Effectiveness of Some Tests of Spatial Randomness in the Detection of Weak Graphical Passwords in *Passpoint*

Joaquín A. Herrera-Macías[1], Lisset Suárez-Plasencia[2], Carlos M. Legón-Pérez[3], Luis R. Piñeiro-Díaz[3], Omar Rojas[4], and Guillermo Sosa-Gómez[4(✉)]

[1] Universidad de Matanzas, Departamento de Matemática, Matanzas, Cuba
joaquin.herrera@umcc.cu
[2] Universidad de Artemisa, Departamento de Matemática-Física, Artemisa, Cuba
l.suarez2@uart.edu.cu
[3] Universidad de la Habana, Facultad de Matemática y Computación, Instituto de Criptografía, Habana, Cuba
clegon58@gmail.com, lrp@matcom.uh.cu
[4] Universidad Panamericana. Facultad de Ciencias Económicas y Empresariales., Álvaro Del Portillo 49, Zapopan, Jalisco 45010, Mexico
orojas@up.edu.mx, gsosag@up.edu.mx

Abstract. This paper explores the usability of the Ripley's K function and the nearest neighbor distance, in the detection of clustered graphical passwords in the graphical authentication stage. For it, both tests were applied to two bases of data of 10,000 clustered graphical passwords each, the first with graphical passwords clustered in an area lesser than the fourth part of the original image, the second clustered in an area lesser than eighth part of the image. The results show that none of these tests is effective in the detection of clustered graphical passwords, the reason of such failure is due to the short size of the spatial pattern in question, only the 5 points of the graphical password analyzed.

Keywords: Point pattern · Graphical password · Ripley's K function · Nearest neighbor distance · Passpoint

1 Introduction

Nowadays, graphical passwords are an important alternative to traditional alphanumeric passwords. The main reason for this is due to the fact that humans have a better ability to remember images than text [10,17]. Therefore, with graphical authentication there is no need to remember long and difficult sequences. Instead, a user can authenticate by recognizing images or parts of them. Among the graphical authentication techniques, the *Passpoint* [18,20,21] is of special interest. During the registration phase while using Passpoint, the user must select 5 points (pixels) on an image as their graphical password, each

J. A. Marmolejo-Saucedo et al. (Eds.): COMPSE 2020, LNICST 359, pp. 173–183, 2021.
https://doi.org/10.1007/978-3-030-69839-3_12

time that user wishes to authenticate they must select 5 points located in a neighborhood of the 5 points selected during registration [18,21]. The points selected as a graphical password must follow a random pattern, otherwise, they are considered weak passwords, since they can be obtained by an attacker using different techniques [6,14,17,19]. It is therefore of great importance to have a tool that warns the user during the registration phase about a possible graphical password with poor randomness.

On the other hand, we have the analysis of spatial point patterns, which is the area of spatial statistics that is dedicated to studying the characteristics of events that can be represented in a specific way in space, as well as their spatial distribution [1,8,9]. Two of the tests most used in this area to check spatial randomness are Ripley's K function test [1–3,5,8,11,13,16] and the nearest neighbor distance test [1,3,8].

Graphical passwords can be interpreted as a 5-point pattern and studied by the various techniques of the theory of spatial randomness to determine their behavior. It happens that a pattern with only 5 points seems to be a sample way too small for these techniques to work. In the literature, the smallest point pattern for which it is concluded that both tests are effective consists of 36 points [15].

In this work the effectiveness of Ripley's K function and the nearest neighbor distance technique is studied, two of the most used tests in the theory of spatial point patterns, in the scenario of graphical authentication with *Passpoint*, to validate whether or not a graphical password belongs to a random pattern. For the experiments, two databases of 10000 graphical passwords clustered on a 1920×1080 image were generated. The results obtained show that both Ripley's K function and nearest neighbor distance, are not effective tests in this scenario, due to the small sample (only 5 points); i.e., they are not able to differentiate between sets of 5 points clustered and random. All the point patterns and experiments were generated in MATLAB R2018a.

