevant features.

In this study, graphical passwords generated by randomly choosing five points in an image are compared with passwords that follow specific patterns of the DIAG and LINE type. The comparison is based on segmenting the passwords that follow these patterns, considering the number of triangles in their Delaunay triangulations (3, 4 or 5). Experimentally it is shown that, for each number of triangles, passwords with DIAG and LINE patterns have a higher AMADT than those generated with random dots. Previous studies support this result and suggest the feasibility of a spatial randomization test to identify weak graphical passwords following DIAG and LINE patterns, using the AMADT as a statistician. The best-fitting distributions for each number of triangles are estimated, a hypothesis test is implemented and validated by estimating type I and II errors. The relevance of this test lies in the similarity of the results with previous tests. It would be crucial to determine whether these findings are redundant or complementary to improve the security of the PassPoint graphical authentication system.

Índice general

Índice de figuras

Índice de Tablas

Introducción

En la actualidad, la gran mayoría de los usuarios tienden a ignorar las recomendaciones de seguridad al momento de crear sus contraseñas. Es común observar el uso por los usuarios de contraseñas cortas y cargadas de información personal, lo cual facilita su memorización, pero aumenta significativamente su vulnerabilidad frente a ataques de fuerza bruta o de diccionario [1, 2, 3, 4].

Debido a esta inherente contradicción entre facilidad y seguridad que presentan las contraseñas alfanuméricas, se han desarrollado nuevos métodos alternativos de autenticación, entre los que se encuentran los métodos basados en contraseñas gráficas. Este nuevo enfoque surge por la capacidad humana de recordar patrones visuales en una imagen con mayor facilidad que largas cadenas de caracteres alfanuméricos aleatorios. En este tipo de contraseñas, el usuario debe recordar una imagen o partes específicas de ella mediante la selección de determinados puntos.

El sistema PassPoint[1] es un método de autenticación gráfica que destaca por su usabilidad y seguridad. Este método consiste en que el usuario seleccione en la fase de registro cinco puntos de una imagen elegida por el usuario o dada por el sistema. Durante la autenticación, el usuario debe hacer click en una determinada vecindad y en el mismo orden de los puntos seleccionados en la fase de registro. Una de las debilidades de este sistema es que los usuarios tienden a seleccionar los Hotspots[4](puntos más probables a seleccionar en una imagen), por esta razón las imágenes usadas en el sistema tienen que poseer cientos de Hotspots dispersos de manera homogénea. Además existen un conjunto de patrones no aleatorios que tienden a seguir los usuarios y su combinación con los Hotspots sería un grave error, pues hace que la contraseña sea muy susceptible a ataques de diccionarios. Estos patrones incluyen formas específicas como Z, W, C, V, patrones agrupados, regulares y los que más suelen seleccionar los usuarios que son los patrones DIAG o LINE (formas de diagonales o línea)[5].

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. Por ello, resulta fundamental desarrollar tests 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 [6, 7] 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 [7, 8] 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 4 tests efectivos [7, 9, 10, 11] para identificar

contraseñas no aleatorias que presentan patrones agrupados o regulares en el contexto de PassPoint. Estos métodos se basan, en el caso de [9], en el promedio de los perímetros de los triángulos de Delaunay, en [7] en la distancia media entre cinco puntos, para el caso de [10] es una aplicación conjunta de los tests [7, 9], y [11] basado en el perímetro de la envoltura convexa. De estos tests [11] es el más efectivo encontrado en la literatura y el segundo más eficiente después de [7].

Teniendo en consideración [12], 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 en [12], 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 o en otras palabras que las curvas formadas entre los 5 puntos sean curvas suaves a pedazos, es decir, que carezca de picos, también se les conoce como patrones suaves. De ahí que, en [13] 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 [5] 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. En este trabajo se referirá al mayor de estos dos ángulos como el ángulo adyacente entre dos segmentos .

Según los resultados obtenidos en [13], la distribución del promedio de los triángulos de Delaunay de las contraseñas gráficas aleatorias, sin tener en cuenta el número específico de triángulos sigue una distribución Normal, por lo que se plantea la hipótesis de que cada una de las distribuciones de los conjuntos cuyas triangulaciones contienen 3, 4 o 5 triángulos también distribuirán Normal pero con diferentes parámetros. Suponiendo que esta hipótesis se cumpla, dada una contraseña ingresada por un usuario se verificará a qué distribución pertenece y se aplicará el *test* con la distribución adecuada. Esto debería mejorar el ajuste de los datos a los *test* de bondad de ajuste y aumentar la efectividad del mismo.

Problema de investigación: ¿Cómo detectar contraseñas gráficas que sigan patrones DIAG y LINE en el sistema de autenticación gráfica PassPoint, teniendo en cuenta el número de triángulos de Delaunay?

Objeto de estudio:

Número de triángulos de las triangulaciones de Delaunay en autentificación gráfica

Campo de acción:

Detección de contraseñas gráficas que sigan patrones DIAG y LINE en el escenario PassPoint utilizando el número de triángulos de las triagulaciones de Delaunay.

Hipótesis:

Es posible detectar contraseñas gráficas que sigan patrones DIAG y LINE en el sis-

tema de autenticación gráfica Passpoint, teniendo en cuenta el número de triángulos de las triangulaciones de Delaunay.

Idea de la solución:

Debido a que en la bibliografía existe un *test* capaz de detectar patrones DIAG y LINE en las contraseñas gráficas de PassPoint basado en el promedio de los ángulos máximos de los triángulos de Delaunay. Se propone construir un *test* para detectar este tipo de patrones en las contraseñas gráficas en dicho escenario, pero teniendo en cuenta el número de triángulos de la triangulación de Delaunay correspondiente. Con el fin de llegar a comparar ambos *test* en cuanto a efectividad, y realizar la aplicación conjunta de ambos si es posible para lograr una mayor efectividad en la detección de estos tipos de patrones.

Objetivos:

Objetivo general: Detectar las contraseñas gráficas que siguen patrones DIAG o LINE en PassPoint para cada número de triángulos en una triangulación de Delaunay.

Objetivos específicos: Para cada número de triángulos en las triangulaciones de Delaunay de 5 puntos:

- Encontrar cómo distribuye el promedio de los ángulos máximos de la triangulación de Delaunay en contraseñas aleatorias.
- Construir un *test* de aleatoriedad basado en la distribución del promedio de los ángulos máximos de los triángulos de Delaunay en contraseñas aleatorias.
- Realizar un análisis estadígrafo con las estimaciones de los errores tipo I y tipo II cometidos para validar el *test*.
- Realizar una comparación con los resultados obtenidos en [13].

Estructura de la tesis

Este trabajo estará dividido en dos capítulos.

En el primero se muestra en qué consiste la técnica de autenticación gráfica PassPoint, así como sus ventajas y desventajas, se describen los patrones comunes que los usuarios suelen seguir al crear sus contraseñas, destacando los patrones DIAG y LINE, se definen las triangulaciones de Delaunay y sus propiedades. Por último se realiza un resumen de los métodos antecedentes en la detección de patrones Diag y Line , uno es el algorimo presentado en [3] para la detección de patrones suaves en PassPoint, y el otro es [13], donde se demuestra que el promedio de los ángulos máximos de los triángulos de Delaunay es un estadígrafo eficaz para detectar patrones DIAG y LINE en contraseñas de PassPoint.

En el segundo capítulo se investiga el promedio de los ángulos máximos de los triángulos de Delaunay en función del número de triángulos que conforman dicha triangulación. Tomando en cuenta el tamaño estándar de las imágenes (1920x1080) para cada posible número de triángulos presentes en las triangulaciones de Delaunay de las contraseñas de 5 puntos (3,4 o 5), se estiman las mejores distribuciones a las que se ajustan, se propone un *test* de detección de patrones DIAG y LINE en PassPoint y se estiman los errores de tipo I y tipo II cometidos por el testI. Posteriormente, se realiza una comparación de los resultados obtenidos y los hallazgos presentados en el estudio[13].

Capítulo 1

Marco Teórico

A medida que las amenazas cibernéticas evolucionan, también lo hacen los métodos de autenticación utilizados para proteger los datos sensibles. Este capítulo se centrará en explorar los principios teóricos que sustentan la autenticación gráfica, específicamente el sistema PassPoint, y los patrones que los usuarios tienden a seguir al crear sus contraseñas. Al comprender estos conceptos, se podrá apreciar mejor la vulnerabilidad inherente a los sistemas de autenticación y la necesidad de desarrollar métodos más robustos para mitigar riesgos.

1.1. PassPoint

La técnica PassPoint diseñada por Wiedenbeck en [1] destaca entre los sistemas de autenticación gráfica del tipo cued-recall por su usabilidad y seguridad. Esta técnica consiste en que, en su fase de registro, el usuario seleccione 5 puntos(píxeles) de una imagen , ya sea seleccionada por el mismo usuario o dada por el sistema, un ejemplo es la figura 1.1. En el proceso de autenticación este debe hacer clic en el mismo orden y en determinada vecindad o región de tolerancia de los puntos escogidos en la fase de registro. Wiedenbeck en su investigación [1], asegura que las imágenes más deseadas para el proceso deben tener contenido significativo para el usuario por lo que deben tener escenas concreta. Otro requisito es que la imagen seleccionada posea cientos de Hotspost (puntos más probables a seleccionar por el usuario o mejor llamados puntos calientes) diseminados de forma homogénea, de no ser así se reduciría el espacio de contraseñas y por ende aumentaría la vulnerabilidad ante diversos ataques. Existe el problema de la improbabilidad de que el usuario en el momento de autenticación seleccione exactamente el mismo punto, como alternativa a este problema surge la discretización, esta 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 [14, 15, 16]. Por otro lado, en [14, 15, 16, 17] se describen los distintos métodos de discretización que se han desarrollado hasta ahora .

En el trabajo [18] 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

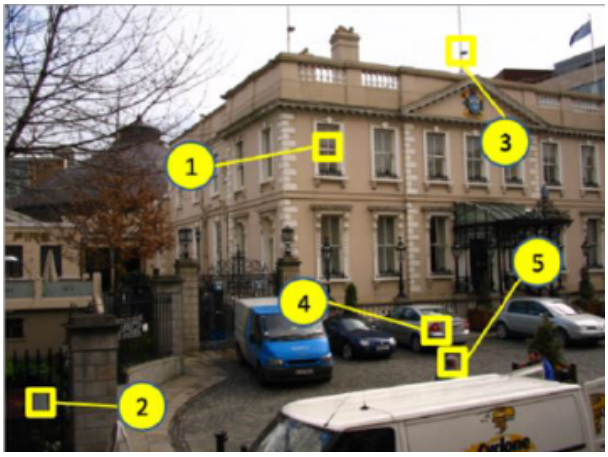

Figura 1.1: PassPoint.

de imágenes. Por otro lado, en el estudio [19] 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 [1], 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 1.1, se muestra 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. Para resoluciones más actuales como 1366x768 (HD) o 1920x1080 (FHD) que son los estándares actuales, el espacio de claves es mucho mayor al de las alfanuméricas, es decir, el espacio de claves mejora con la tecnología y no afecta la memorabilidad, cosa que no sucede con las alfanuméricas.

