

MATHEMATICAL ALGORITHM FOR MAGNETIC RESONANCE IMAGING

HOJONG CHOI AND SEUNG-HYEOK SHIN*

ABSTRACT. In this study, we investigated the noise sources used in random number generators. For the random number generators, conventional methods use noise sources that depend on the hardware and noise sources provided by a specific operating system (OS) as seeds. However, our proposed algorithm presents a new method for generating noise sources independent of the hardware and OS. The noise source presented in this study was used to verify the random number distribution using time series and frequency distribution data and to evaluate the random number using the National Institute of Standards and Technology (NIST) SP800-90B random number tool. The data was randomized using the excessive noise generated. By testing the performance of the conventional and proposed mathematical algorithms, we observed a similar degree of randomness with magnetic resonance imaging data. Therefore, we can confirm that we can use the proposed mathematical algorithm as a noise source in low-end systems, such as microprocessor-based microcomputers, where it is difficult to collect noise sources based on the abundant resources provided by hardware and OSs.

1. INTRODUCTION

MRI can provide non-invasive images with high penetration depth; therefore, it is widely used to obtain disease information from the areas of the shoulder, brain, and lumbar region in universities or small clinics; however, it is extremely expensive and difficult for patients with metallic artificial teeth, inner ears, pacemakers, and spinal implants [18]. The traditional benchtop MRI machine has high-strength MRI scanners higher than 1.0 Tesla (T). In particular, most market shares of high-cost benchtop MRI machines are used in developed countries, such as the USA, Europe, and Japan [19]. In most Asian countries, including India, MRI machines are rarely used for clinical or diagnostic purposes [16].

Cyberattacks on medical infrastructure are known because of the adoption of data sharing technologies [17, 21, 22]. One of the dedicated victims of corrupted data from these cyberattacks was in medical imaging systems globally [7–9]. The European Agency for Network and Information Security states that encrypted health information and data must be protected using proper keys and protocols [14].

Previous studies have been conducted on the development of encryption algorithms for medical imaging modalities. The image encrypted using the watermarking technique was used with the public key RSA (Rivest-Shamir-Adleman) algorithm for general medical image applications [12]. A lossless edge map-based

2020 *Mathematics Subject Classification.* 65C10, 65C99.

Key words and phrases. Random number; magnetic resonance imaging; mathematical algorithm.

*Corresponding author.

cryptosystem was proposed for medical images [5]. Images encrypted using an elliptical curve have been proposed for multiple medical image applications [3]. Medical images encrypted with two watermarks were embedded in high-resolution MRI images [13]. Two discrete logistic maps were used to encrypt the MRI system [10]. A multichaotic map system was used to encrypt medical images [1]. Thus, security and encryption technology are important research issues for medical images.

The remainder of this paper is organized as follows. Section II describes the detailed analysis of the proposed mathematical algorithm. The procedure of the random bit generation will be described. The method for generating the random number by the conventional and proposed algorithms will be described. Section III presents encrypted data with the conventional and proposed methods. The random number generation distribution and times series data when using the conventional and proposed method will be provided. The proposed methods will be provided for further comparison. Finally, Section IV presents the conclusions of the study.

2. METHODS

This section briefly describes the proposed method. First, we constructed the seed from the noise generation method using the existing noise source and mathematical algorithm, and then produced the seed, which is a 128-bit symmetric key block cipher. Second, we generate random bits with a random number generator using seeds. Therefore, random bits were generated using existing noise sources. We must evaluate the randomness of noise sources and random numbers when using existing noise sources and mathematical algorithms. Using National Institute of Standards and Technology (NIST) SP-800 90B, we evaluated randomness of the conventional and proposed mathematical algorithms [6]. Subsequently, we measured the noise after randomization using two random numbers generated by the random number generator. Figure 1 describes the generation process of a random bit.

