International Journal of Computer Applications Technology and Research
Volume 6–Issue 7, 326-328, 2017, ISSN:-2319–8656

A Novel method of true random number generation using water laser interaction.

K.Elampari
Department of Physics
S.T.Hindu College
Nagercoil, India

B.Ramakrishnan
Department of Computer Science
S.T.Hindu College
Nagercoil, India

Abstract: This paper demonstrates the generation of true random number sequence using a simple laser scattering using water. A microcontroller based data acquisition system is used to capture the data and several statistical tests are performed over the generated data to explore the amount of randomness. The test statistic values reveal the possibility of generating a true random sequence of bits using this idea.

Keywords: laser; scattering; pseudo-random generator;true random number;cryptography;randtests; R

1. INTRODUCTION

Random number generation is an important and frequent requirement in various applications. Different applications require various degrees of randomness. Though the output of a pseudo-randomgenerator is deterministic it is sufficent for some applications. But in other situations, such as in cryptographic applications, generated bits must be truly random, otherwise the security of the entire application could be compromised.

In this paper we present a novel method of generating true random number sequence using the interaction between photons and water molecules. The shape of the water is decisive on how the light passes through it. Coming from an optically less dense medium (air) and entering a denser one (water), the light is partly reflected back while partly entering the water. Depending on the shape of the water, the light forms crinkle patterns or becomes diffused randomly in all directions. Also the reflected light is partly polarized (horizontally) and the part that enters the water is vertically polarized. As photons of light move through substances they don't simply pass through unaffected. Photons interacts with atoms and molecules comprising it. Photons carry discrete amounts of energy called quanta which can be transferred to atoms and molecules when photons are absorbed [1].

2. WATER LASER INTERACTION

There are six ways in which photons may interact with matter: Coherent Scattering, Photoelectric Effect, Incoherent Scattering, also known as Compton Scattering or Compton Effect, Pair Production, Triplet Production, Photodisintegration.These may cause the photon to attenuate (lose some of its energy and/or disappear). Coherent (or Rayleigh) scattering occurs at low photon energies. A photon may interact with an orbital electron and is then deflected (or scattered) at a small angle. There is no change in energy of the photon and no other effects occur. Incoherent scattering occurs when a photon has a much greater amount of energy than the binding energy of the electron, effectively considering the electron as 'free'. In this interaction, the photon interacts with the 'free' electron, giving up some of its energy and undergoing scattering. The electron receives the energy and is set in motion in a different direction. Photons may be scattered in any direction and is purely random [2]. Light transmission through a water sample is determined by physical properties such as particle size, shape, suspended solids concentration (SSC), and composition, temperature, and chemical properties such as the presence of nearinfrared (NIR) absorbing dissolved matter. There is enormous variation in these properties in the environment, resulting in a nearly infinite number of unique optical characteristics for water.

Light is an ensemble of photons that are absorbed and scattered by water, suspended particles, and dissolved matter as they travel through a sample. The absorption coefficient is a measure of the conversion of radiant energy to heat and chemical energy. It is numerically equal to the fraction of energy absorbed from a light beam per unit of distance traveled in an absorbing medium.

The angular distribution of light intensity scattered from a beam by a water sample is called the volume scattering function, VSF. The angle between this beam and scattered light rays is the scattering angle. Forward-scattered radiation occupies the hemisphere surrounding the incident beam and orientes away from the source and back scattered radiation fills the opposite hemisphere. Figure 1 shows VSFs computed from Mie theory for air bubbles, mineral grains, and biological material as well as the forward- (0° to 90°) and back-scattering (> 90°) VSF regions.

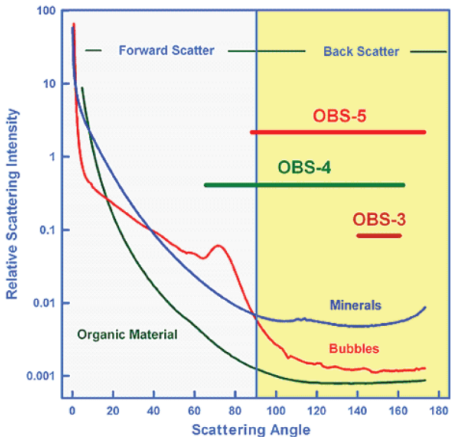

Figure 1. Graph shows VSFs computed from Mie theory

The VSF for bubbles is strongly peaked in the forward direction relative to the other materials and biological material back scatters 10 to 50% less light than the other particles [3]. There are generally two tendencies for the molecules of a material- the tendency to move randomly due to heat and the tendency to want to stick together because of electric charge between molecules. Technically, heat is the flow of thermal,

