Technology and Health Care 31 (2023) S55–S59
DOI 10.3233/THC-236006
IOS Press

Secured computed tomography scanner using a random bit

Hojong Choi[a] and Seung-Hyeok Shin[b,*]
[a]*Department of Electronic Engineering, Gachon University, Seongnam, Korea*
[b]*Department of Mathematics and Big-data Science, Kumoh National Institute of Technology, Gumi, Korea*

Abstract.
BACKGROUND: Patient data in current computed tomography scanner machines are transferred through several communication channels, such as WiFi, to the mobile channel platform. Therefore, patient information is an important security concern. Medical imaging must be protected using various methods.
OBJECTIVE: The current hardware-dependent method for generating random bits exhibits predictable or inconvenient physical characteristics. Therefore, a more flexible random-bit generation technique is to be devised.
METHODS: We propose a deterministic random bit generation algorithm that uses a mathematical periodic function.
RESULTS: After randomizing the image using the proposed random bit, the performance is analyzed and compared with that of the processed image.
CONCLUSION: The random bit generation method using a mathematical algorithm shows higher entropy than the random bit generated by hardware.

Keywords: Computed tomography scanner, random bit, digital periodic function

1. Introduction

Current medical machines can share patient data through secured communication channels, such as wirelines of the cable network and wireless transmission lines [1–4]. However, access from secured channels to private communication devices, such as tablets or cellular phones, has been adopted because of immediate data necessity to healthcare workers [5–9].

Several algorithms have been investigated for various medical equipment to protect patient data, such as text and image data [10–12]. The Rivest-Shamir-Adleman (RSA) algorithm has been widely used for encrypting information in medical equipment [13–15]. A 2048-bit RSA, secure hash, and advanced encryption standard algorithm were used for the data distribution of protected information [16–18]. A prime-number-based RSA-encrypted algorithm was developed to improve security [19–21].

Among these systems, CT provides the highest spatial resolution with the high amount of image data [22–24]. The image data in a CT scanner with a secured encrypted password must be used. Therefore, information security must be protected using cryptographic algorithms to protect patient information. However, data from scanners to private devices can be leaked when transferred [25].

*Corresponding author: Seung-Hyeok Shin, Department of Mathematics and Big Data Science, Kumoh National Institute of Technology, 61, Daehak-ro, Gumi, Gyeongbuk, 39177, Korea. E-mail: shinbaad@kumoh.ac.kr.

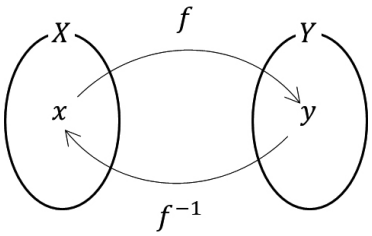

Fig. 1. Onetoone mapping function.

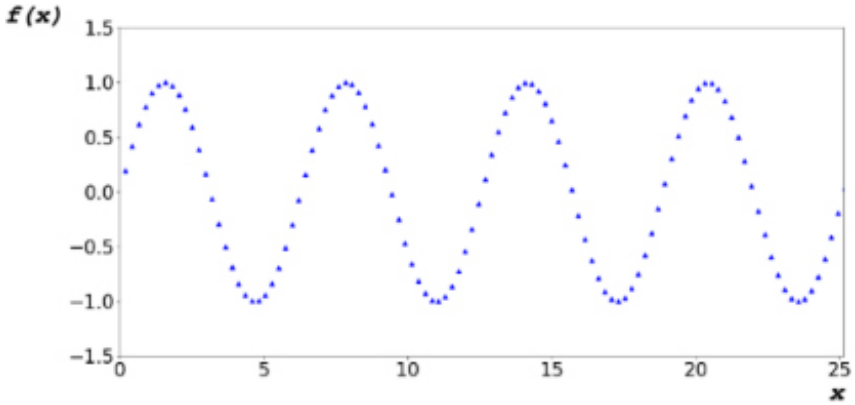

Fig. 2. Periodic function in digital system.

2. Methods

In this study, a true random bit is generated when the probabilities P for events A and B are independent and satisfy the following condition [26,27]:

$$P(A \cup B) = P(A)P(B) \tag{1}$$

True random bits are impossible to generate or identify [28]. Thus, the random bits are deterministic random bits. A deterministic random bit must satisfy the functional relationship of one-to-one correspondence between the independent variable and the dependent variable as shown in Fig. 1 and Eq. (2) [29,30].

$$x_1 \neq x_2 \Leftrightarrow f(x_1) \neq f(x_2) \tag{2}$$

$$f(x + p) = f(x) \tag{3}$$

Equation (3) represents the periodic function. The p value is the periodic number. Mathematically, the periodic function is not one-to-one and can be proved as follows.

