symmetry

MDPI

Article

Test for Detection of Weak Graphic Passwords in Passpoint Based on the Mean Distance between Points†

Joaquín Alberto Herrera-Macías [1], Carlos Miguel Legón-Pérez [2], Lisset Suárez-Plasencia [2], Luis Ramiro Piñeiro-Díaz [2], Omar Rojas [3,*] and Guillermo Sosa-Gómez [3]

1 Departamento de Matemática, Universidad de Matanzas, Matanzas 40100, Cuba; joaquin.herrera@umcc.cu
2 Instituto de Criptografía, Facultad de Matemática y Computación, Universidad de la Habana, Habana 10400, Cuba; clegon58@gmail.com (C.M.L.-P.); lisset.suarezp23@gmail.com (L.S.-P.); lrp@matcom.uh.cu (L.R.P.-D.)
3 Universidad Panamericana, Facultad de Ciencias Económicas y Empresariales, Álvaro del Portillo 49, Zapopan, Jalisco 45010, México; gsosag@up.edu.mx
* Correspondence: orojas@up.edu.mx; Tel.: +52-3313682200
† Herrera-Macías, J.A.; Legón-Pérez, C.M.; Suárez-Plasencia, L.; Piñeiro-Díaz, L.R.; Rojas, G.; Sosa-Gómez, G. Effectiveness of Some Tests of Spatial Randomness in the Detection of Weak Graphical Passwords in Passpoint. In *Computer Science and Health Engineering in Health Services, Proceedings of the 4th EIA International Conference, COMPSE 2020, Virtual Event, 26 November 2020*; Springer International Publishing: Berlin/Heidelberg, Germany, 2021; pp. 173–183.

Abstract: This work demonstrates the ineffectiveness of the Ripley's K function tests, the distance to the nearest neighbor, and the empty space function in the Graphical Authentication scenario with Passpoint for the detection of non-random graphical passwords. The results obtained show that none of these tests effectively detect non-random graphical passwords; the reason for their failure is attributed to the small sample of the spatial pattern in question, where only the five points of the graphical password are analyzed. Consequently, a test based on mean distances is proposed, whose experiments show that it detects with good efficiency non-random graphical passwords in Passpoint. The test was designed to be included in the Graphical Authentication systems with Passpoint to warn the user about a possibly weak password during the registration phase, and in this way, the security of the system is increased.

Keywords: mean distance; Passpoint; weak graphical passwords; authentication; access control

Citation: Herrera-Macías, J.A.; Legón-Pérez, C.M.; Suárez-Plasencia, L.; Piñeiro-Díaz, L.R.; Rojas, O.; Sosa-Gómez, G. Test for Detection of Weak Graphic Passwords in Passpoint Based on the Mean Distance between Points. *Symmetry* **2021**, *13*, 777. https://doi.org/10.3390/sym13050777

Academic Editors: Weizhi Meng, Georgios Kambourakis and Jun Shao

Received: 8 April 2021
Accepted: 27 April 2021
Published: 30 April 2021

1. Introduction

The most traditional and standard method that we know of to authenticate ourselves in a system or computer is the use of user names and alphanumeric passwords. It happens that, practically, this method has been proven to be insecure [1]. Its insecurity is mainly due to the human factor, since users tend to use passwords that are easy to guess, leave the password in writing, in case it is a difficult one to remember, or use the same password for multiple authentication systems. This is why an important alternative to alphanumeric passwords today is graphical passwords. This is mainly due to the well-documented fact that humans are more adept at remembering images than text [2,3]. That is why graphical authentication systems base their security on the user recognizing images, or parts of them, instead of remembering long and complex sequences of characters. Among the Graphical Authentication techniques, the Passpoint [4–6] has received particular attention.

The Passpoint technique requires the user to select as their graphical password a set of five points (pixels) on an image in the so-called registration phase. Every time the user wants to authenticate, they must select five points in a neighborhood of the five points selected as his password during the registration phase [5,6]. For these graphical passwords to be considered secure, they must follow a random pattern; otherwise, they can be obtained by an attacker because they are weak passwords [1,3,7,8]. For this reason,

it is necessary to have a tool capable of alerting the user about a possible graphic password with insufficient randomness during the registration phase, thus increasing the password's security, and therefore, of the system.

Said graphical passwords can be interpreted as a point spatial pattern [9–15] of five points studied by the various techniques of the theory of spatial randomness to determine their behavior. Precisely, two of the tests mostly used in this area to verify spatial randomness are the Ripley's K function test [9,11,13,16–22], and the test of the distance to the nearest neighbor [9–11,17], which were tested in [23] to measure their effectiveness in detecting clustered graphical passwords in the Passpoint scenario. Within it, they concluded that both tests were not effective in detecting the clustered five-point patterns, but they did not conclude anything about the effectiveness of these tests in detecting regular five-point patterns; therefore, it was not possible to conclude whether these tests are not generally effective in detecting non-random five-point patterns. The experiments carried out in [23] were extended in this article to regular graphical passwords, and the effectiveness of a third test, the empty space function test, in detecting non-random passwords, was also analyzed. The experiments carried out in this article show that such tests are not effective in detecting non-random graphical passwords. Therefore, as the main result of this article, a new test was proposed based on the mean distance between the points of a graphical password that detects non-random graphical passwords with good precision.

Generative adversarial networks (GANs) [24] have recently been used to assess the strength of alphanumeric passwords and improve attacks against them. This technology appears to be another promising option for evaluating the strength of graphical passwords as well.

The proposed test can be applied to any Cued-Recall system that uses five points of an image as a graphic password. We also consider that it can be extendable to cases where the amount is greater than but close to 5, although the experiments that demonstrate it are pending.

In [25], five forms of symmetrical patterns were identified that tend to follow the passwords chosen by users: line shape, W shape, Z, V, or C. Approximately only 20% of graphical passwords chosen by users do not follow one of these forms.

This work experimentally demonstrates the ineffectiveness of Ripley's K function, the nearest neighbor technique, and the empty space F-function, which are three of the tests most used in the theory of spatial point patterns, in the Graphical Authentication scenario with Passpoint to validate whether a graphical password belongs to a random pattern. For this, two experiments were carried out to detect clustered patterns, and the other for regular patterns. The results obtained show that, in this scenario, both Ripley's K function test and the distance to the nearest neighbor were not effective in detecting clustering and it was theoretically demonstrated that they were incapable of detecting regularity; the space function test is theoretically shown to be unable to detect clustering and it is totally ineffective in detecting regular patterns. The results obtained were attributed to the small sample (only five points); the tests cannot differentiate between groups of five clustered, regular and random points. Consequently, a test based on the mean distance between the points of a password capable of efficiently detecting non-random graphical passwords was proposed. The experiments were carried out taking as reference dimensions of images of 1920×1080, 1366×768 and 800×480, since they are the most common sizes in personal computers and smartphones. However, the experiments can be extended to other dimensions of images obtaining similar results. All the point patterns and experiments were generated in MATLAB R2018a, using a PC Laptop with an Intel (R) Pentium (R) processor, CPU N5000@1.10GHz (2 CPUs), ~1.6 GHz and 4 GB of RAM.

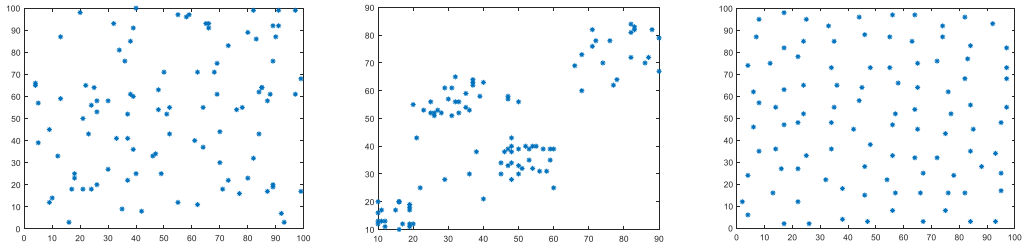
The work in this article is structured as five sections: Section 1 presents the introduction, then Section 2 is composed of spatial point patterns, Ripley's K function, G function, nearest neighbor distance and F function, empty space distance. Section 3 shows the evaluation of the classic tests most used in CSR in the Passpoint scenario; and Section 4 shows

our main contribution: the test for the detection of weak graphical passwords in Passpoint based on the mean distance between points. Finally, Section 5 presents the conclusions.

2. Preliminaries

2.1. Spatial Point Patterns

We call spatial point patterns [9,12,13,26–28] the set of data resulting from the representation by spatial coordinates (x, y) of phenomena that occur in some areas of space, such as earthquakes, plants or animal populations, epidemics, human settlements, among others. From the study of these spatial patterns, conclusions can be reached about the individual's behavior and distribution in each population. Traditionally, these patterns are classified as regular, random, or clustered. In the case of regular patterns, the probability of finding a point in the neighborhood of another is less than that of a random pattern, while in clustered patterns, the probability is higher. Examples of these three patterns are shown in Figure 1:



(**a**) (**b**) (**c**)

Figure 1. Random (**a**); clustered (**b**); and regular (**c**) point patterns, generated in MATLAB.

