New Test to Detect Graphic Passwords Clustered in Passpoints, Based on the Perimeter of the Convex Hull

Joaquín Alberto Herrera-Macías , Lisset Suárez-Plasencia , Carlos Miguel Legón-Pérez , Guillermo Sosa-Gómez * , Omar Rojas

Posted Date: 23 May 2024

doi: 10.20944/preprints202405.1502.v1

Keywords: Passpoints; Convex hull; Clustered graphical passwords; Authentication

 doi:10.20944/preprints202405.1502.v1

Article

New Test to Detect Graphic Passwords Clustered in Passpoints, Based on the Perimeter of the Convex Hull

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

[1] Instituto de Criptografía, Facultad de Matemática y Computación, Universidad de la Habana, Habana 10400, Cuba; lisset.suarez@matcom.uh.cu (L.S.P.); joaquin.herrera@matcom.uh.cu (J.A.H.M); clegon58@gmail.com (C.M.L.P.)
[2] Facultad de Ciencias Económicas y Empresariales, Universidad Panamericana, Álvaro del Portillo 49, Zapopan, Jalisco 45010, Mexico; gsosag@up.edu.mx (G.S.G.), orojas@up.edu.mx (O.R.)
* Correspondence: gsosag@up.edu.mx; Tel.: +52-3313682200

Abstract: This research paper presents a new test based on a novel approach for identifying clustered graphical passwords within the Passpoints scenario. Graphical authentication methods serve as a viable alternative to the conventional alphanumeric password-based authentication method, which is susceptible to known weaknesses arising from user-generated passwords of this nature. The test proposed in this study is based on estimating the distributions of the perimeter of the convex hull. This perimeter is calculated based on the points users select as passwords within an image measuring 1920 × 1080 pixels. The test is formulated once the optimal theoretical distributions that fit the data are identified. Evaluating the proposed test's effectiveness involves estimating type I and II errors. In this study, we compare the effectiveness and efficiency of the proposed test with existing tests from the literature that can detect this type of pattern in Passpoints graphic passwords. Our findings indicate that the new test demonstrates a significant improvement in effectiveness compared to previously published tests. Furthermore, the joint application of the two tests also shows improvement. Depending on the significance level determined by the user or system, the enhancement results in a higher detection rate of clustered passwords, ranging from 0.1% to 8% compared to the most effective previous methods. This improvement leads to a decrease in the estimated probability of committing a type II error. In terms of efficiency, the proposed test outperforms several previous tests; however, it falls short of being the most efficient. It can be concluded that the newly developed test demonstrates the highest effectiveness and the second-highest efficiency level compared to other tests available in the existing literature for the same purpose.

Keywords: passpoints; convex hull; clustered graphical passwords; authentication

1. Introduction

Studies conducted by various researchers [1,2] indicate that using alphanumeric passwords as an authentication method is not advisable due to the vulnerabilities arising from users' password creation practices. The primary vulnerabilities in the security of this password type stem from users' improper selection of characters during the registration process and their tendency to reuse passwords across multiple websites. To facilitate memorization, passwords are typically designed to be short, with limited character variation, and frequently incorporate personal information, thereby enhancing the potential for unauthorized access by imposters [3]. The utilization of artificial intelligence in a recent application aimed at compromising alphanumeric passwords serves as additional evidence for implementing alternative authentication methods [4]. As a means of addressing this issue, graphical passwords have emerged as a potential solution. These authentication systems offer a significantly larger password space compared to alphanumeric passwords. The efficiency of this approach relies on the human capacity to recognize and recall patterns in visual representations, as opposed to memorizing lengthy and intricate sequences of characters [5,6].

The Passpoints system, developed by Wiedenbeck in 2005 [7], is notable for its security and usability compared to other cued-recall type systems [8]. The process involves the user choosing a sequence of five points within an image during the registration phase to serve as their password.

 doi:10.20944/preprints202405.1502.v1

During the process of authentication, it is imperative for the user to accurately and precisely repeat the sequence in the correct order, adhering to the specific tolerance set by the system. The system's weaknesses are evident in the quality of the images chosen by the user or system, the presence of predictable patterns in password creation, and the use of discretization mechanisms that decrease the password space and provide valuable information for conducting dictionary attacks.

To enhance the security of Passpoints, it is crucial to incorporate tools during the registration phase that can notify users about the weakness of their graphic passwords. Additionally, implementing a method during the authentication phase to assess the level of authenticity for each user is equally important. Several articles have been published in recent years addressing the topic at hand. For instance, in the work by [9], a probabilistic model of graphic authentication is proposed for the authentication phase. This model enables the practical measurement of the level of authenticity for each user, categorizing them as high, medium, low, or shallow. Only users with high or medium authenticity levels are authenticated based on the results obtained. In [10] and [11], two spatial randomness tests were introduced to identify non-random, clustered, and regular graphical passwords in Passpoints. These tests were developed in response to the limited effectiveness of traditional tests in verifying complete spatial randomness in this specific scenario [10,12]. Recently, the joint application of the previously mentioned tests has been proposed by [13], making it the most effective alternative currently available as of the time of writing this article. Finally, the proposal presents two tests [14,15] that are proven effective in identifying patterns characterized by points that exhibit a linear or near-linear shape, commonly called smooth patterns. These recent contributions have positioned this graphic authentication system as a viable alternative to conventional authentication methods, offering enhanced security and usability.