	Tamaño de imagen	Tamaño de la cuadrícula (píxeles)	Tamaño del alfabeto/ No.Cuadrículas	Largo/No. puntos de clic	Tamaño de espacio de contraseñas
Alfanumérica	N/A	N/A	64	8	$2.8\text{x}10^{14}$
Alfanumérica	N/A	N/A	72	8	$7.2\text{x}10^{14}$
Alfanumérica	N/A	N/A	96	8	$7.2\text{x}10^{15}$
Gráficas	451x331	20x20	373	5	$7.2\text{x}10^{12}$
Gráficas	1024x752	20x20	1925	5	$2.6\text{x}10^{16}$
Gráficas	1024x752	14x14	3928	5	$9.3\text{x}10^{17}$
Gráficas(1/2 uso de la pantalla)	1024x752	14x14	1964	5	$2.9\text{x}10^{16}$

Tabla 1.1: Alfanuméricas vs Gráficas. Tomada de [1]

1.2. Patrones DIAG y LINE

El problema de que los usuarios seleccionen imágenes que posean una cantidad reducida de Hotspots puede ser solucionado con un procesamiento previo de la misma como se explica en la sección anterior o brindando imágenes seguras por sistema, pero existen debilidades que ocurren independientemente de la imagen empleada. Estas debilidades están relacionadas con el uso de patrones específicos, principios psicológicos o modelos de atención visual. Estos aspectos son habitualmente empleados por los usuarios con el fin de hacer que sus contraseñas sean más fáciles de recordar. Sin embargo, esta estrategia, aunque mejora la memorabilidad, también facilita la creación de diccionarios de ataque para descifrar las contraseñas. Los patrones, en unión con los Hotspots y las reglas perceptuales que los usuarios suelen seguir al elegir sus contraseñas, como la organización visual o la repetición de ciertas formas, hacen que estas sean vulnerables a distintos tipos ataques.

En los estudios reportados en [5, 20, 21, 22, 23, 24, 25], se identificaron varios patrones comunes utilizados por los usuarios en la creación de contraseñas gráficas. Algunos de estos patrones incluyen formas predefinidas como Z, W, V, y C, patrones agrupados, regulares, y patrones LOD (la distancia entre 2 puntos consecutivos es constante), además de los patrones DIAG y LINE, los cuales están relacionados con trayectorias diagonales o en línea. Entre estos, los patrones DIAG y LINE son los más frecuentemente utilizados por los usuarios.

Los patrones DIAG se describen como configuraciones donde los puntos se organizan formando arcos en direcciones horizontales y verticales. Una característica distintiva de estos patrones es que la suma de los valores absolutos de los ángulos entre los puntos es menor a 15 °. Por otro lado, los patrones LINE se caracterizan por ser líneas rectas, ya sean horizontales o verticales. Estos se consideran un subconjunto de los patrones DIAG, ya que ambas configuraciones comparten una estructura similar basada en la alineación de los puntos, pero los patrones LINE son más simples al ser exclusivamente rectos.

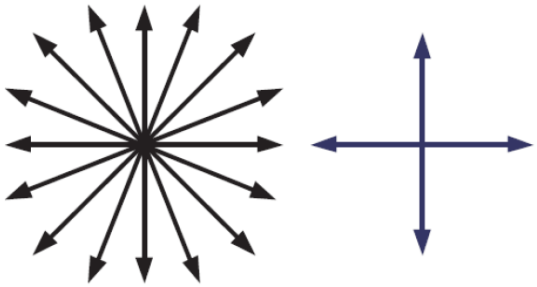

Figura 1.2: DIAG-LINE.

En un estudio realizado por los autores de [21, 22], se investigaron 223 contraseñas gráficas en el sistema PassPoint. Estas contraseñas fueron seleccionadas por estudiantes que interactuaron con dos imágenes diferentes. Cada imagen contenía una cantidad manejable de Hotspots, distribuidos de manera uniforme entre ellas. Durante el experimento, los investigadores intentaron descifrar las contraseñas utilizando ataques de diccionario. Utilizando un diccionario de 235.26 entradas y patrones de tipo DIAG, los atacantes lograron obtener entre el 48.2 % y el 54.1 % de las contraseñas. Además, empleando un diccionario diferente de 229.02 entradas y patrones de tipo LINE, los resultados fueron algo menos efectivos, logrando recuperar entre un 23.7 % y un 52.3 % de las contraseñas.

Estos resultados destacan la efectividad variable de los ataques de diccionario cuando se aplican a contraseñas gráficas en escenarios con patrones específicos.

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 solo si la circunferencia circunscrita de cualquier triángulo en la red no contiene un punto p_i en su interior. Como ejemplos de esta están las figuras 1.4, 1.3 y1.5 . Esta definición es conocida como condición de Delaunay [26, 27, 28].

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 triángulos de Delaunay esta maximizado, es decir, se evita obtener resultados con ángulos demasiados agudos. Como consecuencia de lo anterior, los triángulos generados en una triangulación tienden a ser lo más equilátero posible. Esto es debido a que todo triángulo no equilátero siempre tiene algún ángulo menor que 60°.
3. La triangulación es única cuando ningún borde de la circunferencia circunscrita contiene más de tres vértices de la red.

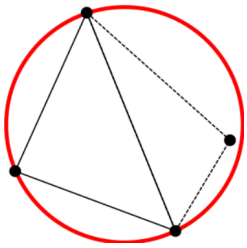

Figura 1.3: Triangulación no cumple condición de Delaunay

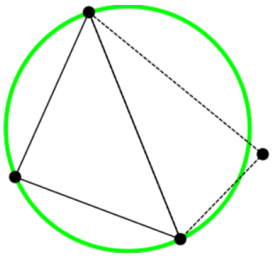

Figura 1.4: Triangulación sí cumple condición de Delaunay

Un aspecto clave al trabajar con triangulaciones de Delaunay es determinar si una triangulación es válida. Para lograr esto, se recurre a la fórmula de Euler, que es una herramienta fundamental en geometría computacional. Considerando un conjunto de puntos P de n elementos, si hay una cantidad h de puntos que pertenecen a la envoltura convexa de dicho conjunto, la fórmula permite calcular ciertas propiedades de la triangulación. Según esta, la triangulación de Delaunay resultante tendrá un total de $2n$-2-h triángulos y $3n$-3-h aristas [29]. Notemos que para 5 puntos de una contraseña, como máximo podemos obtener 5 triángulos de Delaunay pues n=5 y h puede variar entre 3, 4 o 5.

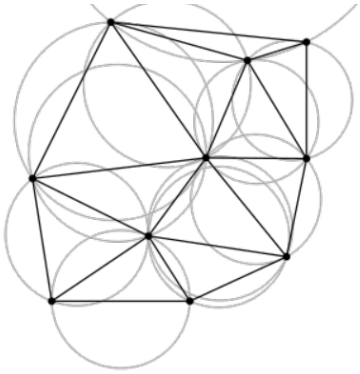

Figura 1.5: Triangulación de Delaunay para 10 puntos

1.4. Antecedentes en la detección de patrones DIAG y LINE o patrones suaves

En el contexto de la seguridad informática, la detección de patrones en contraseñas gráficas ha emergido como un aspecto crucial para garantizar la robustez de los sistemas de autenticación, especialmente en entornos como PassPoint. La identificación y evaluación de patrones específicos, como los patrones DIAG y LINE, se ha vuelto fundamental para mitigar vulnerabilidades y fortalecer la seguridad en estos sistemas.

Los estudios previos han destacado la efectividad de diversos métodos en la detección de contraseñas débiles que siguen patrones suaves. En particular, dos enfoques sobresalen en esta área: el algoritmo diseñado para detectar contraseñas con patrones suaves en PassPoint [3] y el *test* basado en el promedio de los ángulos máximos de los triángulos de Delaunay [13] para la identificación de patrones DIAG y LINE en contraseñas gráficas.

En esta sección, se analizarán en detalle estos dos enfoques, centrándose en su eficacia, metodología y resultados. El objetivo es comprender cómo estos métodos contribuyen a la detección y evaluación de contraseñas débiles que siguen patrones predefinidos, así como su relevancia en la mejora de la seguridad en sistemas de autenticación gráfica como PassPoint.

1.4.1. Algoritmo para la detección de contraseñas con patrones suaves en PassPoint

En [3] se presentó un algoritmo diseñado para identificar contraseñas con patrones suaves en el método PassPoint. Este algoritmo toma como datos de entrada los puntos seleccionados por el usuario al crear su contraseña, junto con un parámetro de tolerancia, representado como $D(\varphi^\circ)$. A partir de los 5 puntos que componen la contraseña, se calculan los tres ángulos formados entre los segmentos consecutivos que conectan dichos puntos. El algoritmo determina que una contraseña presenta un patrón suave cuando los tres ángulos calculados superan el valor del parámetro $D(\varphi^\circ)$.

La cuestión de este algoritmo es la selección del valor $D(\varphi^\circ)$ pues este va a ser el mayor determinante de la decisión del mismo. Para la solución de este problema se contó con una implementación básica del PassPoint para la web con dos imágenes de 700x400. Un grupo de 60 alumnos de la Universidad de Ciencias Informáticas crearon 397 contraseñas, las cuales se clasificaron visualmente y se decidió que 124 de ellas cumplían con el patrón

de suavidad.

En un primer experimento se aplicó el algoritmo propuesto a las 124 contraseñas variando con paso 10 el parámetro $D(\varphi^\circ)$ y de esta manera conocer los falsos negativos obtenidos por el algoritmo para cada valor de $D(\varphi^\circ) \in \{20,30,40,50....,150\}$. Se observó que al aumentar $D(\varphi^\circ)$ reducen los falsos negativos y que para valores de $D(\varphi^\circ)$ mayores a 80° ocurre poca variación en la cantidad de contraseñas detectadas, incluso para $D(\varphi^\circ) = 150^\circ$ aún quedan 3 contraseñas no detectadas, quizás esto pueda ser un error debido a la clasificación del observador.

En un segundo experimento se aplica el algoritmo para las 397 contraseñas registradas inicialmente por los 60 usuarios y los mismos valores de $D(\varphi^\circ)$ que en el experimento anterior, para identificar cuántas nuevas contraseñas detectaba el algoritmo que no estaban en la clasificación inicial. Se pudo apreciar que el número crece a partir de que $D(\varphi^\circ)$ es mayor que 50°. Dada la contradicción entre las contraseñas detectadas por el algoritmo y las clasificadas por el observador, se realizó un análisis de las contraseñas no clasificadas por este pero sí por el algoritmo y se pudo demostrar que sí cumplían con el patrón de suavidad. Esto sugiere que el observador puede haber cometido errores de clasificación, ya que el usuario que eligió la contraseña intentaba establecer conexiones entre los puntos, aunque la suavidad de estas relaciones no sea evidente para quien observa.

Como tercer experimento se aplicó el algoritmo sobre un conjunto de 400 contraseñas aleatorias para detectar los falsos positivos para cada valor de $D(\varphi^\circ)$. Según los resultados, se sugiere usar por defecto $D(\varphi^\circ)$=130°, ya que representa un buen equilibrio entre falsos positivos y falsos negativos. La figura 1.6 extraída de [3] proporciona la información necesaria para ajustar este parámetro según las necesidades del usuario. Incrementar $D(\varphi^\circ)$ mejora la seguridad, mientras que reducirlo favorece la usabilidad del sistema.

