Hindawi
Security and Communication Networks
Volume 2022, Article ID 3624587, 14 pages
https://doi.org/10.1155/2022/3624587

Research Article

Weak PassPoint Passwords Detected by the Perimeter of Delaunay Triangles

Lisset Suárez-Plasencia,[1] **Carlos Miguel Legón-Pérez**,[1] **Joaquín Alberto Herrera-Macías**,[1] **Raisa Socorro-Llanes**,[2] **Omar Rojas**,[3,4] **and Guillermo Sosa-Gómez**[3]

[1] *Universidad de La Habana, Facultad de Matemática y Computación, Instituto de Criptografía, Habana 10400, Cuba*
[2] *Universidad Tecnológica de La Habana, Facultad de Informática, Habana, Cuba*
[3] *Universidad Panamericana, Facultad de Ciencias Económicas y Empresariales, Álvaro Del Portillo 49, Zapopan, Jalisco 45010, Mexico*
[4] *Faculty of Economics and Business, Universitas Airlangga, Surabaya, East Java 60286, Indonesia*

Correspondence should be addressed to Guillermo Sosa-Gómez; gsosag@up.edu.mx

Received 31 January 2022; Revised 27 June 2022; Accepted 11 July 2022; Published 21 September 2022

Academic Editor: Sridhar Adepu

Copyright © 2022 Lisset Suárez-Plasencia et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

PassPoint is a graphical authentication technique that is based on the selection of five points in an image. A detected vulnerability lies in the possible existence of a pattern in the points that make up the password. The objective of this work is to detect nonrandom graphical passwords in the PassPoint scenario. A spatial randomness test based on the average of Delaunay triangles' perimeter is proposed, given the ineffectiveness of the classic tests in this scenario, which only consists of five points. A state-of-the-art of various applications of Voronoi polygons and Delaunay triangulations are presented to detect clustered and regular patterns. The distributions of the averages of the triangles' perimeters in the PassPoint scenario for various sizes of images are disclosed, which were unknown. The test's decision criterion was constructed from one of the best distributions to which the data were adjusted. Type I and type II errors were estimated, and it was concluded that the proposed test could detect clustered and regular graphical passwords in PassPoint, therefore being more effective in detecting clustering than regularity.

1. Introduction

Graphical authentication schemes are alternatives to passwords based on alphanumeric characters. These are used in user authentication or key generation for use in cryptographic algorithms [1]. Graphic passwords can be formed by the combination of photos, images, or iconography. Given the characteristics of the images, they produce a much larger password space and are more resistant to dictionary attacks since alphanumeric password phrases that are relatively easy to predict are often used. These passwords' efficiency is based on the ability of humans to remember patterns in images instead of memorizing sets of characters of great length and complexity.

An updated description and critical assessment of the different graphical authentication schemes' security and usability can be found in [2]. PassPoint is a graphical authentication technique that bases its operation on selecting and remembering patterns of points in images [3]. The authentication process involves the user selecting various points on the image in a particular order. When logging in, the user is supposed to click near the points selected in the registration phase within a tolerance region or neighborhood. One of the vulnerabilities of PassPoint lies in the possible existence of a pattern in the points that make up the password [2]. This pattern can be determined either by selecting the points or by the spatial distribution of them in the image. Considering the latter, a password is considered weak if the points are not randomly distributed and can be obtained by an attacker applying various techniques such as those described in [4–7]. The main types of nonrandomness present between the points, in that case, are clustering, regularity, and smoothness. According to the behavior of the points distributed in the plane (in this case, image), the spatial point patterns are classified into random (homogeneous Poisson point process), regular (uniform or a pattern in inhibition), or clustered (aggregates), [8–12]. During the registration phase of the PassPoint, it is necessary to determine whether the points selected by the user follow a random spatial pattern.

In [13], it is stated that Delaunay triangulation and Voronoi polygons have been widely used to analyze the pattern of distribution of points and measure spatial intensity. To measure the distribution of points, we calculate the nearest neighbor and the point pattern shape. When calculating a Voronoi diagram to a point distribution to test the complete spatial randomness of the point distributions, the characteristics of the Delaunay triangles are extracted (e.g., interior angles and edge lengths). Spatial intensity, i.e., how concentrated the points are in a particular study area, is measured by calculating the area and elongation of the Voronoi polygons. This approach has been used in many applications, including agriculture, microbiology, and astronomy [14].

In this work, a statistical test is proposed to detect clustering or regularity between the points of a graphical password in PassPoint. This test is based on the Delaunay triangles generated by that password, specifically on the average of those triangles' perimeters. The effectiveness of the proposed test is experimentally verified. Type I error resulting when applying them to random passwords is estimated and kept at acceptable levels for practical applications; on the other hand, type II error resulting when applied to clustered and regular passwords is estimated, and as expected, it is observed that it depends on the level of clustering or regularity. The article is structured in 4 sections: Section 1 shows the Introduction; Section 2 is composed of PassPoint, spatial point patterns, classic tests most used in complete spatial randomness, and the applications of Voronoi diagrams and Delaunay triangulations in the detection of spatial point patterns. Section 3 shows our contribution: detection of weak graphical passwords in PassPoint, based on the perimeter of their Delaunay triangles, and finally in Section 4, the conclusions and future work are presented.

2. Preliminaries

2.1. PassPoint. PassPoint is a graphical authentication scheme of the cued-recall type presented in [3]. This technique requires the user to select as their password during the registration phase an ordered set of 5 points (pixels) in an image. In the authentication phase, the same points must be selected approximately and in the same order that they were registered. For the authentication process to be effective and convenient for the user, there must be a tolerance associated with each point (approximately 0.25 cm). It is possible to use any image to select the password points; it can be provided by the user or the system itself. The authors of this scheme recommend using images that have hundreds of Hotspots spread evenly for greater security. The password is not stored explicitly, but a hash of the concatenation of the password points is generated. However, this causes a problem when applying the password hashing function. It is unlikely that the user will select the same points selected in the authentication phase-image in the registration phase, which means that the password hashing function will always be different. To establish the tolerance around each point, a discretization mechanism is used, which reduces the password space and provides relevant information to carry out a dictionary attack [15]. A discussion about the importance of the discretization mechanism in graphic password schemes can be seen in [16–18], while in [16–19], some of the different methods of discretization known so far are presented.

While the selection of images by the user may increase the ability to memorize their password, there is a possibility that, at the same time, security will be compromised with images with few security features (e.g., few memorable points and images that are easy to predict with knowledge about the user) [3]. In several studies such as those presented in [7, 15, 20, 21], dictionary attacks have been carried out using digital image processing techniques. The spatial patterns in the user's selection of points reduce the effective space of a password and give an advantage to possible attackers, who can use this knowledge to increase their attacks' probability of success. In the study presented by [22], it is suggested that it is possible to obtain patterns in the shape and order of the selection of the points without knowing the image used to create the password. Users tend to select their password points in separate compositions from the background images, to facilitate the memorability of their passwords. If the set of points selected by the user as their graphical password does not follow a random pattern, it presents a shape of a straight line, curved or by default (Z, W, C, V), or of every 2 consecutive points out of the 5 that make up the password; they are at constant distances. Then, said graphical password is considered weak, as it can be compromised using dictionary attacks [2, 5, 23].

2.2. Spatial Point Patterns. The phenomena that occur in some regions of space, such as data on human settlements, animals, the cultivation of crops, or information on the behavior of a pandemic (such as COVID-19 in 2020), represent an occurrence through its spatial coordinates (x, y). The datasets generated by these coordinates are called spatial point patterns [8, 10, 11, 24, 25]. From the study of spatial patterns, inferences can be made about the existence of interactions between each population's individuals. Spatial point patterns are classified as random (homogeneous Poisson point process), regular (uniform or an inhibiting pattern), or clustered (aggregated); see Figure 1.

To decide the behavior of an observed point pattern, a complete spatial randomness (CSR) test is applied where it is assumed as a null hypothesis that the pattern comes from the Poisson distribution; that is, that the pattern of points follows a random distribution [8, 26, 27]. The spatial point patterns present two fundamental characteristics [12, 27]. One of them is related to the intensity of the number of points per unit area; the second is based on looking for

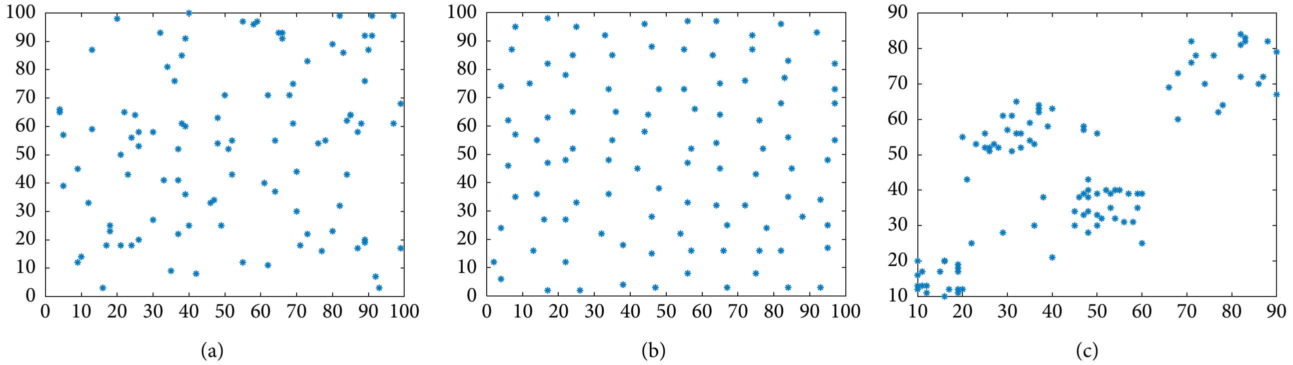


Figure 1: Random point pattern: (a) regular (b) and clustered (c).

relationships between each point with those of its surroundings, mainly through the distance between points.

