

ENCRYPTING ALGORITHM FOR GAMMA CAMERA SYSTEMS

HOJONG CHOI AND SEUNG-HYEOK SHIN*

ABSTRACT. An encrypting algorithm for a gamma camera system is proposed for encrypted images. Secure encryption keys rely on unpredictable random numbers. These random numbers use noise generated by hardware components such as central processing unit frequency, hard-disk rotation speed, vibration, and memory, which cannot be generated artificially. The generated noise goes through a bias removal process and is used as a seed for a deterministic random number generator. We propose a noise that can be easily used in embedded systems by the fact that the square root of the sum of squares of prime numbers is an irrational number and the floating point operation of IEEE 754, which is a feature of 32-bit systems. To evaluate the entropy of noise generated when using the proposed method, we used the standard evaluation method, which is the National Institute of Standards and Technology (NIST) SP 800-90B, to identify the randomness effect. Therefore, we used some indexes to evaluate the image quality of the randomness. The experimental results show that the image synthesized with the proposed algorithm has a higher degree of randomization than the original image. Therefore, we can observe that the randomness of the proposed algorithm is higher than that of the CryptGenRandom function.

1. INTRODUCTION

In nuclear medicine, gamma cameras can be used to detect cancer tumors with a small amount of radiotracer injector [20]. The gamma-ray light emitted from the patient reaches the scintillation crystal and the photomultiplier tube, and then the produced signals are passed through the time and position networks to the digitizer [12]. The digitized data are displayed on imaging devices [15]. Gamma camera systems are one of the main systems that consist of positron emission tomography or single photon emission computed tomography [16]. They are also combined with X-ray-based computed tomography, magnetic resonance, or ultrasound imaging modalities for tumor detection because of low sensitivity, signal-to-noise ratio, and spatial resolution [1, 2].

Previous studies on encrypted algorithms used in general medical imaging modalities, such as computed tomography, positron emission tomography, and gamma camera systems, are described here. A combinational algorithm based on applied principal component analysis, discrete cosine transform, and randomized singular value decomposition was proposed to enhance security in general medical imaging,

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

Key words and phrases. encrypting algorithm; gamma camera; mathematical algorithm.

This research was supported by the regional innovation system and education (RISE)-(Regional Growth Innovation LAB) program through the Gyeongbuk RISE Center, funded by the Ministry of Education (MOE) and the Gyeongsangbuk-do, Republic of Korea (2025-rise-15-105).

*Corresponding author.

such as X-ray, ultrasound, computed tomography, and positron emission tomography imaging [10]. A logistic and cubic mapping function supported encrypting algorithm was proposed to increase key sensitivity up to around 99% for general medical imaging [21]. A two-dimensional logistic function supported plain-image correlative and selective encrypting algorithm was proposed to obtain high visual and informative entropy in the encrypted images [22]. A combinational encrypted algorithm based on stream cipher and block cipher algorithm was used to generate the encrypted images while reducing the distortion of the images of the ultrasound and positron emission tomography system [17]. A joint encrypted and water-marked algorithm was proposed to enhance security attributes in the spatial and encrypting domains of ultrasound and positron emission tomography [4]. An encrypted image based on the gamma phase masks in the gyrator domain was proposed to affect the phase distribution [18]. A hyper-spectral image with a gamma phase marker was proposed when it is integrated with an amplitude image mask with the gyrator transform technique [19]. With periodic composite functions and mean values, the points with the same slope were used [5]. The periodic function in the coordinates at regular intervals was generated as rational numbers [6]. A noise source was generated by rational numbers that can be expressed into irrational and non-repeating numbers [7].

As mentioned in the previous studies, the encrypting algorithms related to the gamma camera system are very limited compared to other imaging modalities such as X-ray, ultrasound, computed tomography, and magnetic resonance imaging. Therefore, our proposed idea could be valuable for the gamma camera with wireless capability in the future. Section 2 describes the concept and mathematical analysis of the noise-generated algorithm. Section 3 provides the encrypted image results with the proposed algorithm and the conventional hardware noise sources. In addition, we describe the discussion of the obtained results with the evaluation measurement indexes. Section 4 is the final conclusion of the paper.