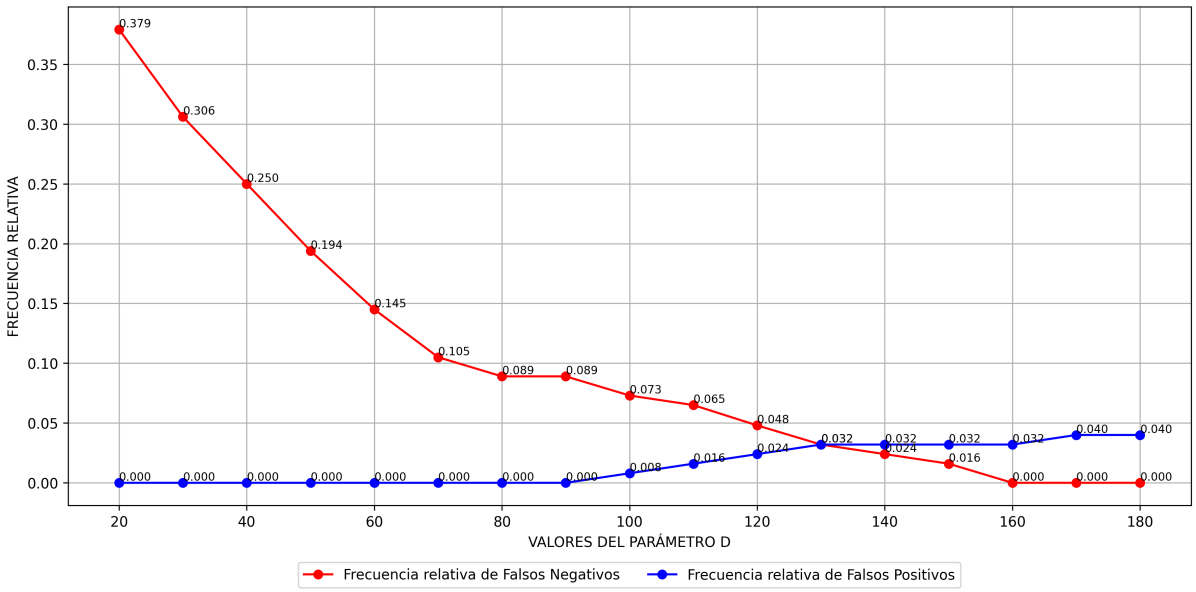

Figura 1.6: Frecuencia de falsos positivos vs falsos negativos según $D(\varphi^\circ)$. Tomada de [3].

A partir de los resultados de cada experimento se pudo afirmar que se obtuvo un criterio efectivo para detectar la existencia de patrones de suavidad en las contraseñas de la técnica de autenticación gráfica PassPoint en imágenes de 700x400 píxeles. En [3] se puede observar el algoritmo propuesto así como una implementación del mismo en

Python. Además el algoritmo permitió constatar que en muchas ocasiones el usuario crea una dependencia entre los puntos que no se nota a simple vista por un observador, sin embargo puede ser detectada por el algoritmo con parámetro de tolerancia variable.

1.4.2. *Test* de detección de patrones DIAG y LINE en el sistema PassPoint basado en los ángulos máximos de los triángulos de Delaunay

En [13] se propuso un innovador *test* para la detección de contraseñas gráficas débiles en el sistema PassPoint, diseñado específicamente para identificar contraseñas que sigan patrones de tipo DIAG y LINE. Este *test* se aplica de manera efectiva a imágenes con una relación de aspecto 16:9, válida para una amplia gama de tamaños de imagen. Para la construcción de este *test*, se desarrolló y probó una hipótesis inicial en la que se utilizó como estadígrafo la media de los ángulos máximos de los triángulos resultantes de la triangulación de Delaunay en los cinco puntos de una contraseña gráfica en PassPoint. Este enfoque demostró ser un método eficaz para evaluar y determinar si la contraseña seleccionada sigue un patrón DIAG o LINE.

Los resultados experimentales revelaron que las contraseñas que se ajustan a estos patrones tenían una media del estadígrafo significativamente más alta que aquellas generadas de forma aleatoria. Además, se comprobó que el estadígrafo utilizado seguía una distribución normal, lo que permitió desarrollar un *test* de una cola (derecha) basado en la media de una distribución normal. Este *test* evalúa la hipótesis nula, que afirma que la contraseña no sigue un patrón DIAG o LINE, frente a la alternativa de que sí sigue uno de estos patrones.

La eficacia del *test* se evaluó utilizando seis bases de datos que contenían 10 000 contraseñas cada una. Tres de estas bases incluían contraseñas que formaban patrones DIAG y tres contenían patrones LINE, y a su vez cada una con distintos niveles de suavidad. Las bases de datos fueron segmentadas según los ángulos entre los segmentos consecutivos, una frecuencia que se determinó en [5] como mayor a la media. El *test* logró detectar el 100 % de las contraseñas gráficas que seguían los patrones DIAG y LINE, para segmentos consecutivos con una amplitud máxima entre 150° y 180° (Db1.DIAG, Db2.DIAG, Db1.LINE, Db2.LINE) en todos los niveles de significación evaluados.

Para contraseñas cuyos patrones tenían una amplitud entre 135° y 150° (Db3.DIAG, Db3.LINE), el *test* logró una detección del 100 % en los niveles de significación $\alpha = 0.2$ y $\alpha = 0.1$. Sin embargo, en los niveles de significación más bajos $\alpha \in \{0.05, 0.02, 0.01\}$, la tasa de detección disminuyó a aproximadamente 88 %, 42 % y 16 %, respectivamente. Para fines generales, los autores recomiendan utilizar un nivel de significación de $\alpha = 0.05$, ya que este valor ofrece resultados superiores al 91 % de detección para patrones DIAG y 88 % para patrones LINE, a cambio de solo un falso positivo cada 20.

Capítulo 2

Detección de patrones DIAG y LINE en PassPoint, basado en el promedio de los ángulos máximos de los triángulos de Delaunay

En [13] se demostró que el promedio de los ángulos máximos de los triángulos de Delaunay es un estadígrafo eficaz para la detección de patrones DIAG y LINE. Teniendo en cuenta que las contraseñas en PassPoint se crean con la selección de 5 puntos, los posibles números de triángulos de Delaunay pueden ser 3, 4 o 5 como se mostró en la sección 1.3. En las próximas secciones se realizarán tres *test* de detección de contraseñas que siguen patrones DIAG o LINE basados en el promedio de los ángulos máximos de los triángulos de Delaunay, pero realizando un análisis separado por cada número de triángulos en su triangulación. En cada subsección se determinará a que distribución pertenecen los promedios de los ángulos máximos de los triángulos de Delaunay para la cantidad de triángulos correspondiente, esto a través del sofware EasyFit, se realizará un test estidístico para la detección de contraseñas con patrones DIAG y LINE, y se evaluará su efectividad estimando los errores de tipo I y de tipo II

2.1. Contraseñas con 3 triángulos en su triangulación de Delaunay

En esta sección cuando se hace referencia al promedio de los ángulos máximos de los triángulos de Delaunay de las contraseñas gráficas en PassPoint, nos referiremos a las contraseñas que posean 3 triángulos en su triangulación de Delaunay.

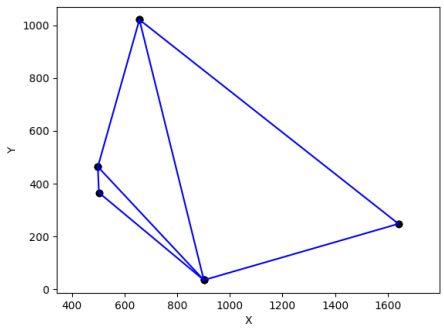

Figura 2.7: Contraseña gráfica de 5 puntos con una triangulación de Delaunay de 3 triángulos

2.1.1. Estimación de la distribución del promedio de los ángulos máximos de los triángulos de Delaunay

Experimento #1.

Para estimar la distribución del promedio de los ángulos máximos de los triángulos de Delaunay para contraseñas gráficas en Passpoint, se generaron aleatoriamente 1000 contraseñas gráficas de 5 puntos en una imagen de 1920x1080. Para cada una de estas contraseñas se construyó su correspondiente triangulación de Delaunay y se determinó el promedio de los ángulos máximos de su triangulación de Delaunay resultante. La base de datos que contiene los 1000 promedios se le denominó DB.1.

Resultados del experimento #1.

En la tabla A.1 se muestran las 6 distribuciones que más se ajustan a los datos encontrados en DB.1, encontrandose en el primer lugar *Jhonson SB* con los parámetros $\gamma = 1{,}9152$ $\delta = 1{,}4296$ $\lambda 134{,}77$ $\xi = 68{,}377$. En la figura 2.8 se muestran los resultados de tres de los tests de bondad de ajuste aplicados a la distribución *Jhonson SB* sobre datos contenidos en DB.1 y en la figura 2.9 se muestra la función de densidad de probabilidad de la misma.

Kolmogorov-Smirnov					
Tamaño de la muestra Estadística Valor P Rango	1000 0.01725 0.92216 1				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	0.03393	0.03867	0.04294	0.048	0.05151
Rechazar?	No	No	No	No	No
Anderson-Darling					
Tamaño de la muestra Estadística Rango	1000 0.26338 1				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	1.3749	1.9286	2.5018	3.2892	3.9074
Rechazar?	No	No	No	No	No
Chi-cuadrado					
Grados de libertad Estadística Valor P Rango	9 5.3831 0.79971 1				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	12.242	14.684	16.919	19.679	21.666
Rechazar?	No	No	No	No	No

Figura 2.8: Tests de bondad de ajuste aplicados a la distribución Jhonson SB sobre DB1.1

A partir de este resultado, en el resto de la sección se asume que la muestra BD.1 y ,por tanto, el promedio de los ángulos máximos de los triángulos de Delaunay para triangulaciones proceden de una distribución *Jhonson SB*, por lo que se puede asumir que las contraseñas que incumplan esta propiedad no son aleatorias. La aplicación práctica de este criterio se facilita porque después de aplicar la transformación de *Jhonson SB* mediante la fórmula**(101 liset)** :

$$P_D^N = J_{SB}(P_D) = \gamma + \delta \times ln\left(\frac{P_D - \xi}{\lambda + \xi - P_D}\right)$$

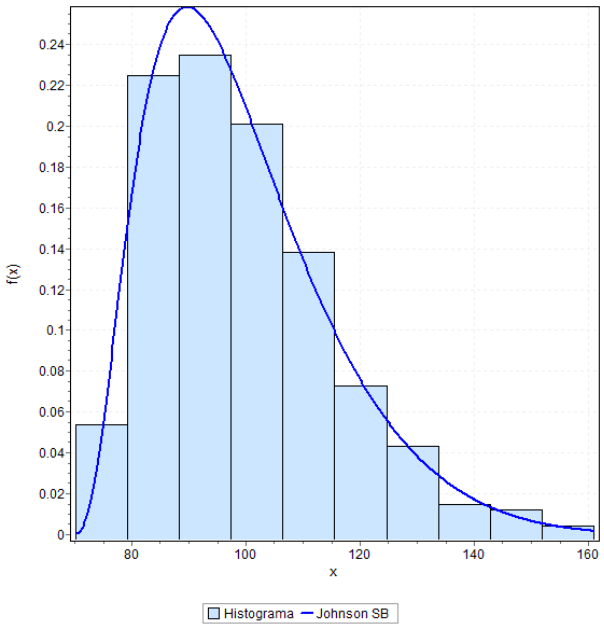

Figura 2.9: Función de densidad de probabilidad de la distribución Jhonson SB para DB1.