2.3. Classic Tests Most Used in Complete Spatial Randomness (CSR)

2.3.1. K-Ripley Function. If a Poisson process randomly distributes a set of points with intensity λ, the expected number of points in a circle of radius r is $\lambda\pi r^2$. The deviation from randomness can be quantified using the K-Ripley function [8, 25, 27], which reflects the type, intensity, and range of the spatial pattern by analyzing the distances between the points, defined as follows:

$$K(r) = \frac{A}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} k_{i,j}(r) e_{i,j}(r), \tag{1}$$

for all $i \neq j$, where n is the number of points in the pattern, A is the area of the region under study, $e_{i,j}(r)$ is the edge correction method, and $k_{i,j}(r)$ is the following indicator function:

$$k_{i,j}(r) = \begin{cases} 1, & \text{if} r_{i,j} \leq r, \\ 0, & \text{if} r_{i,j} > r, \end{cases} \tag{2}$$

where $r_{i,j}$ is the distance between points i and j. The edge effects arise because the points that appear outside the limits of the study area are not taken into account to estimate the statistic, even though they are at a distance less than r from a point located within the area. One of the possible expressions of the K-Ripley function, taking into account one of the edge correction methods, is as follows:

$$K_{\text{bord}}(r) = \frac{A \sum_{i=1}^{n} \xi_i(r) \sum_{j=1}^{n} k_{i,j}(r)}{n \sum_{i=1}^{n} \xi_i(r)}, \tag{3}$$

where ξ_i denotes the indicator function that is equal to 1 if the distance from a point p_i to the edge A is greater than or equal to r and 0 otherwise. It is worth clarifying that there are other ways to correct the edge effect, which lead to alternative expressions of the K function. A detailed review of these methods can be found in [8, 28].

The transformation $\widehat{L}(r) = \sqrt{K(r)/\pi}$ allows linearizing the function $K(r)$ and stabilizing the variance, and by means of the $L(r) = \widehat{L}(r) - r$ transformation, it is possible to adjust the Poisson pattern to the value of zero. A clustered pattern occurs when $L(r)$ is significantly greater than zero, and a regular pattern occurs when $L(r)$ is significantly less than zero.

2.3.2. The G Function, Distance to the Nearest Neighbor. This method is based on the distances from each point to its nearest neighbor [8, 27]. The expected cumulative distribution function for the nearest neighbor distances d is defined by the Poisson distribution:

$$G(d) = 1 - e^{-\lambda\pi d^2}. \tag{4}$$

If over an area A, n points are randomly distributed, where $\lambda = n/A$. To consider the correction of the edge effect, the following function is used:

$$\widehat{G}(d) = \frac{\sum_{i=1}^{n} I_i(d)}{n}, \tag{5}$$

where n is the number of points in the pattern and $I_i(d)$ is the indicator function, which takes the value of one if the Euclidean distance between point i and its closest neighbor is less than d, and 0 otherwise; see [8]. A clustered pattern occurs when $\widehat{G}(d) > G(d)$, while a regular pattern occurs when $\widehat{G}(d) > G(d)$.

2.3.3. The Function F, Distance to the Null Space. The null space distance measures the distance d from each point in an additional m set, called a grid, to the closest of the n points in the observed pattern. For a pattern under the CSR hypothesis, its distribution is the same as for the function $G(d)$, i.e.,

$$F(d) = G(d) = 1 - e^{-\lambda\pi d^2}, \tag{6}$$

where λ is the intensity of the pattern. For estimating distances, a set of m points similar to n of the observed pattern is usually used. The distribution of the observed pattern is estimated by

$$\widehat{F}(d) = \frac{\sum_{j=1}^{m} I_j(\mathrm{d})}{m}, \tag{7}$$

where m is the number of points on the grid and $I_j(d)$ is the indicator function that the value of one if the Euclidean distance between point j on the grid and its closest neighbor in the pattern is less than d, and 0 otherwise.

The use of the $F(d)$ function is similar to that of the $G(d)$ function, using Monte Carlo simulations to estimate its critical values and graphical diagnostic tools in the same way. However, the interpretation of the deviations from the observed distribution is opposite: values more significant than those of the theoretical distribution indicate regularity and smaller values indicate clustering. The F function is usually more effective at detecting CSR deviations towards the cluster; see [27].

2.4. Applications of Voronoi Diagrams and Delaunay Triangulation in the Detection of Spatial Point Patterns. Voronoi diagrams are geometric structures that allow you to build a partition of the Euclidean plane. Given an initial set $P = \{p_1, p_2, \ldots, p_n\}$ of n points in the plane, a Voronoi diagram is defined as a partition of the Euclidean plane into n disjoint regions.

Definition (a planar ordinary Voronoi diagram): Let $P = \{p_1, p_2, \ldots, p_n\} \subset \mathfrak{R}^2$, where $2 \le n < \infty$ and $p_i \ne p_j$, for, $i, j \in J_n$. We call the region given by

$$V(p_i) = \{q: q - p_i\|_2 \le \|q - p_i\|_2, \text{for } j \ne i, j \in J_n\}. \tag{8}$$

The planar ordinary Voronoi polygon associated with p_i (or the Voronoi polygon of p_i), and the set given by

$$V = \{V(p_1), \ldots, V(p_n)\}. \tag{9}$$

The planar ordinary Voronoi diagram by P (or the Voronoi diagram of P): we call p_i of $V(p_i)$ the i th Voronoi polygon, and the set $P = \{p_1, p_2, \ldots, p_n\}$ is the generator set of the Voronoi diagram V (in the literature, a generator point is sometimes referred to as a site). [29].

For the dual graph of a Voronoi diagram is a Delaunay triangulation, see Figure 2. A triangulation of the set P of points on the plane is Delaunay if and only if the circumscribed circumference of any triangle in the lattice does not contain a point of P in its interior. This condition is known as Delaunay's condition. The Voronoi diagrams and the Delaunay triangulation in the two-dimensional case present a series of characteristics determined by the behavior of the point pattern observed in the initial set of points [9, 29, 30].

Since the mid-1980s, some of these characteristics have been used in the study of spatial point patterns. For example, in [31], although the total number of patterns examined is not large, the influence of a Delaunay triangle's interior angles is studied to detect clustering at the points. In general, the authors concluded that the minimum angle seems preferable to the maximum one to detect clustered or regular patterns. However, there are indications that the maximum angle seems to detect some cases of clustering that are not discernible by the minimum angle. In order to analyze whether the characteristics, interior angle of a Delaunay triangle, minimum angle, mean angle, and maximum angle of a Delaunay triangle, length of one side of a Voronoi polygon, the distance between a site and a vertex of its Voronoi polygon (radius of a circle circumscribed in a Delaunay triangle), length of one side of a Delaunay triangle, and area and perimeter of a Delaunay triangle are capable of detecting nonrandomness. In [9], they generated 100 clustered or regular points in a square unit. Obtaining the characteristic "minimum angle of a Delaunay triangle" is more effective in detecting regular patterns than the others in detecting clustered patterns. An adaptive spatial clustering algorithm based on Delaunay triangulation is proposed in [32]. This algorithm uses both the Delaunay triangulation edge's statistical characteristics and a new definition of spatial proximity based on the Delaunay triangulation to detect spatial clusters.

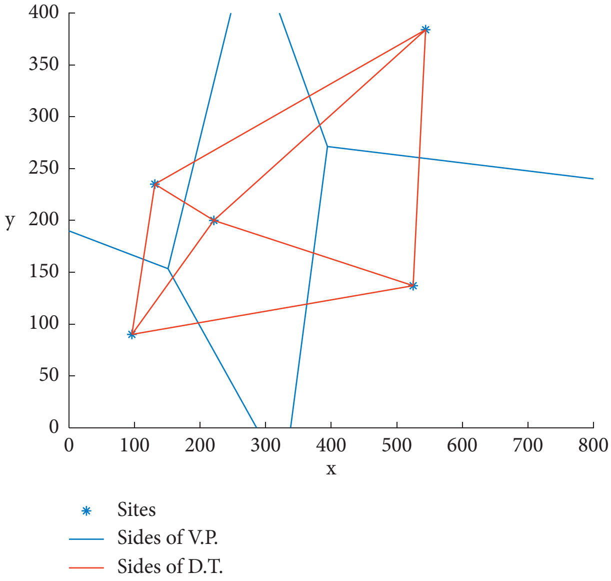


Figure 2: Representation of a Voronoi diagram (VD) and its corresponding Delaunay triangulation (DT).

