Journal of Nonlinear and Convex Analysis
Volume 26, Number 7, 2025, 2391–2399

Yokohama Publishers
ISSN 1880-5221 ONLINE JOURNAL

AN ENCRYPTING ALGORITHM FOR MAGNETIC RESONANCE SYSTEMS

HOJONG CHOI AND SEUNG-HYEOK SHIN*

Abstract. An encrypting algorithm for magnetic resonance systems is proposed to enhance the encrypting capability of the systems. In addition to encryption methods, randomization methods are used to transmit magnetic resonance system images. The randomization of images can be easily and quickly performed using random images of the same resolution size to randomize the image itself without the need for a symmetric key or public key for encryption. Therefore, we propose a mathematical randomization method that can achieve a performance similar to that of a random bit generator used in the existing Windows operating system. This method is suitable for generation in embedded systems or low-spec hardware that does not have an operating system installed. Random bits are extracted using the proposed irrational numbers and modified periodic functions. We compared the random bits of the proposed method with the random bit generator of the Windows operating system when using the NIST-SP 800-90B standard to evaluate randomness. Finally, we show that the randomness of the random bits generated by the proposed method is similar to that of existing methods.

1. Introduction

At present, computed tomography, ultrasound, positron emission tomography, optical imaging, and magnetic resonance imaging are the dominant medical systems [5]. Each of these medical systems possesses specific characteristics by which they provide different information on structural and physiological health [1, 2, 23]. X-ray-based computed tomography provides a high spatial resolution but can cause harmful side effects in tissues [8]. Ultrasound is noninvasive and less harmful, but it does not image hard tissues and bones well [10]. Positron emission tomography can provide valuable information on cancers but has a very low spatial resolution [22]. Optical imaging can provide disease information in the eye and skin [11]. Magnetic resonance has noninvasive characteristics with high spatial resolution but is very expensive [16].

Compared to a benchtop magnetic resonance system with high-strength scanners larger than 1.0 Tesla, most magnetic resonance systems use low-strength scanners smaller than 1.0 Tesla have been used [6]. As a result, magnetic resonance imaging systems are useful for studying plants and foods [18]. Magnetic resonance scanners incur lower development costs, but sacrifice image quality. These imaging systems can be used for surgical intervention in emergencies [17]. Magnetic resonance systems with low-strength scanners have been tested clinically in COVID-19 intensive

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

Key words and phrases. Magnetic resonance system, encrypting algorithm, mathematical algorithm.

*Corresponding author.

care units [19]. Images obtained using the magnetic resonance imaging system must be transferred to other diagnostic terminals via secured communication channels. In this respect, the protection of the patient's data is crucial for magnetic resonance systems when wireless terminals are used.

Previous encrypting algorithms for magnetic resonance systems are described here. Encrypted images with watermarks were created using a magnetic resonance system [12]. Discrete maps were embedded to encrypt the images in a magnetic resonance system [9]. A generative adversarial network with a high encrypting capability was proposed to provide high encrypting capability in the magnetic resonance system [14]. A data-encrypted algorithm based on a logistic map has been proposed for patient data using magnetic resonance brain imaging [7]. Encrypted images based on game theory were optimized using the region of interest in the magnetic resonance imaging data [24]. An encrypted magnetic resonance has been proposed based on a diffusion algorithm with odd and even interleaved points [21]. An encrypted algorithm was proposed based on a chaotic map and a system with Brownian motion in the ultrasound, computed tomography, and magnetic resonance system applications [13].

According to the literature, the ability of magnetic resonance systems to encrypt images is important for systems with wireless communication channels. Therefore, we developed a new mathematical encrypting algorithm for magnetic systems. The remainder of this paper is organized as follows. Section 2 describes the development of an encrypting algorithm based on the proposed mathematical functions. Section 3 presents the encrypted magnetic resonance images obtained using the proposed algorithm. Finally, Section 4 concludes this paper.