, con los parámetros correspondientes, el promedio transformado debe seguir una distribución normal estándar $P_D^N \sim N(0,1)$. Basado en la propiedad anterior , la detección de la no aleatoriedad de las contraseñas se reduce a aplicar un test de media para la distribución normal del estadígrafo muestral transformado a *Jhonson SB*.

2.1.2. Test basado en el promedio de los ángulos máximos de los Triángulos de Delanunay

Dado que el promedio de los ángulos máximos de los triángulos de Delanunay distribuye *Jhonson SB*, se porpone un test estadístico para identificar contraseñas con patrones DIAG y LINE en PassPoint. La propuesta consiste en un test de una cola(Derecha) basado en el promedio de los ángulos máximos de los triángulos de Delaunay transformados a una distribución normal estándar mediante la transformacion *Jhonson SB*. Dado que esta prueba se basa en la anchura de los ángulos y no en la longitud en sí de los lados u otra característica que varie con el tamaño de la imagen será válida para todos los tamaños de imágenes con una relación de 16:9. Dado que las imágenes con esta relación tendrán dimensiones proporcionales iguales y sus triángulos correspondientes serán proporcionales, la prueba propuesta puede formalizarse como sigue:

1. Varaiable aleatoria X: promedio de los ángulos máximos de los triángulos de Delaunay de contraseñas de 5 puntos con 3 triángulos en su triangulación

2. Estadígrafo :
$$Z = J_{SB}(X) = \gamma + \delta \times ln\left(\frac{X-\xi}{\lambda+\xi-X}\right)$$

3. Hipótesis nula :
$$H_0 : E(Z) = 0$$

- La contraseña gráfica seleccionada por el usuario es aleatoria si el promedio de los ángulos máximos de los triángulos de Delaunay transformados mediante la fórmula de *Jhonson SB* a una normal estándar es igual a 0.

4. Hipótesis alternativa :

$$H_a : E(Z) > 0$$

   - La contraseña gráfica seleccionada por el usuario posee patrones DIAG o LINE si el promedio de los ángulos máximos de los triángulos de Delaunay transformado mediante la fórmula de *Jhonson SB* a una normal estándar es mayor a 0.

5. Región de Rechazo: $\{z : Z > z_\alpha\}$,donde α es el nivel de significación establecido por el usuario.

6. Criterio de decisión

   - Para los cinco niveles de significación establecidos, se decide que la contraseña gráfica seleccionada por el usuario no sigue un patrón aleatorio si al transformar el promedio de los ángulos máximos de los triángulos de Delaunay mediante la transformación *Jhonson SB*, el valor obtenido pertenece a la región crítica

2.1.3. Implementacion del Test propuesto :

Para la implementación del test propuesto, se toman las coordenadas (x_i, y_i) de cada uno de los p_i puntos, $i = 1, \ldots, 5$ como valores de entrada. A partir de estos puntos, se construye la triangulación Delaunay utilizando la función *Delaunay* de scipy.spatial.

Luego, la longitud de los lados de cada triángulo se determina por la distancia euclidiana de dos a dos de los puntos que lo forman, de la siguiente manera:

$$a = \sqrt{(x_{pr_1} - x_{pr_2})^2 + (y_{pr_1} - y_{pr_2})^2} = ||pr_{p_i} - pr_{p_j}||.$$

Para encontrar los ángulos de cada triángulo, se aplica la Ley de los Cosenos:

$$\theta = \arccos\left(\frac{c^2 + a^2 - b^2}{2ab}\right), \quad \phi = \arccos\left(\frac{a^2 + b^2 - c^2}{2ab}\right), \quad \psi = \arccos\left(\frac{b^2 + c^2 - a^2}{2bc}\right).$$

Es necesario encontrar el máximo de estos tres ángulos θ, ϕ, y ψ. Es análogo para los triángulos restantes de la triangulación Delaunay. Una vez que se hayan obtenido los ángulos máximos de la triangulación Delaunay, se calcula su promedio, con el cual se obtiene el valor de la estadígrafo X. La hipótesis nula se rechaza dependiendo de si la estadística X pertenece a la región de rechazo para el α establecido. Una posible implementación de esta prueba en python sería:

points: 5 puntos de la contraseña gamma,delta,lambd,xi: parámetros correspondientes a la distribución Jhonson SB obtenida rg:límite inferior de la región de rechazo según el nivel de significación escogido El test devuelve 0 cuando se rechaza la hipótesis nula, en otro caso devuelve 1

```
1         def test(points,gamma,delta,lambd,xi,rg):
2                 triangulation=Delaunay(points)
3                 angles=[]
4                 for i in triangulation:
5                         a=distancia_puntos(points[i[0]],
                             points[i[1]])
6                         b=distancia_puntos(points[i[1]],
                             points[i[2]])
7                         b=distancia_puntos(points[i[2]],
                             points[i[0]])
8                         angles.append(angle_max(a,b,c))
9                 X=mean(angles)
10                Z=gamma + delta * np.log((x - xi) / (lambd -
                     x + xi))
11                if Z>rg:
12                return 0
13                else:
14                return 1
15
16        def distancia_puntos(punto1, punto2):
17                return math.sqrt((punto1[0] - punto2[0])**2 +
18                (punto1[1] - punto2[1])**2)
19
20        def angle_max(distancia_ab, distancia_bc,
             distancia_ca):
21                angulo_A = math.degrees(math.acos(
22                (distancia_bc**2 + distancia_ca**2 -
                     distancia_ab**2)
23                / (2 * distancia_bc * distancia_ca)
24                ))
25                angulo_B = math.degrees(math.acos(
26                (distancia_ca**2 + distancia_ab**2 -
                     distancia_bc**2)
27                / (2 * distancia_ca * distancia_ab)
28                ))
29                angulo_C = 180 - angulo_A - angulo_B
30                return max(angulo_A, angulo_B, angulo_C)
```

En cuanto a la complejidad, las funciones *distancia_puntos* y *angle_max* solo poseen operaciones elementales por lo que su complejidad es *O(1)*. La función test en su primera línea hace un llamado a la función *Delaunay* (línea 2) de *scipy.spatial*, esta posee una complejidad de *O(N logN)* debido a que el algoritmo subyacente utilizado por *Scipy* es el algoritmo de *Qhull*. Seguido en el algoritmo se itera por la triangulación obtenida (líneas 4-8), la cual poseen como máximo n triángulos , dentro de cada iteración se hacen llamados a las funciones *distancia_puntos* y *angle_max* que son *O(1)*, por tanto el costo del iterador es *O(N)*. Las operaciones restantes son *O(1)* (líneas 9-14) ,por tanto el costo total sería *O(1)+O(N)+O(N logN)=O(N logN)* por ley de la suma. e

2.1.4. Estimación de la probabilidad de los errores de tipo I y de tipo II cometidos por el test

Experimento #2 : Estimación del error tipo I

Para estimar la probabilidad de que la prueba decida que la contraseña gráfica contiene un patrón DIAG o LINE cuando ,en verdad, sigue un patrón aleatorio (error de tipo I o falsos positivos), se generó una base de datos DB1.RANDOM con 10 000 contraseñas gráficas aleatorias sobre la imagen. El test descrito en la sección 2.1.3, se le aplicó a cada una de estas contraseñas gráficas para los valores de $z_\alpha \in \{0{,}842, 1{,}282, 1{,}645, 2{,}054, 2{,}326\}$ correspondientes a los niveles de significación $\alpha \in \{0{,}2, 0{,}10{,}05, 0{,}02, 0{,}01\}$.

α	$\alpha = 0{,}2$	$\alpha = 0{,}1$	$\alpha = 0{,}05$	$\alpha = 0{,}02$	$\alpha = 0{,}01$
$\hat{\alpha}$	0.2221	0.1178	0.0605	0.0251	0.0132

Tabla 2.2: Estimación de la probabilidad ($\hat{\alpha}$) del error de tipo I derivado de la prueba.

Resultados del experimento #2.

Las probabilidades estimadas de cometer un error de tipo I ($\hat{\alpha}$) mediante el test son ligeramente superiores a las probabilidades teóricas preestablecidas (α),véase en la figura 2.10 y en la tabla 2.2.

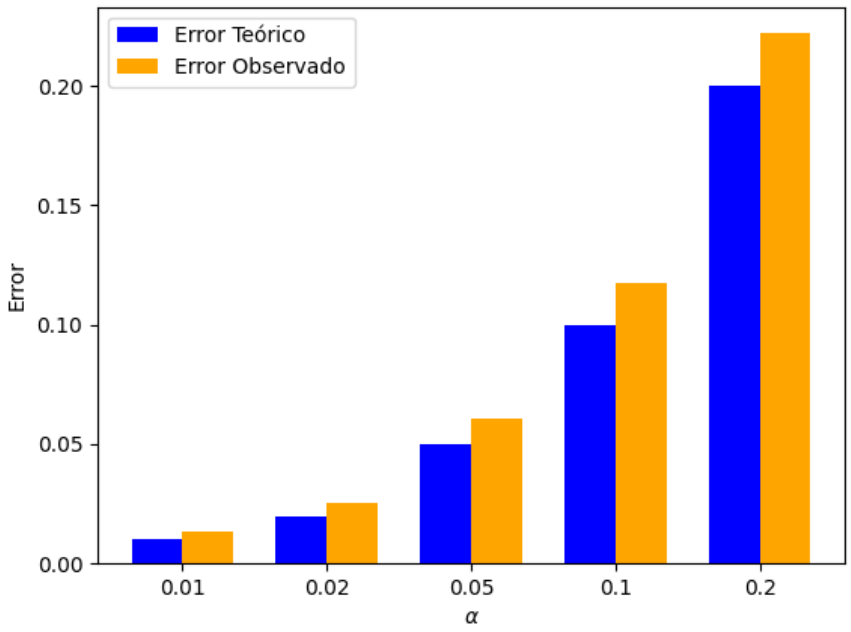

Figura 2.10: Comparación entre las probabilidades teóricas (α) y estimadas ($\hat{\alpha}$) de cometer un error de tipo I

Experimento #3: Estimación del error tipo II

Para estimar la probabilidad de que el test detecte una contraseña gráfica como aleatoria cuando sigue un patrón DIAG o LINE (error tipo II o falsos negativos), se crearon 3 bases de datos que en conjunto contienen el promedio de los ángulos máximos de los

triángulos de Delaunay de 30 000 contraseñas gráficas de 5 puntos que siguen patrones DIAG y LINE ,:

- DB.DIAG_LINE.1.1: 10 000 contraseñas gráficas que siguen patrones DIAG o LINE con una anchura máxima entre dos segmentos consecutivos de 15°
- DB.DIAG_LINE.1.2: 10 000 contraseñas gráficas que siguen patrones DIAG o LINE con una anchura máxima entre dos segmentos consecutivos que varia entre 15°y 30°
- DB.DIAG_LINE.1.3: 10 000 contraseñas gráficas que siguen patrones DIAG o LINE con una anchura máxima entre dos segmentos consecutivos que varia entre 30°y 45°

Resultados del experimento #3

Los resultados obtenidos por el test para cada una de las bases de datos y los niveles de significación preestablecidos se muestran en la tabla 2.3

α	BD.DIAG_LINE.1.1	BD.DIAG_LINE.1.2	BD.DIAG_LINE.1.3
0.2	0	0	0.0571
0.1	0	0	0.2721
0.05	0	0.0029	0.5222
0.02	0	0.0939	0.8508
0.01	0	0.2527	0.9871

Tabla 2.3: Estimación de la probabilidad ($\hat{\alpha}$) del error de tipo I derivado de la prueba.