The convex hull of a set of n points in the plane is a fundamental concept in computational geometry [16–19], being the convex hull of a set of points the smallest convex polygon that contains all the points of the set [16,19–21], whose efficient implementation is an ongoing area of research [22–26] with applications in various fields. However, there is a lack of references to applications related to security issues, such as the one presented in this work. There exist several algorithms for computing the convex hull, whose complexities are of the order $O(n^3), O(n^2), O(n \log n)$. However, in the specific scenario considered in this study, where the n points are randomly distributed, the complexity can be reduced to a linear function of the n of $O(n)$ points.

The primary attributes of the convex hull of a set of points in the plane include its perimeter, area, and the number of vertices. There have been studies on the statistical properties when the number of points tends to infinity [27–29]. Additionally, the convex hull of a random walk determined by an ordered set of points can be calculated, and the statistical properties of this convex hull have also been investigated [30,31]. Research in this field has primarily concentrated on examining the mean limit values of the functional of the convex hull [29], assuming some properties for the set of n points. Currently, the distribution of the perimeter of the convex hull of a random set of points in the plane remains unknown for a finite and significantly small number of points.

This study presents a novel spatial randomness test that can effectively identify graphic passwords clustered in the Passpoints scenario. In this study, a comparative analysis is conducted to evaluate the effectiveness and efficiency of the proposed test in detecting a specific pattern in the graphic passwords of Passpoints. The comparison is made with other tests found in the existing literature that can identify similar patterns. All the implementations and experiments were conducted using M.A.T.L.A.B. R2018a to compare the tests on a P.C. Laptop equipped with an AMD Athlon Silver 3050U processor, running at 2.30GHz, and with 8 G.B. of RAM. The work is organized into five sections: Section 1 1, Introduction, provides an overview of the study; Section 2 2 presents the preliminaries, Passpoints, and known tests to detect graphic passwords in the Passpoints scenario; section 3 3 presents our contribution, which is a new test designed to detect graphical passwords clustered in Passpoints; Section 4 4 shows the comparison with the antecedents; and finally, Section 5 5 presents the conclusions drawn from the study and outlines potential future research directions.

 doi:10.20944/preprints202405.1502.v1

2. Preliminaries

2.1. Passpoints

Using graphical passwords has emerged as a potential solution to address the primary challenge associated with alphanumeric passwords, namely, the user's struggle to remember highly secure passwords. Alphanumeric passwords typically consist of alphabets with up to 90 symbols. The standard length for these passwords, as recommended by the National Institute of Standards and Technology (N.I.S.T.) [32], is eight characters. This results in a total key space of $90^8 = 4.3 \times 10^{15}$. In the context of Passpoints systems, the key space about outdated image resolutions of 800×480 pixels is $V_5^{800\times480} = 8.3 \times 10^{25}$. Since $10^{15} << 10^{25}$, Passpoints not only outperforms alphanumerics in terms of usability but also in terms of security. Graphical authentication methods can be categorized into three groups: Recognition Based Technique, Recall Based Technique, and Cued-Recall Based Technique [33]. The cued-recall type systems distinguish themselves from previous systems due to their unique characteristic of only necessitating users to recall and concentrate on specific locations within an image. This feature aims to alleviate users' cognitive burden by providing a simplified alternative to memorizing a complex array of characters.

Passpoints are notable within the category of graphical authentication systems of the *cued-recall* type due to their commendable combination of usability and security. The system's usability involves the user's selection of five points within an image to serve as their password during the registration phase. The user can either choose the image themselves or have one the system provides. In the authentication process, the user must select the points chosen during the registration phase within a specified neighborhood or tolerance region and in the same sequential order. However, despite the security provided by the large password space, not all images are appropriate for use in Passpoints. One vulnerability of this technique is the potential attack on the points most likely to be selected in the image, commonly referred to as Hotspots in the literature [34]. The recommendation in [7] is to enhance the security of this technique by selecting an image with hundreds of Hotspots that are evenly distributed throughout. Other vulnerabilities arising from user actions, irrespective of the image itself, include the inadvertent selection of specific regions within the image, such as the edges or the center, and the inherent interdependence often observed among the chosen points, such as the password [35,36]. These interdependencies among points are referred to as point patterns [37]. Hackers can exploit the predictability of certain patterns in graphical passwords through various techniques to gain unauthorized access. Therefore, graphical passwords should adhere to a random pattern to maintain security. The strength of a graphical password is compromised when the points are not distributed randomly. Several common non-random patterns have been identified in the study conducted by [38].

2.2. Known Tests to Detect Graphical Passwords Clustered in Passpoints

In this subsection, we present and describe some known tests to detect graphical passwords clustered in Passpoints.