2. Methods

The proposed algorithm converts the decimal part of an irrational number into a k-digit integer as shown in Equation (2.1). Thus, only the integer part of the k-digit integer can be used as a candidate for a random bit when a Gaussian function is used.

$$y = f(x, k) = |x \times 10^k|. \tag{2.1}$$

Equation (2.2) is an example of extracting the integer part of the irrational number π as a candidate random bit when using the given Equation (2.2).

$$f(\pi, 10) = [3.141569265358797 \times 10^{10}] = [3141596253.5897] = 314596253. \tag{2.2}$$

Equation (2.3) is a random bit generator used to extract nonduplicated values by extending the periodic function. This generates a graph that spreads the oscillation of the period by multiplying the periodic function by a real number.

$$f(x) = xcos(x). \tag{2.3}$$

Figure 1 shows a graph representing the function in Equation (2.3). The graph spreads as the period increases when a real number multiple is applied to a periodic function.

The random bit candidates generated from the graph in Figure 1 are shown in Figure 2. Figure 2 shows the discrete points that can be applied to a digital system with the proposed random bit generation function.

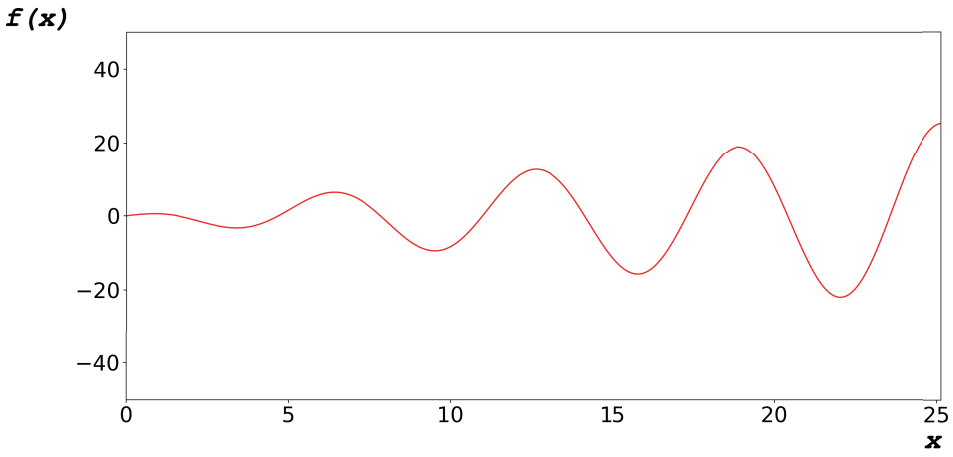


FIGURE 1. The graph for the proposed algorithm.

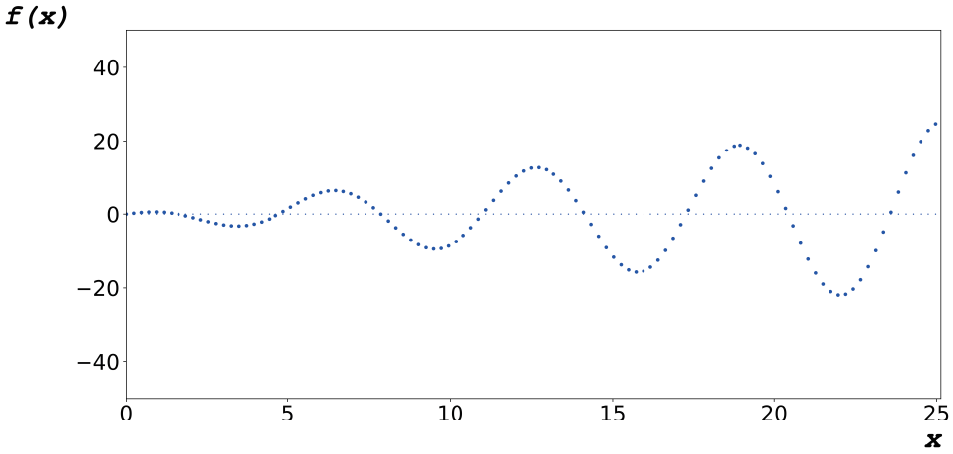


FIGURE 2. The domain for the proposed algorithm.