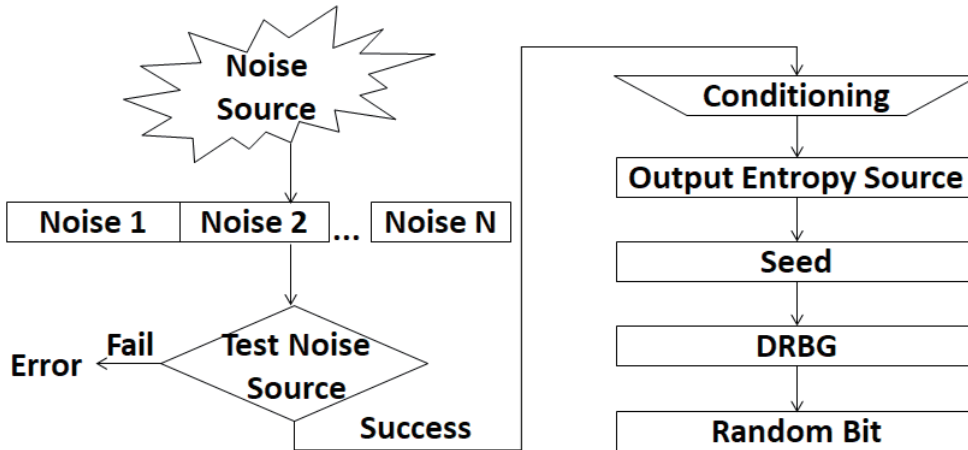


FIGURE 1. The procedure of the random bit generation.

In the proposed algorithm, random numbers must satisfy the following probability functions: For example, probability functions with variables X and Y can be defined as shown in Equation (2.1).

$$(2.1) \quad \text{Probability}(X \cup Y) = \text{Probability}(X)\text{Probability}(Y)$$

Typically, a random bit generated by a mathematical algorithm is assumed to be deterministic. Therefore, we define the relationship in (2.2).

$$(2.2) \quad x_k \neq x_{k+1} \Leftrightarrow f(x_k) \neq f(x_{k+1})$$

where k is a finite number.

We assume that the periodic function fluctuates at the interval p in Equation (2.3) [9, 11].

$$(2.3) \quad f(x) = f(x + p)$$

Equation (2.4) does not reflect a one-to-one correspondence as shown in Equation (2.3). Equation (2.4) is a sine function, which is a typical periodic function [20]. The linear feedback shift register (LFSR) allows the periodic-domain section of the sine function to be adjusted randomly.

$$(2.4) \quad f(x, k) = \sin(x + s_k)$$

The range of the c function is defined in Equation (2.5).

$$(2.5) \quad c_0, c_1, \dots, c_{n-1} = (0, 1)$$

The LFSR used in Equation (2.6) was applied to the function from Equation (2.4). Equation (2.6) represents the LFSR [15]. s_i and c_i represent the initial value and the coefficient of equation $S(s_i)$, respectively.

$$(2.6) \quad s_{i+n} = S(s_i, s_{i+1}, s_{i+2}, \dots, s_{i+n-1}) = c_0 s_i + c_1 s_{i+1} + \dots + c_{n-1} s_{i+n-1}$$

Figure 2 shows the bit operation structure of (2.6). The proposed algorithm defines a function whose domain is irregularly spaced by defining a value that changes to the LFSR in the domain of the sine periodic function.

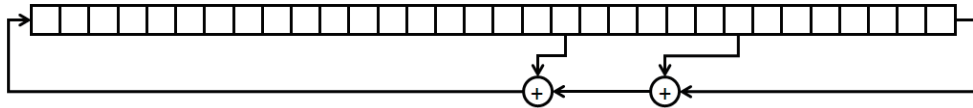


FIGURE 2. The LFSR structure used in the proposed algorithm.

This irregularity guarantees that values in the range of $f(x, k)$ are generated in an irregular state. Equation (2.7) shows the method for generating the final random

number by converting the random bits generated by the conventional and proposed algorithms into eight bits [2, 4].

$$(2.7) \quad y_n = (y/2^{(8n)}) \bmod 256,$$

The random bit generated in Equation (2.4) is calculated in Equation (2.7); therefore, we can generate values between 0 and 255.

