STUDIA UNIV. BABEŞ–BOLYAI, INFORMATICA, Volume **LX**, Number 1, 2015

PERCEPTUAL EVALUATION OF RANDOM NUMBER SEQUENCES USING FILESEER+

KINGA MARTON, DAN PATRASCU, AND ALIN SUCIU

Abstract. The quality assessment of random number sequences based on visual perceptions is meant to complement the more widely used approach of statistical testing that has become a standard method of randomness evaluation. Instead of carrying out a well defined procedure by means of computer instructions which build-up the statistical randomness batteries, in visual assessment we rely on the perceptual system to extract statistical properties from the visual representation of the tested sequence and derive conclusions regarding the quality of randomness accordingly. FileSeer+ is a follow-up work to the research results previously presented in [1] and proposes several visual tests together with an efficient testing environment for random number sequences based on perceptual assessment. Empirical results show that visual evaluation can highly improve the process of randomness assessment by facilitating the understanding and interpretation of randomness through the properties of random sequences that can be visually captured.

1. Introduction

The quality assessment of random number sequences based on visual perceptions is meant to complement the more widely used approach of statistical testing that has become a standard method of randomness evaluation. Through visual assessment the tester can gain insight into the fascinating domain of randomness and randomness testing by understanding what randomness is and how it looks like by appealing to the perceptual instead of the cognitive system.

Received by the editors: January 21, 2015.

2010 *Mathematics Subject Classification.* 94A17, 68U99, 68U10.

1998 *CR Categories and Descriptors.* G.3 [**Probability and statistics**]: Random number generation – ; H.1.2 [**Information Systems**]: User/Machine Systems – *Human information processing*; H.4.2 [**Information Systems**]: Information systems applications – *Decision support*.

Key words and phrases. randomness assessment, visual perception, statistical properties, testing environment.

The human visual system is highly trained to extract features of the surrounding world and summarize these with statistical descriptors. This is due to the fact that our perceptual system is constantly concerned with selecting and organizing the sensory information with the intention of interpreting the outside world. This organizing tendency is so powerful that sometimes it slightly distorts the sensory information, hence sometimes we seem to perceive forms and shapes even when the received stimuli provide a very incomplete evidence of these. At the same time, our visual perceptions are also guided by our expectations of what we will see.

Depending on the nature of the entropy source, the generators can be classified in three categories, namely true random number generators (TRNGs), unpredictable random number generators (URNGs) and pseudo-random number generators (PRNGs). TRNGs extract randomness from a natural physical phenomenon, such as radioactive decay, thermal noise or quantum mechanics, and the properties of independence and unpredictability of the generated values are guaranteed by physical laws. URNGs are based on the unpredictability inherent to human computer interaction and on the undeterminism introduced by the complexity of the underlying phenomenon. PRNGs produce random looking sequences by expanding an initial value, called seed, by means of a deterministic recursive formula.

When applying statistical tests for assessing the randomness quality of a sequence, a finite set of statistical properties is evaluated based on values expected from a perfectly random stream. Instead of carrying out a well defined procedure by means of computer instructions which build-up the statistical randomness batteries, in visual assessment we rely on the perceptual system to extract statistical properties from the visual representation of the sequence and derive conclusion regarding the randomness quality of the sequence accordingly.

Furthermore, statistical tests may capture the lack of randomness but are limited in determining the cause or suggesting ways of readjusting the generators. Perceptual tests are more powerful in this direction, and hence are very useful especially in assessing physical devices (TRNGs) which may show certain disturbances but can be redressed if the cause is known.

This paper is a follow-up to the research results previously presented in [1], where we have highlighted some of the advantages and limitations of visual randomness evaluation and provided several relevant empirical results. The new contributions of the present work include the extended set of visual tests, the possibility to select and focus on a specific area of interest within the visual representation, the ability to generate random walks according to several rules in one and two dimensions. Furthermore, the testing process and its performance is highly improved through the integration of concurrent working threads, allowing the generation and visualization of several representations concurrently. Moreover, the designed testing environment allows for easy and practical organization of the tested sequences, the associated visual representations, and all the generated results. Hence previous tests results can be saved, reloaded and extended through further analysis.

The paper is structured in 5 sections. Section 2 briefly presents the main difficulties in the process of randomness assessment, some scientific evidence which prove that visual perception can effectively contribute to abstract data analysis, and the main limitation in visual assessment, namely that visual randomness cannot guarantee real randomness. Section 3 points out the main contributions of the paper, presenting the included tests and the proposed testing environment, followed by experimental results in section 4, demonstrating the effectiveness of our approach. Section 5 presents final conclusions and further work.

