©2020 Published in 8th International Symposium on Innovative Technologies in Engineering and Science 23-25 October 2020 (ISITES2020 Bursa - Turkey)
https://doi.org/10.33793/acperpro.03.01.60

True - Random Number Generator Based on Image Histogram

*[1]Serkan Dereli
*[1]Bilgisayar Teknolojileri ve Programlama Bölümü, Sakarya Uygulamalı Bilimler Üniversitesi, Sakarya, Türkiye

Abstract

It is the non-repetitive distribution that makes the random numbers important in artificial intelligence techniques, cryptology, transferring a real environment to the virtual world and many more applications. Since the source of true random numbers consists of data from the physical world, the same number chain is never produced. In this study, images taken from the outside world were used as the source of randomness. The resulting image was first converted into an 8-bit gray image, and then the histogram of this gray image was revealed. As is known, an image histogram shows the color distribution in that image. In this study, the color distribution resulting from the histogram has been converted into a random distribution between 0 and 1. As a result, it was observed that the resulting distribution of numbers overlapped with histogram. Since the distribution of the numbers depends on the ratio of the pixels and the ratio of the pixels on the image obtained, the result is a real random number sequence.

Key words: True-random number, histogram, image processing

1. Introduction

Randomness is widely used in different fields of science as well as in all areas of life. Especially it is one of the most fundamental subjects of computer engineering because this is extremely important in simulation [1], cryptography [2], virtual reality [3], numeric analysis [4] and computer networks [5]. For example a random number in cryptography; it should be safe, unpredictable and have good statistical properties [6]. Because, random numbers have an important place in all processes of key generation, initial vector generation, authentication and password generation [7]. In order to meet this need, the scientific world has focused on random number generation and has realized random number generation in two different ways, true and pseudo-numbers [8].

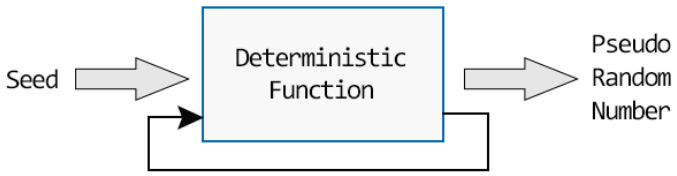

Figure 1. Pseudo Random Number Generator Flow Chart

Pseudo-random numbers (Fig. 1) are developed from a certain initial value with the help of a mathematical model. Since the initial value is constant, the number loop returns to the beginning

*Corresponding author: Address: Department of Computer Technologies and Programming Sakarya University of Applied Sciences, 54187, Sakarya TURKEY. E-mail address: dereli@subu.edu.tr, Phone: +902646160492

after a certain step, so it repeats in the generated numbers. Therefore, if there is a possibility of such a risk to occur, the initial value is changed to change the number sequence [9]. True random numbers are generated by transforming physical quantities obtained from a noise source called entropy. The quality and statistical characteristics of these numbers, which are mostly unpredictable, depend entirely on the source of noise [10]. While it is an advantage that the so-called pseudo random numbers can be produced easily and quickly and do not need any equipment; predictable and repetition possibilities stand out as their disadvantages [11]. On the contrary, the generation of true random numbers requires hardware and is a challenging process, but they are extremely difficult to predict. Therefore, their reliability is extremely high [12].

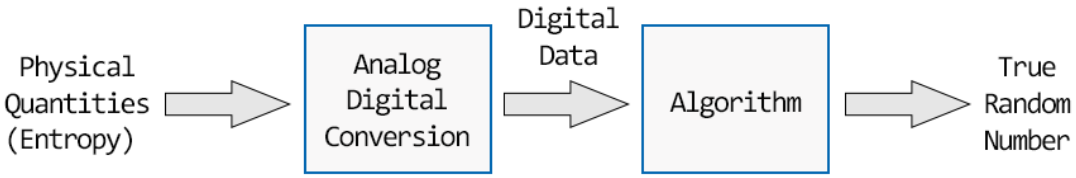

Figure 2. True Random Number Generator Flow Chart

Random numbers have been studied frequently, as they are a popular subject and needed in many disciplines. Koyuncu et al. have realized a new design that generates a real random number based on ANN-Ring for FPGA device. The design also used the VHDL language and 32-bit floating point numbers as numbers [13]. Tuna and Fidan conducted a research study on the importance of chaotic systems in random number generation. In their research, they revealed the comparison between classical methods and FPGA-based methods [14]. Yakut and Özer have developed a system that generates a hybrid random number consisting of a deterministic part and an additional input based on the Keccak algorithm. They subjected the numbers they produced to NIST and autocorrelation tests and analyzed the properties of the numbers statistically [15]. They have realized a real random number generator design inspired by human movements. With a mobile application they developed for this purpose, they transformed the information they received from the GPS and acceleration sensors on the mobile device used by the individual into a series of numbers. Finally, they subjected them to XOR processing to statistically improve the numbers they obtained [16].