3. RESULTS AND DISCUSSION

The existing noise source (CryptGenRandom) had 32-byte sample size. We compared the noise source entropy using the conventional and proposed algorithms. For the conventional algorithm, the mean, median, and mode values were 3921.44, 3902.00, and 3891.00, respectively. The mean, median, and mode values of the proposed algorithm were 3921.66, 3908.50, and 3935.00, respectively.

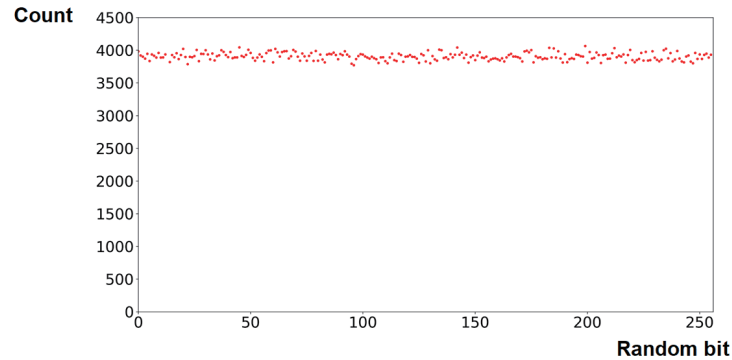


FIGURE 3. The random number generation distribution when using the CryptGenRandom function.

Figure 3 shows the number of counts versus the random bits when using the conventional algorithm. When generating a random number of size $1000 \times 663 \times 3$, we evenly generated a frequency of approximately 4000 in the range of 0 – 255.

In Figures 3 and 4, random bits on the x-axis were extracted by transforming the 32-bit data generated by the CryptGenRandom function. The proposed algorithm into 8-bit data, as shown in Equation (2-6), and they appear as values between 0 and 255. The count on the y-axis indicates the output frequency of an 8-bit random bit consisting of $1000 \times 663 \times 3$.

Figure 4 shows the number of counts versus the random bits when using the proposed algorithm. When generating a random number of size $1000 \times 663 \times 3$, we observed that we still generated a frequency between 3800 and 4000 in the range of 0 – 255.

Figure 5 show time series information for random number generation from 0 to 255 when using the conventional method. We can observe that conventional algorithms generate random data.

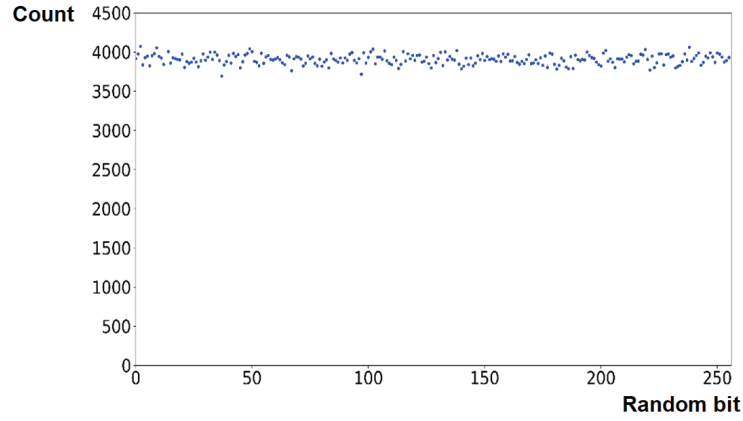


FIGURE 4. The random number generation distribution when using proposed method.

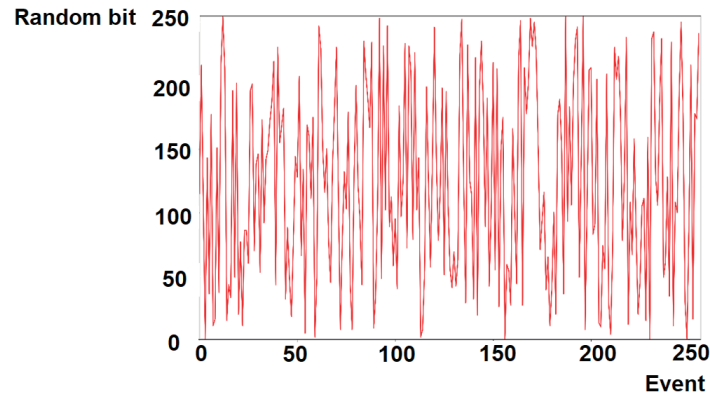


FIGURE 5. Random number generation time series data from zero to 255 when using conventional method.