The proposed algorithm utilizes the characteristics of digital systems, in which mathematical continuity is impossible [31,32]. In other words, it is expressed as shown in Fig. 2.

The algorithm determines the dependent variable of the codomain by adding variable Δx to the first term a, as well as the independent variable of the domain in a constant periodic function. We converted it into hexadecimal defined in IEEE754 [33].

The periodic function contains irrational numbers as the period exhibits one-to-one correspondence [34]. The values of the dependent variable corresponding to independent variable.

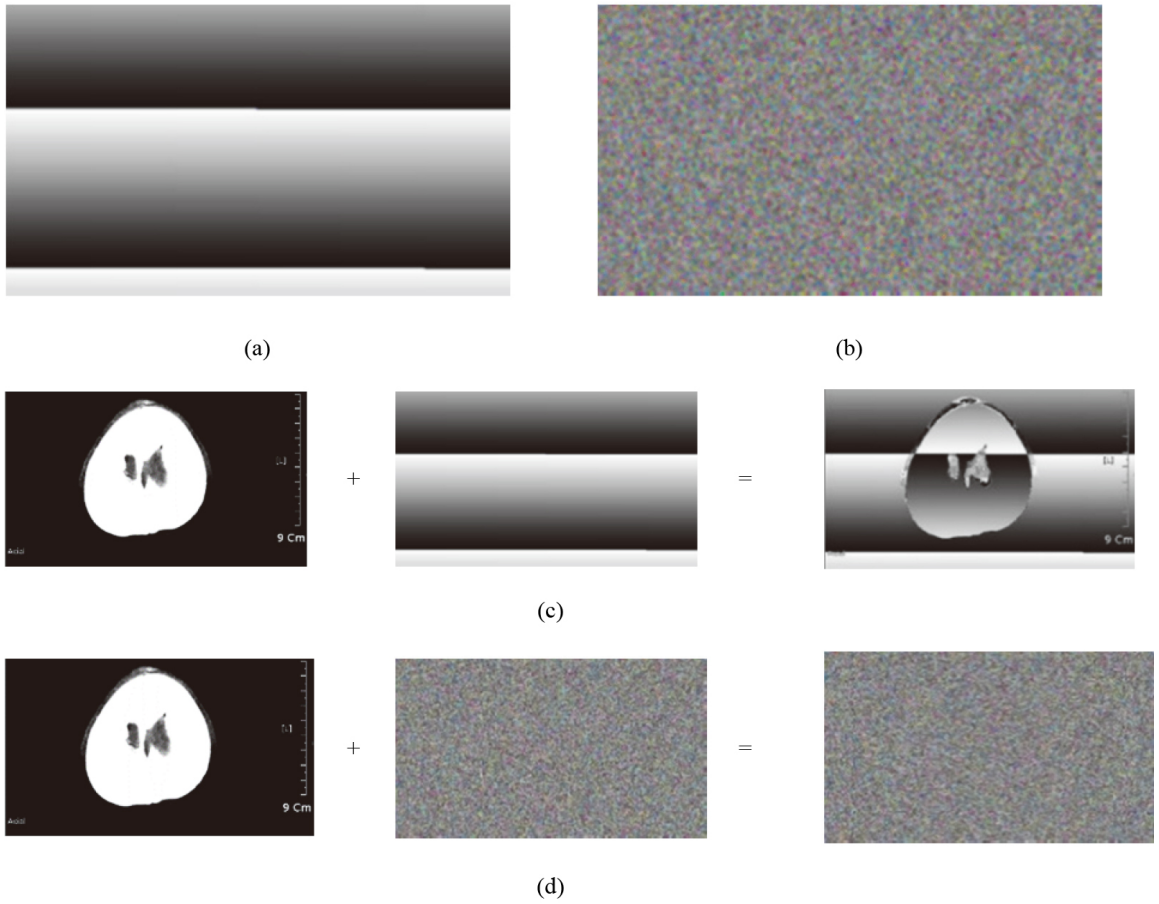

Fig. 3. (a) Image of random bit based on time stamp and (b) from proposed algorithms. (c) Randomized image obtained using time stamp noise and (d) proposed algorithm.