In this study, histogram holding the number of each pixel in an image is used as the source of entropy. The values obtained by the image histogram are mapped to values between 0 and 1 with a certain algorithm. Thus, the desired random number is obtained. In this study, the image histogram obtained from 8-bit images was used in testing.

2. Materials and Method

In this study, the image histogram has been used to obtain random numbers. Histogram contains the color distribution information in an image and is used as a basic image processing technique in many studies [17]. It does this by detecting the value of each pixel according to the bit value of the image and keeping it in an array and the resulting sequence is illustrated in the histogram

chart. Image histogram is frequently used in many areas from cryptography [18] to image enhancement, from statistical properties of the image to image compression [19].

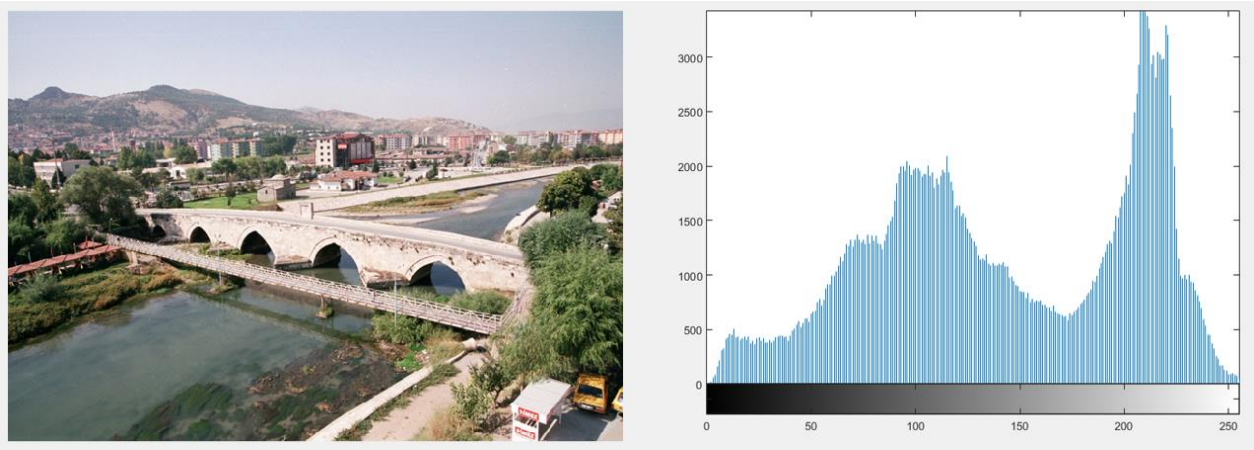

Figure 3. Sample image and its histogram chart

Figure 3 shows a sample image and its histogram graph of this image. According to the graph, the image is 8-bit, so the pixel value range is in the range of 0 to 255. Since this range is also an expression of color tones, it means the distribution of tones according to colors in the chart. It is the horizontal axis that shows this color information in the chart. The vertical axis shows the number of pixels. In this study, pixel numbers in the 0-255 range were scaled to 0-1 and converted into random numbers.

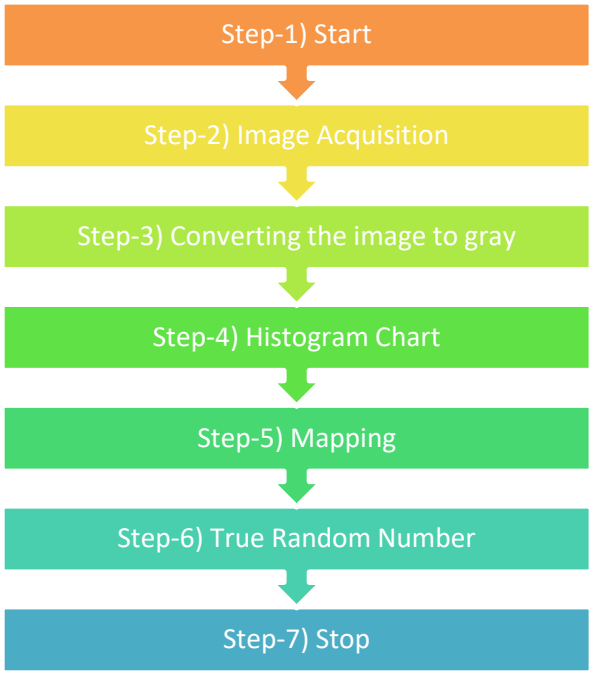

Figure 4. Flow chart the process

Figure 4 shows the true random number generation stages created within the scope of this study. The first four stages consist of basic image processing steps. In step 5, mapping is performed according to the pixel range.