In Figures 5 and 6, the event on the x-axis represents the index of all random bytes from zero to $1000 \times 663 \times 3$, that is, time series data, with a size of 1000. A random bit on the y-axis represents a value ranging from zero to 255 corresponding to the index of each random byte. We confirm that the data generated by the conventional and proposed algorithms exhibit randomness.

Figure 6 shows time series information for random number generation from zero to 255 when using the proposed method. We can observe that proposed algorithm can still generate random data from zero to 255.

The NIST SP-800 90B value evaluates randomness based on eight bits. The closer it is to 8 bits, the greater the entropy (complexity: randomness). In the experimental results with the condition of NIST SP-800 90B, the randomness when using the conventional and proposed algorithms were 3.9918 and 3.9861 bits, respectively. Therefore, these results indicate that comparable randomness values can replace

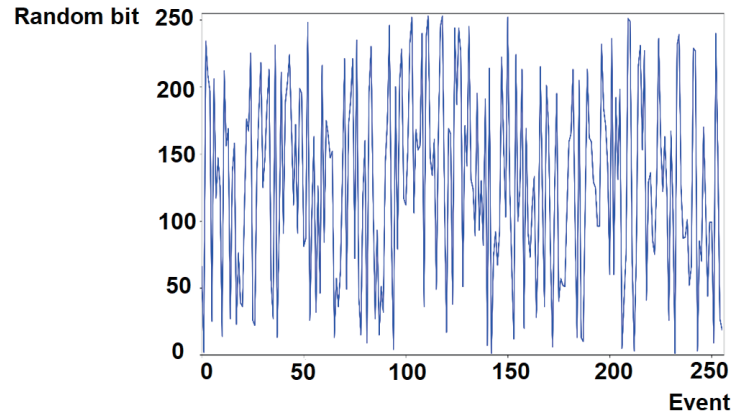


FIGURE 6. Random number generation time series data from zero to 255 using proposed method.

conventional hardware-based methods with mathematical algorithm-based methods.

4. CONCLUSION

We applied the proposed mathematical algorithm for MRI applications. In this study, we propose a random number generation algorithm. LFSR was applied to strengthen the irregularity of random numbers generated from periodic functions.

When generating a random number of size $1000 \times 663 \times 3$ using conventional method, we evenly generated a frequency of approximately 4000 in the range of $0 - 255$. When generating a random number of size $1000 \times 663 \times 3$ using proposed method, we observed that we still generated a frequency between 3800 and 4000 in the range of $0 - 255$.

In the experimental results with the condition of NIST SP-800 90B, the randomness when using the conventional (CryptGenRandom) and proposed algorithms were 3.9918 and 3.9861 bits, respectively. Therefore, we can confirm that a noise source that guarantees similar performance can be implemented through the proposed method, in addition to the random number generation method provided by the current hardware and specific operating system.

We can confirm that the proposed algorithm can be used as a noise source to produce a similar performance in hardware resources or embedded systems that do not have abundant resources, such as Windows or Linux operating systems.

REFERENCES

- [1] R. I. Abdelfattah, H. Mohamed and M. E. Nasr, *Secure image encryption scheme based on DNA and new multi chaotic map*, Journal of Physics **1447** (2020): 012053.
- [2] R. P. Agarwal and H. Agarwal, *Origin of irrational numbers and their approximations*, Computation **9** (2021): 29.
- [3] A. Banik, Z. Shamsi and D. S. Laiphrahpam, *An encryption scheme for securing multiple medical images*, Journal Information Security and Applications **49** (2019): 102398.