3. Results and discussion

The developed algorithm was applied on the obtained image data to verify the encryption capability because the developed system should be used for CT scanners. The image data of the phantom in the axial direction were obtained using a CT scanner (Aquilion ONE^{TM}, Cannon Medical Systems Cor., Tochigi, Japan). Therefore, the data used in conjunction with the proposed algorithm can be verified.

Figure 3a shows an image obtained using the noise of a time-based system. Figure 3b shows an image captured using a random bit generated using the proposed algorithm. As confirmed from the image, the noise generated based on the time stamp exhibits a regular pattern. However, the proposed algorithm exhibits characteristics.

When generating a random bit whose size is equal to that of the entire image, the proposed algorithm can confirm that the generated numbers are independent of each other's independent previous events and they are generated as unpredictable numbers. To verify the performance of the proposed algorithm, we conducted an experiment.

Figure 3c and d show the mixed result with the original image after imaging the random bit generated using the time stamp and proposed algorithm, as shown in Fig. 3a and b, respectively.

The most famous one is RSA-based encrypted algorithms [35,36]. However, these previous RSA-based encrypted algorithms such as 2048-bit RSA and prime-number-based RSA algorithms could be hacked because they have limited numbers of the encrypted keys produced by computer hardware [37].

Compared to previous studies, we use the proposed algorithms. This proposed technique has the functional relationship such that the developed encryption algorithm could be first applied to commercial CT scanners [38]. Therefore, the proposed algorithm could produce the randomized images in the digital system because it could not be produced by the hardware.

4. Conclusion

A random bit algorithm using mathematical modeling was proposed to randomize CT scanner image containing personal information, and randomization using actual CT scanner images was confirmed. The current random bit generation method uses noise provided by a hardware-dependent system.

The disadvantage is that the frequency of noise generation can be predicted. However, the proposed algorithm combines the mathematical periodic function. We observed that when the combinations of periodic functions and initial values for generating random bits and the amount of change were determined, random bits can be generated via the proposed algorithms.

Acknowledgments

This work was supported by the ‘Customized technology partner’ project funded by the Korean Ministry of SMEs and Startups in 2022 (project no. 202201580001).

References

[1] Weibao Q, Yanyan Y, Keung TF, Lei S. A multifunctional, reconfigurable pulse generator for high-frequency ultrasound imaging. IEEE Transactions on Ultrasonic Ferroelectric and Frequency Control. 2012; 59(7): 1558-1567.
[2] Zhou Y, Yao J, Wang LV. Tutorial on photoacoustic tomography. Journal of Biomedical Optics. 2016; 21(6): 061007.
[3] Shung KK. Diagnostic ultrasound: Past, present, and future. Journal of Medical and Biological Engineering. 2011; 31(6): 371-374.
[4] Kripfgans OD, Chan HL. Ultrasonic Imaging: Physics and Mechanism in Dental Ultrasound in Periodontology and Implantology: Examination, Diagnosis and Treatment Outcome Evaluation. Springer International Publishing. 2021; 1-38.
[5] Qiu W, Yu Y, Chabok HR, Liu C, Tsang FK, Zhou Q, Shung KK, Zheng H, Sun L. A flexible annular-array imaging platform for micro-ultrasound. IEEE Transaction on Ultrasonic Ferroelectric and Frequency Control. 2013; 60(1): 178-186.
[6] Shung KK, Smith M, Tsui BM. Principles of Medical Imaging. Cambridge, MA, USA: Academic Press. 2012.
[7] Li X, Wei W, Zhou Q, Shung KK, Chen Z. Intravascular photoacoustic imaging at 35 and 80 MHz. Journal of Biomedical Optics. 2012; 17(10): 106005.
[8] Morse PM, Ingard KU. Theoretical Acoustics. New Jersey, NJ, USA: Princeton university press. 1986.
[9] Chen R, Wu J, Lam KH, Yao L, Zhou Q, Tian J, Han P, Shung KK. Thermal-independent properties of PIN-PMN-PT single-crystal linear-array ultrasonic transducers. IEEE Transaction on Ultrasonic Ferroelectric and Frequency Control. 2012; 59(12): 2777-2784.
[10] Jung U, Choi JH, Choo HT, Kim GU, Ryu J, Choi H. Fully Customized Photoacoustic System Using Doubly Q-Switched Nd: YAG Laser and Multiple Axes Stages for Laboratory Applications. Sensors. 2022; 22(7): 2621.
[11] Jung U, Choi H. Active echo signals and image optimization techniques via software filter correction of ultrasound system. Applied Acoustics. 2022; 188: 108519.
[12] Shung KK. Diagnostic Ultrasound: Imaging and Blood Flow Measurements. Boca Raton, FL, USA: Taylor & Francis. 2015.
[13] Shin SH, Yoo WS, Choi H. Development of public key cryptographic algorithm using matrix pattern for tele-ultrasound applications. Mathematics. 2019; 7(8): 752.