$$C = \frac{Random_{max} - Random_{min}}{Pixel_{max} - Pixel_{min}} \quad (1)$$

The coefficient formula shown in Equation 1 is used for scaling. The pixel value is multiplied by this coefficient and mapped to the [0-1] range. In fact, the coefficient formula reveals a dynamic range and determines the range [0-1] according to the maximum and minimum pixel values. Therefore, a pixel value in the [0-255] range is not always the same number in the range [0-1].

3. Results

In this study, the true random value generation in the range of [0-1] takes place according to the histogram values obtained from an image. The conversion to the value range of [0-1] is performed directly, without any further processing on the histogram values.

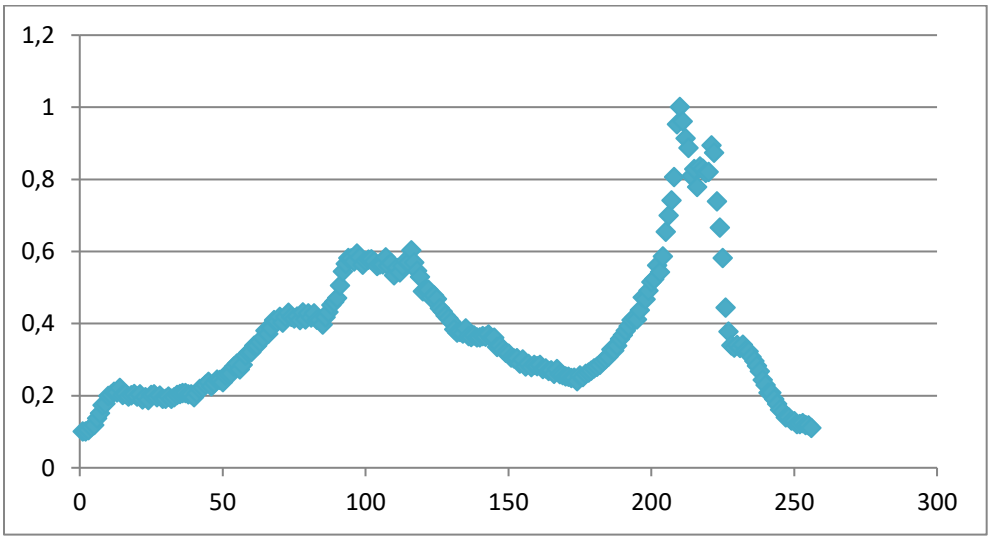

Figure 5. True random numbers obtained

The values shown in Figure 5 have been obtained by mapping the image histogram obtained in Figure 3 to the range [0-1]. With a good look at Figure 5, it is clear that the graph created by the random values obtained corresponds exactly to the histogram curve.

Another important issue in random value generation is the distribution of numbers. Figure 6 shows the distribution ratios of the numbers obtained in this study. In this figure, a sample distribution of 256 numbers obtained with Matlab also appears. While the ratios of the values obtained with Matlab are close to each other, there are big differences between the ratios of the values obtained in this study. This situation is all about the technique of generating random numbers. Because, while the values obtained with Matlab are pseudo random numbers, the values produced within the scope of this study are true random numbers.