Discovery of Spatial Patterns with Extended Objects (DEOSP) [33, 34] is another method that allows for the discovery of patterns for extended objects (straight lines, strings of lines, and collections of the same), although it does not allow operating on the extended objects as areas. DEOSP is based on structures related to the Delaunay triangulation. The work presented in [35] uses the area and perimeter of the Voronoi polygons to analyze changes in the spatial patterns of permanent GNSS (Global Navigation Satellite System) stations ASG-EUPOS (Active Geodetic Network-European Position Determination System) in Poland depending on the scales used. Another vital application of Voronoi polygons is the one presented in [36]. In it, the analysis of macromolecular complexes is presented from a method based on 3D Voronoi tessellations. The method enables local density estimation, segmentation, and quantification of 3D particle localization microscopy data;

specifically, the authors use the area of Voronoi polygons to detect the clustering of particles.

3. Detection of Weak Graphical Passwords in PassPoint, Based on the Perimeter of Their Delaunay Triangles

3.1. Ineffectiveness of the Classic CSR Tests in the PassPoint Scenario. As far as we are aware of, there is no consensus in the current literature on the minimum value of the number of points (n) of the pattern from which the classic tests described in subsection 2.3 are considered effective. In [37], the authors applied the tests to a pattern of 22 points, the smallest pattern of the reference; however, the results achieved are not discussed. Also, in [37], the authors experimented with a pattern of 36 points, for which they concluded that the tests were effective. So we propose the following research question: what will happen in the PassPoint scenario and where are the patterns with only 5 points available?

From the results carried out in [38], it is known that the K-Ripley function tests and those of the distance to the nearest neighbor are ineffective in detecting graphic passwords formed by patterns clustered in PassPoint; however, the experiments were performed for a relatively large number of Monte Carlo simulations. This article analyzes three of the classic tests most used in CSR, including the two tests mentioned above, in detecting nonrandomness in PassPoint passwords, but with a smaller number of Monte Carlo simulations. This difference is given by the existing controversy between the number of simulations in the consulted bibliography, since in [37], the authors state that for a significance level of $\alpha = 0.05$, it is advisable to perform at least 999 simulations, while in [8], they state that for $\alpha = 0.05$ and $\alpha = 0.01$, 40 and 199 Monte Carlo simulations must be performed, respectively.

To analyze the detection of nonrandomness of these tests in the PassPoint scenario, two experiments were carried out on a 1920 × 1080 pixel image, one to measure clustering and the other regularity. The experiments carried out were run in MATLAB version R2018a on an AMD A6-9220e CPU: 1.60 GHz with 4 G of RAM.

The experiments were designed as follows: for experiment 1, two databases were generated, DB. $1.1_{Ag.(IV)}$ and DB. $1.2_{Ag.(VIII)}$, of 10,000 passwords with Poisson aggregate patterns with an aggregation distance of $686u$ and $315u$, respectively, [37]. That is, two databases of passwords were generated, clustered in an area equivalent to a quarter of the image and the other to an eighth, containing the DB. $1.2_{Ag.(VIII)}$ with a higher level of clustering. The clustered (or aggregated) patterns were derived from a Poisson aggregate process: randomly distributed parental points were generated, and subsequently derived points were randomly distributed around the parents within a specified aggregation radius [8, 37]. For experiment 2, the pattern xy with the highest possible regularity level was generated, which is determined by the following points: $(0;0)$, $(1920;0)$, $(0;1080)$, $(1920;1080)$, and $(960;540)$; see Figure 3.

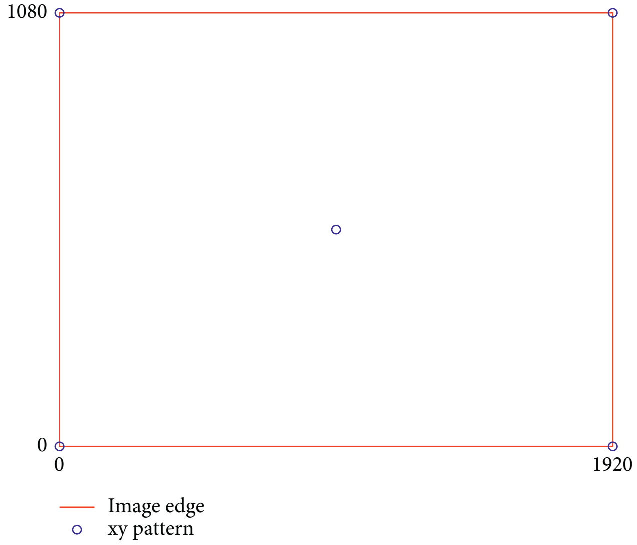


Figure 3: Representation of the xy pattern.

Now we discuss the results obtained after running both experiments. For each of the tests, the critical values were estimated using 199 Monte Carlo simulations of sets of 5 random points on a rectangle of size 1920 × 1080. In addition to the K-Ripley function, the confidence intervals were estimated according to Ripley's approximation + [27, 39], where $A = 1920 \cdot 1080$ and $n = 5$. These Monte Carlo simulations guarantee critical intervals with a significance level of $\alpha = 0.01$ for each test. See Figure 4, where the continuous line represents the theoretical value of the null hypothesis, the dashed lines represent the critical values of each of the tests in 199 simulations of random patterns. In the case of the K-Ripley function, the dashed lines represent the confidence intervals for $\alpha = 0.01$ of the test according to Ripley's approximation. It is observed how the critical values coincide with the minimum value of each function.

From the estimated critical values, an immediate conclusion was obtained: the K-Ripley function tests and the nearest neighbor are not effective in detecting regular patterns, and the null space function test is not very effective in detecting clustered patterns. Furthermore, from the expression of the function $L(r)$, in the K-Ripley function, it is evident that its minimum possible value is $L(r) = -r$. This minimum value coincides with the critical value estimated by the Monte Carlo simulations. Therefore, this test cannot detect a regular pattern since a pattern is considered regular if it is below the critical values estimated by the test. For $\widehat{G}$, it holds that $\widehat{G}(d) \geq 0$, for all d, the lower critical range estimated for the test of the distance to the nearest neighbor is $\widehat{G}(d) = 0$ 0. Therefore, this test will not be able to detect regular patterns either. Like the $\widehat{G}$ function, the minimum value that the $\widehat{F}$ function can take is 0. This minimum value coincides with the lower critical value estimated by Monte Carlo simulations. Therefore, this test is not capable of detecting clustered patterns. Of the 10,000 iterations of the F function test for the xy pattern, which expresses the greatest possible regularity between 5 points in a rectangle, it turns

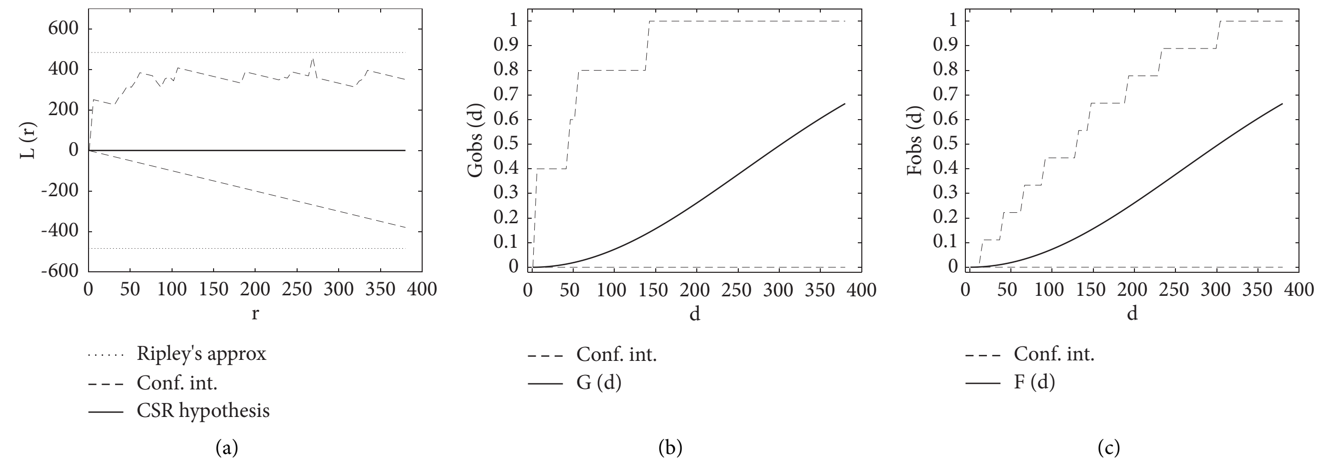


Figure 4: Critical values of the *K*-Ripley tests: (a) the nearest neighbor (b) and empty space (c) for 199 Monte Carlo simulations.

out that none of them detects said pattern as regular. These 10, 000 iterations are because the F function depends on a grid, which is an additional set of random points; therefore, for a pattern, the value of the function can change depending on the grid. Then the 10, 000 iterations were performed for the xy pattern but varying the grid so that the result did not depend on it.