kinetic energy.The effect of heat on water depends on whether the energy is moving into the water (endothermic) or moving out of the water (exothermic). When water molecules gain energy, the average speed of the molecules increases; this is measured as a temperature change if enough energy is gained. Conversely, when energy leaves water molecules, the average speed of the molecule decreases, and a temperature decrease may be observed. Thus the tendency to move randomly is controlled by the temperature. Increase in temperature eventually increases the random movement and at the time of boililing all the water molecules spreads out as much as it can and get more random motion. Next, boiling is the most extreme form of evaporation as individual molecules happen to break away from the liquid through random movements.
Boiling is actually a very efficient heat transfer process. When the bottom of the container is much hotter than the boiling point of the water (i.e) when the boiling point is breached, tiny bubbles of water vapor are produced. The bubbles rise, due to buoyancy, and then collapse as they reach the denser, relatively cooler water at the surface. This motion not only helps to move the water around more quickly, but the bubbles themselves transfer heat energy as well. This bubble formation is called nucleate boiling and it is a far more effective way to transfer heat on its own than natural convection [4][5]

3. EXPERIMENTAL SETUP

The experimental setup consists of a laser source, nucleate boiling water, an array of high sensitive photo diodes as light sensors connected with Arduino Uno microcontroller circuit, and Parallax Data Acquisition tool (PLX-DAQ). When the laser beam is passed through the nucleate boiling water, the photons are scattered in different directions randomly due to the pure random movement of water molecules. The intensity variation of the outgoing beam in different directions is captured by the array of photo diodes. The sensor ouputs from the microcontroller are passed through the Parallax Data Acquisition tool (PLX-DAQ) to the PC for further processing and testing.

4. RANDOMNESS TEST

The desirable properties of random numbers are uniformity and independence. In order to test the amount of randomness present in the generated data, several randomness tests were performed.The algorithms of testing a random number generator are based on some statistics theory, i.e. testing the hypotheses. Although there is no true test to determine whether a sequence is random there are several widely accepted tests that we have utilized. Several of these tests are designed to test a specific null hypothesis. In this case, the hypothesis is that the bit-sequence under test is random. Each of the tests creates a test statistic, which is then used to calculate an associated p-value, which is related to the strength of the evidence against the null hypothesis. This p-value is a value on the interval [0,1], with a p-value of 1 denoting perfect randomness and a p-value of 0 denoting perfect nonrandomness. A significance level (α) is then chosen for the tests. If $p \geq \alpha$, then the null hypothesis is accepted; i.e., the sequence appears to be random. If $p < \alpha$, then the null hypothesis is rejected; i.e., the sequence appears to be nonrandom.Typically α is chosen to be 0.01 meaning that assuming the test is passed the sequence can be said to be random (or nonrandom) with a confidence of 99%.
According to various type of non randomness that may exist in Random bit sequences it is not practical to find non randomness patterns by just using one test. Most of the statistical tests are collection of tests. This collection is generally known as ‘suite’ or ‘battery’ of statistical tests. Some of the important tests carried out over the generated data in this study are

1. Ent Test
2. Bartel Rank Test
3. Cox Stuart Test
4. Turning Point Test
5. Runs Test

All these tests except ENT were performed by using “randtests” package for R [6]. The test results were summarized in the sections 4.1 to 4.5

4.1 The ENT test

Originally ENT test consists of six experiments which are Entropy test, Compression ratio test, Chi-square test, Arithmetic Mean test (AM), Monte Carlo value of PI and Serial Correlation Coefficient (SCC). Each test has a maximum score; Entropy test: 8.0, Compression ratio:0.0, Chi-square test:1.0, AM test:127.5 SCC:0.0, , Monte carlo value of PI: 3.1415926535 (upto 10 places).
The chi-square test is the most commonly used test for the randomness of data, and is extremely sensitive to errors in pseudorandom sequence generators. The chi-square distribution is calculated for the stream of bytes in the file and expressed as an absolute number and a percentage which indicates how frequently a truly random sequence would exceed the value calculated. It is interpreted that the percentage as the degree to which the sequence tested is suspected of being non-random. If the percentage is greater than 99% or less than 1%, the sequence is almost certainly not random. If the percentage is between 99% and 95% or between 1% and 5%, the sequence is suspect. Percentages between 90% and 95% and 5% and 10% indicate the sequence is “almost suspect” [7] .
The ENT test on the data gives, Entropy = 7.999980 bit per cycle, Optimum compression ratio: 0 percent. Chi square distribution for the samples is 294.60, and randomly would exceed this value 4.46 percent of the times , Arithmetic mean value is 127.5136. Monte carlo value for Pi is 3.1415852423 (error = 0.0001 percent) Serial correlation coefficient is -0.000086 (totally uncorrelated = 0.0).
Since the corrleation between a pair of independent random numbers or variables is 0, the auto corrleation function acf() is used to test the generated data. The acf equals 1 at lag 0, and is always between -1 and 1. The plot in figure 2 illustrates the lack of correlation and support randomness.