First, we present a test based on the average distance between the points. In [10], an effective spatial randomness test was proposed to detect non-random graphical passwords in Passpoints. Concluding that the mean distances between the 5 points of a graphic password follow a normal distribution, a two-tailed hypothesis test was constructed to differentiate between clustered, random, and regular graphic passwords. Their experiments demonstrated the overall effectiveness of the test in detecting non-random graphic passwords, with a particular emphasis on its ability to identify clustered patterns. They further demonstrated that the efficacy of the intervention is independent of the image size chosen by the user or system. Utilizing an image of dimensions 1920×1080 pixels as a point of reference, the authors created three distinct databases characterized by varying levels of clustering. In the three levels of clustering examined, the test successfully identified approximately 94%, 99%, and 100% of the passwords analyzed at a significance level $\alpha = 0.1$, as recommended by the authors for widespread application.

 doi:10.20944/preprints202405.1502.v1

A test was proposed in [11] that is based on the average of the perimeters of the Delaunay triangles. The study focuses on identifying non-random graphic passwords composed of five clustered or regularly positioned points. The analysis involves conducting a two-tailed test that is centered around the mean of the perimeters of the Delaunay triangles. The perimeters are transformed using the Johnson SB [39] transformation to ensure normality. To effectively implement this test, the authors have underscored the importance of considering the selected image size, as the Johnson SB parameters vary depending on the image sizes. As in the previous test, passwords were simulated for the same clustering levels. A reference image of 1920×1080 pixels was used, and it was determined that the effectiveness of the test does not depend on the size of the image selected. For the three levels of clustering, the test yielded detection rates of 87.07%, 99.66%, and 100%, respectively, with a significance level of $\alpha = 0.1$. Their results showed that clustering detection is more accurate than regularity.

A joint application of the previous tests in Passpoints. Both tests were designed to be included in graphic authentication systems with the Passpoints technique to enable the system to check the randomness of a password established by the user during the registration phase. Figure 1, extracted from the work of [13], illustrates the schematic representation of the joint application of both tests during the Passpoints registration phase. The authors' decision to initially employ the test utilizing mean distances between points is justified by its greater efficiency and effectiveness. This approach enables the prompt rejection of non-random passwords with high accuracy. Until the time of this publication, this joint test was the one that reported the most significant effectiveness in detecting clustered graphic passwords. Table 1 shows the number of clustered graphical passwords detected using the joint application of both tests for each of the three clustering levels, consisting of 10,000 passwords each.

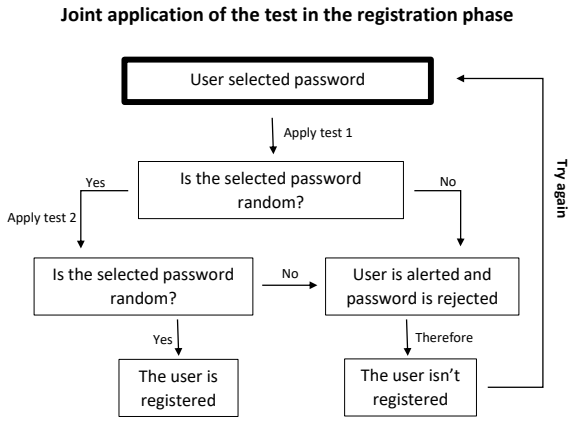


Figure 1. Joint application scheme of the known tests to detect graphic passwords in Passpoints.

Table 1. number of clustered graphical passwords detected using the joint application of both tests for each of the three clustering levels, consisting of 10 000 passwords each. Taken from [13].

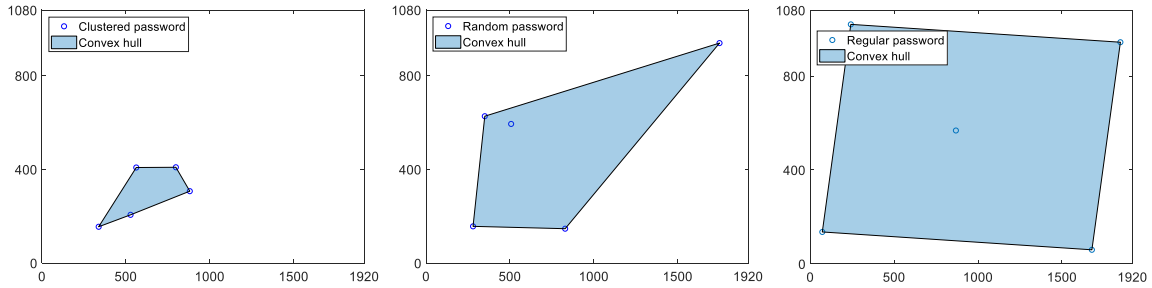
Significance level	1st clustering level	2nd clustering level	3rd clustering level
0.2	9 922	10 000	10 000
0.1	9 358	10 000	10 000
0.05	7 931	9 987	10 000
0.02	5 365	9 576	9 987
0.01	3 652	8 300	9 805

 doi:10.20944/preprints202405.1502.v1

3. Our Contribution: New Test to Detect Graphic Passwords Clustered in Passpoints

3.1. Our Hypothesis

The graphic passwords clustered in Passpoints can be characterized as those with points concentrated in a smaller image area. Considering the above, the hypothesis proposes using the perimeter of the convex hull delimited by the five points as an indicator of the clustering measure of the points. Figure 1 shows the convex hull determined by three graphic passwords with patterns of clustering (a), randomness (b), and regularity (c), respectively. Figure 2 supports the proposed hypothesis.



(a) (b) (c)

Figure 2. Convex hull determined by the points of a clustered (a), random (b), and regular (c) password.

Knowing the probability distribution that best fits the perimeter of the convex hull delimited by five randomly distributed points on the image would enable the development of a hypothesis test capable of differentiating between the three alternative patterns with a predetermined significance level, α.