A spatial randomness test is usually used to classify a specific pattern in one of the three categories mentioned above. These tests assume the null hypothesis that the pattern has a random distribution; the alternative hypotheses are the regular distribution, clustered, or both [9,11,13,17]. In these analyses, two properties of the pattern are generally assumed: homogeneity (the pattern is translation invariant) and isotropism (the pattern is rotation invariant) [13,17,28]. Under these circumstances, the main characteristics of point patterns can be summarized by their first-order property—intensity; the expected number of points per unit area at any location; and by their second-order property, which describes the relationships between pairs of points.

2.2. Ripley's K Function

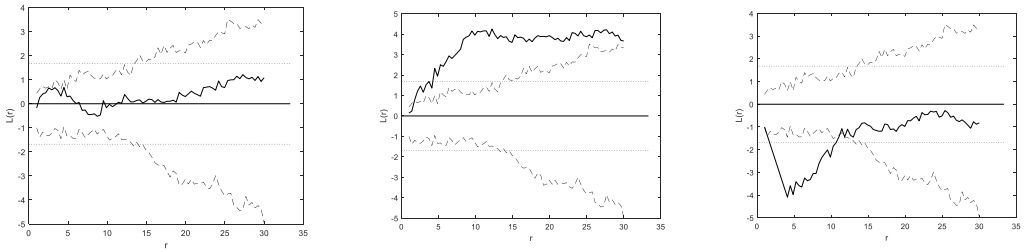
Ripley's K function is one of the most popular distance-based methods for spatial point pattern analysis. It is the cumulative average number of points lying within a distance r of a fixed point in the pattern. It is defined as

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

where n is the number of points in the pattern, A the area of the region under study, $k_{i,j}(r)$ is an indicator function that takes values of 1 if the Euclidean distance between points i and j is less than r and 0 otherwise, and $e_{i,j}(r)$ is the edge correction method. A detailed review of these methods can be found in [9,12,13,17]. Taking into account that a fixed point in the clustered pattern has more close neighbors than a fixed point in the random pattern, which in turn has more close neighbors than a fixed point in the regular pattern, then the interpretation of the results of $K(r)$ should be made by the comparison with the random (or Poisson) pattern πr^2 [9,18,22]. For this reason, values of $K(r) > \pi r^2$ indicate clustering, and values of $K(r) < \pi r^2$ indicate regularity, to the scale r considered.

In practice, the transformation $\hat{L}(r) = \sqrt{\frac{K(r)}{\pi}}$ is used more frequently, which stabilizes the variance of the function [9,13,17], and $L(r) = \hat{L}(r) - r$ sets the null hypothesis to the value 0; these transformations allow a clearer numerical and visual interpretation of the results. Consequently, a clustered pattern occurs when $L(r) > 0$ and a regular pattern occur, when $L(r) < 0$. To perform a hypothesis test with the function $K(r)$ (or the function $L(r)$), it is necessary to estimate the critical values, so we do this through Monte Carlo simulations [9,11,18,20]. We simulate a large number of random patterns with the same intensity and in the same area as the pattern under study, the value of the function is calculated for each of them and the maximum and minimum values are represented for each r reached. The null hypothesis, which would be that of complete spatial randomness (CSR), is rejected if the value of the observed function for some r falls outside the limits of the confidence interval. In some cases, it is not necessary to carry out the Monte Carlo simulation, since the critical limits of the distribution of the test statistic are approximated. Ripley showed [16,17] that for $L(r)$, in rectangular study areas, the approximate critical value with a significance level of $\alpha = 0.01$ is $\pm 1.68\sqrt{A}/n$.

In Figure 2, the function $L(r)$ is represented for each of the patterns in Figure 1—the continuous curve represents the value of the function $L(r)$ for the pattern in question,=; the solid line at $L(r) = 0$ represents the theoretical value of the null hypothesis of CSR; the dotted lines represent the confidence intervals for $\alpha = 0.01$ of the test according to Ripley's approximation: $\pm 1.68\sqrt{A}/n$; and the dashed lines represent the critical values obtained by 100 Monte Carlo simulations. As can be seen, for the random pattern (a), the function is within the confidence intervals, therefore the null hypothesis is accepted. For the clustered pattern (b), the function exceeds the upper limit of the confidence interval for $r > 2.5$ so the null hypothesis is rejected with a significance level of $\alpha = 0.01$ in favor of clustering for distances greater than 2.5. For the regular pattern (c), the function $L(r)$ has less values than the lower limit of the confidence interval for $r \in [2, 11]$, so the null hypothesis is also rejected in favor of clustering between the points at that scale.



(**a**) (**b**) (**c**)

Figure 2. Function $L(r)$ of the random (**a**), clustered (**b**), and regular (**c**) patterns of Figure 1.

2.3. G Function, Nearest Neighbor Distance

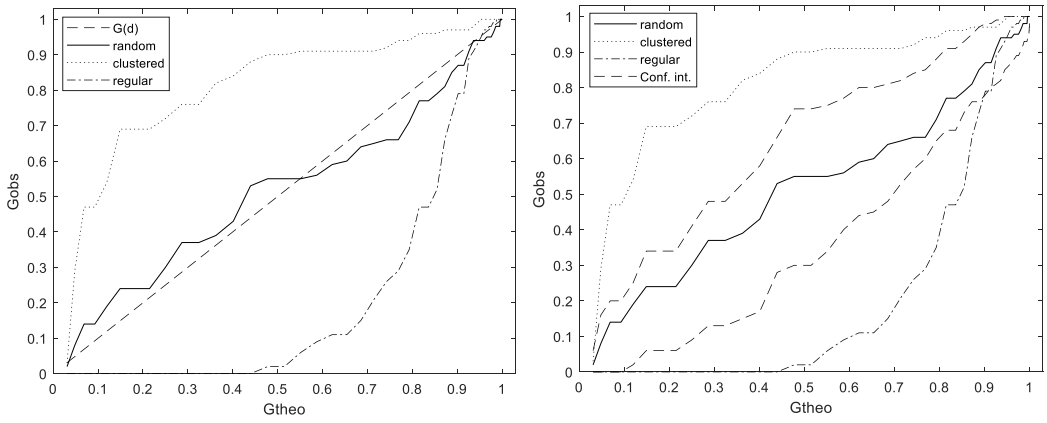
The nearest neighbor distance is an effective method to describe the behavior of spatial point patterns. If over an area, A are randomly distributed n points, the expected cumulative distribution function for the nearest neighbor distances will be given by the Poisson distribution, $G(d) = 1 - e^{-\lambda\pi d^2}$, where d is the distance from any point of the pattern to the closest point, and $\lambda = n/A$ its intensity. The function $G(d)$ represents the theoretical distribution of the pattern under the CSR hypothesis. To compare it with the distribution of the observed pattern, the function [9,11,13] is defined as

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

where n is the number of points in the pattern and $I_i(d)$ is the indicator function that takes the value of 1 if the Euclidean distance between point i and its closest neighbor is less than d, and 0 otherwise. For clustered point patterns, many of the distances between

the closest neighbors will be small; on the contrary, few distances will be small if it is a regular pattern. Therefore, a pattern with a value of $\hat{G}(d)$ greater than the value $G(d)$ is considered clustered, while another with a value of $\hat{G}(d)$ less than $G(d)$ is considered a regular pattern [9–11,13,17].

As for Ripley's K function, by means of Monte Carlo simulations, the critical values of the test that allow accepting or rejecting the null hypothesis of CSR are calculated. In Figure 3, the values of the function $\hat{G}$ are observed for each of the patterns in Figure 1, the critical values of the test were obtained through 100 Monte Carlo simulations. The test rejects the null hypothesis for the case of the clustered and regular patterns as they are above and below the estimated critical values, respectively.



(**a**) (**b**)

Figure 3. Comparison of the values of the function $\hat{G}(d)$ for the three prototypical patterns, using as a reference the theoretical distribution $G(d)$ (**a**), using the confidence intervals as a reference (**b**).

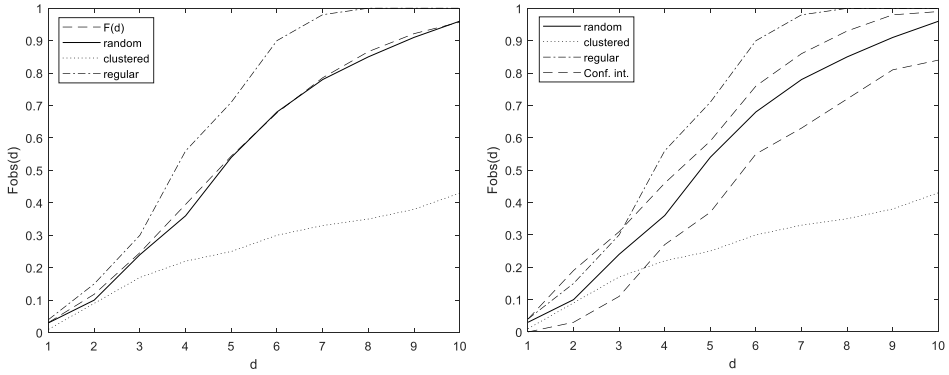
2.4. F Function, Empty Space Distance

The empty space distance measures the distance d from each point in an additional set m, called a grid, to the closest of the n points of the observed pattern. For a pattern under the CSR hypothesis, its distribution is the same as for the function $G(d)$, i.e., $F(d) = 1 - e^{-\lambda\pi d^2}$, where λ is the intensity of the pattern. For the estimation of the distances, a set of m points similar to the n of the observed pattern is usually used [17]. The distribution of the observed pattern is estimated by [9]

$$\hat{F}(d) = \frac{\sum_{j=1}^{m} I_j(d)}{m},$$

where m is the number of points on the grid and $I_j(d)$ is the indicator function that takes a value of 1 if the Euclidean distance between point j of the grid and its closest neighbor of the pattern is less than d; otherwise it takes value of 0. The use of the F function is similar to that of the G and K functions, using Monte Carlo simulations to estimate their critical values and graphic diagnostic tools in the same way. The interpretation of the deviations from the observed distribution, however, are opposite: values greater than those of the theoretical distribution indicate regularity, whereas smaller values indicate clustering. The F function is usually more effective at detecting CSR deviations towards clustering [17].