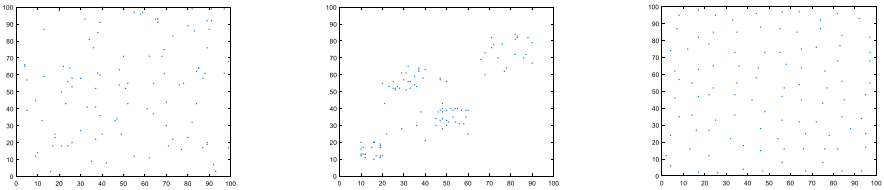
2 Preliminaries

2.1 Spatial Point Patterns

To study the distribution and behavior of phenomena that occur in specific regions of space, such as earthquakes, animal or plant populations, epidemiological information, data on human settlements, etc., its representation by means of spatial coordinates (x, y) is essential. The data set generated by these coordinates is called the *spatial pattern of points* [4,7–9,12]. From the study of the spatial pattern, the existence of interactions between the individuals of each population can be inferred.

A pattern that has special importance, in theory, is the random or Poisson pattern, which is one in which any region of the area of study has the same probability of containing a point, a definition that is equivalent to that of the distribution of Poisson. The other characteristic patterns are regular patterns, where the probability of finding a point in the vicinity of another is less than

that of a random pattern; and clustered patterns, in which the probability is greater. Examples of these three traditional patterns are shown in Fig. 1.



(a) (b) (c)

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

In point pattern analysis, it is generally assumed as a null hypothesis that the pattern of points presents a random distribution, the alternative hypotheses being that the distribution might be regular [1,3,8]. Spatial point patterns have two fundamental properties: homogeneity (the pattern is translation invariant) and isotropism (the pattern is rotation invariant) [3,12]. 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 tests for spatial point pattern analysis. It is a distance-based method that measures the average number of points within a circle of radius r around any 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 study region, $k_{i,j}(r)$ 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. Although the function $K(r)$ can be estimated without taking into account the factor $e_{i,j}(r)$, in [8] it was shown how the use of $K(r)$ without the edge correction effects lead to imprecise estimates of the pattern. However, since these methods are not perfect, it is recommended to calculate $K(r)$ for values of $r < 1/3$ of the length of the shortest side of the area of study when it has a rectangular shape [3]. A detailed review of these methods can be found in [3,8,9].

Taking into account that, in the case of regular patterns, the probability of finding a point in the vicinity of another point is lower than that of a random pattern, while in clustered patterns the probability is higher, then the interpretation of the results of $K(r)$ would be made by the comparison with the random (or Poisson) pattern πr^2 [5,8,16]. 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 Fig. 2 the value is represented by Ripley's K function of the three prototype patterns of Fig. 1, together with the Poisson pattern. The figure shows how the function clearly differentiates between the three patterns.

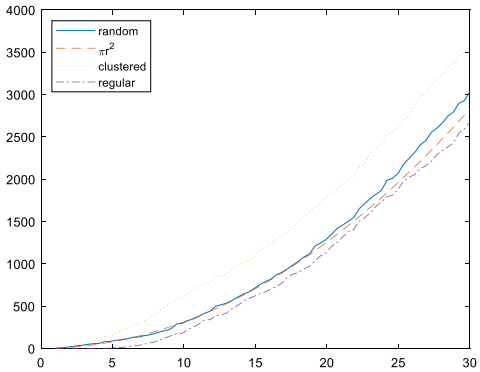


Fig. 2. Comparison of the values of Ripley's K function for the three prototypical patterns.

To facilitate the visual and numerical interpretation of the results of Ripley's K function for a given pattern, the following transformation is usually performed:

$$\hat{L}(r) = \sqrt{\frac{K(r)}{\pi}},$$

which aims to linearize the function and stabilize the variance [3,8]. Finally, the transformation $L(r) = \hat{L}(r) - r$, sets the Poisson pattern to the value 0. Consequently, a clustered pattern occurs when $L(r) > 0$ and a regular pattern occurs 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, we do this through Monte Carlo simulations [1,5,8,11]. 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 value is 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 statistic are approximated. Ripley showed [2,3] 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 Fig. 3, the function $L(r)$ is represented for each of the patterns in Fig. 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 dashed lines represent the confidence intervals for $\alpha = 0.01$ of the test according to Ripley's approximation: $\pm 1.68\sqrt{A}/n$, 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 values less than the lower limit of the confidence interval for $r \in [2, 11]$, so the null hypothesis is also rejected in favor of grouping between the points at that scale.