First, we define the x-coordinate that can be extracted from a digital system with discontinuous characteristics. Equation (2.4) represents the domain for extracting the points shown in Figure 2.

$$x|x = a_0 + idx, a_0 = 0.3, dx = 0.2312, i = 0, 1, 2, \ldots. \tag{2.4}$$

The proposed random function is a function of the spreading amplitude. As shown in points of one to four (Figure 3), the values for the same period have different values.

The characteristics of the digital system are shown in Figure 4. In previous papers [3,4], we first applied Equation (2.1), rather than applying the exact period and then extracted values for similar periods. However, in this paper, we extracted the values of periods that could be generated mathematically.

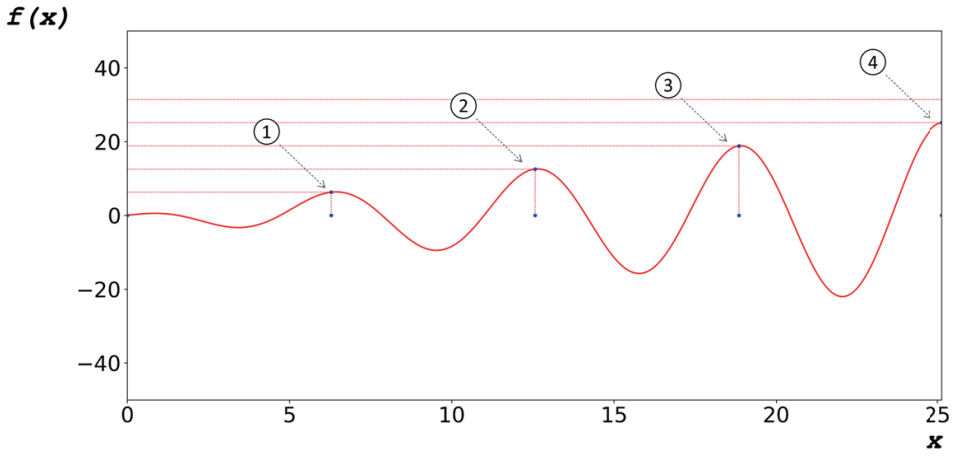


FIGURE 3. The random bits around the period of the proposed algorithm.

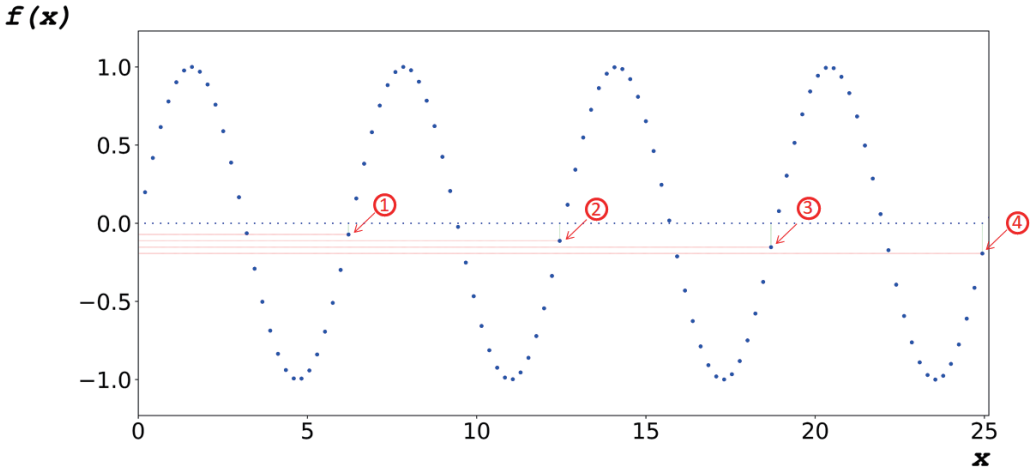


FIGURE 4. The random bit when using the previous approach.

As a result, the proposed idea has the advantage of obtaining nonduplicated f(x) values from exact values of the same period. Figure 5 shows the range that can be extracted from the domain using the proposed random bit which generates the function and Equation (2.3).