2. METHODS

The noise sources of random numbers, which are supposed to be unpredictable, are mainly generated by analog computer hardware [8]. The noise generated from computer hardware has unpredictable and irregular characteristics [11]. Therefore, it is often used as a noise source in deterministic random number generators. TTAK.KO-12.0235 provides an application processing interface (API) in the operating system environment to extract noise generated from such hardware [14]. TTAK.KO-12.0235 describes a method for collecting noise generated in hardware. However, it is an API mainly provided by the operating system. Therefore, it is not suitable for use in systems where it is difficult to install an operating system, such as microcomputers and embedded systems.

The proposed algorithm uses a mathematical algorithm as a hardware-independent noise source generation method. To generate a random number, noise must be used as the seed, which is the entropy input of the random number generator. The proposed algorithm is a mathematical noise that can be used in a deterministic random bit generator. The random number we propose serves as a seed for a random number generator, which plays a major role in key generation for cryptographic

algorithms. The square root of the sum of the squares of prime numbers is also called a Pythagorean number, and they are always irrational numbers [3]. We propose that the irrational numbers generated in this way can be applied to embedded systems with limited hardware resources when using floating-point operations of IEEE754, which is a feature of 32-bit systems. The imperfections of IEEE 754 floating-point numbers reduce the predictability of random numbers generated using mathematical methods. To evaluate the randomness of the proposed algorithm, we use the National Institute of Standards and Technology special publication (NIST SP) 800-90B, which is provided from the NIST, which is one of the United States government standard agencies [13]. In addition, the conventional hardware noise source and the proposed random number are generated in the form of an image, and then synthesized with gamma camera images to be evaluated.

This section describes the proof-of-concept for our proposed mathematical algorithm for the gamma camera. The square root of the sum of two different prime numbers is an irrational number. For two different prime numbers, p and q , $\sqrt{p^2 + q^2}$ is supposed to be an irrational number. First, we need to assume the conditions of two variables of r and Q as shown in Equation (2.1). We assume that the sum of the squares of p and q is a rational number.

$$(2.1) \quad \sqrt{p^2 + q^2} = r, (r \in Q, \text{rational}).$$

With this assumption, we can obtain another Equation (2.2).

$$(2.2) \quad p^2 + q^2 = r^2.$$

When r is a rational number to satisfy this condition, r must be a perfect square. To be a perfect square, we must obtain the form of $r = 4k$ or $4k + 1$ for all integers k . When the rational numbers p and q are assumed to be $p = 2n$ or $2n+1$ and $q = 2m$ or $2m+1$, we can obtain the following relationship in Equation (2.3).

$$(2.3) \quad (2n + 1)^2 + (2m + 1)^2 = r^2.$$

We need to make square terms in Equation (2.4).

$$(2.4) \quad 4n^2 + 4n + 1 + 4m^2 + 4m + 1 = r^2.$$

We can finally show the form in the following Equation (2.5)

$$(2.5) \quad 4(n^2 + m^2) + 4(n + m) + 2 = r^2$$

where k and m are arbitrary integers.

According to the given assumption, the above equation must be the square root of the form $4k$ or $4k+1$. However, we can prove that it is not a rational number when $p = 2n$ or $2n+1$ and $q = 2m$ or $2m+1$. In conclusion, we can observe that the proposed formula is always irrational. With this condition, we can also conclude that the variable as shown in (2.1) is supposed to be irrational.

3. RESULTS AND DISCUSSION

The obtained gamma camera images were used to test the encrypted algorithm's capability [9]. Figures 1 and 2 show the results of random numbers that generated 8-bit images. They generate 8-bit-sized random numbers and show the distribution

of random numbers generated within the range of 0 to 255. Figure 1 is the data of the random number distribution when using the proposed algorithm.

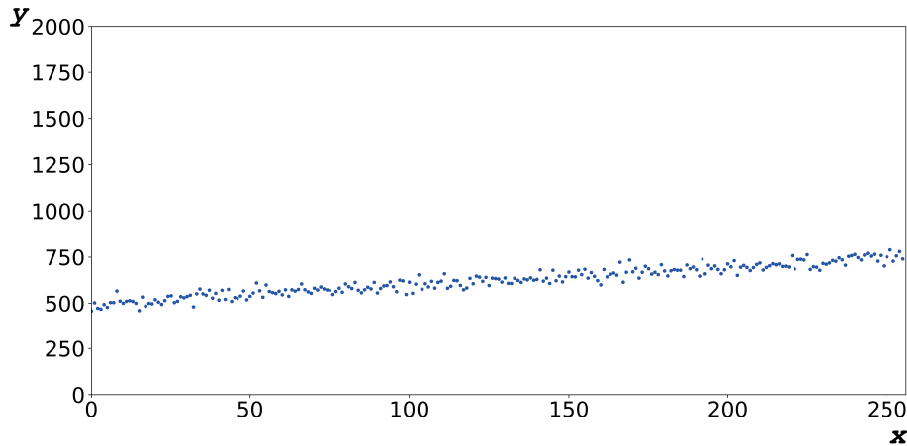


FIGURE 1. Random number generation distribution generated by the proposed algorithm.