El test propuesto durante este experimento mostró una alta capacidad para detectar las contraseñas encontradas en DB.DIAG_LINE.1.1 y en DB.DIAG_LINE.1.2, lo que para esta ultima con los niveles de significación de $\alpha \in \{0{,}2, 0{,}1, 0{,}05\}$. Para las contraseñas de DB.DIAG_LINE.1.3 no se obtuvieron buenos resultados, llegando a detectar para el nivel de significación $\alpha = 0{,}01$ solo un 1 %.

2.2. Contraseñas con 4 triángulos en su triangulación de Delaunay

En esta sección cuando se hace referencia a el promedio de los ángulos máximos de los triángulos de Delaunay de las contraseñas gráficas en PassPoint, nos referiremos a las contraseñas que posean 4 triángulos en su triángulacion de Delaunay.

2.2.1. Estimación de la distribución del promedio de los ángulos máximos de los triángulos de Delaunay

Experimento #1.

Para estimar la distribución del promedio de los ángulos máximos de los triángulos de Delaunay para contraseñas gráficas en Passpoint, se generaron aleatoriamente 1000 contraseñas gráficas de 5 puntos en una imagen de 1920x1080. Para cada una de estas contraseñas se contruyó su correspondiente triangulación de Delaunay y se determinó el promedio de los ángulos máximos de su triangulación de Delaunay resultante. La base de datos que contiene los 1000 promedios se le denominó DB.2.RANDOM .

Resultados del experimento 1

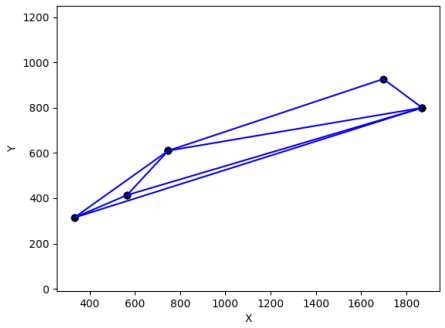

Figura 2.11: Contraseña gráfica de 5 puntos con una triangulación de Delaunay de 4 triángulos

En la tabla A.2 se muestran las 6 distribuciones que más se ajustan a los datos encontrados en DB1.1, encontrandose en el primer lugar Log-Logistic (3P) con los parámetros $\alpha = 6{,}4824$, $\beta = 46{,}461$ $\gamma = 68{,}566$. En la figura 2.12 se muestran los datos de tres de los tests de bondad de ajuste aplicados a la distribución obtenida sobre los datos contenidos en DB.2.RANDOM y en la figura 2.13 se muestra la función de densidad de probabilidad de la misma.

Kolmogorov-Smirnov					
Tamaño de la muestra Estadística Valor P Rango	1000 0.01309 0.9947 1				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	0.03393	0.03867	0.04294	0.048	0.05151
Rechazar?	No	No	No	No	No
Anderson-Darling					
Tamaño de la muestra Estadística Rango	1000 0.21014 1				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	1.3749	1.9286	2.5018	3.2892	3.9074
Rechazar?	No	No	No	No	No
Chi-cuadrado					
Grados de libertad Estadística Valor P Rango	9 0.82785 0.99974 1				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	12.242	14.684	16.919	19.679	21.666
Rechazar?	No	No	No	No	No

Figura 2.12: Tests de bondad de ajuste para la distribución Log-Logistic (3P) sobre DB.2.RAMDON

Como se observa en la figura 2.12, para los tres métodos de bondad de ajuste (Kolmogorov-Smirnov, Anderson-Darling y Chi-cuadrado), no se rechaza la hipótesis nula de que los datos provienen de la distribución teórica Log-logistic (3P), en ningún nivel de significación evaluado, indicando un buen ajuste hacia la misma.

A partir de este resultado , en el resto de la sección se asume que la muestra DB.2.RAMDON y ,por tanto, el promedio de los ángulos máximos de los triángulos de Delaunay prodecen

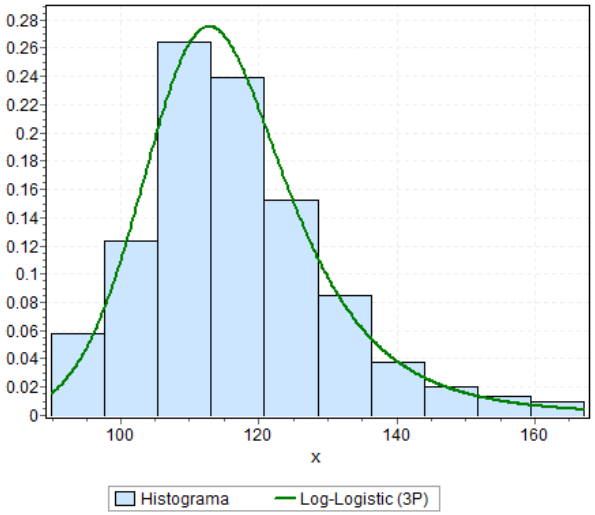

Figura 2.13: Función de densidad de probabilidad de la distribución Log-Logistic (3P) para DB.2.RAMDON

de una distribución Log-logistic (3P), por lo que se puede asumir que que las contraseñas que incumplan esta propiedad no son aleatorias.

2.2.2. Test basado en el promedio de los ángulos máximos de los triángulos de Delanunay

Dado que el el promedio de los ángulos máximos de los triágulos de Delanunay distribuye Log-LogistIC, se propone un test estadístico para seleccionar contraseñas con patrones DIAG y LINE. La propuesta consiste en un test de una cola(Derecha) basado en el promedio de los ángulos máximos de los triángulos de Delanunay . Al igual que el test anterior, este se basa en la anchura de los ángulos y no en la longitud en sí de los lados u otra característica que varie con el tamaño de la imagen, por lo que será válida para todos los tamaños de imágenes con una relación de 16:9. Dado que las imágenes con esta relación tendrán dimensiones proporcionales iguales y sus triángulos correspondientes serán proporcionales: la prueba propuesta puede formalizarse como sigue:

1. Variable aleatoria X: promedio de los ángulos máximos de los triángulos de Delaunay en un conjunto de 5 puntos, con 4 triángulos en su triangulación.

2. Estadígrafo : X

3. Hipótesis nula :
$$H_0 : E(X) = 0$$

4. Hipótesis alternativa :
$$H_a : E(X) > 0$$

5. Región de Rechazo: $\{z : Z > z_\alpha\}$,donde α es el nivel de significación establecido por el usuario, y el valor de z_α estará dado por la evaluación de los respectivos niveles de confianza en la inversa de la función de distribución acumulada de Log-Logistic (3P) con los parámetros obtenidos:

$$FDA(x;\alpha,\beta,\gamma) = \frac{1}{1+\left(\frac{\beta}{x-\gamma}\right)^{\alpha}}, \quad x > \gamma$$

- Para hallar la inversa de la función de distribución acumulada se debe despejar x: Para despejar x, seguimos los pasos:

  Paso 1: Igualar $F(x;\alpha,\beta,\gamma)$ a y

  $$y = \frac{1}{1+\left(\frac{\beta}{x-\gamma}\right)^{\alpha}}$$

  Paso 2: Invertir la fracción

  $$\frac{1}{y} = 1 + \left(\frac{\beta}{x-\gamma}\right)^{\alpha}$$

  Paso 3: Restar 1 de ambos lados

  $$\frac{1}{y} - 1 = \left(\frac{\beta}{x-\gamma}\right)^{\alpha}$$

  Paso 4: Escribir con denominador común

  $$\frac{1}{y} - 1 = \frac{1-y}{y}$$

  Por lo tanto:

  $$\frac{1-y}{y} = \left(\frac{\beta}{x-\gamma}\right)^{\alpha}$$

  Paso 5: Elevar ambos lados a la $\frac{1}{\alpha}$ potencia

  $$\left(\frac{1-y}{y}\right)^{\frac{1}{\alpha}} = \frac{\beta}{x-\gamma}$$

  Paso 6: Invertir la fracción de la derecha

  $$x - \gamma = \frac{\beta}{\left(\frac{1-y}{y}\right)^{\frac{1}{\alpha}}}$$

  Paso 7: Pasar $\left(\frac{1-y}{y}\right)^{\frac{1}{\alpha}}$ multiplicando a β

  $$x - \gamma = \beta \cdot \left(\frac{1-y}{y}\right)^{-\frac{1}{\alpha}}$$

  Paso 8: Simplificar x

  $$x = \gamma + \beta \cdot \left(\frac{1-y}{y}\right)^{-\frac{1}{\alpha}}$$

$$x = \gamma + \beta \cdot \left(\frac{1}{\frac{1}{y} - 1} \right)^{\frac{1}{\alpha}}$$

Finalmente, sustituyendo $y = F(x; \alpha, \beta, \gamma)$, la solución general es:

$$x = \gamma + \beta \cdot \left(\frac{1}{\frac{1}{F(x;\alpha,\beta,\gamma)} - 1} \right)^{\frac{1}{\alpha}}$$

6. Criterio de decisión

   - Para los cinco niveles de significación establecidos, se decide que la contraseña gráfica seleccionada por el usuario no sigue un patrón aleatorio si su promedio de los ángulos máximos de los triángulos de Delaunay pertenece a la región crítica.