3.2. Estimate of the Probability Distribution of the Perimeter of the Convex Hull

The following experiment was conducted to determine the probability distribution of the perimeter of the convex hull formed by five points uniformly distributed on an image with dimensions of 1920×1080 pixels.

Experiment 1: A total of 1 000 graphical passwords were randomly distributed over an image with dimensions of 1920×1080 pixels were simulated. For each of these passwords, the perimeter of the convex hull they determine was calculated, resulting in a database (DB.1) of 1 000 real values that can be analyzed. To assess the goodness of fit of the data to various probability distributions, we utilized the EasyFit v.5.6 software.

Results of Experiment 1: The data showed an excellent fit to the Johnson SB distribution with parameters $\gamma = -0.65612$, $\delta = 1.5922$, $\lambda = 4575.1$, $\xi = 495.15$. Figure 3 illustrates the fit of the Johnson SB distribution to the data. Three goodness-of-fit tests were used to measure the fit of the data: Anderson-Darling, Kolmogorov-Smirnov, Chi-Square; Table 2 shows the results of these tests.

 doi:10.20944/preprints202405.1502.v1

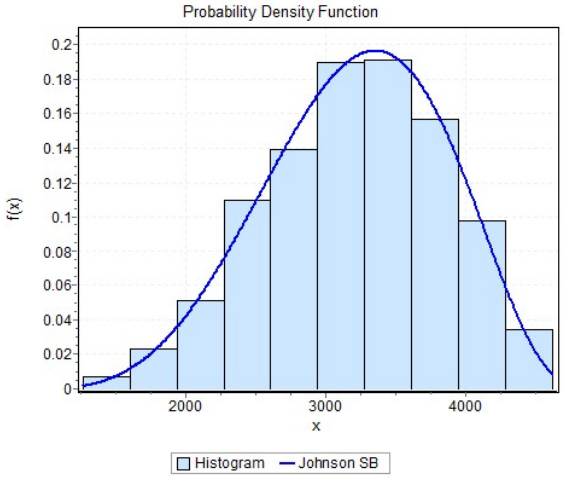


Figure 3. Histogram of the perimeter database of the convex hull and its fit to a Johnson SB distribution.

Table 2. Results of the goodness-of-fit tests applied to the Johnson SB distribution estimated from the data contained in DB.1, for the significance levels $\alpha \in \{0.02, 0.01, 0.05, 0.1, 0.2\}$.

Goodness-of-fit test	Kolmogorov-Smirnov	Chi-Square	Anderson-Darling
p-value	0.98139	Accepted	0.79775
Accepted for each α	5/5	5/5	5/5

Knowing these results, it is assumed that the distribution sought is a Johnson SB, whose parameters are shown in Table 3.

Table 3. Parameters of the Johnson SB distribution $(\gamma, \delta, \lambda, \xi)$ of the perimeter of the convex hull $P_{P_{EC}} \sim J_{SB}(\gamma, \delta, \lambda, \xi)$.

Image size	γ	δ	λ	ξ
1920×1080	-0.65612	1.5922	4575.1	495.15

3.3. Hypothesis Test Based on the Perimeter of the Convex Hull

Once the probability distribution is known as a Johnson SB, the practical application of this criterion is facilitated by considering the desirable characteristic of the Johnson SB distribution, which can be transformed into a standard Normal distribution. Applying the transformation

$$P_{EC}^{N} = J_{SB}(P_{EC}) = \gamma + \delta \times ln[(P_{EC} - \xi)/(\lambda + \xi - P_{EC})], \tag{1}$$

using the parameters of Table 3, it is obtained that $P_{E.C.}^{N} \sim N(0,1)$, where $P_{E.C.}^{N}$ represents the perimeter of the convex hull after performing the Johnson SB transformation. Using this property, the definition of a clustered graphical password detection test is reduced to applying a mean test for the standard Normal distribution $P_{E.C.}^{N}$.

The proposal consists of a two-tailed test based on the perimeter of the convex hull delimited by the 5 points of a graphic password. The Johnson S.B. transforms these points into a standard Normal distribution. To apply this test, the image size that the user selects must be considered, as the estimated parameters for the Johnson SB distribution depend on it.

 doi:10.20944/preprints202405.1502.v1

3.3.1. Definition of the Proposed Test

The null hypothesis

$$H_0 : E[P^N_{E.C.}] = 0$$

is proposed, indicating that the graphic password selected by the user is random if the transformation through the Johnson SB of the perimeter of the convex hull to a standard Normal distribution is equal to 0. As an alternative hypothesis, we have

$$H_1 : E[P^N_{E.C.}] \neq 0$$

if the evidence is less than zero, which indicates clustering; otherwise, it indicates regularity. As a test statistic, the Johnson SB transformation of the perimeter of the convex hull is bounded by the points of a graphic password

$$Z = J_{SB}(P_{P_{EC}}) = \gamma + \delta \times ln[(P_{P_{EC}} - \xi)/(\lambda + \xi - P_{P_{EC}})], \tag{2}$$

with the selection of values for the parameters according to the size of the image, with critical region $\{z : Z < -z_{\alpha/2} \text{ or } Z > z_{\alpha/2}\}$, where α is the significance level previously established by the user or system.