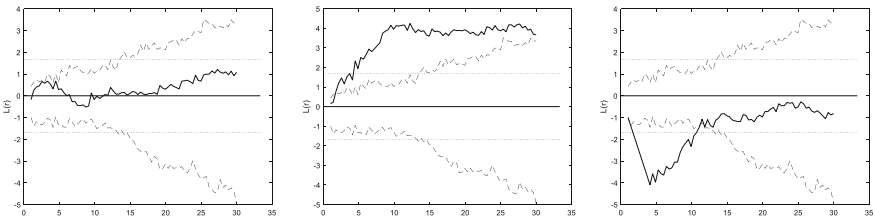


Fig. 3. Function $L(r)$ of the random (a), clustered (b), and regular (c) patterns of Fig. 1

2.3 Nearest Neighbor Distance

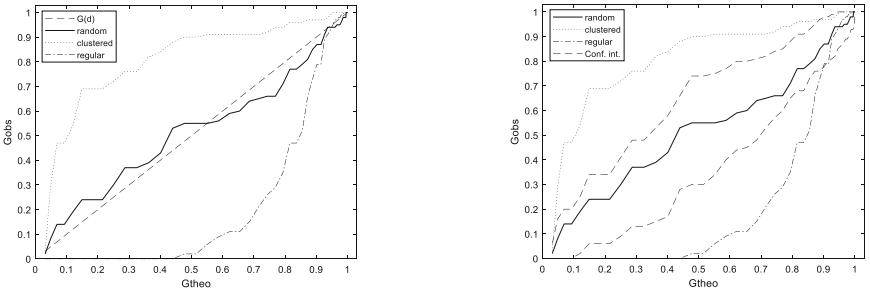
Another effective method to describe the behavior of a pattern of spatial points is the analysis of the nearest neighbor distance. If n points are randomly distributed over an area A, the expected cumulative distribution function for the nearest neighbor distances will be given by the Poisson distribution $G(d) = 1 - e^{-\lambda\pi d^2}$, 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 [1,8] 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 $I_i(d)$ 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.

If the point pattern is clustered, many of the distances will be small; in the same way, if it is a regular pattern, a few distances will be small. So, values of $\hat{G}(d)$ greater than the theoretical value $G(d)$ indicate clustering, while values of $\hat{G}(d)$ less than the theoretical value $G(d)$ indicate regularity [1,3,8].

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 Fig. 4, the values of the function $\hat{G}$ are observed for each of the patterns in Fig. 1, the critical values of the test were obtained through 500 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)

Fig. 4. Comparison of the values of the function $\hat{G}(d)$ for the three prototypical patterns, using as a reference the theoretical distribution $G(d)$ that represents the null hypothesis. It looks like the difference function between the three patterns.

3 *Passpoint* Scenario

As can be seen from the formulas of Ripley's K function and the nearest neighbor distance, their precision is directly proportional to n, but what is the minimum value of n for both tests to be considered accurate? We have not found this data in the literature consulted. In [15] both tests are applied to a 22-point pattern, the smallest pattern we have 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 [15] 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 5 points are available?

3.1 Design of the Experiment

In this work, the detection of clustering is analyzed, for which both tests were applied to two databases of clustered graphic passwords.

Database 1 (BD.1): Consists of 10000 graphical passwords generated randomly within a rectangle of 1920×1080 that satisfy that the area covered by the 5 points of each password is less than the quarter of the area of the rectangle. These passwords will be considered clustered.

Database 2 (BD.2): Also out of 10000 randomly generated graphical passwords within the 1920×1080 rectangle, each graphical password delimits an area smaller than one-eighth of the original rectangle. To discern the points BD.2 from the ones from BD.1, the aforementioned will be considered as strongly clustered.