2. Randomness assessment and visual perception

2.1. **Difficulties in randomness assessment.** Randomness assessment is a rather complex and resource expensive process characterized by peculiar properties, a few of which are briefly described in the following.

There is no finite amount of testing that can guarantee perfect randomness, but applying several relevant tests could increase the confidence in accepting the sequence as being random or rejecting it due to evidence of nonrandomness.

Selecting a relevant set of tests is difficult, because accurate results are expected from a relatively reduced number of tests and within a relatively short period of time. Hence a fair balance is needed between thoroughness and performance, though, no set of tests can be considered complete.

The most widely used randomness tests are statistical tests, which can be grouped together forming batteries of tests, such as the NIST statistical test suite [3], TestU01 [5] designed by LEcuyer and Simard, the Diehard test suite [9] developed by Marsaglia, and John Walkers ENT [7]. Statistical tests are usually based on hypotheses testing, summarizing their results in so called P-values, probability values between 0 and 1. Results may include a multitude of P-values, and are relatively hard to interpret by users unfamiliar with concepts of mathematical statistics.

A very important aspect which adds to the complexity of testing is the size of the tested sequence, considering that even perfectly random sequences contain subsequences that look deterministic and hence may fail some of the tests, yet the assessment process has to avoid reaching to an incorrect conclusion and consider the whole sequence as being nonrandom. At the same time nonrandom sequences may contain subsequences which look random and consequently pass the majority of tests, yet the sequence as a whole may show repeating patterns, correlations or other traces of lack of randomness. Therefore the sequence to be tested has to be long enough to allow the evaluation process to arrive to the correct conclusion.

2.2. **Data analysis using human visual perceptions.** The theory and research in the domain of human perception and sensation has known very important advancements in the last few decades and continues to receive valuable contributions with rich experimental support. In our research we use several results from this field which prove that statistical information about a set of similar objects could be perceived by the perceptual system as accurately as the characteristics of a single object.

In particular, we rely on the work of Ariely [6] who studied the way a set of similar objects are perceived, and showed that the human visual system creates an internal representation of the overall statistical properties of the set, such as mean and distribution. Furthermore he experimentally showed (focusing on mean discrimination and member identification), that the visual system decides for which part of the set to retain the individual representation and for which to extract only the global statistical properties.

Chong and Treisman in [8, 4] are concerned with the way statistical properties are encoded and represented, and empirically measure and prove that our perceptual system is indeed highly capable of accurately judging the mean of items, with focus on the size and orientation property.

In [2] Robitaille and Harris provide evidence that the process of estimating the statistical properties by the visual system can highly benefit from enlarging the set of objects.

In the following we present how these results are adapted and used in our goal of assessing the quality of random number sequences.

In visual randomness testing the sequence of random numbers is graphically represented as one image or several images. Therefore the elementary object forming the random sequence in visual representation is a pixel, and the human perceptual system is required to extract statistical properties of the set of pixels which form the image, or a selected part of the image.

For a high quality random number sequence we expect to perceive uniform distribution and patternlessness in the image representation whether black and white, grayscale or color. The perceptual system identifies areas where the sequence seems to fulfill these requirements and creates an internal representation of the overall statistical properties of the area. Similarly, our visual system discriminates areas where there are visual traces of lack of randomness, such as certain (possibly repeating) patterns, bias towards a certain value, or certain types of correlations. Furthermore, the human visual system is capable of capturing several statistical properties of the visual representation almost simultaneously.

The process of visual analysis can highly benefit from enlarging the visual representations by testing larger sequences of random numbers and by providing several different representations of the same sequence.

2.3. **Visual randomness.** The perceptual evaluation of random number sequences using the human visual system, in a way similar with every other statistical randomness tests, does not provide a method for proving randomness. Instead it takes advantage of our perceptual system to quickly spot tracks of predictability or non-randomness in the sequence and facilitates the understanding of randomness and lack of randomness.

Nevertheless, by representing a sequence of numbers graphically, the human visual system is only capable of determining the degree to which the representation satisfies visual randomness but is unable to tell the difference between real randomness and visual paternlessness.

In this context, visual analysis is not to be used exclusively, but rather as an efficient component of a larger randomness testing system which also includes powerful statistical test suites and other approaches to randomness evaluation.