3.3.2. Evaluation of the Effectiveness of the Proposed Test

According to the definition of the test, obtaining values of $E[P^N_{E.C.}] > 0$ would indicate a pattern of regularity. However, the results obtained in this aspect during the experiments are not significant compared to those reported by previous studies. Therefore, it is not necessary to include them in this article. In this section, only the results concerning the detection of clustered patterns are reported, which constitutes the main contribution of this work. The following experiments were conducted to estimate the type I and type II errors made by the proposed test.

Experiment 2: To estimate the probabilities of committing a Type I error, we simulated 10 000 new graphic passwords. The points in these passwords were randomly distributed over the image. These passwords are clustered in the database and labeled as DB.2. The proposed test was applied to each of these passwords, and the number of false positives obtained for each significance level were counted for $\alpha \in \{0.2, 0.1, 0.05, 0.02, 0.01\}$. The results of experiment 2 are summarized in the following Table 4.

Table 4. Comparison between the I error made by the test ($\hat{\alpha}$) and the expected theoretical error (α).

α (theoretical)	$CR.$ of H_0	$\hat{\alpha_1}$ DB.2
0.2	$Z < -1.282$ *or* $Z > 1.282$	0.2029
0.1	$Z < -1.645$ *or* $Z > 1.645$	0.1019
0.05	$Z < -1.960$ *or* $Z > 1.960$	0.0535
0.02	$Z < -2.326$ *or* $Z > 2.326$	0.0234
0.01	$Z < -2.575$ *or* $Z > 2.575$	0.0136

In each case, the estimated probability of committing a type I error corresponds to the predetermined theoretical significance levels. Observe that this proper adjustment is only expected if the procedures carried out up to the moment of adjusting to the Johnson SB distribution and its subsequent transformation are correct. Therefore, these values contribute to the validity of the proposed test.

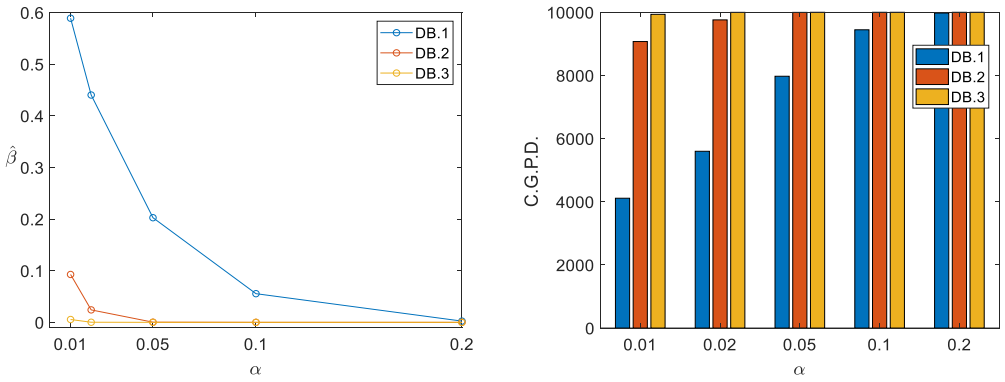
Experiment 3: To evaluate the effectiveness of the proposed test in detecting clustered graphical passwords, a total of 30 000 graphical passwords distributed across three clustering levels were generated. The first clustering level, DB.3.1, comprises 10 000 graphical passwords generated using an aggregation distance of 410 pixels. The second clustering level, DB.3.2, comprises 10 000 graphical passwords generated using an aggregation distance of 335 pixels. The third level, DB.3.3, comprises

 doi:10.20944/preprints202405.1502.v1

10 000 graphical passwords generated using a 290-pixel aggregation distance. The proposed test was applied to each of these passwords, and the number of passwords detected for each clustering level was recorded, obtaining an estimate of the type II error committed. Table 5 and Figure 4 present the estimation of the probability of committing a type II error. Figure 4 illustrates the number of clustered passwords detected by the test for each database.

Table 5. Estimated probability ($\hat{\beta}$) on DB.3.1, DB.3.2, DB.3.3 of accepting a pooled graphical password as a random password.

Significance level	Critical Region	($\hat{\beta}$) DB.3.1	($\hat{\beta}$) DB.3.2	($\hat{\beta}$) DB.3.3
0.2	$-1.282 < Z < 1.282$	0.0024	0	0
0.1	$-1.645 < Z < 1.645$	0.0555	0	0
0.05	$-1.960 < Z < 1.960$	0.2026	0.0003	0
0.02	$-2.326 < Z < 2.326$	0.4402	0.0241	0.0002
0.01	$-2.575 < Z < 2.575$	0.5889	0.0927	0.0055



(a) (b)

Figure 4. Estimated probability $\hat{\beta}$ of commit a II type error (a), clustered graphic passwords detected (C.G.P.D.) by the proposed test (b).

The obtained results provide evidence of the validity and effectiveness of the proposed test. Observe that while for DB.3.1, the minimum detection value recorded is 41.1%, for DB.3.2 and DB.3.3, the values exceed 90.7% and 99.4%, respectively. This is a clear sign that the test becomes more effective with the increase in the clustering level, which is consistent with the formulated hypothesis. The test is particularly effective for the significance levels $\alpha = 0.1$ and $\alpha = 0.2$, achieving detection rates of over 94.4% and 99.7%, respectively, in all cases. These two levels may be suitable for systems or users with high-security requirements. However, due to their high rate of false positives, using $\alpha = 0.05$ as the standard for more general purposes is recommended. This threshold achieves a detection rate close to 80% in all cases, with a false positive rate of 1 in 20.