The domain of the function whose amplitude can be spread operates as the period of Equation (2.5).

$$z = p((f(x), 10). \tag{2.5}$$

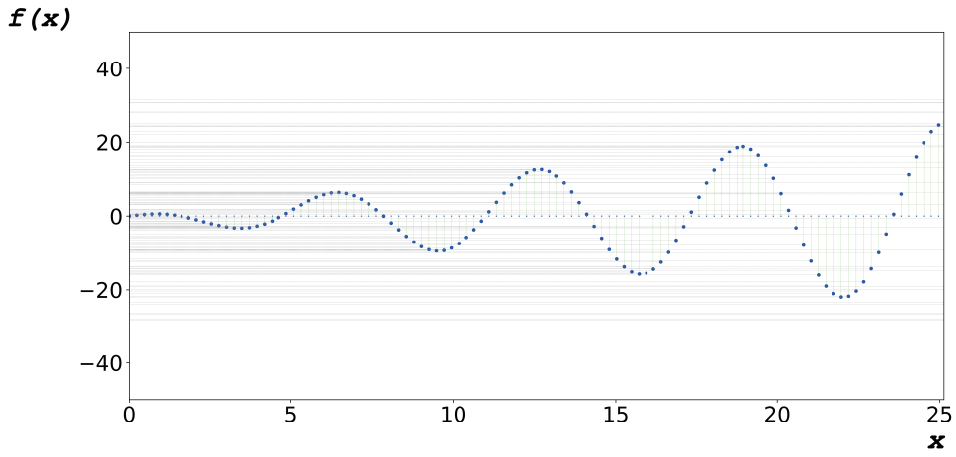


FIGURE 5. The candidates of the random bit.

The seed for extracting the random bit candidates generated in the domain of Equation (2.4) is converted into a period as shown in Equation (2.5). The values of the domain were restricted to discrete forms using the congruent equation shown in Equation (2.6). Therefore, it can be operated within the finite range of the digital systems.

$$Z_m = Z(z, m) = |z|(mod\ m). \tag{2.6}$$

This method generates random bits of a certain size or larger, such as 128, 192, and 256 bits, using the random bits generated by Equations (2.1), (2.2), (2.3), (2.4), (2.5), and (2.6).

In Figure 5, if the equation $p_0 = (f(x_0), 10)$ is selected and the value of $f(p_0)$ is selected as a 32-bit integer random bit, then the random bit can be determined by connecting the values of $f(p_0)$, $f(p_1)$, $f(p_2)$, and $f(p_3)$ when using Equation (2.7) to generate a 128-bit random bit.

$$r = R(Z_m, n) = \sum_{i=0}^{n-1} (Z_m)_i \times (i \times m/2^4). \tag{2.7}$$

3. Results and discussion

We first performed a simulation to verify the proposed encrypting algorithm. Figure 6 shows a diagram visualizing the distribution of random bits generated using the proposed algorithm.

Figure 7 shows a visual image of the random bits generated using the CryptGenRandom function provided by Microsoft operating system to compare the performance of the proposed algorithm. The CryptGenRandom function is the most widely used function for random bit generation [15]. CryptGenRandom was tested by the United States of America National Institute of Standards and Technology (NIST) standard protocol (NIST-800 90B).

FIGURE 6. The random bit image when using the proposed algorithm.

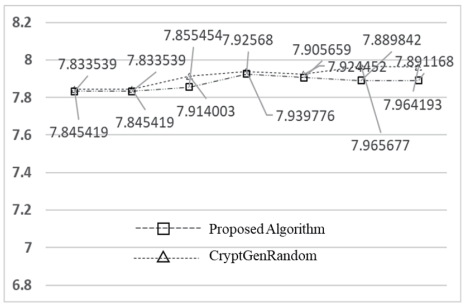
FIGURE 7. The random bit image when using the CryptGenRandom function run by the window system.