3. The inspection tool: FileSeer+

FileSeer+ is a visual evaluation environment and is the result of a follow up work to the inspection tool named FileSeer, presented in [1]. The most important features are listed bellow with emphasis on the original contributions of the present evaluation environment.

Both tools provide the possibility to represent the tested sequence in three different image forms as: black and white (1 bit/pixel), grayscale (1 byte/ pixel) or color images (3 or 4 bytes/pixel) using BMP files. But while the original tool had a predefined dimension of the image in length and width, FileSeer+ allows the tester to adjust these parameters. Furthermore, FileSeer+ allows the visualization of several representations of the same sequence concurrently. These new features may significantly aid the visual system in spotting certain regularities and patterns and may facilitate the understanding of the underlying problem in the random number generator that produced the tested sequence.

The image representations of the sequence can be zoomed in for a more detailed visual inspection and FileSeer+ allows the selection of an interest area for further analysis.

Another completely new feature of FileSeer+ is the integration of several image filters which can be applied on the visual representation of the random sequences in order to emphasize certain deviations from randomness, especially bias and repeating patterns. The integrated filters include edge detection, mean and median filtering, blurring, sharpening and smoothing algorithms.

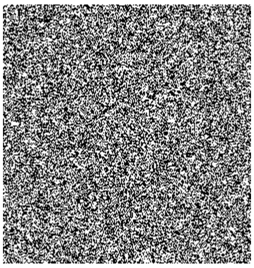
Another powerful component of FileSeer+ is the generation of random walks in one and two dimensions, in the latter case considering eight or four neighbors respectively. When generating random walks we expect a random sequence to show a tendency to fill the available space without showing repetitive patterns or rapidly leaving the area. Random walks can be drawn in black and white, grayscale or color and may be generated step-by-step or only the final result. Another important feature is that the visual area follows the current position in the random walk and it expends as the walk covers a larger space.

As we have already mentioned before, the human visual system is only capable of determining the degree to which the representation satisfies visual randomness but is unable to tell the difference between real randomness and visual paternlessness. Hence, in order to help the human analyzer in reaching to a correct decision on the quality of the tested sequences, certain statistical properties are visually represented, such as balance, entropy and histogram of values. Entropy is the numerical measure of uncertainty, usually expressed in bits per symbol (byte), hence the higher the entropy, the more difficult it is to predict the sequence. The balance expresses the extent to which 0 and 1 bits appear with the same probability and the histogram shows the number of occurrences for every one, two, four and eight bit values from the input file.

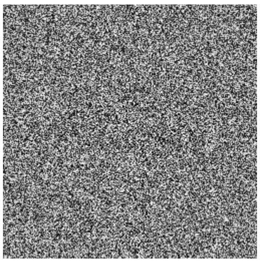
FileSeer+ is a visual testing environment providing a well structured working space where randomness testing projects can be created. Projects can be opened, modified, closed or removed and in each project files with random number sequences can be added or removed. For each file the tester may choose to create several representations, apply image filters, visualize statistical properties, generate random walks and save the desired results in the structure of the project for further use, significantly improving the testing process.

4. Experimental results

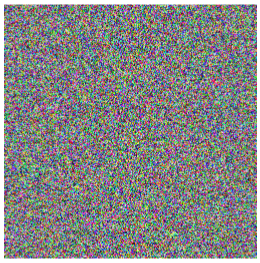
The visual randomness evaluation environment was tested using a large number (more than one thousand) of input files containing data of various level of randomness quality, which was also measured using well known statistical batteries for randomness assessment such as the NIST STS [3] and TestU01 [5].



(A)



(B)



(C)

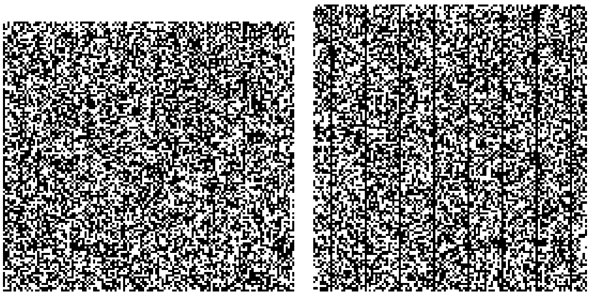
FIGURE 1. Image representation of a high quality random number sequence: (a) black and white image, (b) grayscale image, (c) color image

As we have already mentioned before, in the process of visual analysis we expect to perceive uniform distribution and patternlessness in the image representation whether black and white, grayscale or color - of a high quality random number sequence. Figure 1 shows the image representations for a high quality random number sequence generated by a true random number generator (TRNG).