4. Comparison with Other tests in the Literature

The test proposed in this article was compared to previous methods in terms of its effectiveness in detecting clustered graphic passwords and its efficiency. For this study, the tests to be compared will be denoted as follows: Test 1, which is based on the average distance between the points [10]; Test 2, which is based on the average of the perimeters of the Delaunay triangle [11]; Test 3, which is the joint application of the previous tests [13]; and Test 4, which is the test proposed in this study. Of the references consulted, the one that has shown the highest effectiveness is test 3. Therefore, it will serve

 doi:10.20944/preprints202405.1502.v1

as our benchmark in this regard. Regarding efficiency, the best option is test 1; we will compare our test with it.

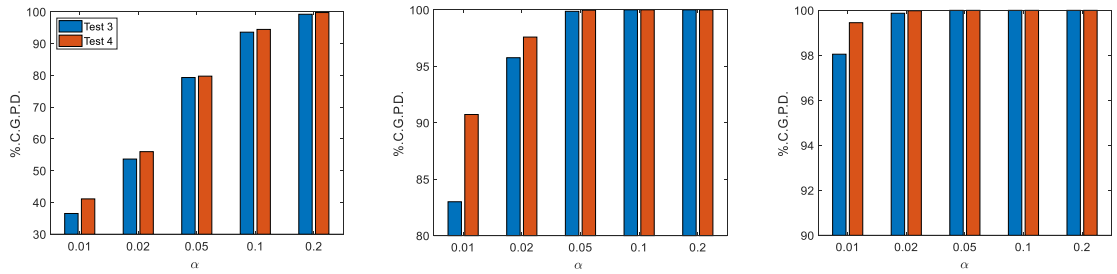
4.1. Effectiveness

Since the pooled password databases used in this work were generated following the same algorithm described in [13], it is possible to compare the reported results directly. Table 6 shows the difference in type II errors of Test 3 compared to the proposed Test 4.

Table 6. Variation (↓,↑) in the estimated probability of the type error II ($\hat{\beta}$) committed by the test 4 concerning test 3 in the DB.3.1, DB.3.2, DB.3.3.

Significance level	Critical region	($\hat{\beta}$) DB.3.1	($\hat{\beta}$) DB.3.2	($\hat{\beta}$) DB.3.3
0.2	$-1.282 < Z < 1.282$	↓0.0054	0	0
0.1	$-1.645 < Z < 1.645$	↓0.0087	0	0
0.05	$-1.960 < Z < 1.960$	↓0.0043	↓0.0010	0
0.02	$-2.326 < Z < 2.326$	↓0.0233	↓0.0241	↓0.0011
0.01	$-2.575 < Z < 2.575$	↓0.0459	↓0.0773	↓0.0140

The proposed test reduces the type II error when determining the best antecedents for each analyzed significance level α. This results in an increase in the percentage of graphic passwords detected, as shown in Figure 5 and, therefore, in the overall effectiveness of the test.



(a) (b) (c)

Figure 5. number of clustered graphical passwords detected by each of the tests in the databases DB.3.1(a), DB.3.2(b), DB.3.3(c).

4.2. Efficiency

To assess the efficiency of the proposed tests, they were implemented in Matlab 2018 software, adhering to the guidelines outlined in their respective original articles. Subsequently, the execution time of 100 graphical passwords was measured. The results are summarized in Table 7. Regarding efficiency, the proposed test outperforms Test 3 in the three times measured but is surpassed by Test 1 in all cases.

Table 7. Execution times (s), taking 100 passwords as a sample.

	Minimum time	Average time	Maximum time
Test 1	0.001	0.006	0.084
Test 3	0.001	0.045	0.155
Test 4	0.017	0.033	0.110

5. Conclusions and Future Work

This paper proposes a new test for detecting clustered graphic passwords in Passpoints. This test's novelty is that its estimated type II error and detection rate are the best reported so far. The

 doi:10.20944/preprints202405.1502.v1

execution time of the test was greater in the experiments conducted than in the previous best results. However, this difference is insignificant regarding the test's usability, as it is imperceptible to the users.

In this work, we proposed the hypothesis that the perimeter of the convex hull determined by the 5 points of a graphical password Passpoints would be an effective test statistic in detecting clustering patterns. This hypothesis is based on intuitive and visual evidence that the perimeter decreases when the points are closest. It was demonstrated using the EasyFit software and several goodness-of-fit tests that the proposed test statistic follows a Johnson SB distribution with parameters $\gamma = -0.65612$, $\delta = 1.5922$, $\lambda = 4575.1$, $\xi = 495.15$. The Johnson S.B. transformation was used to convert the data to a standard Normal distribution. A mean test was then conducted to evaluate graphical passwords. The effectiveness experiments considered three levels of clustering, following the guidelines established by the antecedents to enable a direct comparison with them. For the first clustering level, the test was able to detect significance levels $\alpha \in \{0.2, 0.1, 0.05, 0.02, 0.01\}$ with percentages greater than 99.7%, 94.4%, 79.7%, 55.9%, and 41.1% respectively. In the second level, the percentages were 100%, 100%, 99.9%, 97.5%, and 90.7%, respectively. In the third level, the percentages were 100%, 100%, 100%, 99.9%, and 99.4%, respectively. These results allowed us to accept the proposed hypothesis and validate the effectiveness of the proposed test.