The results obtained are summarized in Table 1, where t he sign "–" means that the corresponding test is not applicable in the case in question. The results show that the K-Ripley function and the nearest neighbor tests are not effective in detecting clustered 5-point patterns and are not capable of detecting regular 5-point patterns. For its part, the empty space distance test showed an effectiveness of 0% in detecting regular patterns and is unable to detect clustered patterns. Therefore, these three analyzed spatial randomness tests turn out to be ineffective in detecting nonrandom graphical passwords in the scenario PassPoint.

Recently, in [30], the application of the characteristic "number of sides of the Voronoi polygons" was evaluated for the detection of graphical passwords formed by patterns clustered in PassPoint, but it also proved to be ineffective using the proposed criteria.

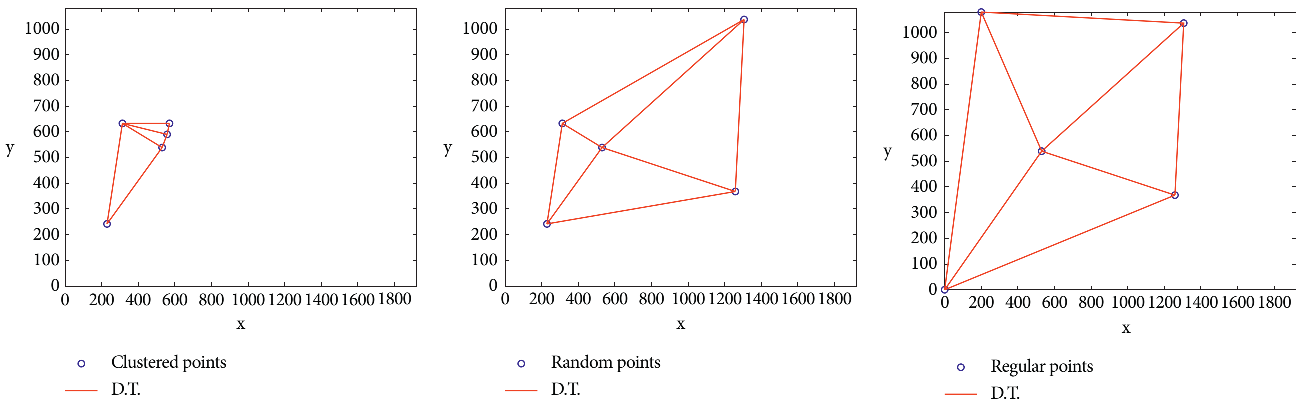
3.2. *The Sample Mean, Sample Variance, and Distribution of the Averages of the Perimeters of the Delaunay Triangles.*

In Section 2.4, we discussed the use of some of the features of Voronoi diagrams and Delaunay triangulations to detect spatial point patterns. In the PassPoint scenario, the points (pixels) of a clustered password are very close between them, and those of a regular graphical password are far from each other for a higher level of consistency. Considering this, in this work, we propose to use the perimeter of the Delaunay triangles to detect randomness between the password points instead of some other characteristic. However, it may be the case that in a password where the points are randomly distributed, the perimeter of one of its Delaunay triangles is just as small as that of one in a clustered password or just as big as one of the triangles of a password with regularly distributed points. In Figure 5, it is observed how the maximum perimeter of the Delaunay triangles of the clustered points coincides with the minimum perimeter of the Delaunay triangles of the random points, as the maximum perimeter of the triangles of Delaunay of the random points coincides with the minimum perimeter of the regular points. This suggests using the average of the perimeters of the Delaunay triangles as decision criteria to detect clustering or regularity between the pixels of a password in PassPoint and not the minimum or maximum value of the Delaunay triangles perimeter.

Table 1: Percentage of nonrandom graphical passwords detected by each test in each experiment.

Test	DB. $1.1_{Ag.(IV)}$	DB. $1.2_{Ag.(VIII)}$	xy
Null space	—	—	0%
K-Ripley	5.31%	26.55%	—
Nearest neighbor	1.88%	8.90%	—

Thus, it is then necessary to determine the probability distribution that best fits the distribution of the average of the perimeters of the Delaunay triangles of a password; for this, experiment 3 was designed and carried out in the following way. 1, 000 random graphic passwords were generated in each of the three image sizes, 800×480, 1366×768, and 1920×1080 pixels, as the first image is the most common in mobile phones and the other two in computers. For each of these passwords, its Delaunay triangulation is constructed and the average of the perimeters of its Delaunay triangles is calculated, obtaining a total of three random databases of 1, 000 averages each. The first database (DB.3.1) contains the averages of the image of 800×480 and the second one (DB.3.2) those of 1366×768, whereas the third one (DB.3.3) contains the averages of the last image. To measure the fit of the data to some known theoretical distribution, the EasyFit 5.6 software was used, which allows the distributions to be automatically adjusted to the sample data and the best model selected in a few seconds [40, 41]. The EasyFit 5.6 consists of 54 theoretical distributions, with some of them for various parameter sets, making a total of 61 possible options to fit for the data.



(a)

(b)

(c)

Figure 5: Delaunay triangulations of clustered points (a), random points (b), and regular points (c).

Table 2: Mean, sample variance, and standard deviation of the averages of the perimeters of Delaunay triangles (P_{P_D}) in the DBs: 3.1, 3.2, and 3.3, respectively.

P_{P_D}	DB.3.1	DB.3.2	DB.3.3
$E[P_{P_D}]$	872	1,439	2,038
$V[P_{P_D}]$	39,391	102,250	210,330
σ	199,902	319,766	458,617

Table 3: The six best theoretical distributions adjusted by the data from the random database (DB.3.1) with an image size of 800 × 480 pixels using the Kolmogorov–Smirnov (K-S), Anderson–Darling (A-D), and Chi-Square (χ^2), using the significance levels $\alpha \in \{0.2; 0.1; 0.05; 0.02; 0.01\}$, and its p-values associated with the Kolmogorov–Smirnov and Chi-Square tests.

Distribution	Number of acceptances	K–S	A-D	χ^2
Weibull (3P)	15/15	0.98070	Accepted	0.99858
Kumaraswamy	15/15	0.97874	Accepted	0.99892
Gen. Extreme value	5/10	0.94770	Rejected	N/A
Log-Pearson 3	15/15	0.94350	Accepted	0.98486
Johnson SB	15/15	0.94114	Accepted	0.99858
Weibull	15/15	0.77054	Accepted	0.65173

Table 4: The six best theoretical distributions adjusted by the data from the random database (DB.3.2) with an image size of 1366 × 768 pixels using the Kolmogorov–Smirnov (K–S), Anderson–Darling (A-D). and Chi-Square (χ^2), using the significance levels $\alpha \in \{0.2; 0.1; 0.05; 0.02; 0.01\}$, and its p-values associated with the Kolmogorov–Smirnov and Chi-Square tests.

Distribution	Number of acceptances	K–S	A-D	χ^2
Johnson SB	15/15	0.95628	Accepted	0.31172
Gen. Extreme value	5/10	0.95460	Rejected	N / A
Kumaraswamy	15/15	0.88420	Accepted	0.56845
Error	14/15	0.87086	Accepted	$\alpha \neq 0.2$ 0.16329
Weibull(3P)	15/15	0.79740	Accepted	0.50346
Log-Pearson 3	14/15	0.77399	Accepted	$\alpha \neq 0.2$ 0.15881

Table 5: The six best theoretical distributions adjusted by the data from the random database (DB.3.3) with an image size of 1920 × 1080 pixels using the Kolmogorov–Smirnov (K–S), Anderson–Darling (A-D), and Chi-Square (χ^2), using the significance levels $\alpha \in \{0.2; 0.1; 0.05; 0.02; 0.01\}$, and its p-values associated with the Kolmogorov–Smirnov and Chi-Square tests.

Distribution	Number of acceptances	K–S	A-D	χ^2
Error	15/15	0.99459	Accepted	0.69818
Johnson SB	15/15	0.98592	Accepted	0.83378
Gen. Extreme value	15/15	0.97157	Accepted	0.74561
Log-Pearson 3	15/15	0.96973	Accepted	0.73518
Kumaraswamy	15/15	0.90786	Accepted	0.66530
Weibull (3P)	15/15	0.90681	Accepted	0.55614

From experiment 3, we obtained the following results. Table 2 shows the sample mean and variance corresponding to the averages of the perimeters of the Delaunay triangles for each of the random password databases. Tables 3–5 show the six best models of distributions to which the data were fitted. Table 6 presents the results of the three goodness-of-fit tests applied to the Johnson SB distribution and the estimated distribution of the averages of the perimeters of the Delaunay triangles in each of the random databases corresponding to the sizes of studio images. However, when measuring the adjustment of the 1,000 averages of the perimeters of the Delaunay triangles estimated in each of the random databases to a known theoretical distribution, it was obtained that in each of the databases, it was possible to adjust the averages of the perimeters to more than 20 distributions, with some of them accepted by the three goodness-of-fit tests (Kolmogorov–Smirnov, Anderson–Darling, and Chi-square) with the significance levels $\alpha \in \{0.02, 0.01, 0.05, 0.1, 0.2\}$.