Figure 2 is the data of the random number distribution when using the Win32 CryptGenRandom function, respectively.

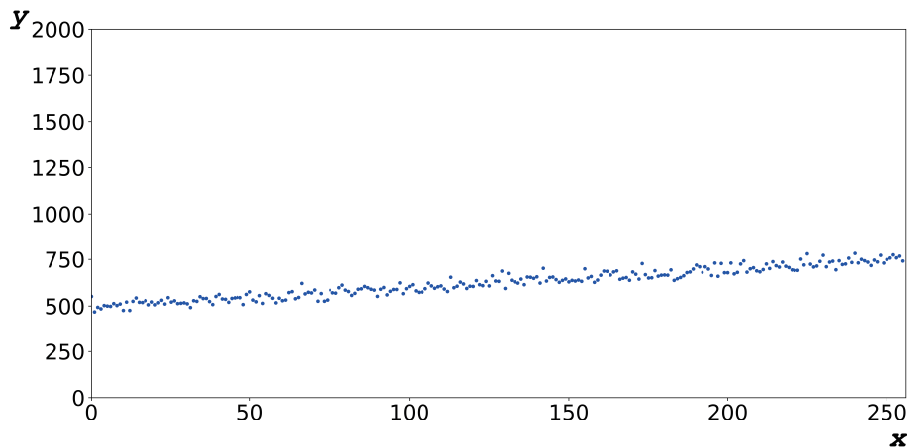


FIGURE 2. Random number generation distribution generated by the Win32 CryptGenRandom function.

According to the method for evaluating randomness measured by NIST 800 90B, we compared the differences with the hardware-dependent noise source extracted by the conventional CryptGenRandom function. The most commonly used method for evaluating randomness utilizes data with random numbers. This method evaluates sample duplication and repetition using over 1 million samples. The proposed

algorithm demonstrates that duplication and repetition are within acceptable limit in a sample of 1 million, as shown in Figures 1 and 2.

Figure 3 shows the randomness data evaluated when using NIST-800 90B, and the minimum entropy among 8 bits is as follows. The minimum entropy by the proposed algorithm is 7.5792478 bits, and the minimum entropy of random numbers generated by conventional hardware noise sources is 7.670695 bits. Both random numbers show a minimum entropy close to 8 bits. Therefore, they are noise sources with high randomness.

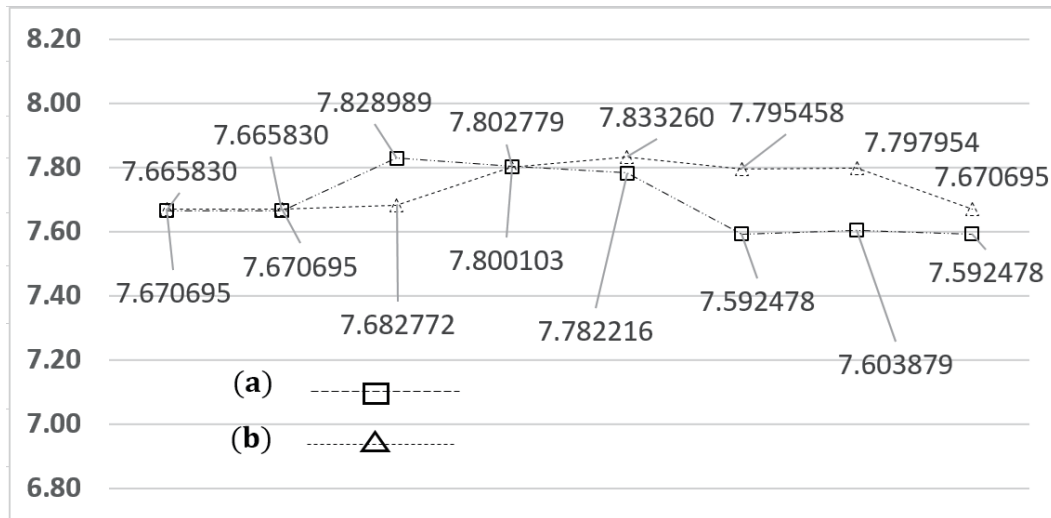


FIGURE 3. (a) Random number generation distribution data generated by the proposed algorithm and (b) the Win32 CryptGenRandom function.