Figure 4 shows the values of the $\hat{F}$ function for each of the patterns in Figure 1: the critical values of the test were obtained through 100 Monte Carlo simulations; and the test rejects the null hypothesis for the case of the clustered and regular patterns as they are below and above the estimated critical values, respectively.



(**a**) (**b**)

Figure 4. Comparison of the values of the function $\hat{F}(d)$ for the three prototypical patterns, using as a reference the theoretical distribution $F(d)$ (**a**), using the confidence intervals as a reference (**b**).

3. Evaluation of the Classic Tests Most Used in CSR in the Passpoint Scenario

In these CSR tests, as the number n of pattern points decreases, the power of the test also decreases, and its ability to discern between different patterns is lost [29,30]—but what is the minimum value of n for these three tests to be considered accurate? We have not found this datum in the literature consulted. In [31], Ripley's K test and the nearest neighbor distance test were applied to a 22-point pattern, the smallest pattern we have as a reference for which both tests are applied; however, they did not conclude the result of said experiment or whether any of the tests were effective or not. In [31], they also experimented with a 36-point pattern for which they concluded that both tests were effective. So what will happen in the Passpoint scenario where patterns with only five points are available?

This question was given an initial answer in [23], but only for clustered patterns and only for Ripley's K and nearest neighbor tests, resulting in these tests not being effective in detecting graphical passwords clustered in Passpoint. This section expands the experiments carried out in [23] for a third CSR test, the empty space function F test, and also analyzes the detection of regular 5-point patterns by these three tests, thus allowing to conclude whether or not these tests are capable of detecting non-random patterns in a general way. Unlike [23], the experiments in this section were performed for 199 Monte Carlo simulations which guarantees, according to [9], a significance level of $\alpha = 0.01$.

3.1. Design of Experiments

To analyze the detection of non-random patterns in this section, two experiments were designed:

Experiment 1: To measure clustering, the three tests were applied to two databases, DB.1.1 and DB.1.2, of clustered graphic passwords. Said passwords were generated following a Poisson aggregate process with radius of 686 u and 315 u, respectively; therefore, they approximately delimited a maximum area equivalent to one fourth and eighth parts, respectively, of a rectangle of dimensions 1920×1080. We will refer to these databases as the first level of clustering and third level of clustering, respectively (the second level of clustering will be introduced in later experiments).

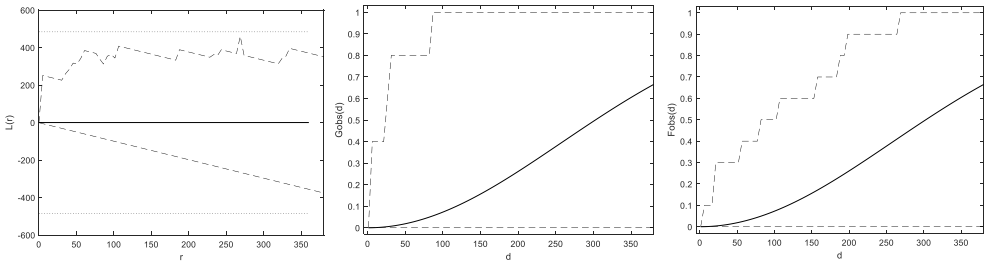
Experiment 2: For the second experiment, the three tests were applied to the xy pattern, with:

$$xy = [0\ \ 0;\ 1920\ \ 0;\ 1920\ \ 1080;\ 0\ \ 1080;\ 960\ \ 540]$$

being the pattern that expresses the maximum possible regularity for five points in the rectangle in question.

For each of the tests, the critical values were estimated using 199 Monte Carlo simulations of sets of five random points on a rectangle of size 1920×1080; in addition to Ripley's K function, the confidence intervals were estimated according to the approximation Ripley's $\pm 1.68\sqrt{A}/n$, where $A = 1920 \times 1080$ and $n = 5$. These Monte Carlo simulations guarantee

critical intervals with a significance level $\alpha = 0.01$ for each test [9], and can be seen in Figure 5, where the solid line represents the theoretical value of the null hypothesis, the dashed lines represent the critical values of each of the tests in 199 random pattern simulations, in the case of Ripley's K function, the dotted lines represent the confidence intervals for $\alpha = 0.01$ of the test according to Ripley's approximation.



(**a**) (**b**) (**c**)

Figure 5. Critical values of Ripley's K tests (**a**); the nearest neighbor (**b**); and empty space (**c**) for 199 Monte Carlo simulations. It is observed how the critical values coincide with the minimum value of each function.

From the estimated critical values, the immediate conclusion that was obtained is that Ripley's K function and the nearest neighbor tests are not effective in detecting regular patterns, and the empty space function test is not effective in detecting clustered patterns.

3.2. Results

3.2.1. Ripley's K Test Effectiveness

Ripley's K function test applied to DB.1.1 shows that only 531 of the 10,000 sets exceeded the critical values estimated for the Monte Carlo simulation test, which represent 5.31% of all the cases analyzed and only 25 of these sets of five points are above the confidence interval estimated by the Ripley approximation, which represent 0.25% of the cases analyzed. For the DB.1.2 of the 10,000 sets of points with second-level clustering, 2655 of them exceeded the critical values obtained by the Monte Carlo simulation for the test, which represents 26.55% of the total of cases analyzed; and 262 reported values of Ripley's K function as more significant than the confidence intervals estimated by the Ripley approximation, which represents 2.62% of the cases analyzed.

From the expression of the function $L(r)$, it is evident that its minimum possible value is $L(r) = -r$: this minimum value coincides with the critical values estimated by Monte Carlo simulations, therefore, it is impossible that this test detects a pattern as regular since a pattern is considered regular if it is below the critical values estimated by the test.

3.2.2. Nearest Neighbor Test Effectiveness

The results obtained by the distance to the nearest neighbor test for DB.1.1 show that only 188 of the 10,000 sets of five points with first-level clustering exceeded the critical values estimated for the test by Monte Carlo simulation, which represent 1.88% of all cases. In the experiment with the 10,000 sets of five points with second-level clustering of DB.1.2, only 890 sets exceeded the critical values obtained by Monte Carlo simulation, which represent 8.90% of the cases analyzed. The function $\hat{G}$ fulfills that $\hat{G}(d) \geq 0$, $\forall d$, and the lower critical interval estimated for this test is $\hat{G}(d) = 0$, and therefore, this test will not be able to detect clustered patterns either.

3.2.3. Effectiveness of the Empty Space Distance Test

Like the $\hat{G}$ function, the minimum value that the $\hat{F}$ function can take is 0. This minimum value coincides with the lower critical values estimated by Monte Carlo simulations; therefore, this test cannot detect clustered patterns. Of the 10,000 iterations of the test of function

F for the pattern xy, which expresses the greatest possible regularity between 5 points in a rectangle, it turns out that none of them detect said pattern as regular.

3.3. Discussion of the Results

3.3.1. Clustering Detection

The F function test is totally ineffective in detecting clustering in Passpoint since the lower critical values were estimated using Monte Carlo simulations to coincide with their theoretical minimum value. Despite the visible clustering of the graphical passwords generated in DB.1.1 and DB.1.2, as shown in Figure 6, both Ripley's K test and the nearest neighbor test were ineffective in detecting the DB.1.1 sets as clustered. Ripley's K test offered the best results, which detected only 5.31% of the cases. In the database DB.1.2, it was expected that the function has a better success rate due to the strong clustering of the sets. However, these patterns of points belonging to the second level of clustering are unlikely to be found in practice since it would suppose selecting the five points in an area equivalent to one eighth of the image area, something unlikely that a responsible user will do, a graphical password with these characteristics would undoubtedly offer inadequate security. However, experiments with DB.1.2 confirm the ineffectiveness of both tests in detecting clustering in five-point patterns. Once again, the best results were obtained by Ripley's K test, which detected 26.55% of the cases, a considerable improvement compared to the 5.31% obtained for DB.1.1, but a very discreet value yet to be considered effective as it fails in more than 73% of the cases analyzed. These results are summarized in Table 1, where the "-" means that the corresponding test is not applicable in this case.