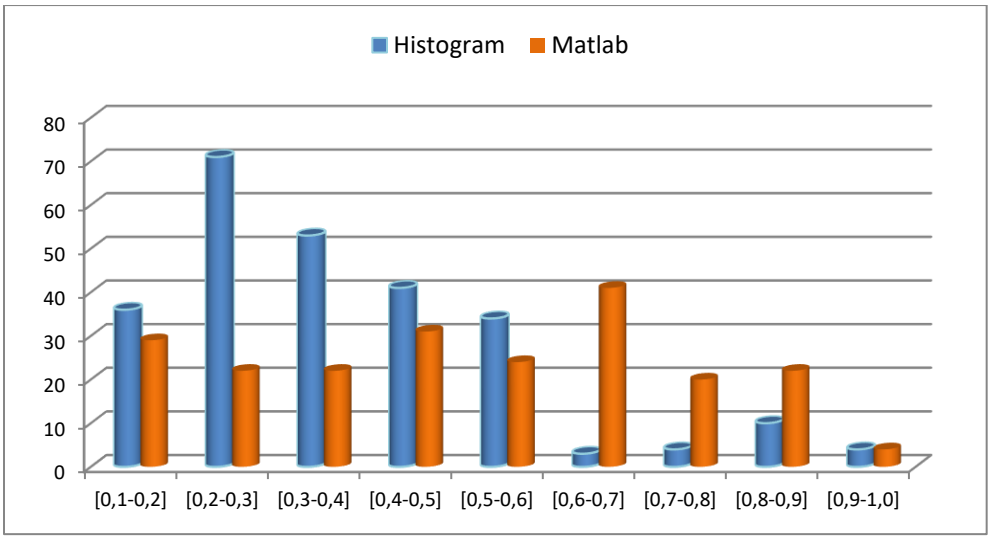

Figure 6. Distribution of true random numbers

Figure 7 shows the comparison of the true random numbers obtained within the scope of this study and the pseudo-random numbers obtained by Matlab in terms of distribution. It is clear that the image obtained in Figure 7 is parallel to the ratios obtained in Figure 6.

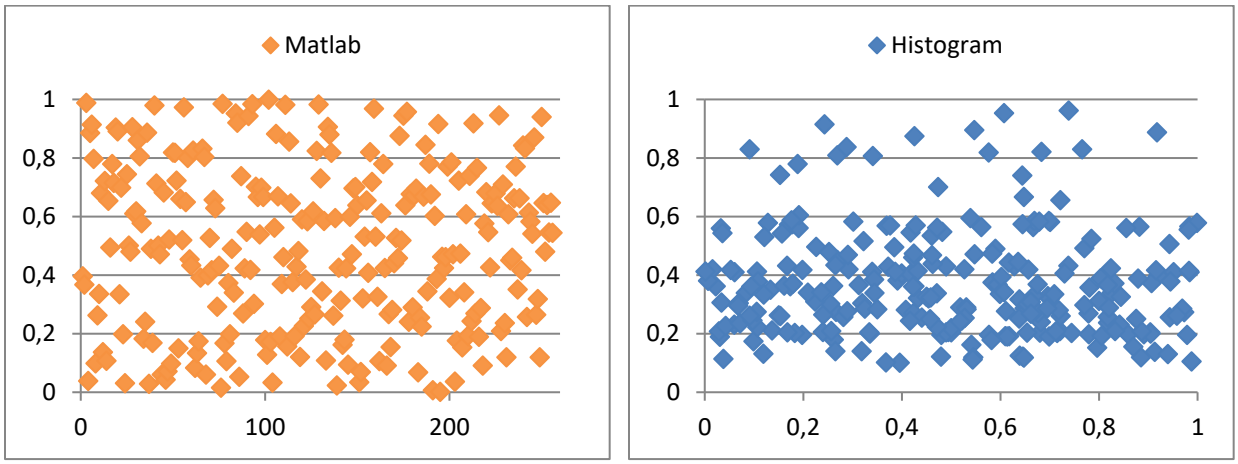

Figure 7. Distribution comparison of random numbers

As a result, true random numbers may not have a normal distribution because they are generated in the frame of data obtained by hardware. This situation does not cause any negativity in the use of random numbers. On the contrary, it is an expected situation. However, if the distribution is desired to be more regular, there are algorithms developed for this and called "finishing". The most widely used of these are the XOR [20] and Von Neuman algorithms [21].

Conclusions

In this study, the histogram curve obtained from the images, which is one of the most fundamental topics in image processing, is taken as an entropy source used to generate true

random numbers in the range of [0-1]. For this, the pixel value range in the image is mapped to the value range [0-1] by means of a mathematical formula. No post-processing has been applied to the random numbers obtained and they have been accepted directly. For this reason, the distribution of random numbers exactly overlaps with the histogram curve. In the result section, the distribution and value ranges analysis of the true random numbers generated were performed and additionally compared with the pseudo-random numbers generated by Matlab. It was clearly seen that the pseudo-random numbers generated by Matlab have a normal distribution, and the distribution of the true random numbers produced within the scope of this study is related to the data from the entropy source.