For each of the tests, the critical values were estimated by 5000 Monte Carlo simulations of sets of 5 random points on a rectangle of size 1920×1080, in addition to Ripley's K function the confidence intervals were estimated according to Ripley's approximation $\pm 1.68\sqrt{A}/n$, where $A = 1920 * 1080$ and $n = 5$. These values for Ripley's K function can be seen in Fig. 5, the solid line at $L(r) = 0$ represents the theoretical value of the null hypothesis, the dashed lines represent the intervals of confidence for $\alpha = 0.01$ of the test according to the Ripley approximation and the dashed lines represent the critical values of the function $L(r)$ in 5000 random pattern simulations.

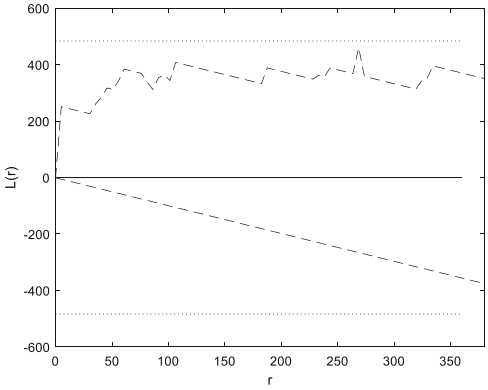


Fig. 5. Confidence intervals and critical values of Ripley's K function test for 5-point patterns.

3.2 Results

Ripley's K Test Effectiveness. Ripley's K function test applied to BD.1 shows that only 22 of the 10000 sets exceed the critical values estimated for the Monte Carlo simulation test, which represents 0.22% of all the cases analyzed, and only 1 of these sets of 5 points is above the confidence interval estimated by Ripley's approximation, which represents 0.01% of the cases analyzed. Some particular cases are shown in Fig. 6, in the first two cases it is observed how the K function is contained within the critical values, in the third, the function is above the critical values in the interval $[156, 241]$ but below the Ripley confidence

interval, the fourth case is the only one in which values of the K function were obtained above the confidence interval according to Ripley's approximation for $r \in [145, 245]$.

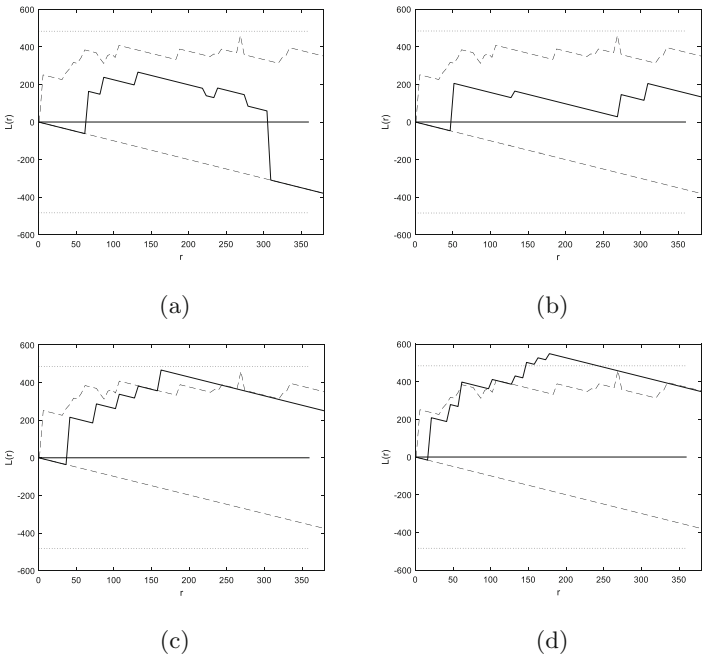
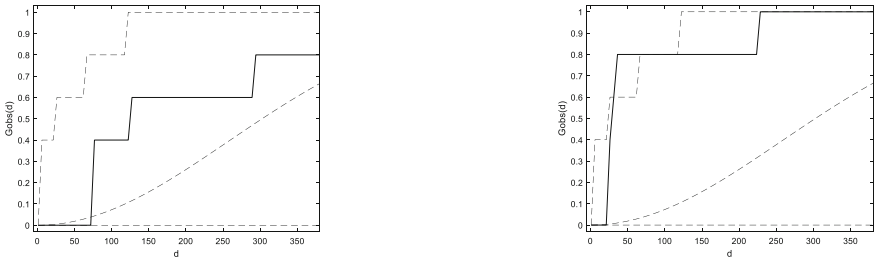


Fig. 6. Result of Ripley's K function test for 4 of the 10000 sets analyzed.