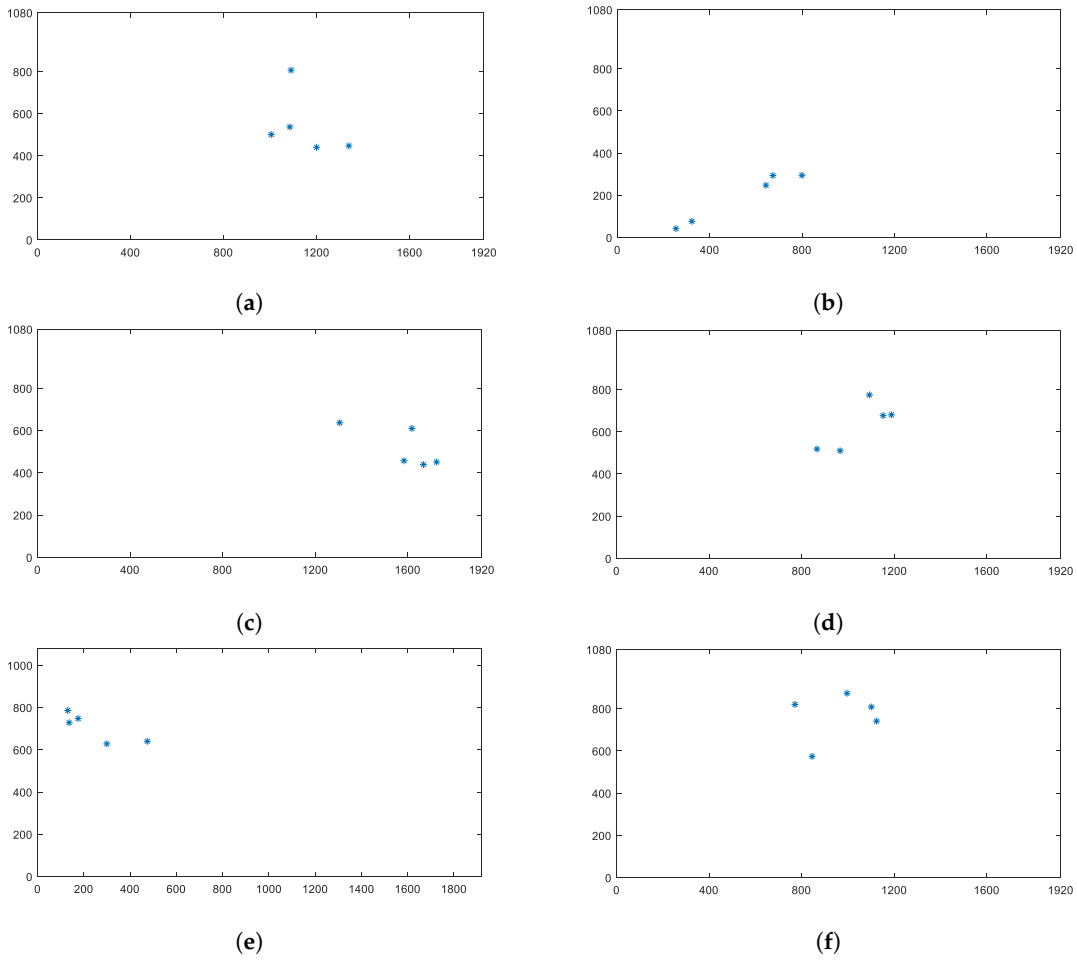


Figure 6. Some visibly clustered graphical passwords of DB.1.1 (**a**–**c**) and DB.1.2 (**d**–**f**) which were not detected by the tests presented.

Table 1. Percentage of non-random graphical passwords detected by each test in each experiment.

	DB.1.1	DB.1.2	xy
Empty space	-	-	0%
Ripley's K	5.31%	26.55%	-
Nearest neighbor	1.88%	8.90%	-

3.3.2. Regularity Detection

The lower critical values estimated using Monte Carlo simulations coincide with the minimum values that the $L(r)$ and $\hat{G}(d)$ functions can reach; therefore, the tests of the Ripley's K function and the nearest neighbor are totally ineffective at detecting regular patterns in this scenario. For its part, the test of the empty space function F was not able to detect any of the 10,000 iterations made to the pattern xy as regular, xy the one being the pattern that expresses the maximum possible regularity between five points in a rectangle. These results are summarized in Table 1.

4. Test for Detection of Weak Graphical Passwords in Passpoint Based on the Mean Distance between Points

The main reason that the classical tests presented above were constructed using the Monte Carlo method is that the theoretical distribution, even for simple point patterns, could be mathematically unknown or intractable; therefore, this method is used whose main advantage is its easy application to estimate the mean, the sample distribution of the test statistic and the confidence intervals. This method has one main disadvantage: it involves randomness; therefore, the values obtained may change if the process is repeated. This brings a certain loss of power to the test that, together with the small sample typical of our scenario, leads to the results set out above. Therefore, our approach to finding a spatial randomness test capable of detecting non-random graphical passwords in Passpoint with good efficiency will be to find a test statistic that allows us to differentiate between random, clustered, and regular passwords—and whose sample distribution is calculable. In this way, a hypothesis test could be built without using the typical Monte Carlo simulations and thus avoiding its intrinsic randomness and associated loss of power.

4.1. Statistic and Sampling Distribution

The statistic that is proposed to be used is that of the mean distance between the points of the pattern, in this case, the five points corresponding to the graphical password. It is not possible to assume the normal distribution of the mean in this scenario due to the small sample size ($n = 10 < 30$) [32]. In order to estimate the sampling distribution of the mean distance between 5 points, the following experiment was carried out:

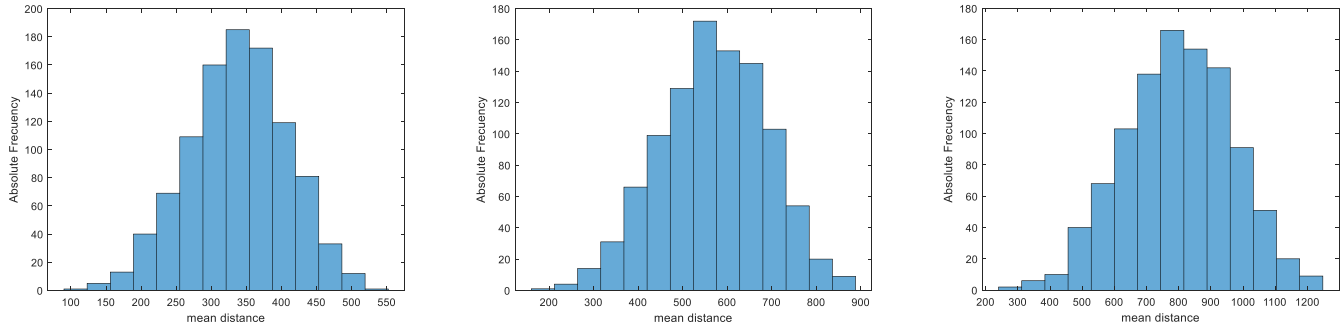
Experiment 3: 1000 sets of five random points were generated on three different image sizes—800 × 480, 1366 × 768 and 1920 × 1080—sizes which were selected for being the most common in the use of computers and smartphones. For each of these 1000 sets, their mean distances were found, so there are three databases of 1000 random mean distances, each DB.2.1, DB.2.2, and DB.2.3 respectively, for each one of the image sizes.

Results of experiment 3: Figure 7 shows the frequency histograms for each of the databases found; the histograms have the traditional symmetric bell shape, so the data seem to come from a normal distribution.

It was estimated that the intervals cover the parameters for said distribution $\mu_1 \in [333, 342]$, $\sigma_1 \in [68, 74]$ for DB.2.1; $\mu_2 \in [562, 576]$, $\sigma_2 \in [115, 126]$ for DB.2.2 and $\mu_3 \in [787, 808]$, $\sigma_3 \in [161, 175]$ for DB.2.3 to the 95%. In [33], they present a formula to determine the expected mean distance between two random points within a rectangle of dimensions a, b:

$$E(L) = \frac{1}{3}(a^2+b^2)^{1/2} + \frac{a^2}{6b} ln\left(\frac{b+(a^2+b^2)^{1/2}}{a}\right) + \frac{b^2}{6a} ln\left(\frac{a+(a^2+b^2)^{1/2}}{b}\right) - \frac{(a^2+b^2)^{5/2}}{15a^2b^2} + \frac{a^5+b^5}{15a^2b^2},$$

therefore, we can precisely calculate at $\mu_1 = 339$, $\mu_2 = 568$ and $\mu_3 = 798$, that these values approximately coincide with the mean value of their respective confidence intervals; on the other hand, $\sigma_1 = 71$, $\sigma_2 = 120$ and $\sigma_3 = 168$ were estimated by point estimation. These parameter values and the estimated normal distribution to which each database fits are shown in Table 2. Figure 8 shows the fit of each database to its standardized normal distribution, and in each case the visual fit is good.