Table 6: Results of the three goodness-of-fit tests with the significance levels $\alpha \in \{0.02, 0.01, 0.05, 0.1, 0.2\}$, applied to the Johnson SB distribution estimated by the data for each of the random databases DBs: 3.1, 3.2, and 3.3.

Goodness-of-fit test	DB.3.1	DB.3.2	DB.3.3
Kolmogorov–Smirnov	0.94114	0.95628	0.98592
Chi-square	0.99858	0.31172	0.83378
Anderson–Darling	Accepted	Accepted	Accepted
Number of acceptances	15/15	15/15	15/15

Table 7: Parameters of the Johnson SB distribution $(\gamma, \delta, \lambda, \xi)$ of the averages of the perimeters of the Delaunay triangles in the DBs: 3.1, 3.2, and 3.3, respectively, $P_{P_D} \sim J_{SB}(\gamma, \delta, \lambda, \xi)$.

DB.	Image size	γ	δ	λ	ξ
DB.3.1	800 × 480	−0.44981	2.7884	2 295.3	−365.06
DB.3.2	1366 × 768	−0.25323	1.9873	2 700.2	8.2037
DB.3.3	1920 × 1080	−0.21458	2.0283	3 940.5	−30.961

We now discuss the results of experiment 3. Table 2 illustrates that the sample mean and variance differ between the databases due to the inequality between the image sizes. The averages of the perimeters of the Delaunay triangles belonging to the three sizes of the images under study did not fit the distributions with the same parameters (Table 7) or in the same order of the best models fitted by EasyFit, but the fitted distributions for each image size mostly match. Among the best distributions that fit the perimeters of the Delaunay triangles ($\forall \alpha$) for the random databases DB.3.1, DB.3.2, and DB.3.3 is the Johnson SB, which occupies the fifth, first, and second place among the best possible models, respectively (Figure 6). This distribution allows for the transformation of the data to a standard normal distribution using the following formula [42]:

$$P_D^N = J_{SB}(P_D) = \gamma + \delta \times \ln\left[\frac{(P_D - \xi)}{(\lambda + \xi - P_D)}\right], \tag{10}$$

$P_D^N \sim N(0,1)$. This transformation makes it easy to apply normality tests based on the fit of the data. Then, under the randomness hypothesis, the average of the perimeters of the Delaunay triangles of a graphical password in PassPoint when transforming the data to a standard normal distribution is 0. Therefore, it can be assumed that the passwords that violate the above proposition do not follow a random pattern.

3.3. Test Based on the Average of the Perimeters of the Delaunay Triangles. In this subsection, we propose a statistical test to detect nonrandom passwords in PassPoint. This test constitutes the main contribution of this article, considering that the classic tests are ineffective in detecting nonrandom graphical passwords in the PassPoint scenario. Although, recently [43], a test (of spatial randomness based on the mean distance between the points) was proposed with the same objective as the test proposed in this work, to detect nonrandom and, therefore, weak graphical passwords introduced by users during the registration phase in a PassPoint system, it is considered necessary to carry out in the next future works a comparison in terms of effectiveness and errors made between these two tests. The proposal of this work consists of a two-tailed hypothesis test based on the average of the Delaunay triangles' perimeters transformed to a standard normal distribution using the Johnson SB transformation. To apply this test, it is necessary to consider the size of the image selected by the user since the Johnson SB parameters are different for the sizes of images analyzed, as shown in Table 7.

3.3.1. Spatial Randomness Test Based on the Average of the Perimeter of Delaunay Triangles to Detect Nonrandom Passwords in PassPoint. We propose the following null hypothesis:

$$H_0\colon E\left[P_D^N\right] = E\left[J_{SB}(P_D)\right] = 0, \tag{11}$$

which states that the graphical password selected by the user is random if the average of the perimeters of the Delaunay triangles transformed by Johnson SB to a standard normal is equal to 0, with an alternative hypothesis given by H_1: $E(P_D^N) = E[J_{SB}(P_D)] \neq 0$. In order to test the hypothesis, the test statistic, based on the average perimeters of Delaunay triangles of the points of a user-selected password transformed by Johnson SB to a standard normal, is used. It is given by the following:

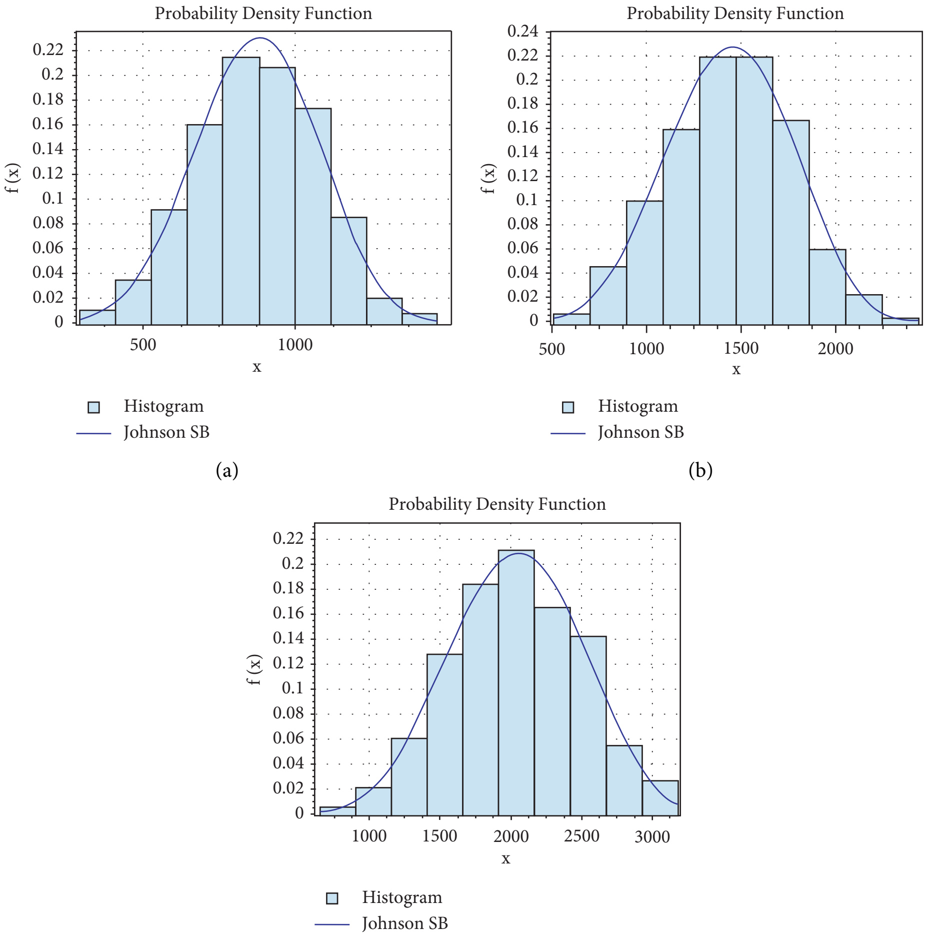
$$Z = J_{SB}\left(P_{P_D}\right) = \gamma + \delta \times \ln\left[\frac{\left(P_{P_D} - \xi\right)}{\left(\lambda + \xi - P_{P_D}\right)}\right]. \tag{12}$$

From Table 7, selecting the values of the transformation parameters depends on the image's size. The user or system can set the significance level α, whereas the critical region is $CR. = \{z\colon Z < -z_{\alpha/2} \text{ or } Z > z_{\alpha/2}\}$. Finally, with respect to the decision criteria, it is decided that the graphical password selected by the user does not follow a random pattern if, when transforming the average of the perimeters of its Delaunay triangles through the Johnson SB transformation, the value obtained belongs to the critical region.

3.4. Validation of the Effectiveness of the Proposed Test. To evaluate the effectiveness of the proposed test by means of type I and type II errors, Experiments 4 and 5 were carried out, respectively.

To estimate the probabilities of type I error from the proposed decision criterion, experiment 4 was designed. Three new random databases were generated, DB.4.1, DB.4.2, and DB.4.3, with 10,000 random graphical passwords each in each of the three image sizes, 800 × 480, 1366 × 768, and 1920 × 1080 pixels, respectively.