References

[1] Sugisaka JI, Yasui T, Hirayama K. Fast actual-size vectorial simulation of concave diffraction gratings with structural randomness. JOSA A 2017; 34:2157-2164.

[2] Austrin P, Chung KM, Mahmoody M, Pass R, Seth K. On the impossibility of cryptography with tamperable randomness. Algorithmica 2017; 79:1052-1101.

[3] Pataky TC, Lamb PF. Effects of physical randomness training on virtual and laboratory golf putting performance in novices. Journal of Sports Sciences 2018; 36:1355-1362.

[4] Nahum A, Ruhman J, Huse DA. Dynamics of entanglement and transport in one-dimensional systems with quenched randomness. Physical Review B 2018; 98.

[5] Dereli S. Yüksek Hızlı FPGA ile Yeni Bir LFSR Tabanlı 32-Bit Kayan Noktalı Rastgele Sayı Üreteci Tasarımı. International Journal of Advances in Engineering and Pure Sciences 2020; 32:219-228.

[6] Cardell SD, Requena V, Fúster-Sabater A, Orúe AB. Randomness Analysis for the Generalized Self-Shrinking Sequences. Symmetry 2019; 11:1460-1471.

[7] Avaroğlu E, Türk M. Son işlemin Gerçek Rasgele Sayı Üreteçleri Üzerindeki etkisinin İncelenmesi. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı 2013.

[8] Wang L, Cheng H. Pseudo-random number generator based on logistic chaotic system. Entropy 2019; 21:960.

[9] Bakiri M, Guyeux C, Couchot JF, Oudjida AK. Survey on hardware implementation of random number generators on FPGA: Theory and experimental analyses. Computer Science Review 2018; 27:135-153.

[10] Koyuncu İ, Tuna M, Pehlivan İ, Fidan CB, Alçın M. Design and implementation of chaos based true random number generator on FPGA. Analog Integrated Circuits and Signal Processing 2020; 102:445-456.

[11] Aydın Ö, Dalkılıç G. A hybrid random number generator for lightweight cryptosystems: xorshiftLplus. The 3rd International Conference on Engineering Technology and Applied Sciences (ICETAS) 2018.

[12] Avaroğlu E, Çavdar T. Kuantum Rasgele Sayı Üreteçleri. International Conference on Artificial Intelligence and Data Processing (IDAP) 2018:1-4.

[13] Koyuncu İ, Erdogmus P, Tuna M, Alçın M. FPGA Üzerinde YSA-RİNG Tabanlı Yeni Bir Gerçek Rasgele Sayı Üreteci. I. International Science and Innovation Congress 2019.

[14] Fidan CB, Tuna M. Kaotik sistemler ve FPGA tabanlı kaotik osilatörlerin gerçek rasgele sayı üretimindeki (GRSÜ) önemi üzerine bir araştırma. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi 2018; 33:473-491.

[15] Yakut S, Özer AB. Efficient Hybrid Random Number Generator Based on Keccak. International Conference on Artificial Intelligence and Data Processing (IDAP) 2018.

[16] Tuncer SA, Genç Y. İnsan Hareketleri Tabanlı Gerçek Rasgele Sayı Üretimi. Bitlis Eren Üniversitesi Fen Bilimleri Dergisi 2019; 8:261-269.

[17] Kılıçaslan M, Tanyeri U, Demirci R. Renkli Görüntüler İçin Tek Boyutlu Histogram. Düzce Üniversitesi Bilim ve Teknoloji Dergisi 2018; 6:1094-1107.

[18] Kurnaz H, Konyar MZ, Sondaş A. Yakın Histogramlar Temelli Yeni Bir Hibrit Veri Gizleme Yöntemi. Avrupa Bilim ve Teknoloji Dergisi 2020; 18:683-694.

[19] Alkan A, Selcuk T, Çolakoğlu AS. Görüntü İşleme Teknikleri Kullanılarak Ekmek Doku Analizi Ve Arayüz Programının Oluşturulması. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi 2018; 33:31-41.

[20] Han Y, He W, Dong H, Liu J. A verifiable visual cryptography scheme based on XOR algorithm. IEEE 14th International Conference on Communication Technology 2012; 673-677.

[21] Boche H, Schaefer RF, Baur S, Poor HV. On the algorithmic computability of the secret key and authentication capacity under channel, storage, and privacy leakage constraints. IEEE Transactions on Signal Processing 2019; 67:4636-4648.