- [4] G. Bergman, *A number system with an irrational base*, Oxford, Mathematics Magazine **31** (1957), 98–110.
- [5] W. Cao, Y. Zhou, C. L. P. Chen and L. Xia, *Medical image encryption using edge maps*, Signal Processing **132** (2017), 96–109.
- [6] D. Chen, H. Chen, L. Fan and K. Luo, *Error analysis of NIST SP 800-22 test suite*, IEEE Transactions on Information Forensics and Security **18** (2023), 3745–3759.
- [7] H. Choi and S.-H. Shin, *Novel random number generation for ultrasound systems*, Journal of Nonlinear and Convex Analysis **24** (2023), 1835–1841.
- [8] M. Eichelberg, K. Kleber and M. K. 辰 mmerer, *Cybersecurity in PACS and medical imaging: an overview*, Journal of Digital Imaging **33** (2020), 1527–1542.
- [9] N. J. Fine and H. S. Wilf, *Uniqueness theorems for periodic functions*, Proceedings of the American Mathematical Society **16** (1965), 109–114.
- [10] S. M. Ismail, L. A. Said, A. A. Rezk, A. G. Radwan, A. H. Madian, M. F. Abu-ElYazeed and A. M. Soliman, *Biomedical image encryption based on double-humped and fractional logistic maps*, in: 2017 6th International Conference on Modern Circuits and Systems Technologies (MOCASST), 2017, pp. 1–4.
- [11] U. Jung and H. Choi, *Active echo signals and image optimization techniques via software filter correction of ultrasound system*, Applied Acoustics **188** (2022): 108519.
- [12] P. Kishore, N. Venkatram, C. Sarvya and L. Reddy, *Medical image watermarking using RSA encryption in wavelet domain*, in: 2014 First International IEEE Conference on Networks and Soft Computing (ICNSC), 2014, pp. 258–262.
- [13] N. Kittawi and A. Al-Haj, *Reversible data hiding in encrypted images*, in: 2017 8th International Conference on Information Technology (ICIT), 2017, pp. 808–813.
- [14] H. Kwon, S. An, H.-Y. Lee, W. C. Cha, S. Kim, M. Cho and H.-J. Kong, *Review of smart hospital services in real healthcare environments*, Healthcare Informatics Research **28** (2022), 3–15.
- [15] R. Oommen, M. K. George, and S. Joseph, *Study and analysis of various LFSR architectures*, in: 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), 2018, pp. 1–6.
- [16] M. Sarraçanie and N. Salameh, *Low-field MRI: How low can we go? A fresh view on an old debate*, Frontiers in Physics **8** (2020): 172.
- [17] S.-H. Shin, W.-S. Yoo and H. Choi, *Development of public key cryptographic algorithm using matrix pattern for tele-ultrasound applications*, Mathematics **7** (2019): 752.
- [18] P. Strojnik and P. H. Peckham, *The Biomedical Engineering Handbook*, CRC Press, Boca Raton, FL, USA, 2000.
- [19] P. Suetens, *Fundamentals of Medical Imaging*, Cambridge, Cambridge University Press, United Kingdom, 2017.
- [20] N. J. Wildberger, *A rational approach to trigonometry*, Math Horizons **15** (2007), 16–20.
- [21] A. Yazdinejad, A. Dehghantanha, R. M. Rarizi, G. Srivastava and H. Karimipour, *Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks*, Computers In Industry **144** (2023): 103801.
- [22] A. Yazdineja, E. Rabieinejad, T. Hasani and G. Srivastava, *A BERT-based recommender system for secure blockchain-based cyber physical drug supply chain management*, Cluster Computing **26** (2023), 3389–3403.

HOJONG CHOI

Department of Electronic Engineering, Gachon University, Seongnam, South Korea

E-mail address: `hojongch@gachon.ac.kr`

SEUNG-HYEOK SHIN

Department of Mathematics and Big-data Science, Kumoh National Institute of Technology, Gumi,
South Korea

E-mail address: `shinbaad@kumoh.ac.kr`