Current magnetic resonance systems can be used to obtain lumbar images for laboratory or research purposes [20]. Image data from the lumbar training phantom were obtained using a commercial 3.0T magnetic resonance system which is currently used to diagnose knee, shoulder, cervical, brain, and lumbar diseases at universities and small clinics.

To compare the performances of the encrypting algorithms of the magnetic resonance system, we used three typical measurement indices: peak signal-to-noise ratio (PSNR), structural similarity index measure (SSIM), and mean square error (MSE).

The PSNR values obtained using the CryptGenRandom function and the proposed algorithm were 5.98571242 dB and 5.9078501995 dB, respectively. The SSIM values when using the CryptGenRandom function and the proposed algorithm were 0.255421107 and 0.255140541, respectively. The MSE when using the CryptGenRandom function and the proposed algorithm were 16387.3647 and 16414.59461, respectively. Therefore, there was almost no difference in image quality between the two randomized images.

Figure 8 shows that the randomness of the proposed algorithm is similar to that of Microsoft's CryptGenRandom function as a result of NIST SP800-90B for evaluating randomness.



	Proposed Algorithm	CryptGenRandom
Markov Test (1 bit)	0.888814	0.91192
Compression Test (1 bit)	7.833539	7.845419
T-Tuple Test (8 bit)	7.833539	7.845419
LRS Test (8 bit)	7.855454	7.914003
MultiMCW (8 bit)	7.92568	7.939776
Lag Prediction Test (8 bit)	7.905659	7.924452
MultiMMC (8 bit)	7.889842	7.965677
Min Entroypy	**7.110515**	**7.295363**

FIGURE 8. Test results of the NIST SP800-90B with the proposed algorithm and CryptGenRandom function.

4. Conclusion

We applied the proposed mathematical encryption algorithm to a traditional magnetic resonance system that is currently used in hospitals. In this study, we compared the performance of the CryptGenRandom function, which is a random bit generator used in the Windows operating system, and a random bit generator using a mathematically encrypted algorithm. The results of the random bit evaluation using NIST SP800-90B confirmed that the minimum entropy for the randomness of the proposed algorithm and the random bit generator based on the existing operating system was over 7 bits. Therefore, the results showed a similar level of performance, close to 8 bits. For high-speed real-time data transmission, we believe that the magnetic resonance system images can be randomized and transmitted more efficiently than encryption using encryption keys and initialization vectors. When applying the proposed algorithm to an actual system using several

random images per transmission frame, we can expect the efficiency of the magnetic resonance system to increase.

References

[1] M. U. Abbasi, A. Rashad, G. Srivastava and M. Tariq, *Multiple contaminant biosignal quality analysis for electrocardiography*, Biomedical Signal Processing Control **71** (2022): 103127.

[2] M. Ahmed, A. R. Dar, M. Helfert, A. Khan and J. Kim, *Data provenance in healthcare: Approaches, challenges, and future directions*, Sensors **23** (2023): 6495.

[3] H. Choi and S.-H. Shin, *Novel random number generation for ultrasound systems*, Journal Nonlinear and Convex Analysis **24** (2023), 1835–1841.

[4] H. Choi and S.-H. Shin, *Mathematical algorithm for magnetic resonance imaging*, Journal of Nonlinear and Convex Analysis **25** (2024), 1511–1518.

[5] D. Dhingra and M. Dua, *Medical video encryption using novel 2D Cosine-Sine map and dynamic DNA coding*, Medical and Biological Engineering and Computing **62** (2024), 237–255.

[6] M. Faheem, H. Z. Tam, M. Nougom, T. Suaris, N. Jahan, T. Lloyd, L. Johnson, S. Aggarwal, M. Ullah, E. W. Thompson and A. R. Brentnall, *Role of supplemental breast MRI in screening women with mammographically dense breasts: A systematic review and meta-analysis*, Journal of Breast Imaging **6** (2024), 355–377.

[7] N. George and M. Manuel, *A secure data hiding system in biomedical images using grain 128a algorithm, logistic mapping and elliptical curve cryptography*, Multimedia Tools and Applications **84** (2025), 2005–2028.