2.2.3. Implementación del Test propuesto :

Para la implementación del test propuesto, se toman las coordenadas (x_i, y_i) de cada uno de los p_i puntos, $i = 1, \ldots, 5$ como valores de entrada. A partir de estos puntos, se construye la triangulación Delaunay utilizando la funcion *Delaunay* de scipy.spatial

Luego, la longitud de los lados de cada triángulo se determina por la distancia euclidiana de dos a dos de los puntos que lo forman, de la siguiente manera:

$$a = \sqrt{(x_{pr_1} - x_{pr_2})^2 + (y_{pr_1} - y_{pr_2})^2} = ||pr_{p_i} - pr_{p_j}||.$$

Para encontrar los ángulos de cada triángulo, se aplica la Ley de los Cosenos:

$$\theta = \arccos\left(\frac{c^2 + a^2 - b^2}{2ab}\right), \quad \phi = \arccos\left(\frac{a^2 + b^2 - c^2}{2ab}\right), \quad \psi = \arccos\left(\frac{b^2 + c^2 - a^2}{2bc}\right).$$

Es necesario encontrar el máximo de estos tres ángulos θ, ϕ, y ψ. Es análogo para los triángulos restantes de la triangulación Delaunay. Una vez que se hayan obtenido los ángulos máximos de la triangulación Delaunay, se calcula su promedio, con el cual se obtiene el valor de la estadígrafo X. La hipótesis nula se rechaza dependiendo de si la estadística X pertenece a la región de rechazo para el α establecido. Una posible implementación de esta prueba en python sería:

amadt: promedio de los ángulos máximos de los triángulos de Delaunay

alpha ,beta,gamma: parámetros de la distribución Log-Logistic (3P)

nivel_conf: nivel de confianza correspondiente al nivel de significación escogido rg: región crítica correspondiente al nivel de significación escogido

```
def test(points, alpha, beta, gamma,nivel_sig):
        triangulation=Delaunay(points)
        angles=[]
        for i in triangulation:
                a=distancia_puntos(points[i[0]],points[i[1]])
                b=distancia_puntos(points[i[1]],points[i[2]])
```

```
7                   b=distancia_puntos(points[i[2]],points[i[0]])
8                   angles.append(angle_max(a,b,c))
9           X=mean(angles)
10          rg= beta * ((1 / (1 / (1-nivel_sig) - 1)) ** (1 /
               alpha)) + gamma
11          if X>rg:
12                  return 1
13          else:
14                  return 0
15
16  def distancia_puntos(punto1, punto2):
17          return math.sqrt((punto1[0] - punto2[0])**2 +
18           (punto1[1] - punto2[1])**2)
19
20  def angle_max(distancia_ab, distancia_bc, distancia_ca):
21          angulo_A = math.degrees(math.acos(
22          (distancia_bc**2 + distancia_ca**2 - distancia_ab**2)
23          / (2 * distancia_bc * distancia_ca)
24          ))
25          angulo_B = math.degrees(math.acos(
26          (distancia_ca**2 + distancia_ab**2 - distancia_bc**2)
27          / (2 * distancia_ca * distancia_ab)
28          ))
29          angulo_C = 180 - angulo_A - angulo_B
30          return max(angulo_A, angulo_B, angulo_C)
```

En cuanto a la complejidad, las funciones *distancia_puntos* y *angle_max* solo poseen operaciones elementales por lo que su complejidad es *O(1)*. La función test en su primera línea hace un llamado a la función *Delaunay* (línea 2) de *scipy.spatial*, esta posee una complejidad de *O(N logN)* debido a que el algoritmo subyacente utilizado por *Scipy* es el algoritmo de *Qhull*. Seguido en el algoritmo se itera por la triangulación obtenida (líneas 4-8), la cual poseen como máximo n triángulos , dentro de cada iteración se hacen llamados a las funciones *distancia_puntos* y *angle_max* que son *O(1)*, por tanto el costo del iterador es *O(N)*. Las operaciones restantes son *O(1)* (líneas 9-14) ,por tanto el costo total sería *O(1)+O(N)+O(N logN)=O(N logN)* por ley de la suma.

2.2.4. Estimación de la probabilidad de los errores de tipo I y de tipo II cometidos por el test

Experimento #2 : Estimación del error tipo I

Para estimar la probabilidad de que la prueba decida que la contraseña gráfica contiene un patrón DIAG o LINE cuando ,en verdad, sigue un patrón aleatorio (error de tipo I o falsos positivos), se generó una base de datos llamada DB.2.RANDOM con 10 000 contraseñas gráficas aleatorias sobre la imagen. El test descrito en la sección 2.2.3, se le aplicó a cada una de estas contraseñas gráficas ,obteniendo como límites inferiores de la región crítica a $rg \in \{126{,}105, 133{,}772, 141{,}739, 153{,}254, 162{,}959\}$para los respectivos niveles de significación $\alpha \in \{0{,}2, 0{,}10{,}05, 0{,}02, 0{,}01\}$.

Resultados del experimento #2.

α	$\alpha = 0{,}2$	$\alpha = 0{,}1$	$\alpha = 0{,}05$	$\alpha = 0{,}02$	$\alpha = 0{,}01$
$\hat{\alpha}$	0.2032	0.1083	0.0552	0.0134	0.0034

Tabla 2.4: Estimación de la probabilidad ($\hat{\alpha}$) del error de tipo I derivado de la prueba.

Las probabilidades estimadas de cometer un error de tipo I ($\hat{\alpha}$) mediante el test poseen gran similitud a las probabilidades teóricas preestablecidas (α),véase en la figura 2.10

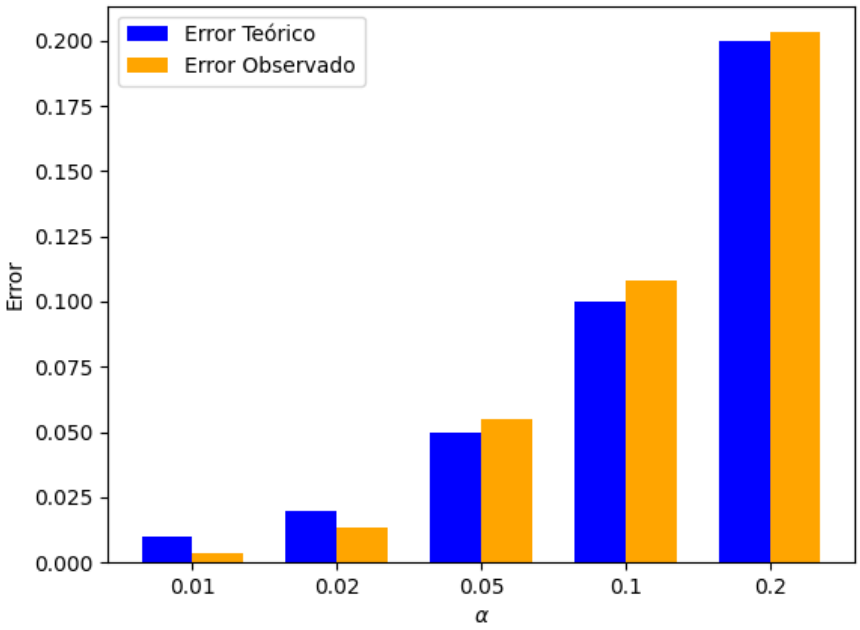

Figura 2.14: Comparación entre las probabilidades teóricas (α) y estimadas ($\hat{\alpha}$) de cometer un error de tipo I

Experimento #3: Estimación del error tipo II

Para estimar la probabilidad de que el test detecte una contraseña gráfica como aleatoria cuando sigue un patrón DIAG o LINE (error tipo II o falsos negativos), se crearon 3 bases de datos que en conjunto contienen 30 000 contraseñas gráficas de 5 puntos que siguen patrones DIAG y LINE ,:

- DB.DIAG_LINE.2.1: 10 000 contraseñas gráficas que siguen patrones DIAG o LINE con una anchura máxima entre dos segmentos consecutivos de 15°
- DB.DIAG_LINE.2.2: 10 000 contraseñas gráficas que siguen patrones DIAG o LINE con una anchura máxima entre dos segmentos consecutivos que varia entre 15°y 30°
- DB.DIAG_LINE.2.3: 10 000 contraseñas gráficas que siguen patrones DIAG o LINE con una anchura máxima entre dos segmentos consecutivos que varia entre 30°y 45°

Resultados del experimento #3

Los resultados obtenidos por el test para cada una de las bases de datos y los niveles de significación preestablecidos, se muestran en las tablas 2.5

α	BD.DIAG_LINE.2.1	BD.DIAG_LINE.2.2	BD.DIAG_LINE.2.3
0.2	0	0	0.0001
0.1	0	0	0.0174
0.05	0	0	0.2577
0.02	0	0.0642	0.9798
0.01	0	0.8688	1.0000

Tabla 2.5: Estimación de la probabilidad ($\hat{\alpha}$) del error de tipo II derivado de la prueba.

El test propuesto durante este experimento mostró una alta capacidad para detectar las contraseñas encontradas en BD.DIAG_LINE.2.1, pues detectó el 100 % de estas para todos los niveles de significación, en BD.DIAG_LINE.2.2 detectó el 100 % para los niveles de significación $\alpha \in \{0{,}2, 0{,}1, 0{,}05\}$ y 93 % para $\alpha = 0{,}02$. Para las contraseñas de BD.DIAG_LINE.2.3 no se obtuvieron buenos resultados, llegando a detectar para el nivel de significación $\alpha = 0{,}01$ solo un 1 %.

2.3. Contraseñas con 5 triángulos en su triangulación de Delaunay

En esta sección cuando se hace referencia a el promedio de los ángulos máximos de los triángulos de Delaunay de las contraseñas gráficas en PassPoint, nos referiremos a las contraseñas que posean 4 triángulos en su triángulacion de Delaunay.

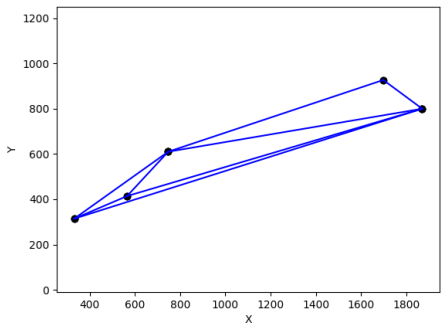

Figura 2.15: Contraseña gráfica de 5 puntos con una triangulación de Delaunay de 4 triángulos

2.3.1. Estimación de la distribución del promedio de los ángulos máximos de los triángulos de Delaunay

Experimento #1.

Para estimar la distribución del promedio de los ángulos máximos de los triángulos de Delaunay para contraseñas gráficas en Passpoint, se generaron aleatoriamente 1000 contraseñas gráficas de 5 puntos en una imagen de 1920x1080. Para cada una de estas contraseñas se contruyó su correspondiente triangulación de Delaunay y se determinó el promedio de los ángulos máximos de su triangulación de Delaunay resultante. La base de datos que contiene los 1000 promedios se le denominó DB.2.RANDOM .

Resultados del experimento 1

En la tabla A.2 se muestran las 6 distribuciones que más se ajustan a los datos encontrados en DB1.1, encontrandose en el primer lugar Log-Logistic (3P) con los parámetros $\alpha = 6{,}4824$, $\beta = 46{,}461$ $\gamma = 68{,}566$. En la figura 2.16 se muestran los datos de tres de los tests de bondad de ajuste aplicados a la distribución obtenida sobre los datos contenidos en DB.2.RANDOM y en la figura 2.17 se muestra la función de densidad de probabilidad de la misma.

Kolmogorov-Smirnov					
Tamaño de la muestra Estadística Valor P Rango	1000 0.01309 0.9947 1				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	0.03393	0.03867	0.04294	0.048	0.05151
Rechazar?	No	No	No	No	No
Anderson-Darling					
Tamaño de la muestra Estadística Rango	1000 0.21014 1				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	1.3749	1.9286	2.5018	3.2892	3.9074
Rechazar?	No	No	No	No	No
Chi-cuadrado					
Grados de libertad Estadística Valor P Rango	9 0.82785 0.99974 1				
α	0.2	0.1	0.05	0.02	0.01
Valor crítico	12.242	14.684	16.919	19.679	21.666
Rechazar?	No	No	No	No	No

Figura 2.16: Tests de bondad de ajuste para la distribución Log-Logistic (3P) sobre DB.2.RAMDON

Como se observa en la figura 2.12, para los tres métodos de bondad de ajuste (Kolmogorov-Smirnov, Anderson-Darling y Chi-cuadrado), no se rechaza la hipótesis nula de que los datos provienen de la distribución teórica Log-logistic (3P), en ningún nivel de significación evaluado, indicando un buen ajuste hacia la misma.