In Figure 3, the first, second, third, fourth, fifth, sixth, seventh, 8 bit randomness data evaluated with the NIST-800 90B method represent the MCV, T-turtle test, LRS test, multiMCW, Lag prediction test, multiMMC, LZ78Y prediction, and min, respectively. As a result, there is not much difference between the noise source generated by the conventional hardware-dependent noise source and the noise source generated by the proposed algorithm. Figure 4 is the image synthesized with a random image generated by a proposed algorithm and the CryptGenRandom function.

According to the NIST 800-90B evaluation methods, both random numbers were judged to have randomness because they satisfied the minimum entropy of 7 bits or more. To further evaluate randomness, the original image and random image were synthesized, and then the PSNR and MSE indexes were analyzed accordingly. The image results consist of 24-bit true color. Therefore, randomizing each RGB 8-bit with an XOR operation is the fastest and clearest way to synthesize it.

PSNR represents the signal-to-noise ratio of the evaluated encrypted images. Therefore, a small value in the PSNR index means a higher level of noise. While NIST 800-90B presents measurements to demonstrate entropy suitability, we measured them using PSNR and MSE. MSE is a value that indicates the error between the original and the transformed images for a more intuitive and mathematical

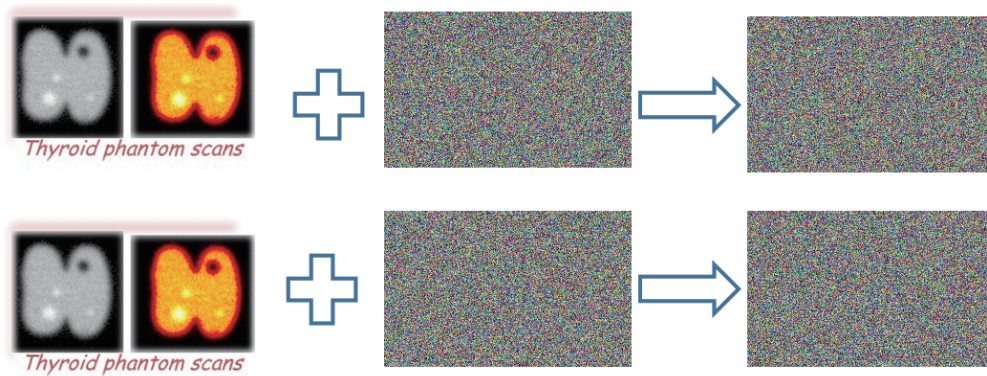


FIGURE 4. An image randomized when using the original image and the proposed algorithm (top) and an image randomized when using the original image and the CryptoGenRandom function (bottom).

performance comparison of the two algorithms. MSE represents the mean square error. Therefore, it is useful to measure the difference between the encrypted images. As shown in Figure 5, we can confirm that the PSNR of the original image and the image synthesized with the proposed algorithm (6.136116444 dB) is smaller than that of the original image and the image synthesized with CryptoGenRandom (6.159592278 dB).