[8] H. Hooshangnejad, D. China, Y. Huang, W. Zbijewski, A. Uneri, T. McNutt, J. Lee and K. Ding *XIOSIS: an X-ray-based intra-operative image-guided platform for oncology smart material delivery*, IEEE Transaction on Medical Imaging **43** (2024), 3176–3187.

[9] 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 (MOCAST), IEEE, 2017, pp. 1–4.

[10] U. Jung and H. Choi, *Active echo signals and image optimization techniques via software filter correction of ultrasound system*, Applied Acoustics **188** (2022): 108519.

[11] I. Khalil, A. Mehmood, H. Kim and J. Kim, *OCTNet: A Modified Multi-Scale Attention Feature Fusion Network with InceptionV3 for Retinal OCT Image Classification*, Mathematics **12** (2024): 3003.

[12] N. Kittawi and A. Al-Haj, *Reversible data hiding in encrypted images*, in: 2017 8th International Conference on Information Technology, IEEE, 2017, pp. 808–813.

[13] F. Masood, M. Driss, W. Boulila, J. Ahmad, S. Rehman, S. U. Jan, A. Qayyum and W. J. Buchanan, *A lightweight chaos-based medical image encryption scheme using Random shuffling and XOR operations*, Wireless Personal Communications **127** (2022), 1405–1432.

[14] S. Padhy, S. Dash, T. N. Shankar, V. Rachapudi, S. Kumar and A. Nayyar *A hybrid crypto-compression model for secure brain MRI image transmission*, Multimedia Tools and Applications **83** (2024), 24361–24381.

[15] P. Pavithran, S. Mathew, S. Namasudra and G. Srivastava, *A novel cryptosystem based on DNA cryptography, hyperchaotic systems and a randomly generated Moore machine for cyber physical systems*, Computer Communications **188** (2022), 1–12.

[16] M. Sarracanie and N. Salameh, *Low-Field MRI: How low can we go? A fresh view on an old debate*, Frontiers in Physics, **8** (2020): 00172.

[17] C. Senft, V. Seifert, E. Hermann and T. Gasser, *Surgical treatment of cerebral abscess with the use of a mobile ultralow-field MRI*, Neurosurgical Review **32** (2008), 77–85.

[18] A. P. Sobolev, C. Ingallina, M. Spano, G. Di Matteo and L. Mannina, *NMR-based approaches in the study of foods*, Molecules **27** (2022): 7906.

[19] J. Turpin, P. Unadkat, J. Thomas, N. Kleiner, S. Khazanehdari, S. Wanchoo, K. Samuel, B. O. Moclair, K. Black, A. R. Dehdashti, R. K. Narayan, R. Temes and M. Schulder, *Portable Magnetic Resonance Imaging for ICU Patients*, Critical Care Explorations **2** (2020): e0306.

[20] L. Wald, P. C. McDaniel, T. Witzel, J. P. Stockmann and C. Z. Cooley, *Low-cost and portable MRI*, Journal of Magnetic Resonance Imaging **52** (2020), 686–696.
[21] X. Wang and Y. Wang, *Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd-even interleaved points*, Expert Systems with Applications, **213** (2023): 118924.
[22] K. Xu and H. Kang, *A review of machine learning approaches for brain positron emission tomography data analysis*, Nuclear Medicine and Molecular Imaging **58** (2024), 203–212.
[23] N. Yaqub, J. Zhang, M.I. Khalid, W. Wang, M. Helfert, M. Ahmed and J. Kim, *Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records*, PeerJ Computer Science **11** (2025): e2647.
[24] J. Zhou, J. Li, and X. Di, *A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position*, IEEE Access **8** (2020), 122210–122228.

Manuscript received September 18, 2024
revised December 22, 2024

H. Choi
Department of Electronic Engineering, Gachon University, Seongnam, South Korea
E-mail address: hojongch@gachon.ac.kr

S.-H. Shin
School of Big data & Industrial Engineering, Kumoh National Institute of Technology, Gumi, South Korea
E-mail address: shinbaad@kumoh.ac.kr