The importance of allowing the tester to specify the image dimensions in length or width, is a simple but powerful feature because in case of input sequences which show a regular bias, certain dimensions of the image representation can ease the spotting of repeating patterns and nonuniform distribution more than others. Figure 2 depicts the image representations of such a sequence that has a severe bias of every 16th bit towards 0 values. The image on the right expresses more pronouncedly the existence of this bias that forms repetitive patterns.

While analyzing the image it is very useful to get a closer look to a selected area by zooming in. FileSeer+ provides five zooming levels that can be adjusted between one and five times the original size. Figure 3 depicts the color image representation of a larger sequence from the same input file as in the previous experiment, together with a three times zoom level of a selected area in which the colored strikes due to the above mentioned bias are more clearly visible.

Correlations between the subsequences within the input file and repetitions which can be due to exceeding a pseudorandom generators period or a reinitialization with the same seed may form visible traces, as shown in Figure 4, where the same input file is represented in both black and white and grayscale image respectively. There are several repeating patterns which can be easily



(A) (B)

FIGURE 2. Two black and white image representations for the same sequence with different image dimensions

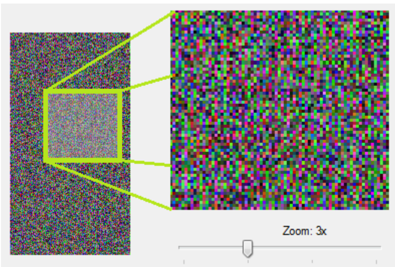
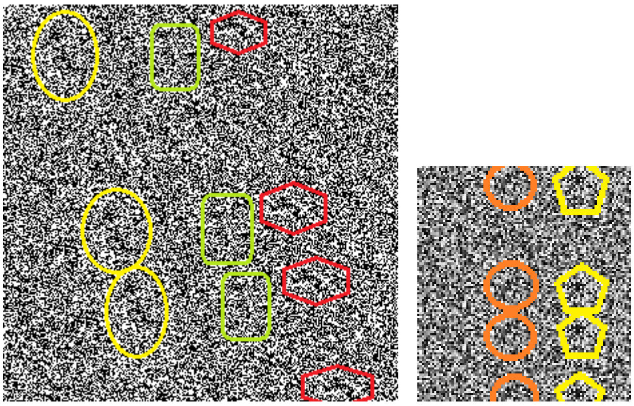


FIGURE 3. Color image representation of a biased sequence and a 3x zoom of a selected area

spotted and some of the most visible patterns are circled with different shapes and colors here to facilitate their tracking.

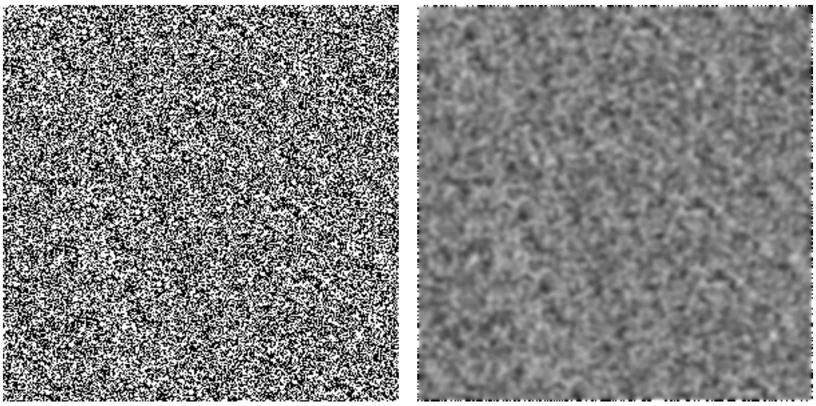
In order to aid the tracking of patterns and nonuniform distribution, FileSeer+ provides a set of image filters (several smoothing and sharpening filters and edge detectors) which can be applied on the visual representation of the sequence in any order and possibly multiple times, allowing also to undo any filtering step if the tester considers its effect unhelpful. Figure 5 exemplifies the usefulness of applying image filters on images when the existing patterns are not easily visible to the human eye. The original black and white image representing the tested sequence is provided on the left side and on the right we can see the effect of applying smoothing filters.

Another way to visualize the tested sequence is by generating random walks. FileSeer+ provides the possibility of creating one and two dimensional walks, and for the latter the user may select between considering four or eight



(a) (b)

Figure 4. Black and white and grayscale image representation of an input file with correlations and repetitions. Some repeating patterns are circled



(a) (b)

Figure 5. Smoothing filters for highlighting patterns: (a)original black and white image, (b) filtered image

neighbors in determining the direction of the next step in the walk. Figure 6 shows the encodings used for the two dimensional walks.