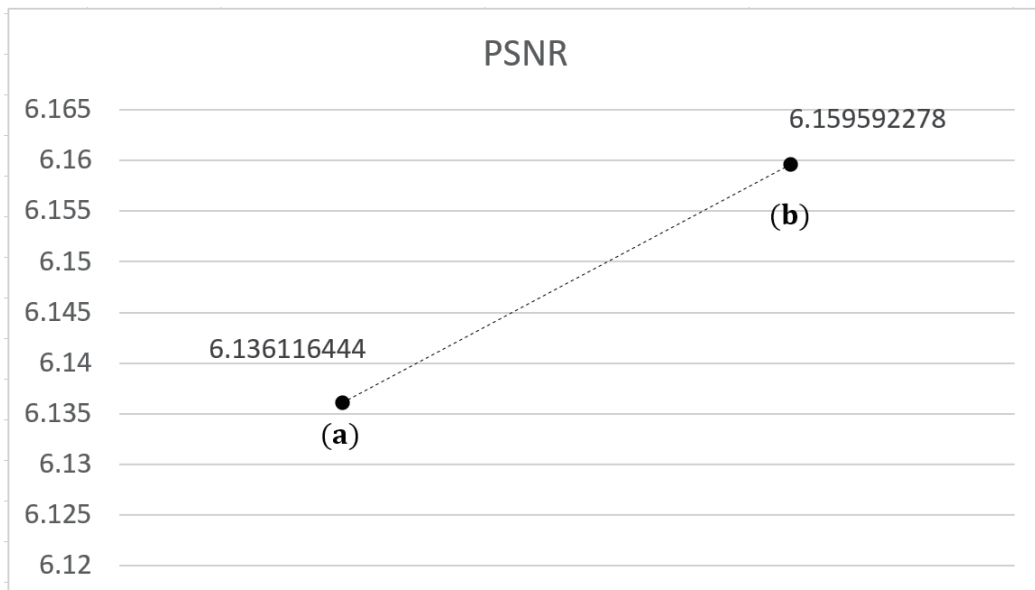


FIGURE 5. Comparison of PSNR measurements.

As shown in Figure 6, MSE can confirm that the value of the image synthesized by the proposed algorithm is larger (15829.55538). A larger MSE value of the randomization result of the original image indicates that the original image is more

damaged. Therefore, we can observe that the random number generated by the proposed algorithm is superior to the CryptoGetRandom function.

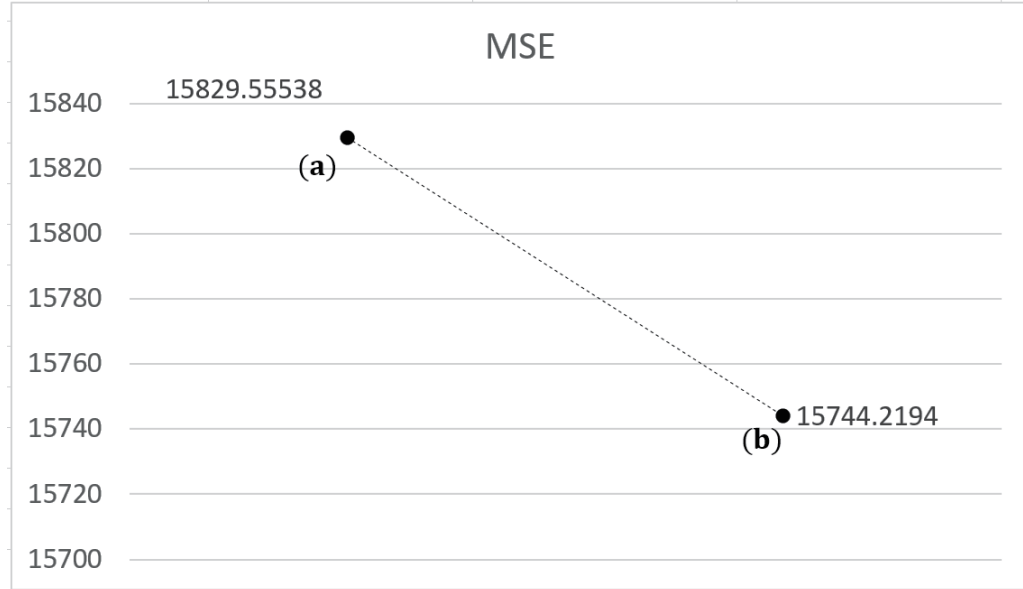


FIGURE 6. Comparison of MSE measurements.

4. CONCLUSION

The current gamma camera has been developed as a portable system or bench-top system with wireless capabilities. However, there are very limited encrypted image research studies with cryptographic algorithms. Therefore, our proposed idea could be valuable for researchers or developers to consider how to apply encrypted images to the gamma camera system.

In this paper, we studied a random number generation technique that can be widely used in various devices by generating random numbers dependent on hardware noise sources. It has the advantage of using mathematically generated random numbers in microcomputers and embedded devices that do not have abundant hardware resources. The proposed random numbers were evaluated for randomness using NIST SP 800-90B, which is a widely used standard evaluation method. The obtained random numbers were imaged, and then the original images were synthesized and further evaluated with some measurement indexes.