A partir de este resultado , en el resto de la sección se asume que la muestra DB.2.RAMDON y ,por tanto, el promedio de los ángulos máximos de los triángulos de Delaunay prodecen de una distribución Log-logistic (3P), por lo que se puede asumir que que las contraseñas que incumplan esta propiedad no son aleatorias.

2.3.2. Test basado en el promedio de los ángulos máximos de los triángulos de Delanunay

Dado que el el promedio de los ángulos máximos de los triágulos de Delanunay distribuye Log-LogistIC, se propone un test estadístico para seleccionar contraseñas con patrones DIAG y LINE. La propuesta consiste en un test de una cola(Derecha) basado en el promedio de los ángulos máximos de los triángulos de Delanunay . Al igual que el test anterior, este se basa en la anchura de los ángulos y no en la longitud en sí de los lados u otra característica que varie con el tamaño de la imagen, por lo que será válida para

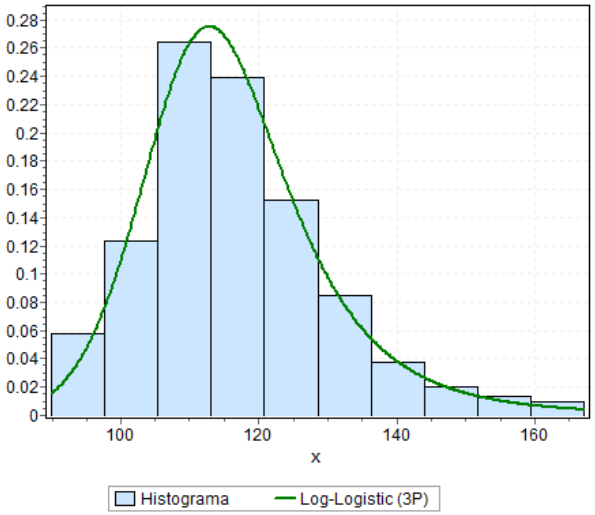

Figura 2.17: Función de densidad de probabilidad de la distribución Log-Logistic (3P) para DB.2.RAMDON

todos los tamaños de imágenes con una relación de 16:9. Dado que las imágenes con esta relación tendrán dimensiones proporcionales iguales y sus triángulos correspondientes serán proporcionales: la prueba propuesta puede formalizarse como sigue:

1. Variable aleatoria X: promedio de los ángulos máximos de los triángulos de Delaunay en un conjunto de 5 puntos, con 4 triángulos en su triangulación.

2. Estadígrafo : X

3. Hipótesis nula :
$$H_0 : E(X) = 0$$

4. Hipótesis alternativa :
$$H_a : E(X) > 0$$

5. Región de Rechazo: $\{z : Z > z_\alpha\}$,donde α es el nivel de significación establecido por el usuario, y el valor de z_α estará dado por la evaluación de los respectivos niveles de confianza en la inversa de la función de distribución acumulada de Log-Logistic (3P) con los parámetros obtenidos:

$$FDA(x;\alpha,\beta,\gamma) = \frac{1}{1+\left(\frac{\beta}{x-\gamma}\right)^{\alpha}}, \quad x > \gamma$$

   - Para hallar la inversa de la función de distribución acumulada se debe despejar x: Para despejar x, seguimos los pasos:
     Paso 1: Igualar $F(x;\alpha,\beta,\gamma)$ a y

$$y = \frac{1}{1+\left(\frac{\beta}{x-\gamma}\right)^{\alpha}}$$

     Paso 2: Invertir la fracción

$$\frac{1}{y} = 1 + \left(\frac{\beta}{x-\gamma}\right)^{\alpha}$$

Paso 3: Restar 1 de ambos lados

$$\frac{1}{y} - 1 = \left(\frac{\beta}{x-\gamma}\right)^{\alpha}$$

Paso 4: Escribir con denominador común

$$\frac{1}{y} - 1 = \frac{1-y}{y}$$

Por lo tanto:

$$\frac{1-y}{y} = \left(\frac{\beta}{x-\gamma}\right)^{\alpha}$$

Paso 5: Elevar ambos lados a la $\frac{1}{\alpha}$ potencia

$$\left(\frac{1-y}{y}\right)^{\frac{1}{\alpha}} = \frac{\beta}{x-\gamma}$$

Paso 6: Invertir la fracción de la derecha

$$x - \gamma = \frac{\beta}{\left(\frac{1-y}{y}\right)^{\frac{1}{\alpha}}}$$

Paso 7: Pasar $\left(\frac{1-y}{y}\right)^{\frac{1}{\alpha}}$ multiplicando a β

$$x - \gamma = \beta \cdot \left(\frac{1-y}{y}\right)^{-\frac{1}{\alpha}}$$

Paso 8: Simplificar x

$$x = \gamma + \beta \cdot \left(\frac{1-y}{y}\right)^{-\frac{1}{\alpha}}$$

$$x = \gamma + \beta \cdot \left(\frac{1}{\frac{1}{y} - 1}\right)^{\frac{1}{\alpha}}$$

Finalmente, sustituyendo $y = F(x; \alpha, \beta, \gamma)$, la solución general es:

$$x = \gamma + \beta \cdot \left(\frac{1}{\frac{1}{F(x;\alpha,\beta,\gamma)} - 1}\right)^{\frac{1}{\alpha}}$$

6. Criterio de decisión

- Para los cinco niveles de significación establecidos, se decide que la contraseña gráfica seleccionada por el usuario no sigue un patrón aleatorio si su promedio de los ángulos máximos de los triángulos de Delaunay pertenece a la región crítica.

2.3.3. Implementación del Test propuesto :

Para la implementación del test propuesto, se toman las coordenadas (x_i, y_i) de cada uno de los p_i puntos, $i = 1, \ldots, 5$ como valores de entrada. A partir de estos puntos, se construye la triangulación Delaunay utilizando la funcion *Delaunay* de scipy.spatial

Luego, la longitud de los lados de cada triángulo se determina por la distancia euclidiana de dos a dos de los puntos que lo forman, de la siguiente manera:

$$a = \sqrt{(x_{pr_1} - x_{pr_2})^2 + (y_{pr_1} - y_{pr_2})^2} = ||pr_{p_i} - pr_{p_j}||.$$

Para encontrar los ángulos de cada triángulo, se aplica la Ley de los Cosenos:

$$\theta = \arccos\left(\frac{c^2 + a^2 - b^2}{2ab}\right), \quad \phi = \arccos\left(\frac{a^2 + b^2 - c^2}{2ab}\right), \quad \psi = \arccos\left(\frac{b^2 + c^2 - a^2}{2bc}\right).$$

Es necesario encontrar el máximo de estos tres ángulos θ, ϕ, y ψ. Es análogo para los triángulos restantes de la triangulación Delaunay. Una vez que se hayan obtenido los ángulos máximos de la triangulación Delaunay, se calcula su promedio, con el cual se obtiene el valor de la estadígrafo X. La hipótesis nula se rechaza dependiendo de si la estadística X pertenece a la región de rechazo para el α establecido. Una posible implementación de esta prueba en python sería:

amadt: promedio de los ángulos máximos de los triángulos de Delaunay

alpha ,beta,gamma: parámetros de la distribución Log-Logistic (3P)

nivel_conf: nivel de confianza correspondiente al nivel de significación escogido rg: región crítica correspondiente al nivel de significación escogido

```
1         def test(points, alpha, beta, gamma,nivel_sig):
2         triangulation=Delaunay(points)
3         angles=[]
4         for i in triangulation:
5         a=distancia_puntos(points[i[0]],points[i[1]])
6         b=distancia_puntos(points[i[1]],points[i[2]])
7         b=distancia_puntos(points[i[2]],points[i[0]])
8         angles.append(angle_max(a,b,c))
9         X=mean(angles)
10        rg= beta * ((1 / (1 / (1-nivel_sig) - 1)) ** (1 /
             alpha)) + gamma
11        if X>rg:
12        return 1
13        else:
14        return 0
15
16        def distancia_puntos(punto1, punto2):
17        return math.sqrt((punto1[0] - punto2[0])**2 +
18        (punto1[1] - punto2[1])**2)
19
20        def angle_max(distancia_ab, distancia_bc,
             distancia_ca):
21        angulo_A = math.degrees(math.acos(
22        (distancia_bc**2 + distancia_ca**2 - distancia_ab**2)
```

```
23          / (2 * distancia_bc * distancia_ca)
24          ))
25          angulo_B = math.degrees(math.acos(
26          (distancia_ca**2 + distancia_ab**2 - distancia_bc**2)
27          / (2 * distancia_ca * distancia_ab)
28          ))
29          angulo_C = 180 - angulo_A - angulo_B
30          return max(angulo_A, angulo_B, angulo_C)
```

En cuanto a la complejidad, las funciones *distancia_puntos* y *angle_max* solo poseen operaciones elementales por lo que su complejidad es *O(1)*. La función test en su primera línea hace un llamado a la función *Delaunay* (línea 2) de *scipy.spatial*, esta posee una complejidad de *O(N logN)* debido a que el algoritmo subyacente utilizado por *Scipy* es el algoritmo de *Qhull*. Seguido en el algoritmo se itera por la triangulación obtenida (líneas 4-8), la cual poseen como máximo n triángulos , dentro de cada iteración se hacen llamados a las funciones *distancia_puntos* y *angle_max* que son *O(1)*, por tanto el costo del iterador es *O(N)*. Las operaciones restantes son *O(1)* (líneas 9-14) ,por tanto el costo total sería *O(1)+O(N)+O(N logN)=O(N logN)* por ley de la suma.

2.3.4. Estimación de la probabilidad de los errores de tipo I y de tipo II cometidos por el test

Experimento #2 : Estimación del error tipo I

Para estimar la probabilidad de que la prueba decida que la contraseña gráfica contiene un patrón DIAG o LINE cuando ,en verdad, sigue un patrón aleatorio (error de tipo I o falsos positivos), se generó una base de datos llamada DB.2.RANDOM con 10 000 contraseñas gráficas aleatorias sobre la imagen. El test descrito en la sección 2.2.3, se le aplicó a cada una de estas contraseñas gráficas ,obteniendo como límites inferiores de la región crítica a $rg \in \{126{,}105, 133{,}772, 141{,}739, 153{,}254, 162{,}959\}$para los respectivos niveles de significación $\alpha \in \{0{,}2, 0{,}10{,}05, 0{,}02, 0{,}01\}$.

α	$\alpha = 0{,}2$	$\alpha = 0{,}1$	$\alpha = 0{,}05$	$\alpha = 0{,}02$	$\alpha = 0{,}01$
$\hat{\alpha}$	0.2032	0.1083	0.0552	0.0134	0.0034

Tabla 2.6: Estimación de la probabilidad ($\hat{\alpha}$) del error de tipo I derivado de la prueba.

Resultados del experimento #2.