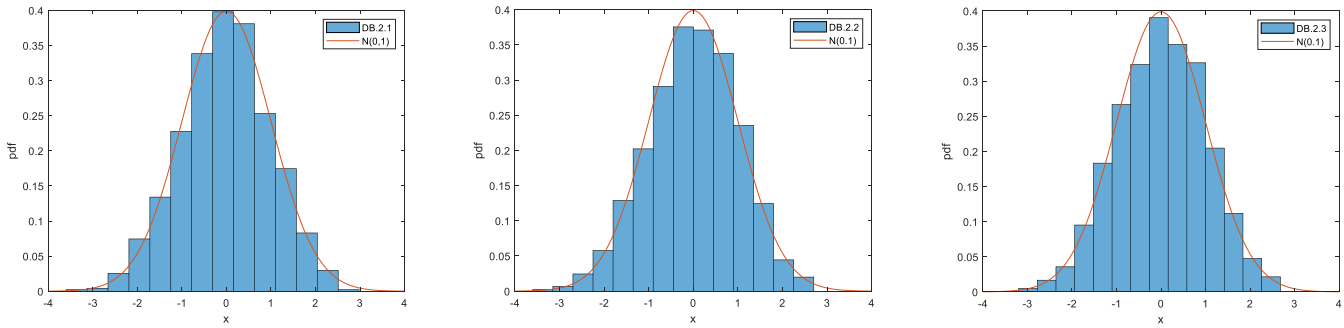


(**a**) (**b**) (**c**)

Figure 7. Histogram of databases DB.2.1 (**a**); DB.2.2 (**b**); and DB.2.3 (**c**).

Table 2. Parameters and estimated normal distribution for each of the databases DBs.2 1, 2.2, 2.3.

Dimension	μ		σ		Estimated
	Interval	Estimate	Interval	Estimate	Distribution
800×480	$[333, 342]$	339	$[68, 74]$	71	$N(339, 71)$
1366×768	$[562, 576]$	568	$[115, 126]$	120	$N(568, 126)$
1920×1080	$[787, 808]$	798	$[161, 175$	168	$N(798, 168)$



(**a**) (**b**) (**c**)

Figure 8. Adjustment of each of the databases DB.2.1 (**a**), DB.2.2 (**b**) and DB.2.3 (**c**) to the normal standard $N(0, 1)$.

Three normality tests were applied to check whether DBs.2.1, 2.2, 2.3 came from a normal distribution: Anderson–Darling, Kolmogorov–Smirnov and chi-square. The results are shown in Table 3.

Table 3. Normality test applied to data from DBs.2.1, 2.2, and 2.3. The three tests accept with a high p-value that the data come from a normal distribution with a significance level $\alpha = 0.05$.

	Anderson–Darling			**Kolmogorov–Smirnov**			**Chi-Squared**		
	DB.2.1	**DB.2.2**	**DB.2.3**	**DB.2.1**	**DB.2.2**	**DB.2.3**	**DB.2.1**	**DB.2.2**	**DB.2.3**
Result	Accepted			Accepted			Accepted		
Significance level (α)	0.05			0.05			0.05		
p-valor	0.778	0.452	0.768	0.590	0.461	0.687	0.406	0.779	0.881

4.2. Construction of the Proposed Test

The proposed test is a classical hypothesis test. Let X be the random variable of the distance two by two between five random points; the sample in each case will be the 10 resulting distances, this sample is rather small in the sense of the Central Limit Theorem, however, it was already shown previously that $\bar{X}$ distributes normally, therefore, the test statistic $Z = \frac{\bar{X}-\mu_i}{\sigma_i}$ $(i = 1, 2, 3)$ distributes $N(0, 1)$ in each case. Since under the randomness hypothesis, a 5-point graphical password has a mean distance of μ_i, then it can be assumed that those graphical passwords whose mean distances are significantly different from μ_i come from a non-random pattern. In that sense, it can be found in the left hand tail or the right hand tail of the distribution: if it is the left tail, the distances between the points will be less than the mean, so the evidence points to a clustered pattern; if it is the right tail, the distances between the points are greater than the mean, so the evidence points towards a regular pattern. In the case of non-random patterns, the hypotheses of the test will be the following:

- Null hypothesis H_0: the points have a mean distance of μ_i so they are assumed to be random.
- Alternative hypothesis H_1: the points have a mean distance other than μ_i so they are assumed to be non-random.

The significance level α can be set by the user or system, depending on the level of non-randomness that one wishes to allow in the password. The critical region of the test will be $\{z : Z < -z_{\alpha/2} \text{ or } Z > z_{\alpha/2}\}$.

4.3. Experimental Validation of the Proposed Test

In order to estimate the errors made by the proposed test and check if they conform to the known theoretical errors of the normal distribution, the following experiments were carried out:

Experiment 4: It is well known that the error that was committed for a normal distribution in the intervals may be $[\mu - \sigma, \mu]$, $[\mu - 2\sigma, \mu - \sigma]$, $[\mu - 3\sigma, \mu - 2\sigma]$, $[0, \mu - 3\sigma]$ from the left tail and $[\mu, \mu + \sigma]$, $[\mu + \sigma, \mu + 2\sigma]$, $[\mu + 2\sigma, \mu + 3\sigma]$, $[\mu + 3\sigma, +\infty]$ from the right tail. In order to estimate in the proposed test, the probability that the Z statistic belongs to each of these intervals and to compare whether they correspond to the known theoretical probabilities, 10,000 sets of five random points were generated in each of the image sizes, obtaining three databases DB.3.1, DB.3.2, DB.3.3 of 10,000 random graphic passwords each.

Results of experiment 4: The result of the experiment for each of the estimated distributions $N(339, 71)$, $N(568, 120)$, $N(798, 168)$ are shown in the Table 4.

Table 4. Comparison between the estimated and theoretical probabilities that Z belongs to one of the intervals from the left or right tail of the distribution.

Intervals	Observed Error			Theoretical Error
	DB.3.1 $(\mu = 339, \sigma = 71)$	**DB.3.2** $(\mu = 568, \sigma = 120)$	**DB.3.3** $(\mu = 768, \sigma = 168)$	
$[\mu - \sigma, \mu]$	31.64%	31.42%	32.52%	34.1%
$[\mu, \mu + \sigma]$	34.88%	34.98%	35.01%	
$[\mu - 2\sigma, \mu - \sigma]$	14.19%	14.61%	13.99%	13.6%
$[\mu + \sigma, \mu + 2\sigma]$	14.82%	14.93%	14.51%	
$[\mu - 3\sigma, \mu - 2\sigma]$	2.59%	2.49%	2.32%	2.1%
$[\mu + 2\sigma, \mu + 3\sigma]$	1.76%	1.44%	1.53%	
$[0, \mu - 3\sigma]$	0.09%	0.08%	0.08%	0.1%
$[\mu + 3\sigma, +\infty]$	0.03%	0.05%	0.04%	

As can be seen, for the three image sizes, the estimated probabilities that the statistic Z of the test belongs to each of the intervals from the left and right tails of the distribution fit well with the theoretical probabilities. This contributes to the validity and accuracy of the test.

Experiment 5: To experimentally verify the type I error committed by the test, it was applied to each of the sets of databases DBs.3.1, 3.2, and 3.3 for five of the most common significance levels α : 0.2, 0.1, 0.05, 0.02, 0.01.

Experiment results 5: Table 5 shows how the frequency obtained in the experiment for each of the databases of random graphic passwords detected as non-random by the proposed test is adjusted to the theoretical probabilities.

Table 5. Comparison between the I error made by the test and the expected theoretical error.

	Type I Error Observed		
	DB.3.1	**DB.3.2**	**DB.3.3**
$\alpha = 0.2$	0.2111	0.2071	0.2028
$\alpha = 0.1$	0.1019	0.0964	0.0970
$\alpha = 0.05$	0.0500	0.0452	0.0446
$\alpha = 0.02$	0.0159	0.0158	0.0142
$\alpha = 0.01$	0.0056	0.0075	0.0057

The type I errors observed and those expected for the proposed test fit well for the five levels of significance analyzed in each image.

Experiment 6: To measure the proposed test's effectiveness, five non-random graphic password databases were generated for each image, of which three were clustered passwords and two were regular. The clustered databases were generated following a Poisson aggregate process; the regular ones were generated establishing inhibition distances.

- For the image 800 × 480, the aggregation distances were 175 u, 145 u, and 125 u of the radius, obtaining the clustered databases DB.5.1.1, DB.5.1.2, and DB.5.1.3, respectively; the regular databases DB.5.2.1 and DB.5.2.2 were generated by inhibition distances of 140 u and 220 u, respectively.
- For the image 1366 × 768, the aggregation distances were 290 u, 240 u, and 210 u of the radius, obtaining the clustered databases DB.6.1.1, DB.6.1.2, and DB.6.1.3, respectively; the regular databases DB.6.2.1 and DB.6.2.2 were generated by inhibition distances of 210 u and 350 u, respectively.
- For the image 1920 × 1080, the aggregation distances were 410 u, 335 u, and 290 u of the radius, obtaining the clustered databases DB.7.1.1, DB.7.1.2, and DB.7.1.3,

respectively; the regular databases DB.7.2.1 and DB.7.2.2 were generated by inhibition distances of 300 u and 505 u, respectively.

It should be noted that the first aggregation distances in each of the image dimensions (175 u, 290 u, 410 u) determine graphic passwords that cover approximately a maximum area equivalent to a quarter of the total area of their respective images—a fact which will generally assumed to refer to databases DBs.5.1.1, 6.1.1, 7.1.1 as first level clustering. Similarly, the second distances (145 u, 240 u, 335 u) determine approximately one sixth of the area of their respective images and generalize the databases DBs.5.1.2, 6.1.2, 7.1.2 as the second level of clustering and the third distances (125 u, 210 u, 290 u) of one eighth, generalizing the databases (DBs.5.1.3, 6.1.3, 7.1.3) as the third level of clustering. The databases DBs.5.2.1, 6.2.1, 7.2.1 will be generalized as the first level of regularity and the databases DBs.5.2.2, 6.2.2, 7.2.2 as the second level of regularity.