The results of experiment 4 are shown in Table 8. Note that the probability of obtaining the type I error corresponds approximately to the established level of significance (alpha theoretical) for all cases, which shows that the probabilities



(a)

(b)

(c)

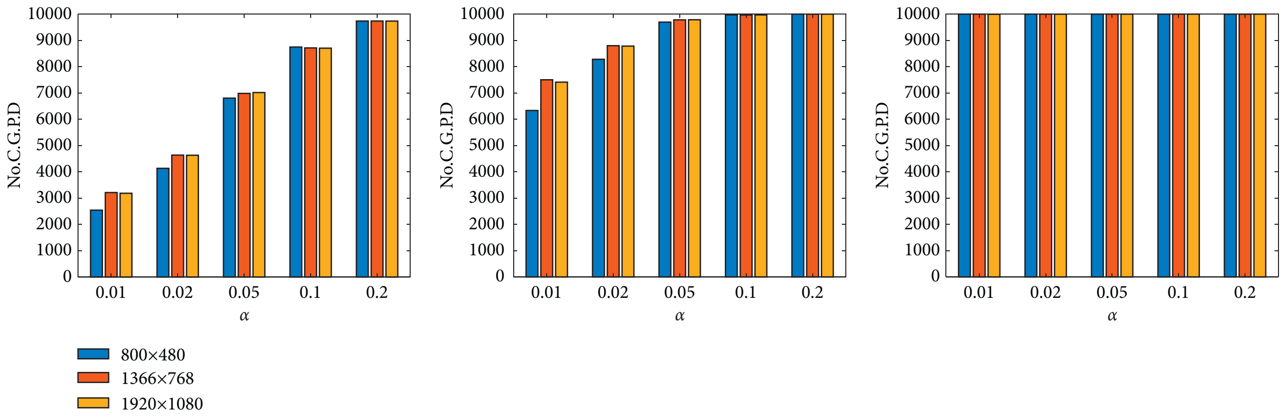
Figure 6: Histograms of the averages of the perimeters of the Delaunay triangles associated with the random graphical passwords in DB.3.1 (a), DB.3.2 (b), and DB.3.3 (c), respectively, and their comparison with the Johnson SB.

Table 8: Estimation of type I error (estimated alpha, $\widehat{\alpha}$), that is, of the probability that in DB.4.1, DB.4.2, and DB.4.3, the average of the perimeters of the triangles of a random graphical password belongs to the critical region. Comparison with the preset theoretical alpha (α).

α (Theoretical)	*CR.* Of H_0	$\widehat{\alpha}_1$ DB.4.1	$\widehat{\alpha}_2$ DB.4.2	$\widehat{\alpha}_3$ DB.4.3	$\sum_{i=1}^{3} \widehat{\alpha}_i/3$
0.2	$Z < -1.282 o Z > 1.282$	0.1803	0.1962	0.1885	0.1883
0.1	$Z < -1.645 o Z > 1.645$	0.0853	0.1023	0.0918	0.0931
0.05	$Z < -1.960\ o\ Z > 1.960$	0.0403	0.0545	0.0499	0.0482
0.02	$Z < -2.326 o Z > 2.326$	0.0166	0.0248	0.0213	0.0209
0.01	$Z < -2.575 o Z > 2.575$	0.0081	0.0157	0.0116	0.0118

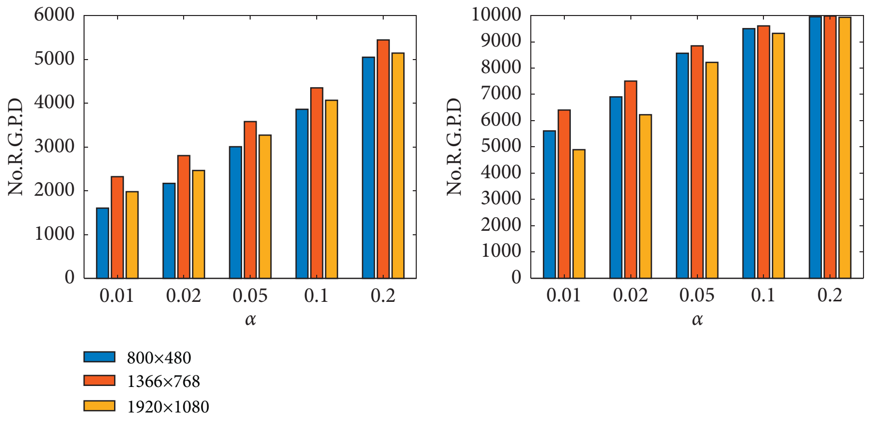
of type I errors do not seem to depend on the image size and that the proposed decision criterion is valid.

Now, for experiment 5, 50,000 nonrandom graphical passwords are generated in total, 30,000 clustered (10,000 in an area equivalent to a quarter of the image, 10,000 in an area equal to one-sixth of the image, and the other 10,000 in an area equivalent to the eighth of the image), and regular 20,000 (with a lower and higher level of regularity), for each of the study images. This means that, for the 800×480 image, the aggregation distances were $175u$, $145u$, and $125u$ radius; for the 1366×768, they were $290u$, $240u$, and $210u$ of radius; for the image of 1920×1080, the aggregation distances were $410u$, $335u$, and $290u$ of radius, respectively; the regular databases were generated by inhibition distances of $140u$ and $220u$, $210u$ and $350u$, and $300u$ and $505u$ of radius, respectively. The regular patterns were derived from a simple inhibition process: random locations of points were generated, verifying that at each new point, the distance to its closest neighbor was equal to or greater than a specified inhibition distance [8, 37]. In each of these databases, the type II error was estimated, and the number of passwords detected was calculated for the different levels of clustering and regularity.



(a) (b) (c)

Figure 7: Number of clustered graphical passwords detected (No. of CGPD) in each of the image sizes for clustered pattern databases (in an area equivalent to one-fourth (a), one-sixth (b), and one-eighth (c) of the image), with significance level α.



(a) (b)

Figure 8: Number of regular graphical passwords detected (No. of RGPD) in each of the image sizes for databases with regular patterns (with lower (a) and higher (b) levels of regularity), with significance level α.

The results of experiment 5 are as follows. Figures 7 and 8 show the number of nonrandom graphical passwords detected in each of the nonrandom databases for the analyzed image sizes, and Table 9 represents the probabilities of type II errors estimated in nonrandom databases for an image size of 1920 × 1080.

These results clearly show that by increasing the level of clustering or the regularity level, the test becomes more effective, as was to be expected. The decision criterion is usually quite effective in detecting clustered graphical passwords, especially for the significance levels $\alpha = 0.1$ and $\alpha = 0.2$ for which it detects 87% and 97% of the passwords, respectively (see Figure 7 and Table 9), in an area equivalent to one-fourth of the image; on the other hand, in the regular graphical passwords with a lower level of regularity, for $\alpha = 0.2$, it only detects approximately 50 of the passwords (see Figure 8 and Table 9). The criterion reaffirms Chiu's approach in [9], since the average of the Delaunay triangles' perimeters is more effective in detecting clustering than regularity. Figures 7 and 8 show that the probabilities of type II errors do not seem to depend on the image size since their estimated values are similar for the different sizes of images; therefore, only the type II error was shown (Table 9) for each of the nonrandomized study databases of one of the image sizes.

This test was designed exclusively to detect graphical passwords with clustered or regular patterns in PassPoint. Therefore, other types of patterns identified in the bibliography [22], such as soft ones or with different predetermined shapes (see Figure 9), will only be detected by the test proposed if these also present a certain level of clustering or regularity (as shown in Figure 10). Therefore, if the patterns are not clustered, it cannot be said that the test can detect these patterns since these patterns have to fulfill the property that when forming their respective Delaunay triangles, one of the interior angles of the triangle has to be obtuse so that the triangle is as devoid of peaks as possible and a relatively smooth curve is formed. Visually, it could be interpreted as patterns in the form of a straight line (or almost straight, given the

TABLE 9: Probability estimated $(\widehat{\beta})$ in DB. 5.1.1$_{Ag.(IV)}$, DB. 5.1.2$_{Ag.(VI)}$, DB. 5.1.3$_{Ag.(VIII)}$, DB. 5.2.1$_{\text{Reg}}$ (less regular), and DB. 5.2.2$_{+_{\text{Reg}}}$ (more regular) to accept a random graphical password when it is actually a clustered or regular graphical password.

Significance	Error of	$(\widehat{\beta})$	$(\widehat{\beta})$	$(\widehat{\beta})$	$(\widehat{\beta})$	$(\widehat{\beta})$
Level	Tipo II	DB. 5.1.1$_{Ag.(IV)}$	DB. 5.1.2$_{Ag.(VI)}$	DB. 5.1.3$_{Ag.(VIII)}$	DB. 5.2.1$_{\text{Reg.}}$	DB. 5.2.2$_{+_{\text{Reg}}}$
0.2	$-1.282 < Z < 1.282$	0.0262	0.0002	0	0.4856	0.0047
0.1	$-1.645 < Z < 1.645$	0.1293	0.0034	0	0.5933	0.0500
0.05	$-1.960 < Z < 1.960$	0.2982	0.0219	0	0.6729	0.1436
0.02	$-2.326 < Z < 2.326$	0.5368	0.1201	0.0001	0.7537	0.3096
0.01	$-2.575 < Z < 2.575$	0.6814	0.2498	0.0005	0.8021	0.4391

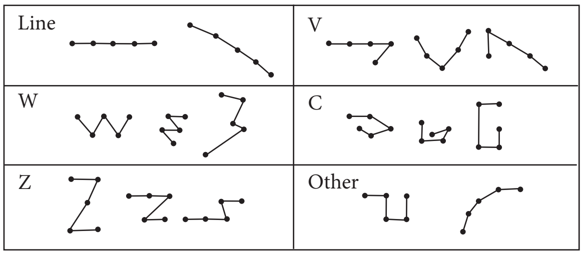


FIGURE 9: Patterns with different predetermined shapes.