For BD.2 of the 10000 sets of strongly clustered points, 590 of them exceed the critical values obtained by Monte Carlo simulation for the test, which represents 5.9% of the total number of cases analyzed; and 24 report values of the K function greater than the confidence intervals estimated by Ripley's approximation, which represents 0.24% of the cases analyzed.

Effectiveness of the Test of the Nearest Neighbor Distance. The results obtained by the nearest neighbor distance test for BD.1 show that only 14 of the 10000 sets of 5 clustered points exceed the critical values estimated for the test by Monte Carlo simulation, which represents the 0.14% of all cases.

In the experiment with the 10000 sets of 5 strongly clustered points from BD.2, only 72 sets exceed the critical values obtained by Monte Carlo simulation, which represents 0.72% of the cases analyzed. Two particular cases are shown in the Fig. 7, in the first graph it is observed how the function $\hat{G}$ falls within the confidence intervals, therefore the CSR hypothesis is accepted; in the second, the function exceeds the value of the upper confidence interval for $d \in [16, 26]$ so the null hypothesis is rejected.



(a) (b)

Fig. 7. Result of the nearest neighbor test for 2 of the 20000 sets analyzed.

3.3 Discussion of the Results

Both Ripley's K test and the nearest neighbor distance test were ineffective in detecting BD.1 sets as clustered. The best results were offered by Ripley's K test, which detected only 0.22% of the cases. Of these 22 sets in which the null hypothesis is rejected in the experiment, 11 of them correspond to sets of points that cover an area less than one-eighth of the image. Taking into account that, since they were not generated in a uniform way, only 194 of the 10000 sets of points of the BD.1 are in an area smaller than one-eighth of the image, then only 1.94% of cases have 50% of successes. Therefore, the function is expected to have a better success rate for the tightly clustered sets in the second database. Although these patterns of strongly clustered points are unlikely to be found in practice since it would mean selecting the 5 points in an area equivalent to one-eighth of the image area, something unlikely that a responsible user will perform, without a doubt, a graphic password with these characteristics it would offer very low security. However, experiments with BD.2 confirm the ineffectiveness of both tests in detecting clustering in 5-point patterns. Once again, the best results were obtained by Ripley's K function test, which detected 5.9% of the cases, a considerable improvement compared to the 0.22% obtained for BD.1, but still a very discreet value to be considered effective as it fails in more than 94% of the cases analyzed. These results are summarized in Table 1.

Table 1. Percentage of clustered graphical passwords detected by each test for BD.1 and BD.2

	BD.1	BD.2
Ripley's K function	0.22%	5.9%
Nearest neighbor distance	0.14%	0.72%

4 Conclusions

The experiments carried out show that both Ripley's K test and the nearest neighbor distance test, despite being some of the most used tests in the detection of clustering in finite patterns of spatial points, are not effective in detecting graphical passwords clustered in the *Passpoint* scenario, in which these passwords only consist of 5 points. The first experiment carried out for the 10000 sets of 5 points, which delimit an area smaller than a quarter of the original image area, shows that Ripley's K function test only detects 22 out of the 10000 sets of points as clustered, which represents 0.22% of the cases. The nearest neighbor distance test detected only 14 sets, for 0.14% of the cases. The second experiment, despite being with much more clustered points, since they cover an area smaller than one-eighth of the image, and yielding detection values significantly higher than those obtained for the clustered points, also shows the inefficiency of both tests in the *Passpoint* scenario since of the 10000 strongly clustered sets simulated Ripley's K function test only detects 590, which represents 5.9% of the cases; while the closest neighbor detected 72, for 0.72% of the cases.

Since these two spatial pattern analysis techniques are not effective in detecting clustering in the graphical authentication scenario with *Passpoint*, it is necessary to develop methods to detect clustering in graphical passwords of only 5 points, which it would allow users to warn about a possible weak graphical password. The use of some of the improved variants of these tests could be explored, but taking into account the small sample size, our future research will be directed in another direction, the development of new methods that allow detecting clustering in the said scenario with high reliability.