Experiment results 6: In Tables 6–8, the estimates of type II error are shown, through the number of non-random graphical passwords detected by the test proposed, for each of the image dimensions respectively.

Table 6. Estimation of the probability of committing an error of type II by the test proposed in the image 800 × 480 for the clustered passwords of DBs.5.1.1, 5.1.2, 5.1.3 and regular DBs. 5.2.1, 5.2.2.

Significance	Estimated Type II Error				
Level	DB.5.1.1	DB.5.1.2	DB.5.1.3	DB.5.2.1	DB.5.2.2
$\alpha = 0.2$	0.0075	0.0000	0.0000	0.1879	0.0000
$\alpha = 0.1$	0.0613	0.0001	0.0000	0.3859	0.0126
$\alpha = 0.05$	0.2003	0.0016	0.0000	0.5046	0.0686
$\alpha = 0.02$	0.4621	0.0481	0.0018	0.6234	0.2107
$\alpha = 0.01$	0.6504	0.1856	0.0265	0.6936	0.3543

Table 7. Estimation of the probability of committing an error of type II by the test proposed in the image 1366 × 768 for the clustered passwords of DBs.6.1.1, 6.1.2, 6.1.3 and regular DBs.6.2.1, 6.2.2.

Significance	Estimated Type II Error				
Level	DB.6.1.1	DB.6.1.2	DB.6.1.3	DB.6.2.1	DB.6.2.2
$\alpha = 0.2$	0.0084	0.0000	0.0000	0.1956	0.0000
$\alpha = 0.1$	0.0680	0.0000	0.0000	0.4005	0.0129
$\alpha = 0.05$	0.2215	0.0012	0.0000	0.5109	0.0741
$\alpha = 0.02$	0.4891	0.0473	0.0015	0.6253	0.2270
$\alpha = 0.01$	0.6744	0.1817	0.0242	0.6982	0.3844

Table 8. Estimation of the probability of committing an error of type II by the test proposed in the image 1920 × 1080 for the clustered passwords of DBs.7.1.1, 7.1.2, 7.1.3 and regular DBs.7.2.1, 7.2.2.

Significance	Estimated Type II Error				
Level	DB.7.1.1	DB.7.1.2	DB.7.1.3	DB.7.2.1	DB.7.2.2
$\alpha = 0.2$	0.0085	0.0000	0.0000	0.1928	0.0000
$\alpha = 0.1$	0.0697	0.0000	0.0000	0.3930	0.0127
$\alpha = 0.05$	0.2236	0.0013	0.0000	0.5079	0.0700
$\alpha = 0.02$	0.4893	0.0439	0.0013	0.6241	0.2189
$\alpha = 0.01$	0.6640	0.1774	0.0202	0.6921	0.3714

A comparison between the three tables shows that the type II errors made by the proposed test for each image size are similar. This visual comparison is provided in Figure 9 for clustered passwords, and in Figure 10 for regular passwords.

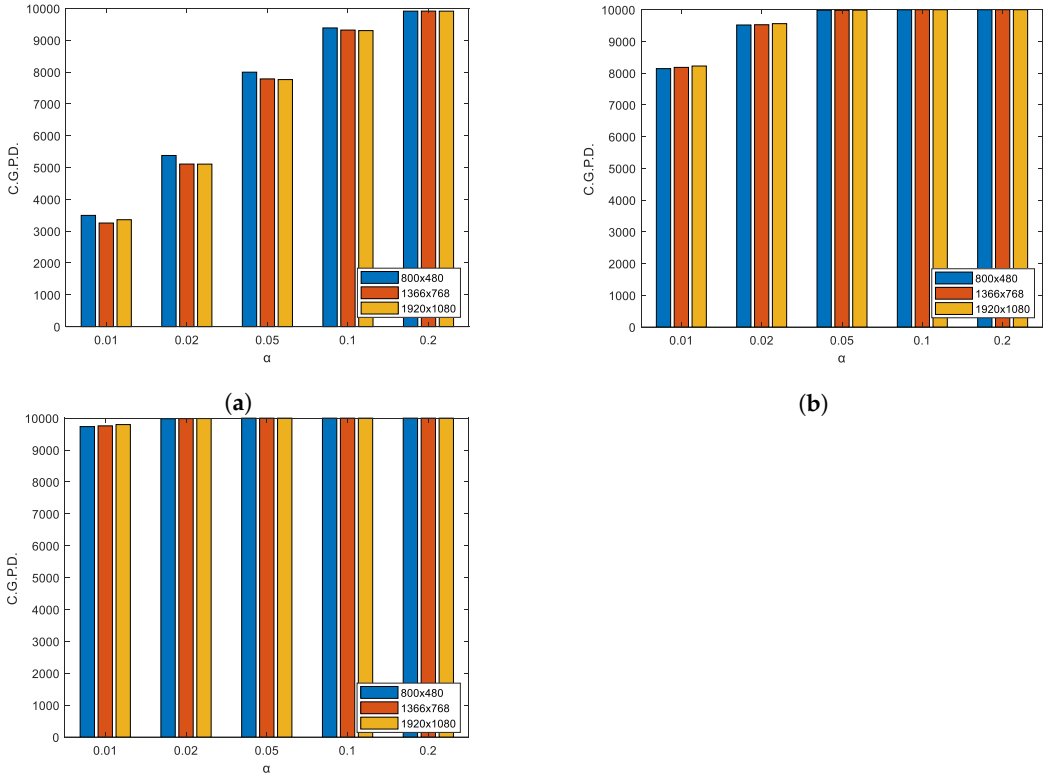


Figure 9. Comparison between the number of clustered graphic passwords detected (C.G.P.D) by the test in each of the images for each of the levels of significance analyzed at the three levels of clustering analyzed: first level (**a**), second level (**b**), third level (**c**).

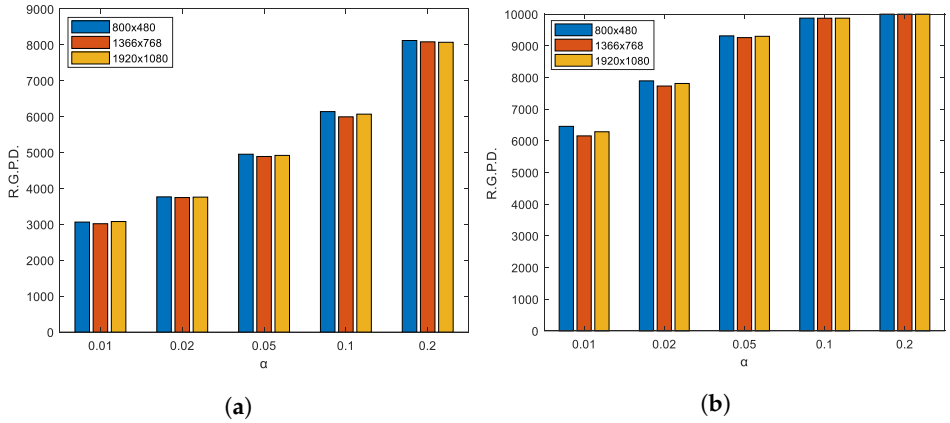


Figure 10. Comparison between the number of regular graphic passwords detected (R.G.P.D) by the test in each of the images for each of the levels of significance analyzed at the two levels of regularity analyzed: first level (**a**), second level (**b**).

4.4. Discussion of the Results

In Table 5 it can be seen how the errors of type *I* made by the test are very close for each of the three dimensions of the images analyzed; the same happens for errors of type *II* (Figures 9 and 10) in each of the levels of clustering and regularity analyzed for the three sizes of images. Therefore, it is possible to discuss the results and conclude regardless of the size of the image used.

The theoretical errors committed in the standard normal distribution are adjusted to those observed in the experiments, which validates and gives reliability to the proposed test. The same happens for the error of type *I* committed, which closely matches those observed

experimentally for the test for each of the significance levels $\alpha \in \{0.2, 0.1, 0.05, 0.02, 0.01\}$. The test turned out to be quite effective in detecting the graphical passwords clustered in a general way. For the first clustering level analyzed, the best detection rates were reached for the levels $\alpha = 0.2$ and $\alpha = 0.1$ for which it detects more than 99% and 93% of passwords, respectively, and for the other three levels tested, the detection rate was close to 71.5%, 51% and 32.5% for the levels $\alpha = 0.05$, $\alpha = 0.02$, and $\alpha = 0.01$, respectively. For the 2nd level of clustering, the test detected all the graphical passwords analyzed for the $\alpha = 0.2$ level, more than 99.8 % for the levels $\alpha = 0.1$ and $\alpha = 0.05$ and approximately 93 % and 81% for the levels $\alpha = 0.02$ and $\alpha = 0.01$. For the case of the third level of clustering, the test detected all the passwords analyzed for the levels $\alpha = 0.2$, $\alpha = 0.1$ and $\alpha = 0.05$; more than 99% for level $\alpha = 0.02$ and more than 97% for level $\alpha = 0.01$.