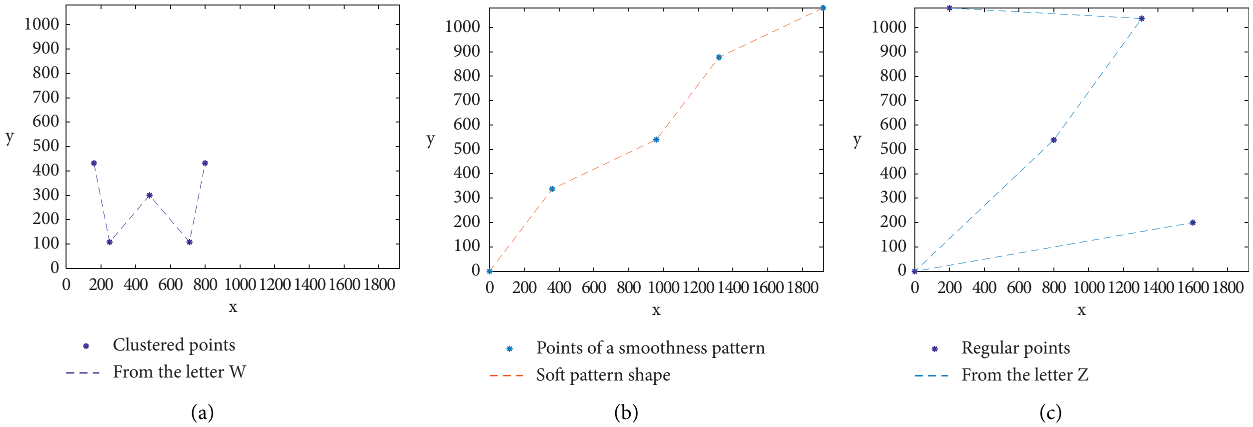


FIGURE 10: Pattern with default shape w, which also follows a clustering pattern (a), the pattern on with default shape (soft) but is detected as random (b), and pattern on with default shape Z, which also follows a regularity pattern (c).

TABLE 10: Number and proportion of nonrandom graphical passwords detected in the databases DB. 1.1$_{Ag.(IV)}$, DB. 1.2$_{Ag.(VIII)}$, and the regularity pattern xy, by means of the empty space function, the nearest neighbor distance test, the K-Ripley function, and the proposed test.

Test	DB. 1.1$_{Ag.(IV)}$	DB. 1.2$_{Ag.(VIII)}$	xy
Empty space	–	–	0%
Nearest neighbor	$188/10,000 = 0.0188$	$890/10,000 = 0.0890$	–
K-Ripley	$531/10,000 = 0.0513$	$2655/10,000 = 0.2655$	–
Proposed test	$3,212/10,000 = 0.3212$	$10,000/10,000 = 1.0000$	Detected

low probability that the user will select the points of his graphical password in such a way that they form exactly a straight line). This discussion suggests that a test to detect weak passwords can be constructed from the Delaunay triangles' interior angles, which is left proposed for future work, as well as its comparison with the test proposed in [44].

3.5. Comparison in PassPoint of the Proposed Test and the Tests Most Used in CSR. Table 10 shows the comparison between the proposed test, the K-Ripley function, the test of the distance to the nearest neighbor, and the empty space function in terms of the effectiveness in the detection of clustered and regular graphical passwords onstage PassPoint, for a significance level of $\alpha = 0.01$.

The image size of 1920 × 1080 pixels was used to make this comparison. The results for the other sizes of images studied in this work have a similar behavior. For an image of this size, the average of the perimeters of the Delaunay triangles of the pattern xy is $3,702.9u$, whereby transforming this average from a Johnson SB distribution to a standard normal using the statistic Z (12) to get $Z = 5.6558 > 2.575 = z_{0.005}$. Then, by means of the proposed test, the xy pattern is rejected with a 99 confidence, the expected occurrence given its ability to detect regular graphical passwords. This convincingly demonstrates the superiority of the proposed test over the classical tests of spatial randomness to detect nonrandom passwords in PassPoint.

3.6. Application of the Proposed Test in PassPoint. In graphical authentication, in the PassPoint scenario, the proposed spatial randomness test allows the user to verify the strength of their password during the registration phase. This is possible due to its ability to detect spatial patterns of clustering or regularity between the points that make up the password. The user must define the level of significance with which they want to verify their password, although it is recommended to use $\alpha = 0.2$ for greater effectiveness. During the PassPoint registration phase, the test can be included by following these steps:

Step 1. The user selects the 5 points (pixels) of his password in an image.

Step 2. Calculate the average of the perimeters of the Delaunay triangles in the password.

Step 3. Calculate the test statistic Z Equation (11) by performing the Johnson SB transformation to the average of the perimeters calculated in Step 2.

Step 4. Determine the critical region taking into account the specified significance level.

Step 5. Decision criteria: if the test statistic calculated in Step 3 does not belong to the critical region, the registration is successfully completed, but if it belongs to the critical region, the user is notified that the password is weak and returns to Step 1.

The proposed test must apply to other systems of the cued-recall type that uses 5 points, or a number close to 5, as its graphical password in an image. The experiments that prove it are left to be published in future research.

4. Conclusions and Future Work

In this work, it was shown that three of the most used classical tests in complete spatial randomness are inefficient in detecting nonrandom passwords in the PassPoint scenario, so the average of the perimeters of the Delaunay triangles was investigated to extract dependency information between password points. Its distribution was estimated in each of the random databases, which was adjusted to more than 20 known distributions for each of the study image sizes, the Johnson SB distribution for each image being among the five best fits. Different parameters of the Johnson SB distribution were obtained from the averages of the perimeters of the Delaunay triangles for the three sizes of images analyzed. Therefore, it was assumed with an established significance level that graphical passwords that violate this property are not random. The application of this criterion is facilitated because after applying the Johnson SB transformation with the parameters of the Johnson SB distribution established for each image size, the transformed average must follow a standard normal distribution. Based on the average of the Delaunay triangles perimeters transformed to a standard normal distribution by the Johnson SB transformation, a test was proposed to detect weak graphical passwords formed by clustered or regular points. Type I and type II errors were estimated, and the number of graphical passwords detected by this test was calculated for various levels of clustering and regularity. It was concluded that regardless of the image size, their estimates of type I and type II errors roughly coincide for an established level of significance and thus, the number of passwords detected. It is concluded that the proposed criterion based on the average of the perimeters of the Delaunay triangles is efficient for detecting weak graphical passwords in PassPoint, formed by five clustered points or by five regular points, although it is more precise in detecting clustering than regularity. Despite the effectiveness of the proposed test being tested for various levels of clustering or regularity, with different type II errors, the minimum level of clustering or regularity for which the test's effectiveness remains acceptable in application practices is still unknown. This aspect will be investigated in future work. Another open problem that will be discussed soon is the reduction of type II errors. The proposed 2-tailed test assesses deviations from randomness, and its effectiveness was evaluated in the detection of two types of patterns, clustered or regular. If hypotheses of the type H_1: clustered or H_1: regular are considered separately as alternative hypotheses, a one-tailed test will be obtained in each case, and a reduction of the type II error can be expected. This approach has the limitation of evaluating the existence of a specific type of nonrandom pattern, and a different test should be applied for each type of pattern. Its advantage is that it can be more effective in determining the type of pattern once it is decided to reject randomness. In future works, experiments will be carried out to evaluate the proposed test to detect passwords formed by soft patterns or with different predetermined forms. Another aspect to evaluate is the comparison in terms of effectiveness and errors made of the proposed test and the spatial randomness test based on the mean distance between the points. In addition, combinations of the different tests will be analyzed to increase the effectiveness in detecting nonrandom passwords without significantly compromising the implementation time. It is also proposed to evaluate the effectiveness of other characteristics of Delaunay triangulation to detect patterns in PassPoint, such as the minimum angle of a Delaunay triangle to detect regularity

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Swapnil Sunil, D. Prakash, and Y. Ramesh Shivaji, "Cued click points: graphical password authentication technique for security," *International Journal of ComputerScience and Information Technologies*, vol. 5, no. 2, 2014.

[2] O. Rodriguez, C. M. Legón, and R. Socorro, "Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica," *Revista Cubana de Ciencias Informáticas*, vol. 12, no. 13–27, 2018.

[3] S. Wiedenbeck, J. Waters, J. C. Birget, A. Memon, and N. Memon, "PassPoints: design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 102–127, 2005.

[4] H. Gao, W. Jia, F. Ye, and L. Ma, "A survey on the use of graphical passwords in security," *Journal of Software*, vol. 8, no. 7, pp. 1678–1698, 2013.

[5] R. G. Rittenhouse, J. Ahsenali Chaudry, and M. Lee, "Security in graphical authentication," *International Journal of Security and Its Applications*, vol. 7, no. 3, pp. 347–356, 2013.