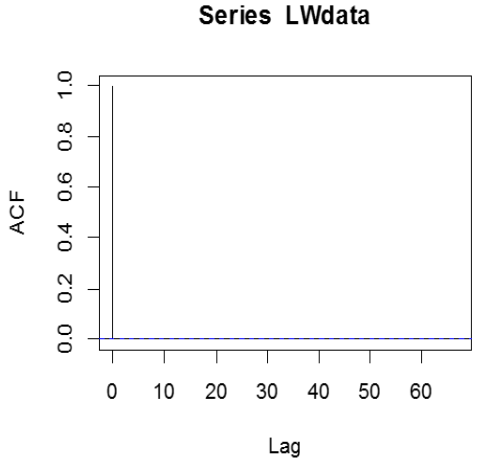

Figure 2. ACF of Generated Data

4.2 Bartels Rank Test

This is the rank version of von Neumann's Ratio Test for Randomness. Suppose that in the sequence of n measurements R_i is rank i of observation i_x . The hypothesis H_0 under test is rejected at large in modulus values of the statistics [8]. The value of the normalized test statistic for the generated random numbers is 2.0 and the p-value is 0.05 with the alternative hypothesis of non-randomness.

4.3 Cox Stuart test

Cox-Stuart nonparametric test can be used to verify the sequence of measurements to determine the presence of a trend in the mean, as well as in the variance. Data is grouped in pairs with the i^{th} observation of the first half paired with the i^{th} observation of the second half of the data. If the length of the data stream is odd the middle observation is eliminated [9]. The cox stuart test is then simply a sign test applied to these paired data [10]. The test statistic value (the number of pairs with a signal "+") is 1309300, n = 2621400 with a p-value of 0.09429, where n is the number of pairs, after eliminanting ties.

4.4 Turning Point Test

A turning point test is a statistical test of the independence of a series of random variables and the test is reasonable for a test against cyclicity [11][12]. The test statistic value is 1.1145 with p=0.2651. Since the the critical value ($\alpha = 0.01$) 2.33 is > test statistic value the alternate hypothesis of non-randomness is rejected.

4.5 Runs Test

The Runs Test performs the Wald-Wolfowitz test of randomness for continuous data [13]. A run is defined as a succession of similar events preceded and followed by a different event. The length of the run is the number of events that occurs in the run. An up run is a sequence of numbers each of which is succeeded by a larger number. Similarly, a down run is a sequence of numbers each of which is succeeded by a smaller number. The test statistic value for the data is 0.71887 < the critical value (p = 0.4722) and the alternative hypothesis is rejected.

5. RESULTS AND CONCLUSION

A set of five statistical tests were used to test the randomness of the generated data. Other than Bartel Rank test all tests statistic values reveal that there is an evidence for rejecting the alternate hypothesis of non-randomness. For further powerful testing of randomness of the sequence, test suits like DIEHARD and NIST may be used. This study reveals the possibility of generation of random bits based on the interaction of water and photons. By using proper optical components and well adujstable photon source it is possible to generate a true sequence of random bits.

6. REFERENCES

[1] Diemer, G.S., 2009. Quinta Essentia - Part 1- A practical guide to space- Time engineering, https://books.google.co.in/books?isbn=1409202720

[2] Photon Interactions OzRadOnc, http://ozradonc.wikidot.com/photoninteractions)

[3] John Downing, 2008. Effects of Light Absorption and Scattering in Water Samples on OBS Measurements, Campbell Scientific, Inc

[4] Tara Ruttley, 2011. T*he physical science of boiling in space.* https://blogs.nasa.gov/ISS_Science_Blog/2011/04/15/post_1301433765536/

[5] https://socratic.org/questions/how-does-heat-energy-affect-the-movement-of-water-molecules

[6] Frederico Caeiro and Ayana Mateus, 2014. randtests: Testing randomness in R. R package version 1.0. https://CRAN.R-project.org/package=randtests

[7] Walker, J. 1998. ENT Test suite, http://www.fourmilab.ch/random

[8] Bartels, R., 1982. The Rank Version of von Neumann's Ratio Test for Randomness, Journal of the American Statistical Association, 77(377), 40–46

[9] Cox, D. R., and Stuart, A. 1955. Some quick sign test for trend in location and dispersion, Biometrika, 42, 80-95.

[10] Sprent, P. and Smeeton, N.C. 2007. Applied Nonparametric Statistical Methods, 4th ed., Chapman and Hall/CRC Texts in Statistical Science.

[11] Brockwell, P.J, and Davis, R.A. 2002. Introduction to Time Series and Forecasting, 2nd edition, Springer (p. 36).

[12] Mateus, A. and Caeiro, F. 2013. Comparing several tests of randomness based on the difference of observations. In T. Simos, G. Psihoyios and Ch. Tsitouras (eds.), AIP Conf. Proc. 1558, 809–812

[13] Gibbons, J.D. and Chakraborti, S. 2003. Nonparametric Statistical Inference, 4th ed. (pp. 78–86). URL: http://books.google.pt/books?id=dPhtioXwI9cC&lpg=PA97&ots=ZGaQCmuEUq