Las probabilidades estimadas de cometer un error de tipo I ($\hat{\alpha}$) mediante el test poseen gran similitud a las probabilidades teóricas preestablecidas (α),véase en la figura 2.18

Experimento #3: Estimación del error tipo II

Para estimar la probabilidad de que el test detecte una contraseña gráfica como aleatoria cuando sigue un patrón DIAG o LINE (error tipo II o falsos negativos), se crearon 3 bases de datos que en conjunto contienen 30 000 contraseñas gráficas de 5 puntos que siguen patrones DIAG y LINE ,:

- DB.DIAG_LINE.2.1: 10 000 contraseñas gráficas que siguen patrones DIAG o LINE con una anchura máxima entre dos segmentos consecutivos de 15°

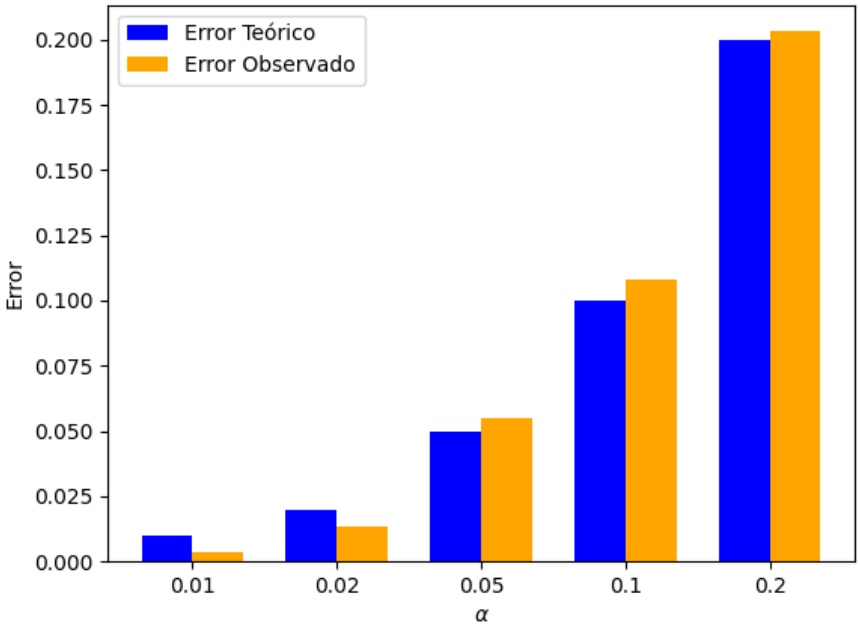

Figura 2.18: Comparación entre las probabilidades teóricas (α) y estimadas ($\hat{\alpha}$) de cometer un error de tipo I

- DB.DIAG_LINE.2.2: 10 000 contraseñas gráficas que siguen patrones DIAG o LINE con una anchura máxima entre dos segmentos consecutivos que varia entre 15°y 30°
- DB.DIAG_LINE.2.3: 10 000 contraseñas gráficas que siguen patrones DIAG o LINE con una anchura máxima entre dos segmentos consecutivos que varia entre 30°y 45°

Resultados del experimento #3

Los resultados obtenidos por el test para cada una de las bases de datos y los niveles de significación preestablecidos, se muestran en las tablas 2.7

α	BD.DIAG_LINE.2.1	BD.DIAG_LINE.2.2	BD.DIAG_LINE.2.3
0.2	0	0	0.0001
0.1	0	0	0.0174
0.05	0	0	0.2577
0.02	0	0.0642	0.9798
0.01	0	0.8688	1.0000

Tabla 2.7: Estimación de la probabilidad ($\hat{\alpha}$) del error de tipo II derivado de la prueba.

El test propuesto durante este experimento mostró una alta capacidad para detectar las contraseñas encontradas en BD.DIAG_LINE.2.1, pues detectó el 100 % de estas para todos los niveles de significación, en BD.DIAG_LINE.2.2 detectó el 100 % para los niveles de significación $\alpha \in \{0{,}2, 0{,}1, 0{,}05\}$ y 93 % para $\alpha = 0{,}02$. Para las contraseñas de BD.DIAG_LINE.2.3 no se obtuvieron buenos resultados, llegando a detectar para el nivel de significación $\alpha = 0{,}01$ solo un 1 %.

3. Resultados

3.1. asdadasd

a

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] Wiedenbeck, S.; Waters, J.; Birget, J.C.; Brodskly, A.; Memon, N.: *Passpoints: Design and longitudinal evaluation of a graphical pass- word system.* International Journal of Human-Computer Studies, Vol. 63(1-2):102-127, 2005.

[2] Sunil, S.S; Prakash, D.; Shivaji, Y.R.: *Cued click points: Graphical password authentication technique for security.* International Journal of Computer Science and Information Technologies, 5(2), 2014.

[3] Rodríguez, O.:*Algoritmo para la detección de claves débiles en la técnica de autenticación gráfica passpoints.* Tesis presentada en opción al título Máster en Ciencias Matemáticas, Universidad de la Habana, Facultad de Matemática y Computación, Instituto de Criptografía, 2019.

[4] Rodríguez, O.; Legón, C.M.; Socorro, R.: *Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica.* Revista Cubana de Ciencias Informáticas, Vol. 12, No. Especial UCIENCIA, 13-27, 2018.

[5] Sonia Chiasson; Alain Forge; Robert Biddle:*User interface design affects security:Patterns in click-based graphical passwords.*School of Computer Science and Human Oriented Technology Lab.Carleton University

[6] Herrera, J.A.; Suárez, L.; Legón, C.M.; Piñeiro, L.R.; Rojas, O.; Sosa, G. *Effectiveness of Some Tests of Spatial Randomness in the Detection ofWeak Graphical Passwords in Passpoint.* In *Computer Science and Health Engineering in Health Services*; Marmolejo-Saucedo, J.A., Vasant, P., Litvinech, I., Rodriguez-Aguilar, R., Martinez-Rios, F., Eds.; COMPSE 2020; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer: Cham, Switzerland, 2020; Volume 359.

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

[8] Suárez, L; Legón, C.M.; Herrera, J.A; Socorro, R.; Rojas, O.; Sosa, G.: *Weak PassPoint passwords detected by the perimeter of Delaunay triangles.* Enviado a publicación 16 Marzo 2021, Journal Sensors. Security and Communication Networks,Issue 1,3624587.

[9] L. Suárez. *Test para la detección de contraseñas gráficas débiles en PassPoint, basado en el promedio de los perímetros de los triángulos de Delaunay.* Master's thesis, Universidad de la Habana, 2021.

[10] Herrera, J.A.; Suárez, L.; Legón, C.M.;Sosa, G. *Comparison and combination of two effective tests in the detection of nonrandom graphical passwords in Passpoints.*Revista Cubana de Ciencias Informáticas 2023,17,1

[11] Herrera, J.A.; Suárez, L.; Legón, C.M.; Sosa, G. and O. Rojas: *New test to detect clustered graphical passwords in Passpoints, based on the perimeter of the convex hull.* Information 2024, 15, 447

[12] Chiu, S.N. *Spatial point pattern analysis by using Voronoi diagrams and Delaunay tessellations-A comparative study.* Biometr. J. 2003, 45, 367–376.

[13] L. Suárez, J. A. Herrera, C. M. Legón, G. Sosa, and O. Rojas. *Detection of DIAG and LINE Patterns in PassPoints Graphical Passwords Based on the Maximum Angles of Their Delaunay Triangles.Sensors*, 22 (5), 2022a.

[14] Birget, J.C.; Hong, D.; Memon, N.D.: *Robust discretization, with anapplication to graphical passwords.* IACR Cryptology ePrint Archive, 2003:168, 2003.

[15] Chiasson, S.; Srinivasan, J.; Biddle, R.; van Oorschot, P.C.: *Centered discretization with application to graphical passwords.* In UPSEC, Citeseer, 2008.

[16] Bicakci, K.: *Optimal discretization for high-entropy graphical passwords. In Computer and Information Sciences.* ISCIS'08, 23rd International Symposium on, pages 1-6, IEEE, 2008.

[17] Kirovski, D.; Jogic, N.; Roberts, P.: *Click Passwords.* Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA, 2007.

[18] Dirik, A.E.; Memón, N.; Birget, J.C. Modeling user choice in the PassPoints graphical password scheme. In Proceedings of the 3rd Symposium on Usable Privacy and Security 2007, Pittsburgh, PA, USA, 20–28 July 2007.

[19] Thorpe, J.; Al-Badawi, M.; MacRae, B.; Salehi-Abari, A. The presentation effect on graphical passwords. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Toronto, ON, Canada, 26 April–1 May 2014.

[20] Thorpe, J.; Van Oorschot, P.C. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. In USENIX ó7: *Proceedings of the 16th USENIX Security Symposium*; USENIX: Berkeley, CA, USA, 2007; pp. 103–118.

[21] Salehi, A.; Thorpe, J.; Van Oorschot, P.C. On Purely Automated Attacks and Click-Based Graphical Passwords. In Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC), Anaheim, CA, USA, 8–12 December 2008.

[22] Van Oorschot, P.C.; Salehi, A.; Thorpe, J. Purely automated attacks on passpoints style graphical passwords. *IEEE Trans. Inf.Forensics Secur.* 2010, 5, 393–405.

[23] Vorster, J.S.; Van Heerden, R.P.; Irwin, B. The patterns-richness of graphical passwords. In Proceedings of the 15th International Information Security South Africa Conference (ISSA 2016), Pretoria, South Africa, 17–18 August 2016.

[24] Princes, P.S.S.; Andrews, J. Analysis of various authentication schemes for passwords using images to enhance network security through online services. In Proceedings of the 2017 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 23–24 February 2017.

[25] Parish, Z.; Salehi, A.; Thorpe, J. A study on priming methods for graphical passwords. J. Inf. Secur. Appl. 2021, 62, 102913.

[26] Okabe, A.; Boots, B.; Sugihara, K.; Chiu, S.N.: *Spatial tessellations: Concepts and Applications of Voronoi Diagrams*. British Library Cataloguing in Publication Data, ISBN 0-471-98635-6, 2000.

[27] Romero, N.; Barrón, R.: Validación de la triangulación de Delaunay empleando geometría conforme. Sist, Vol.20, No.4, ISSN 1405-5546, http://doi.org/10.13053/cys-20-4-2387, 2016.

[28] Romero, J.N.: *Álgebra geométrica para la generación de regiones de Voronoi*. Tesis para obtener el grado de Doctor en Ciencias de la Computación, Instituto Politécnico Nacional, Laboratorio de Inteligencia Articial, México D.F., 2017.

[29] De Berg, M.; Cheong, O.; Van Kreveld, M.; Overmars, M. *Computational Geometry: Algorithms and Applications*, 3rd ed.; Springer: Berlin/Heidelberg, Germany, 2008; ISBN 978-3-540-77973-5.

A. Anexos

Jhonson SB
Fatigue Life (3P)
Inv. Gaussian (3P)
Gen. Gamma (4P)
Gamma(3P)
Beta

Tabla A.1: 6 disribuciones mas ajustadas teóricamente a BD1

Log-Logistc (3P)
Burr
Gen. Extreme Value
Pearson 5 (3P)
Pearson 6 (4P)
Lognormal (3P)

Tabla A.2: 6 disribuciones mas ajustadas teóricamente a BD2