In comparison to the antecedents, it can be observed that the effectiveness was superior to that reported by other tests available in the literature for the three clustering levels and the five significance levels. Consequently, this new proposal's estimated type II error was also lower than that reported in previous studies, reducing up to about 0.08 in the best cases. The measured execution time of the proposed test ranks it second among the previous tests. However, the differences between these times are indistinguishable in practice. Therefore, we believe the most important factor to consider when selecting a test is its effectiveness. The experiments conducted in this study and the comparisons made with the existing literature suggest that the proposed test is the most effective option for determining clustered graphic passwords in Passpoints. However, the selection of the significance level to be used is left to the choice of the user or system, depending on their security needs. The authors recommend using a standard significance level of $\alpha = 0.05$ for general purposes. With this level, a detection rate of more than 79.7% is achieved in each case, with one false positive for every 20 attempts. The test was designed to be integrated into graphical authentication systems of the cued-recall type, preventing users from selecting easily guessable passwords. Graphics with clustered patterns contribute to the strength of passwords and enhance the system's security.

In future work, the hypothesis of complementarity between the newly proposed test and those already existing in the literature is left open. A possible scenario where two or more of the tests complement each other would allow for increased detection values and a reduction in type II error.

Author Contributions: Conceptualization, L.S.-P., C.M.L-.P., and J.A.H.-M.; methodology, L.S.-P., C.M.L-.P., G.S.-G., and O.R.; validation, L.S.-P., C.M.L-.P., and G.S.-G.; formal analysis, L.S.-P., J.A.H.-M., C.M.L-.P., O.R., and G.S.-G.; investigation, L.S.-P., C.M.L-.P., J.A.H.-M., O.R., and G.S.-G.; writing—original draft preparation, L.S.-P., C.M.L-.P., J.A.H.-M., O.R., and G.S.-G.; writing—review and editing, L.S.-P., C.M.L-.P., O.R., and G.S.-G.; visualization, L.S.-P. and J.A.H.-M.; supervision, L.S.-P., C.M.L-.P., J.A.H.-M., 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.

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

References

1. David, L. & Wool, A. An explainable online password strength estimator. *Computer Security–E.S.O.R.I.C.S. 2021: 26th European Symposium On Research In Computer Security, Darmstadt, Germany, October 4–8, 2021, Proceedings, Part I 26*. pp. 285-304 (2021). https://doi.org/10.1007/978-3-030-88418-5_14.
2. Awan, K., Ud Din, I., Almogren, A., Kumar, N. & Almogren, A. A Taxonomy of Multimedia-based Graphical User Authentication for Green Internet of Things. *A.C.M. Transactions On Internet Technology (T.O.I.T.)*. **22**, 1-28 (2021). https://doi.org/10.1145/3433544.