[6] O. Rogriguez, C. M. Legón, R. Socorro, and P. Navarro, "Patrones en el orden de los clics y su influencia en la debilidad de las claves en la técnica de autenticacion gráfica passpoints," *Revista Cubana de Ciencias Informáticas*, vol. 12, no. 7, pp. 37–47, 2019.

[7] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in click-based graphical passwords," *Journal of Computer Security*, vol. 19, no. 4, pp. 669–702, 2011.

[8] A. Baddeley, E. Rubak, and R. Turner, *Spatial Point Patterns: Methodology and Applications with R*, CRC Press, Boca Raton, FA, USA, 2015.

[9] S. N. Chiu, "Spatial point pattern analysis by using Voronoi diagrams and Delaunay tessellations - a comparative study," *Biometrical Journal*, vol. 45, no. 3, pp. 367–376, 2003.

[10] A. E. Gelfand, P. Diggle, P. Guttorp, and M. Fuentes, *Handbook of Spatial Statistics*, Handb. Spat. Stat. Chapman & Hall/CRC, Boca Raton, FA, USA, 2010.

[11] B. Li, Q. Meng, and H. Holstein, "Point pattern matching and applications - A review," in *Proceedings of the SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme - System Security and Assurance (Cat. No.03CH37483)*, vol. 1, IEEE, Washington, DC, USA, November 2003.

[12] N. Oliver and D. Knitter, *Modelling human behaviour in landscapes*, Springer International Publishing, New York, NY, USA, 2016.

[13] E. A. Wentz, "Pattern analysis based on type, orientation, size, and shape," *Geographical Analysis*, vol. 40, no. 2, pp. 97–122, 2008.

[14] M. Erwig, "The graph voronoi diagram with applications," *Networks*, vol. 36, no. 3, pp. 156–163, 2000.

[15] B. B. Zhu, D. Wei, M. Yang, and J. Yan, "Security implications of password discretization for click-based graphical passwords," in *Proceedings of the 22nd international conference on World Wide Web*, pp. 1581–1591, Association for Computing Machinery, Rio de Janeiro, Brazil, May 2013.

[16] J. C. Birget, D. Hong, and N. Memon, "Robust Discretization, with an Application to Graphical Passwords," 2004, https://eprint.iacr.org/2003/168.

[17] S. Chiasson, J. Srinivasan, R. Biddle, and P. C. van Oorschot, "Centered discretization with application to graphical passwords (full paper)," in *Proceedings of the UPSEC'08: Proceedings of the 1st Conference on Usability, Psychology, and Security*, Berkeley, CA, USA, April 2008.

[18] K. Bicakci, "Optimal discretization for high-entropy graphical passwords," *1008 23rd Int. Symp. Comput. Inf. Sci. Isc.*vol. 2008, 2008.

[19] D. Kirovski, N. Jojić, and P. Roberts, "Click passwords," *IFIP Int. Fed. Inf. Process.*vol. 201, pp. 351–363, 2006.

[20] A. Emir Dirik, N. Memon, and J. Camille Birget, "Modeling user choice in the passpoints graphical password scheme," in *Proceedings of the 3rd symposium on Usable privacy and security*, vol. 20–28, Pittsburgh, PA, USA, July 2007.

[21] M. Devlin, R. Nurse, C. Hodges, H. Goldsmith, M. Creese, and S. Creese, "Predicting graphical passwords," in *Proceedings of the International Conference on Human Aspects of Information Security, Privacy and Trust at the 17th International Conference on Human-Computer Interaction (HCI)*, pp. 23–35, Springer International Publishing, Los Angeles, CA, USA, August 2015.

[22] S. Chiasson, A. Forget, R. van Oorschot, and P. C. Van Oorschot, "User interface design affects security: patterns in click-based graphical passwords," *International Journal of Information Security*, vol. 8, no. 6, pp. 387–398, 2009.

[23] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on PassPoints-style graphical passwords," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 393–405, 2010.

[24] J. D. Peter, *Statistical Analysis of Spatial and Spatio-Temporal point Patterns*, CRC Press, Boca Raton, FA, 2013.

[25] J. Illian, A. Penttinen, H. Stoyan, and S. Dietrich, *Statistical analysis and modelling of spatial point patterns*, Wiley, Hoboken, NJ, USA, pp. 1–534, 2008.

[26] Y. Beatriz Caballero and H. Giraldo Ramón, "Test de aleatoriedad para procesos puntuales espaciales basados en el cálculo de la dimensión fractal. Tesis presentada para optar el título de Magíster en Ciencias Estadísticas," Technical report, Universidad Nacional de Colombia, Bogotá, Colombia, 2017.

[27] M. De La Cruz, "Métodos para analizar datos puntuales," *Introd. al Análisis Espac. Datos en Ecol. y Ciencias Ambient. Métodos y Apl*, pp. 75–127, Asociación Española De Ecología Terrestre, Madrid, Spain, 2008.

[28] T. Wiegand and A. Kirk, *Handbook of spatial point-pattern analysis in ecology*, Routledge, England, UK, 2013.

[29] A. Okabe, B. Boots, K. Sugihara, S. N. Chiu, and D. G. Kendall, "Definitions and basic properties of voronoi diagrams," *Spatial Tessellations: Concepts and Applications of Voronoi Diagrams*, Vol. 43–112, John Wiley & Sons, , Hoboken, NJ, USA, 2000.

[30] L. Suárez-Plasencia, J. A. Herrera-Macías, and C. M. Legón-Pérez, "Analysis of the number of sides of voronoi polygons in passpoint," in *Proceedings of the Computer Science and Health Engineering in Health Services: 4th EAI International Conference, COMPSE 2020*, vol. 4, pp. 184–200, Springer International Publishing, New York, NY, USA, November 2021.

[31] B. N. Boots, “Using angular properties of delaunay triangles to evaluate point patterns,” *Geographical Analysis*, vol. 18, no. 3, pp. 252–259, 2010.

[32] M. Deng, Q. Liu, T. Shi, and Y. Shi, “An adaptive spatial clustering algorithm based on delaunay triangulation,” *Computers, Environment and Urban Systems*, vol. 35, no. 4, pp. 320–332, 2011.

[33] R. Bembenik, A. Protaziuk, and G. Protaziuk, “Discovering collocation rules and spatial association rules in spatial data with extended objects using Delaunay diagrams,” in *Rough Sets and Intelligent Systems Paradigms*, vol. 8537 LNAI, pp. 293–300, Springer-Verlag, Berlin, Germany, 2014.

[34] R. Bembenik, W. Protaziuk, and G. Protaziuk, “Methods for mining co-location patterns with extended spatial objects,” *International Journal of Applied Mathematics and Computer Science*, vol. 27, no. 4, pp. 681–695, 2017.

[35] B. Calka, E. Bielecka, and M. Figurski Open Geosciences, *Spatial Pattern of ASG-EUPOS Sites*, Degruyter.com, Berlin, Germany, 2017.

[36] L. Andronov, J. Michalon, and K. Ouararhni, “3D Clustering Analysis of Super-resolution Microscopy Data by 3D Voronoi Tessellations,” *Bioinformatics*, vol. 34, 2017.

[37] V. Camarero and J. J. Camarero, “Spatial analysis techniques applied in forest ecology: point pattern analyses,” *Investigación Agraria: Sistemas y Recursos Forestales*, vol. 14, no. 1, p. 79, 2005.

[38] J. A. Herrera-Macías, L. Suárez-Plasencia, and C. M. Legón-Pérez, “Effectiveness of some tests of spatial randomness in the detection of weak graphical passwords in passpoint,” in *Proceedings of the Computer Science and Health Engineering in Health Services: 4th EAI International Conference, COMPSE 2020*, vol. 4, pp. 173–183, Springer International Publishing, New York, NY, USA, November 2021.

[39] B. D. Ripley, “Tests of ’randomness’ for spatial point patterns,” *Journal of the Royal Statistical Society: Series B*, vol. 41, no. 3, pp. 368–374, jul 1979.

[40] K. Schittkowski, *Numerical data fitting in dynamical systems: a practical introduction with applications and software*, Vol. 77, Springer Science & Business Media, , Berlin, Germany, 2002.

[41] K. Schittkowski, “Easy-Fit: A Software System for Data Fitting in Dynamical Systems,” *Structural and Multidisciplinary Optimization*, vol. 23, 2002.

[42] I. Juliana Lagos and J. A. Vargas, “Sistema de familias de distribuciones de Johnson, una alternativa para el manejo de datos no normales en cartas de control,” *Revista Colombiana de Estadística*, vol. 26, no. 1, 2003.

[43] J. A. Herrera-Macías, C. M. Legón-Pérez, L. Suárez-Plasencia, L. R. Piñeiro-Díaz, O. Rojas, and G. Sosa-Gómez, “Test for detection of weak graphic passwords in passpoint based on the mean distance between points,” *Symmetry*, vol. 13, no. 5, p. 777, 2021.

[44] O. Rodriguez, “Algoritmo para la detección de contraseñas gráficas con patrón de suavidad en la técnica de autenticación gráfica passpoints. tesis presentada en opción al título máster en ciencias matemáticas,” Technical report, Universidad De La Habana, Havana, Cuba, 2019.