In the case of PSNR, which represents the signal-to-noise ratio of the evaluation results visualized, the proposed algorithm is 6.13611 dB, and CryptGenRandom is 6.15959 dB, respectively. A small value in PSNR indicates a higher level of noise. MSE is the mean square error, which is a measure of the difference between the original image and the synthesized image. A larger value indicates a greater difference between the original image and the synthesized image. The experimental results show that the image synthesized when using the proposed algorithm has a

higher degree of randomization than the original image. Ultimately, we can observe that the randomness of the proposed algorithm is higher than that of the CryptGenRandom function.

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] D. L. Bailey, D. W. Townsend, P. E. Valk and M. N. Maisey, *Positron Emission Tomography: Basic Sciences*, Springer, London, 2005.
- [3] J. Bird, *Engineering Mathematics*, 7th ed, Routledge, London, 2014.
- [4] D. Bouslimi, G. Coatrieux and C. Roux, *A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images*, Computer Methods Programs in Biomedicines **106** (2012), 47–54.
- [5] H. Choi and S.-H. Shin, *Novel random number generation for ultrasound systems*, Journal Nonlinear and Convex Analysis **24** (2023), 1835–1841.
- [6] H. Choi and S.-H. Shin, *Secured computed tomography scanner using a random bit*, Technology and Health Care **31** (2023), 55–59.
- [7] H. Choi and S.-H. Shin, *Mathematical algorithm for magnetic resonance imaging*, Journal Nonlinear and Convex Analysis **25** (2024), 1511–15181.
- [8] J. E. Gentle, *Random Number Generation and Monte Carlo Methods*, Statistics and Computing, Springer, NY, 2003.
- [9] M. L. Georgosopoulou, *Planar gamma camera overall performance*, Available from: <http://www.medimaging.gr/cd/pages/all.htm> (accessed 14. 12. 2024).
- [10] Sajeer M and A. Mishra, *A DCT-based robust and secure dual watermarking approach for color medical scans with joint permutation and diffusion encryption*, Multimedia Tools and Applications **83** (2024), 44251–44271.
- [11] 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.
- [12] R. A. Powsner and E. R. Powsner, *Essential Nuclear Medicine Physics*, Wiley, 2006.
- [13] N. Rangarakan, S. Patnaik, J. Knechtel, S. Rakheja and O. Sinanoglu, *Next Era in Hardware Security: A Perspective on Emerging Technologies for Secure Electronics*, Springer, 2021.
- [14] J. Ryu, G. Kim, J. Ko, D. Kang, J.-S. Kang and Y. Yeom, *Entropy harvest and key derivation from the image sensors in IP camera*, Journal of Surveillance, Security and Safety **5** (2024), 234–257.
- [15] K. K. Shung, M. Smith and B. M. Tsui, *Principles of Medical Imaging*, Academic Press, 2012.
- [16] J. A. Sorenson and M. E. Phelps, *Physics in Nuclear Medicine*, Grune and Stratton, 1987.
- [17] G. Suganya and K. Amudha, *Medical image integrity control using joint encryption and watermarking techniques*: 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), 2014, pp. 1–5.
- [18] W. Sun, L. Wang, J. Wang, H. Li and Q. Wu, *Optical image encryption using gamma distribution phase masks in the gyrator domain*, Journal of the European Optical Society-Rapid Publications **14** (2018): 28.
- [19] W. Sun, L. Wang, J. Wang, H. Li and Q. Wu, *Optical hyperspectral data encryption by using gamma distributed phase masks in gyrator domain*, Optical Review **26** (2019), 332–341.
- [20] D. Volterrani, P. A. Erba, I. Carrio', H. W. Stauss and G. Mariani, *Nuclear Medicine Textbook: Methodology and Clinical Applications*, Springer, 2019.
- [21] H. Xie, Y. Zhang, J. Bian and H. Zhang, *A secure and privacy-preserving technique based on coupled chaotic system and plaintext encryption for multimodal medical images*, Multimedia Tools and Applications **84** (2024), 22701–22726.
- [22] B. Zhang, R. Rahmatullah, S. L. Wang and Z. Liu, *A plain-image correlative semi-selective medical image encryption algorithm using enhanced 2D-logistic map*, Multimedia Tools and Applications **82** (2023), 15735–15762.

Manuscript received May 15, 2025

revised December 26, 2025

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`