 doi:10.20944/preprints202405.1502.v1

3. Nosenko, A., Cheng, Y. & Chen, H. Password and Passphrase Guessing with Recurrent Neural Networks. *Information Systems Frontiers*. **25**, 549-565 (2023,4,1), https://doi.org/10.1007/s10796-022-10325-x
4. Rando, J., Perez-Cruz, F. & Hitaj, B. PassGPT: Password Modeling and (Guided) Generation with Large Language Models. (2023)
5. Itti, L. & Koch, C. Computational modelling of visual attention. *Nature Reviews Neuroscience*. **2**, 194-203 (2001,3,1), https://doi.org/10.1038/35058500
6. Valdés, O., Legón, C., Socorro, R. & Navarro, P. Patrones en el orden de los clics y su influencia en la debilidad de las claves en la técnica de autenticacion gráfica passpoints. *Serie Científica De La Universidad De Las Ciencias Informáticas*. **12**, 37-47 (2019)
7. Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A. & Memon, N. PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal Of Human-Computer Studies*. **63**, 102-127 (2005), HCI research in privacy and security
8. Rodriguez Valdés, O., Legón, C. & Socorro Llanes, R. Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica.. *Revista Cubana De Ciencias Informáticas*. **12** pp. 13-27 (2018)
9. Legón, C., Socorro, R., Navarro, P., Rodríguez, O. & Borrego, E. Nuevo modelo probabilístico en autenticación gráfica. *Ingeniería Electrónica, Automática Y Comunicaciones*. **40** pp. 92-104 (2019)
10. Herrera-Macías, J., Legón-Pérez, C., Suárez-Plasencia, L., Piñeiro-Díaz, L., Rojas, O. & Sosa-Gómez, G. Test for detection of weak graphic passwords in passpoint based on the mean distance between points. *Symmetry*. **13**, 777 (2021)
11. Suárez-Plasencia, L., Legón-Pérez, C., Herrera-Macías, J., Socorro-Llanes, R., Rojas, O. & Sosa-Gómez, G. Weak PassPoint Passwords Detected by the Perimeter of Delaunay Triangles. *Security And Communication Networks*. **2022**
12. Herrera-Macías, J., Suárez-Plasencia, L., Legón-Pérez, C., Piñeiro-Díaz, L., Rojas, O. & Sosa-Gómez, G. Effectiveness of some tests of spatial randomness in the detection of weak graphical passwords in passpoint. *International Conference On Computer Science And Health Engineering*. pp. 173-183 (2020)
13. Macías, J., Plasencia, L., Pérez, C. & Gomez, G. Comparación y combinación de dos test efectivos en la detección de contraseñas gráficas no aleatorias en Passpoints. *Revista Cubana De Ciencias Informáticas*. **17** (2023)
14. Valdés, O. Algoritmo para la detección de Contrasenas Gráficas con patrón de suavidad en la Técnica de Autenticación Gráfica Passpoints. (Universidad de la Habana,2019)
15. Suárez-Plasencia, L., Herrera-Macías, J., Legón-Pérez, C., Sosa-Gómez, G. & Rojas, O. Detection of DIAG and LINE Patterns in PassPoints Graphical Passwords Based on the Maximum Angles of Their Delaunay Triangles. *Sensors*. **22**, 1987 (2022)
16. Li, F. & Klette, R. Euclidean Shortest Paths. *Euclidean Shortest Paths: Exact Or Approximate Algorithms*. pp. 3-29 (2011), https://doi.org/10.1007/978-1-4471-2256-2_1
17. Preparata, F. & Shamos, M. Computational geometry: an introduction. (Springer Science & Business Media,2012)
18. Mark, D., Otfried, C., Marc, V. & Mark, O. Computational geometry algorithms and applications. (Springer,2008)
19. ORourke, J. Computational geometry in C. (Cambridge University Press,1998)
20. Rockafellar, R. Convex analysis. (Princeton University Press,1997)
21. de Berg, M.; van Kreveld, M.; Overmars, M.; Schwarzkopf, O.: *Computational Geometry: Algorithms and Applications (3rd ed.)*. Springer, 2008.
22. Candela, C., Sepúlveda, L., Chavarro, J., Meneses, C., Sanabria, J. & Arcila, O. Implementación de algoritmos para calcular el Convex Hull. *Entre Ciencia E Ingeniería*. **16**, 27-34 (2022)
23. Gamby, A. & Katajainen, J. A faster convex-hull algorithm via bucketing. *International Symposium On Experimental Algorithms*. pp. 473-489 (2019)
24. Gamby, A. & Katajainen, J. Convex-hull algorithms: Implementation, testing, and experimentation. *Algorithms*. **11**, 195 (2018)
25. Keith, A., Ferrada, H. & Navarro, C. Accelerating the Convex Hull Computation with a Parallel GPU Algorithm. *2022 41st International Conference Of The Chilean Computer Science Society (S.C.C.C.)*. pp. 1-7 (2022)
26. Tabacman, M. Implementing and visualizing algorithms for computing Convex Hulls in the plane. (2021)
27. Efron, B. The convex hull of a random set of points. *Biometrika*. **52**, 331-343 (1965)

28. Groeneboom, P. Limit theorems for convex hulls. *Probability Theory And Related Fields*. **79**, 327-368 (1988,10,1). https://doi.org/10.1007/BF00342231
29. Khamdamov, I., Chay, Z. & Sharipova, L. The limit distribution of the perimeter of a convex hull generated by a Poisson point process in a convex polygon. *Vestnik Tomskogo Gosudarstvennogo Universiteta. Matematika I Mekhanika*., 44-57 (2022)
30. McRedmond, J. & Wade, A. The convex hull of a planar random walk: perimeter, diameter, and shape. (2018)
31. McRedmond, J. & FERGAL, W. Convex hulls of random walks. (Durham University,2019)
32. NIST Special Publication 800-63B: *Digital Identity Guidelines. Authentication and Lifecycle Management.* http://doi.org/10.6028/NIST.SP.800-63b, june 2017.
33. Ray, P. Ray's scheme: Graphical password-based hybrid authentication system for smart hand-held devices. *J. Inf. Eng. Appl*. **2**, 1-12 (2012)
34. Dirik, A., Memon, N. & Birget, J. Modeling user choice in the PassPoints graphical password scheme. *Proceedings Of The 3rd Symposium On Usable Privacy And Security*. pp. 20-28 (2007)
35. Van Oorschot, P., Salehi-Abari, A. & Thorpe, J. Purely automated attacks on passpoints-style graphical passwords. *IEEE Transactions On Information Forensics And Security*. **5**, 393-405 (2010)
36. Zhu, B., Wei, D., Yang, M. & Yan, J. Security implications of password discretization for click-based graphical passwords. *Proceedings Of The 22nd International Conference On World Wide Web*. pp. 1581-1591 (2013)
37. Floch, J., Marcon, E. & Puech, F. Spatial distribution of points. *Handbook Of Spatial Analysis: Theory And Application With R.; Loonis, V., Bellefon, MP, Eds*. pp. 77-111 (2018)
38. Chiasson, S., Forget, A., Biddle, R. & Oorschot, P. User interface design affects security: Patterns in click-based graphical passwords. *International Journal Of Information Security*. **8** pp. 387-398 (2009)
39. Pogoda, P., Ochał, W. & Orzeł, S. Performance of Kernel estimator and Johnson SB function for modeling diameter distribution of black alder (Alnus glutinosa (L.) Gaertn.) stands. *Forests*. **11**, 634 (2020)