[14] Qiu W, Wang C, Li Y, Zhou J, Yang G, Xiao Y, Feng G, Jin Q, Mu P, Qian M, Zheng M. A scanning-mode 2D shear wave imaging (s2D-SWI) system for ultrasound elastography. Ultrasonics. 2015; 62: 89-96.
[15] Daemen J, Rijmen V. The Design of Rijndael: AES-the Advanced Encryption Standard. Berlin, Germany: Springer Science & Business Media. 2013.
[16] Halmann MN, Urness MS. Methods and systems for managing distribution of protected information on a medical display. 2017 US Patents 14/866.252.
[17] Katz J, Menezes AJ, Oorschot PCV, Vanstone SA. Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press. 1996.
[18] Stallings W. Cryptography and Network Security: Principles and Practice. London, United Kingdom: Pearson Education. 2003.
[19] Thangavel M, Varalakshmi P, Murrali M, Nithya K. An Enhanced and Secured RSA Key Generation Scheme (ESRKGS). Journal of Information Security and Applications. 2015; 20: 3-10.
[20] Blake I, Seroussi G, Seroussi G, Smart N. Elliptic Curves in Cryptography. Cambridge, United Kingdom: Cambridge university press. 1999.
[21] Delfs H, Knebl H, Knebl H. Introduction to Cryptography. Berlin, Germany: Springer. 2002.
[22] Stacy, Essentials of Biological and Medical Physics. New York, NJ, USA: McGraw-Hill. 1955.
[23] Sun P, Zhou Q, Zhu B, Wu D, Hu C, Cannata JM, Tian J, Han P, Wang G, Shung KK. Design and fabrication of PIN-PMN-PT single-crystal high-frequency ultrasound transducers. IEEE Transaction on Ultrasonic Ferroelectric and Frequency Control. 2009; 56(12): 2760-2763.
[24] Sun P, Wang G, Wu D, Zhu B, Hu C, Liu C, Djuth FT, Zhou Q, Shung KK. High frequency PMN-PT 1-3 composite transducer for ultrasonic imaging application. Ferroelectrics. 2010; 408(1): 120-128.
[25] Eren H, Webster JG. Telemedicine and Electronic Medicine. Boca Ration, FL, USA: CRC Press. 2015.
[26] Hogg RV, Craig AT. Introduction to Mathematical Statistics. Upper Saddle River, NJ, USA: Prentice Hall. 1995.
[27] Dass H. Advanced Engineering Mathematics. New Delhi, India: S. Chand Publishing. 2008.
[28] Avriel M, Golany B. Mathematical Programming for Industrial Engineers. Boca Raton, FL, USA: CRC Press. 1996.
[29] Zill D, Wright WS, Cullen MR. Advanced Engineering Mathematics. Burlington, MA, USA: Jones & Bartlett Learning. 2011.
[30] Galbraith SD. Mathematics of Public Key Cryptography. Cambridge, United Kingdom: Cambridge University Press. 2012.
[31] Deisenroth MP, Faisal AA, Ong CS. Mathematics for machine learning. Cambridge, United Kingdom: Cambridge University Press. 2020.
[32] Duffy DG. Advanced Engineering Mathematics with MATLAB. Boca Raton, FL, USA: Chapman and Hall. 2016.
[33] Hough D. Applications of the proposed IEEE 754 standard for floating-point arithetic. Computer. 1981; 14(03): 70-74.
[34] Bird J. Engineering Mathematics. Abingdon-on-Thames, United Kingdom: Routledge. 2014.
[35] Patidar R, Bhartiya R. Modified RSA cryptosystem based on offline storage and prime number. Proceeding IEEE Computational Intelligence and Computing Research. Madurai, India. 2013; 1-6.
[36] Cohen H, Frey G, Avanzi R, Doche C, Lange T, Nguyen K, Vercauteren F. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Boca Raton, FL, USA: Chapman and Hall. 2005.
[37] Stinson DR. Cryptography: Theory and Practice. Boca Raton, FL, USA: Chapman and Hall. 2005.
[38] Forouzan BA. Cryptography & Network Security. New York, NJ, USA: McGraw-Hill, Inc. 2007.