For a high quality random number sequence we expect the random walk to fill the available space without showing repetitive patterns or a tendency to rapidly leave the area. Figure 7 presents the random walk generated using four

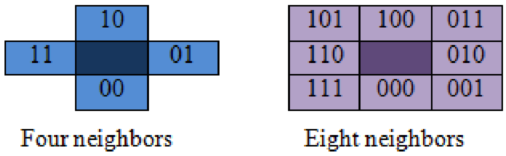


FIGURE 6. Encodings used for the two dimensional random walks

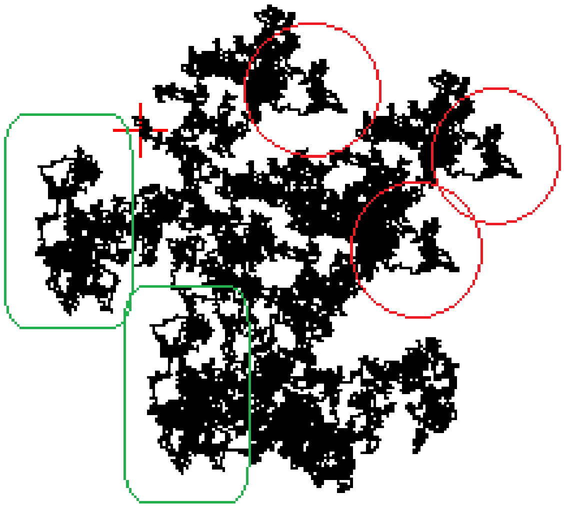
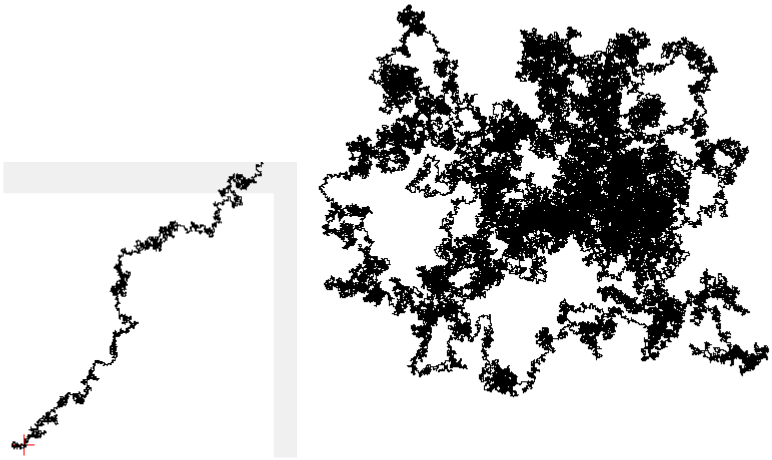


FIGURE 7. Random walk with 4 neighbors for a sequence containing repeating subsequences. The most visible repeating patterns are circled

neighbors and the most visible repetitive patterns are circled. These pattern show that the tested sequence contains recurrent subsequences or correlations. The red cross indicates the starting point of the random walk.

Another evidence of the lack of randomness is shown in Figure 8a, where the sequence is significantly biased towards certain values and hence there is a slight trace while leaving behind the available space, even if the considered sequence is very large. For comparison, Figure 8b depicts the random walk created by a high quality random number sequence.

The randomness evaluation based solely on the analysis of image representations has the serious limitation of not being able to discern between real randomness and visual paternlessness. Hence, before drawing a conclusion it is very helpful to visualize some very basic statistical properties, such as the



(A) (B)

FIGURE 8. Figure 8. Random walks: (a) biased sequence, (b) high quality random number sequence

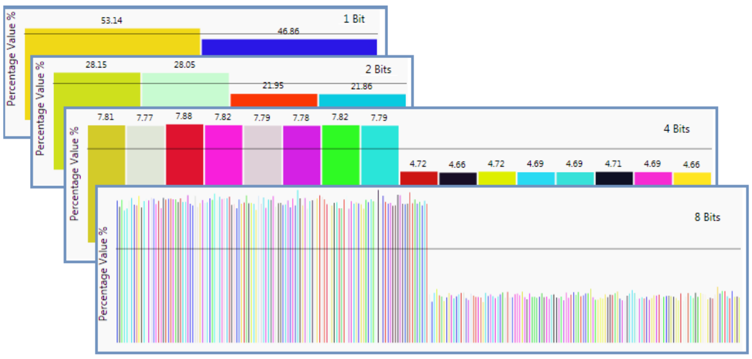


FIGURE 9. Histograms considering 1, 2, 4 and 8 bit values

frequency, the entropy or the balance of values, which can be rapidly computed and graphically represented for the whole sequence or for selected interest areas. Figure 9 presents the one, two, four and eight bits histograms for visually analyzing the frequency of values in the sequence represented as black and white image in Figure 2. The bias towards lower values is clearly visible.