In the case of regularity, the proposed test turns out to be less effective compared to clustering, for the databases corresponding to the first level of regularity, the test detected 80%, 59.9%, 48% , 37% and 30%, respectively, for each of the significance levels $\alpha = 0.2$, $\alpha = 0.1$, $\alpha = 0.05$, $\alpha = 0.02$, $\alpha = 0.01$. For the second level of regularity, the detection levels reached were 100%, 98.7%, 92.5%, 77% and 61.5% for each of the significance levels, respectively.

Although the selection of the optimal α parameter is left to the choice of the user or the system, it should be noted that values of $\alpha \leq 0.02$ minimize the probability of type *I* error but are not very sensitive to non-random passwords, as it fails in more than 48% of the cases for clustered passwords and in more than 62% for regular passwords; on the other hand, a value of $\alpha \geq 0.2$ would be susceptible to non-randomness, but in turn, it would detect more than one out of five random passwords as clustered. Therefore, the recommended significance levels are $\alpha = 0.1$ and $\alpha = 0.05$, highlighting the $\alpha = 0.1$ level that guarantees the detection of more than 93% of clustered passwords and more than 60% of the regular ones—this being the level of significance recommended by the authors for general purposes. However, a user or system with high-security requirements might want to default to the $\alpha = 0.2$ level, which achieves the detection of more than 99% of clustered passwords and more than 80% of regular passwords with the disadvantage of erroneously detecting one random one out of five.

4.5. Comparison of the Proposed Test with the CSR Tests Analyzed in Passpoint

Table 9 shows the comparison between the proposed test, Ripley's K function, the nearest neighbor distance test, and the empty space function in terms of the effectiveness in detecting random non-graphical passwords in Passpoint. The comparison was made considering the image size of 1920×1080 and the significance level $\alpha = 0.01$. This comparison is valid for the other two sizes of images studied since, as mentioned above, the proposed test's detection values are similar in each one of them.

Table 9. Comparison of the non-random password detection levels between the CSR tests and the proposed test.

	1st Level of Clustering	**3rd Level of Clustering**	***xy***
Empty space	-	-	0%
Ripley's K	5.31%	26.55%	-
Nearest neighbor	1.88%	8.90%	-
Proposed test	33.6%	97.98%	Detected

The difference between the proposed test's effectiveness and the classic ones is evident, so it leaves no doubt from our point of view of its superiority in the Passpoint scenario. The most notable difference is perhaps in the regular patterns, since the classic tests could not detect even the most regular pattern possible. In contrast, the proposed test detects it in more than 99.9% of the cases and detects it with good effectiveness compared to other levels of regularity (Figure 10).

4.6. Application of the Test Proposed in Passpoint

The proposed spatial randomness test was designed to be included in the Graphic Authentication systems with the Passpoint technique so that it allows the system to check the security of a password established by the user during the registration phase. The level of significance, and therefore the level of non-randomness to be allowed, must be established in advance by the user or by the system itself depending on its security requirements. For general purposes, $\alpha = 0.1$ is recommended; for high levels of security, it would be best to use $\alpha = 0.2$. The test would be executed by following the following steps:

Step 1: The user selects the five points (pixels) of their password on an image (it is assumed that the image selected by the user or those offered by the system are of one of the following dimensions 800×480, 1366×768 or 1920×1080);

Step 2: Calculate the mean distance between the points of the set password;

Step 3: Calculate the Z statistical according to the dimension of the chosen image;

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

Step 5: If the statistic calculated in step 3 does not belong to the critical region, the password is accepted and the registration phase ends. If it falls in the critical region, the user is notified that the password is weak (depending on whether it falls in the critical region of the left or right tail of the distribution, the user can be notified about the type of weak, clustered or regular password respectively) and returns to step 1. These steps are shown in Figure 11.

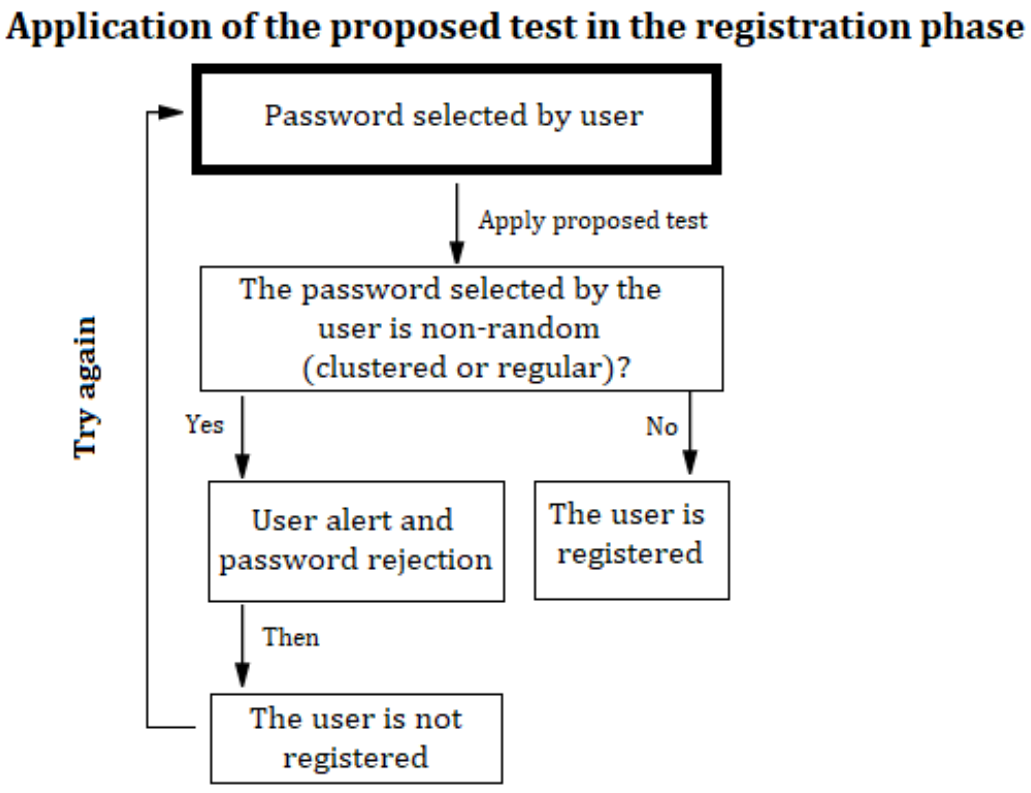


Figure 11. Application diagram of the proposed test to a Passpoint Graphic Authentication system.

Example 1. *Let (982, 318); (729, 379); (550, 435); (1289, 571); (1056, 266), be five points corresponding to a graphical password, on an image of size* 1920×1080 *and* $\alpha = 0.1$*:*

$H_0 : \mu_0 = 798$

$H_1 : \mu_0 \neq 798$

$$Z = \frac{\bar{X} - \mu_0}{\sigma} = \frac{399 - 798}{168} = -2.375$$

$$-Z_\alpha = -Z_{0.1} = -1.645 > -2.375$$

Therefore, it is rejected that the points have a mean distance of 798 and therefore that they are random, in favor of the fact that the mean distance is significantly different from 798, and therefore that the points are clustered with a significance level of 10%.

5. Conclusions and Future Work

The experiments show that Ripley's K tests, the distance to the nearest neighbor and the empty space function, despite being some of the most used tests in the detection and characterization of non-random patterns, are not effective in the detection of non-random graphical passwords in the Passpoint scenario, where these passwords only consist of five points. Consequently, a test was proposed based on the mean distance between the five points of a graphical password that allows detecting non-random graphical passwords with good effectiveness. It was shown that the mean distances between sets of five points follow a normal distribution, which made it possible to carry out a hypothesis test and classify the observed patterns of points into clustered or regular according to the negative or positive deviation, respectively, of the mean distance observed with respect to the mean calculated for random patterns, the normal distribution also allows knowing the theoretical errors committed by the test, thus avoiding the intrinsic randomness of the confidence intervals characteristically obtained for these CSR tests using Monte Carlo simulations. The estimated probabilities that the Z statistic belongs to each of the intervals of the left tail and right tail of the distribution fit the known theoretical probabilities for the normal distribution, and the observed probability of making a type error I is adjusted with each of the five significance levels analyzed $\alpha = 0.2$, $\alpha = 0.1$, $\alpha = 0.05$, $\alpha = 0.02$, $\alpha = 0.01$. The experiments carried out show that the test is effective in general to detect non-random graphical passwords, being particularly effective in detecting clustered patterns in which it managed to detect approximately 94%, 99% and 100% of the three clustering levels, respectively, analyzed for the significance level $\alpha = 0.1$ recommended by the authors for general use. The regular pattern detection values reached were 60% and 98%, respectively, for the two levels of regularity analyzed with the significance level $\alpha = 0.1$; these values, although more discrete than the clustering ones, represent the greatest difference concerning the classic CSR tests compared, since their effectiveness in detecting regular patterns was 0%. The application proposed for the test was to alert a user about a possible non-random (and therefore weak) password during the registration phase in a system that has Graphic Authentication implemented as a security system using Passpoint.

It is suggested to explore two aspects in future works: first, the application of GAN to evaluate the strength of graphic passwords; second, symmetric patterns due to their non-random nature are potentially detectable by our test; however, the necessary experiments and the criteria to discern between each pattern are left proposed; a possible approximation would be to use the maximum likelihood estimator, as done in [34].