References

1. Caballero Pérez, Y.B.: Test de aleatoriedad para procesos puntuales espaciales basado en el cálculo de la dimensión fractal. Estadística (2017)
2. Casanova, M.R., Orts, V., Albert, J.M., Mateu, J.: Distance-based methods: Ripley's k function vs. k density function. Tech. rep., European Regional Science Association (2011)
3. De La Cruz, M.: Métodos para analizar datos puntuales. Introd. al Análisis Espac. Datos en Ecol. y Ciencias Ambient. Métodos y Apl., pp. 75–127 (2008). https://dialnet.unirioja.es/servlet/articulo?codigo=2771482
4. Diggle, P.J.: Statistical Analysis of Spatial and Spatio-temporal Point Patterns. 3rd edition. CRC Press (2013). https://doi.org/10.1201/b15326
5. Dixon, P.M.: Ripley's K function. In: Wiley StatsRef Stat. Ref. Online. John Wiley & Sons, Ltd. (2014). https://doi.org/10.1002/9781118445112.stat07751
6. Gao, H., Jia, W., Ye, F., Ma, L.: A survey on the use of graphical passwords in security. J. Softw. **8**(7), 1678–1698 (2013). https://doi.org/10.4304/jsw.8.7.1678-1698
7. Gelfand, A., Diggle, P., Guttorp, P., Fuentes, M.: Handbook of spatial statistics. Handb. Spat. Stat. (2010). https://doi.org/10.1201/9781420072884
8. Gómez-Rubio, V.: Spatial Point Patterns: Methodology and Applications with R. J. Stat. Softw. 75(Book Review 2) (2016). https://doi.org/10.18637/jss.v075.b02, http://www.spatstat.org/

9. Illian, J., Penttinen, A., Stoyan, H., Stoyan, D.: Statistical Analysis and Modelling of Spatial Point Patterns. vol. 70. John Wiley & Sons (2008). https://doi.org/10.1002/9780470725160
10. Itti, L., Koch, C.: Computational modelling of visual attention. Nat. Rev. Neurosci. **2**(3), 194–203 (2001). https://doi.org/10.1038/35058500, https://www.nature.com/articles/35058500
11. Kopczewska, K.: Cluster-based measurement of agglomeration, concentration and specialisation. Measuring Regional Specialisation, pp. 69–171. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-51505-2_2
12. Nakoinz, O., Knitter, D.: Modelling Human Behaviour in Landscapes. QAAM. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-29538-1
13. Ripley, B.D.: Tests of 'Randomness' for spatial point patterns. J. R. Stat. Soc. Ser. B **41**(3), 368–374 (1979). https://doi.org/10.1111/j.2517-6161.1979.tb01091.x
14. Rittenhouse, R.G., Chaudry, J.A., Lee, M.: Security in graphical authentication. Int. J. Secur. Its Appl. **7**(3), 347–356 (2013)
15. Rozas, V., Camarero, J.: Técnicas de análisis espacial de patrones de puntos aplicadas en ecología forestal. Forest Syst. **14**(1), 79–97 (2008)
16. Schabenberger, O., Gotway, C.A.: Statistical Methods for Spatial Data Analysis. CRC Press (2017). https://doi.org/10.1201/9781315275086
17. Valdés, O.R., Legón, C.C.M., Socorro, C.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. IV Semin. Cient\ifico Nac. Criptograf\ia (2018)
18. Valdés, O.R., Legón, C.M., Llanes, R.S.: Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica. Rev. Cubana Cien. Inform. **12**, 13–27 (2018)
19. Van Oorschot, P.C., Thorpe, J.: Exploiting predictability in click-based graphical passwords. J. Comput. Secur. **19**(4), 699–702 (2011). https://doi.org/10.3233/JCS-2010-0411
20. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., Memon, N.: Authentication using graphical passwords: effects of tolerance and image choice. ACM Int. Conf. Proc. Ser. **93**, 1–12 (2005). https://doi.org/10.1145/1073001.1073002
21. 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. **63**(1–2), 102–127 (2005). https://doi.org/10.1016/j.ijhcs.2005.04.010