The testing environment provides a highly organized work space where testing projects can be created grouping together test files and folders and where all visual representations can be saved for further use and analysis. Furthermore, each visualization process is handled separately by a different thread so that several visual representations can be generated for the tested sequences helping the tester to compare the results and choose to record the most representative and relevant results.

5. Conclusions

In this work we have presented a testing environment for random number sequences based on visual perceptions. The domain of visual perceptions provides us with a large amount of scientific evidence which show that the human visual system is highly adapted to analyze large sets of similar objects and to extract individual or global statistical properties of the set. This ability is employed by our visual inspection environment in analyzing visual representations of the input sequences and based on the received visual perceptions help the tester to quickly decide whether to reject the sequence for evident traces of lack of randomness, or to further analyze the sequence with other assessment methods, such as statistical testing batteries.

The testing environment, named FileSeer+, provides several methods for visualizing the tested sequence such as black and white, grayscale and color image representations, (with the important feature of adjustable dimensions), the selection of an interest area, several levels of zooming, image filtering and random walks. These are complemented by the visualization of certain statistical properties of the sequence such as the one, two, four and eight bit histograms, the entropy and balance of values.

We have empirically shown how the human tester can use these methods to search for traces of nonrandomness in the visual representation of the tested sequence. Non-uniform distribution of values, the presence of repeating patterns, bias towards certain values and correlation within the sequence can be visually captured and the results demonstrate that the process of visual assessment is very efficient in complementing other more standard randomness evaluation approaches, such as statistical testing. Furthermore perceptual analysis has the major advantage of facilitating the tester to gain insight into the fascinating domain of randomness and randomness testing by understanding what randomness is and how it looks like by applying to the perceptual instead of the cognitive system.

FileSeer+ is not just a tool, but a complex testing environment which allows the tester to create testing projects and efficiently organize the working space. The tester can generate several different visual representations for the tested sequences, keep these representation in the working space for comparative analysis and may choose to save some or all the representations and associate them with the sequence within the created testing project as evidences or for further analysis.

We aim to further improve the testing environment by extending the provided visual representation methods, design an automated method for recognizing problematic areas, and integrate parallel processing for a more efficient assessment of input sequences.

Acknowledgments

This paper was supported by the Post-Doctoral Programme POSDRU /159/1.5/S/137516, project co-funded from European Social Fund through the Human Resources Sectorial Operational Program 2007-2013.

References

[1] D. Ariely, *Seeing sets: representation by statistical properties*, Psychological Science, 12 (2001), pp. 157-162.

[2] S. C. Chong, A. Treisman, *Representation of statistical properties*, Vision Research, 43 (2003), pp. 393–404.

[3] S. C. Chong, A. Treisman, *Statistical processing: Computing the average size in perceptual groups*, Vision Research, 45 (2005), pp. 891-900.

[4] P. L'ecuyer, R. SIMARD. *TestU01: A C Library for Empirical Testing of Random Number Generators*, ACM Trans. Math. Software, Article 22.

[5] G. Marsaglia. *The Diehard test suite*, 2003, Available online: `http://www.csis.hku.hk/diehard/`

[6] K. Marton, I. Nagy, A. Suciu, *Visual Inspection of Random Number Sequences with FileSeer*, Automat. Comput. Appl. Math., 19/1 (2010), pp. 3–10.

[7] N. Robitaille, I. Harris, *When more is less: extraction of summary statistics benefits from larger sets*, Journal of Vision, 11/12 (2011), pp. 1–8.

[8] A. Rukhin et al. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, NIST Special Publication 800-22 (with revisions dated April, 2010).

[9] J. Walker. *ENT - A Pseudorandom Number Sequence Test Program* . Fourmilab, 2008, Available online: `http://www.fourmilab.ch/random/`

Computer Science Department, Technical University of Cluj-Napoca
E-mail address: {`Kinga.Marton, Dan.Patrascu, Alin.Suciu`}`@cs.utcluj.ro`