Although the analyzes carried out in this article were made in particular for images of the dimensions 800×480, 1366×768 and 1920×1080, as they are the most used sizes in ordinary computers and smartphones, and are extensible to images of any other dimension.

Author Contributions: Conceptualization, J.A.H.-M., C.M.L.-P., L.R.P.-D. and L.S.-P.; methodology, J.A.H.-M., C.M.L.-P., G.S.-G., O.R. and L.R.P.-D.; validation, J.A.H.-M., C.M.L.-P., G.S.-G.; formal analysis, J.A.H.-M., L.R.P.-D., L.S.-P., C.M.L.-P., O.R. and G.S.-G.; investigation, J.A.H.-M., C.M.L.-P., L.R.P.-D., L.S.-P., O.R. and G.S.-G.; writing—original draft preparation, J.A.H.-M., C.M.L.-P., L.R.P.-D., L.S.-P., O.R. and G.S.-G.; writing—review and editing, J.A.H.-M., C.M.L.-P., L.R.P.-D., O.R. and G.S.-G.; visualization, J.A.H.-M. and L.S.-P.; supervision, J.A.H.-M., C.M.L.-P., L.R.P.-D., L.S.-P., O.R. and G.S.-G.; project administration, C.M.L.-P. and O.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: This research was developed within the framework of the project "Mathematical Investigations of Modern Cryptography for the Development of the Computerization of the Cuban Society (PN223LH010-024)" of the Basic and Natural Sciences program of the ACC.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rittenhouse, R.G.; Chaudry, J.A.; Lee, M. Security in Graphical Authentication. *Int. J. Secur. Its Appl.* **2013**, *7*, 347–356
2. Itti, L.; Koch, C. Computational modelling of visual attention. *Nat. Rev. Neurosci.* **2001**, *2*, 194. [CrossRef] [PubMed]
3. Valdés, O.R.; Legón, C.C.M. Patrones en el orden de los clics y su influencia en la debilidad de las claves de la Técnica de Autenticación Gráfica Passpoints. *Rev. Cuba. Cienc. Inform.* **2019**, *12*, 37–47.
4. Shammee, T.I.; Akter, T.; Mou, M.; Chowdhury, F.; Ferdous, M.S. A Systematic Literature Review of Graphical Password Schemes. *J. Comput. Sci. Eng.* **2020**, *14*, 163–185. [CrossRef]
5. Rodriguez Valdés, O.; Legón, C.M.; Socorro Llanes, R. Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica. *Rev. Cuba. Cienc. Inform.* **2018**, *12*, 13–27.
6. Wiedenbeck, S.; Waters, J.; Birget, J.C.; Brodskiy, A.; Memon, N. Passpoints: Design and longitudinal evaluation of a graphical password system. *Int. J. Hum.-Comput. Stud.* **2005**, *63*, 102–127. [CrossRef]
7. Gao, H.; Jia, W.; Ye, F.; Ma, L. A survey on the use of graphical passwords in security. *JSW* **2013**, *8*, 1678–1698. [CrossRef]
8. Van Oorschot, P.C.; Thorpe, J. Exploiting predictability in click-based graphical passwords. *J. Comput. Secur.* **2011**, *19*, 669–702. [CrossRef]
9. Baddeley, A.; Rubak, E.; Turner, R. *Spatial Point Patterns: Methodology and Applications with R*; CRC Press: Boca Raton, FL, USA, 2015; ISBN 978-1-4822-2021-7.
10. Boots, B.N.; Getis, A. *Point Pattern Analysis*; Web Book Version, 2020; Sage Publication:Thousand Oaks, CA, USA, 1988; ISBN 0803922450/9780803922457.
11. Caballero, Y. Test de Aleatoriedad Para Procesos Puntuales Espaciales Basado en el Cálculo de la Dimensión Fractal. Master's Thesis, Universidad Nacional de Colombia, Bogotá, Colombia, 2017.
12. Yates, L.A.; Brook, B.W.; Buettel, J.C. Spatial pattern analysis of line segment data in ecology. *bioRxiv*, **2021**. [CrossRef]
13. Wieg, T.; Moloney, K.A. *Handbook of Spatial Point-Pattern Analysis in Ecology*; CRS Press: Boca Raton, FL, USA, 2014; ISBN 978-1-4200-8255-5.
14. Araújo, E.S.B.; Scalon, J.D.; Batista, L.S. Exploratory spectral analysis in three-dimensional spatial point patterns. *Rev. Bras. Biom.* **2021**, *39*, 177–193. [CrossRef]
15. Baddeley, A.; Nair, G.; Rakshit, S.; McSwiggan, G.; Davies, T.M. Analysing point patterns on networks—A review. *Spat. Stat.* **2021**, *42*, 100435. [CrossRef]
16. Arbia, G.; Espa, G.; Giuliani, D.; Dickson, M.M. Effects of Missing Data and Locational Errors on Spatial Concentration Measueres Based on Ripley's K-Function. *Spat. Econ. Anal.* **2017**, *12*, 326–346. [CrossRef]
17. De la Cruz, M. *Métodos Para Analizar Datos Puntuales*; Universidad Rey Juan Carlos, Servicio de Publicaciones: Madrid, Spain, 2008; pp. 75–127. ISBN 978-84-9849-308-5.
18. Sporring, J.; Waagepetersen, R.; Sommer, S. Generalizations of Ripley's K-function with Application to Space Curves. In *Information Processing in Medical Imaging*; Chung, A., Gee, J., Yushkevich, P., Bao, S., Eds.; Springer: Cham, Switzerland, 2019. [CrossRef]
19. Nastaran, M.; Zamiri, M.R. Quantitative evaluation of spatial distribution of land use in Bojnord Using Ripley's K function. *Geogr. Space* **2018**, *18*, 273–289.
20. Kopczewska, K. Distance-Based Measurement of Agglomeration, Concentration and Specialisation. *Meas. Reg. Spec.* **2017**, 173–216. [CrossRef]
21. Ripley, B.D. Tests of "Randomness" for Spatial Point Patterns. *J. R. Stat. Soc.* **1979**, *41*, 368–374. [CrossRef]
22. Schabenberger, O.; Gotway, C.A. *Statistical Methods for Spatial Data Analysis*; CRS Press: Boca Raton, FL, USA, 2004.
23. Herrera-Macías, J.A.; Legón-Pérez, C.M.; Suárez-Plasencia, L.; Piñeiro-Díaz, L.R.; Rojas, G.; Sosa-Gómez, G. Effectiveness of Some Tests of Spatial Randomness in the Detection of Weak Graphical Passwords in Passpoint. In *Computer Science and Health Engineering in Health Services, Proceedings of the 4th EIA International Conference, COMPSE 2020, Virtual Event, 26 November 2020*; Springer International Publishing: Berlin/Heidelberg, Germany, 2021; pp. 173–183.
24. Nam, S.; Jeon, S.; Kim, H.; Moon, J. Recurrent GANs Password Cracker For IoT Password Security Enhancement. *Sensors* **2020**, *20*, 3106. [CrossRef]
25. Chiasson, S.; Forget, A.; Biddle, R.; Oorschot, P.C. User interface design affects security: Patterns in click-based graphical passwords. *Int. J. Inf. Secur.* **2009**, *8*, 387. [CrossRef]
26. Diggle, P.J. *Statistical Analysis of Spatial and Spatio-Temporal Point Patterns*, 3rd ed.; Chapman and Hall/CRC: Boca Raton, FL, USA, 2014.
27. Gelfand, A.E.; Fuentes, M.; Hoeting, J.A.; Smith, R.L. *Handbook of Environmental and Ecological Statistics*; CRS Press: Boca Raton, FL, USA, 2019; ISBN 9780367731786.
28. Nakoinz, O.; Knitter, D. *Modelling Human Behaviour in Landscapes*; Springer: Berlin/Heidelberg, Germany, 2016; ISBN 978-3-319-29536-7.
29. Perry, G.L.W.; Miller, B.P.; Enright, N.J. A comparison of Methods for the Statistical Analysis of Spatial Point Patterns in a Plant Ecology. *Plant Ecol.* **2006**, *187*, 59–82. [CrossRef]
30. Plotkin, J.B.; Potts, M.D.; Leslie, N.; Manokaran, N.; LaFrankie, J.; Ashton, P.S. Species-area curves, spatial aggregation, and habitat specialization in tropical forests. *J. Theor. Biol.* **2000**, *207*, 81–99. [CrossRef]

31. Rozas, V.; Camarero, J.J. Técnicas de análisis espacial de patrones de puntos aplicados en ecología forestal. *Invest Agrar Sist Recur*, **2005**, *14*, 79–97. [CrossRef]
32. Dodge, Y. *The Concise Encyclopedia of Statistics*; Springer:Berlin/Heidelberg, Germany, 2009; ISBN 978-0-387-32833-1.
33. Gaboune, B.; Laporte, G.; Soumis, F. Expected Distances Between Two Uniformly Distributed Random Points in Rectangles and Rectangular Parallelepipeds. *J. Oper. Res. Soc.* **1993**, *44*, 513–519. [CrossRef]
34. Bormashenko, E.; Legchenkova, I.; Frenkel, M. Symmetry and Shannon Measure of Ordering: Paradoxes of Voronoi Tessellation. *Entropy* **2019**, *21*, 452. [CrossRef] [PubMed]