Development of modified RSA algorithm using fixed mersenne prime numbers for medical ultrasound imaging instrumentation

Seung-Hyeok Shin, Won Sok Yoo and Hojong Choi

ABSTRACT

Purpose: Encryption of patient information has become an important issue in medical ultrasound instrumentation to secure information when images are accessed off-site. The proposed algorithm is used to encrypt private medical images and transfer the encrypted images to improve the encryption capability and elapsed time.

Materials and methods: We generate a public key using three prime numbers, including a fixed Mersenne prime number, in the modified Rivest-Shamir-Adelman (RSA) algorithm to compare the encryption capability. We calculated and compared the elapsed time using the modified RSA algorithm with a breast phantom in the medical ultrasound imaging instrumentation.

Results: The encryption capability is improved because the elapsed time when using three prime numbers is longer (1.2337 s) than that when using two prime numbers (1.0712 s). However, the elapsed time using fixed Mersenne prime numbers (0.8360 s) is similar to that using two prime numbers (0.8389 s).

Conclusions: Our proposed cryptographic algorithm provides improved encryption in medical ultrasound imaging compared to algorithms that use two prime numbers that are not Mersenne prime numbers, while transmitting images with adequate elapsed times.

KEYWORDS

Mersenne prime number; modified RSA algorithm; ultrasound imaging instrumentation

Introduction

Ultrasound is used in a variety of applications such as medical diagnostics and therapy, non-destructive testing, and sound navigation and range [1–3]. In particular, medical ultrasound imaging is a non-invasive and inexpensive technique compared to X-ray, computed tomography, and positron emission tomography [4,5]. Owing to the developments in the semiconductor industry, medical ultrasound imaging instrumentation has been widely used for cost-effective diagnostic solutions [6,7]. Therefore, ultrasound imaging is one of the most useful medical techniques that can be used for direct on-site diagnosis in emergency rooms, as well as an off-site diagnostic tool in ambulances; however, diagnosis in an ambulance increases the chance of invasion of patient information [8,9]. Therefore, encrypting patient information has become important in medical ultrasound instrumentation to secure this information when images are accessed off site.

Rivest-Shamir-Adelman (RSA) is one of the private-key based algorithms to transmit secure data for e-mail, web, and ATM machines [10]. In the RSA algorithm, the encryption of the public key is known and the decryption of the private key is secret such that the encryption and decryption of the complexity mechanism is basically based on the number of prime numbers in the key that need to be factorized [11]. To use completely secure data transmission, prime numbers that have more than 100 digits need to be factorized because very long computing time and huge powerful computing power are essential for the decryption of the prime numbers compared to the factorization of only two prime numbers; this is because only two prime numbers are typically easily breakable [12]. The use of three prime numbers was proposed to improve the security and reduce the processing time [13]. However, the proposed scheme requires the use of a large database. Four prime numbers were utilized to improve complexity and increase the security of the systems such that the key
encryption and decryption time increased considerably [14]. Therefore, the RSA algorithms using four prime numbers or three prime numbers may not be highly effective for use in emergency rooms and ambulances for patient diagnosis because of the encryption/decryption time and large database.

A Kobayashi algorithm was developed to encrypt pixel data of digital images for secured image transmission. This algorithm extracts the pixel and security data to achieve the required security [15]. The Hamming code was also used to reduce error in the data using an error correction technique [16]. The decryption algorithm using the RC4 cipher and two substitutive modulations with sufficient capacity was proposed to show the image reliability [17]. Recently, a 1024-bit RSA encryption algorithm was proposed to protect the patient information [18].

However, our proposed modified RSA-based algorithm using Mersenne prime numbers is a very simple cryptographic algorithm without complex encoding/decoding programming techniques. Therefore, we first propose a novel modified RSA algorithm using Mersenne prime number to transmit secure patient imaging data with appropriate computing time. In the Method section, we describe the development of the modified RSA algorithms to verify the encryption capability. In Result section, we describe the application of the developed modified RSA algorithms to the encryption and decryption of medical images obtained from a breast phantom; moreover, we compare the RSA algorithms using two prime numbers with our developed modified RSA algorithms using two prime and one fixed Mersenne prime number. Conclusion section presents the conclusion of our paper.

**Method**

Figure 1 shows the architecture of the medical ultrasound instrumentation with cryptosystem. The breast phantom images obtained are transferred through the cryptosystem to evaluate the encryption capability of the developed modified RSA algorithms using fixed Mersenne prime numbers.

In mathematics, a Mersenne prime is a very special prime number one less than a power of two. That is, it is a prime number \( p \) of the form \( M_p = 2^p - 1 \) [19]. RSA is a well-known cryptographic algorithms that use two prime numbers; it is still widely used for ATM machines in banks [10]. Our proposed modified RSA algorithm uses three prime numbers—\( P_1, P_2, \) and \( P_x \), where \( P_x \) is a fixed Mersenne prime number. The selected numbers that consist of three prime numbers are more difficult to factorize than numbers consisting of two prime numbers [10,20]. Table 1 shows the detailed procedure of the proposed cryptographic algorithm using three prime numbers including a Mersenne prime number.

We randomly select three prime numbers 43, 53, and 31, which are fixed prime numbers. To compare the factoring, we select two more prime numbers. One is 1327, which is less than 1333 \( (= \Phi (31 \times 43)) \); the other is 1361, which is greater than 1333. \( n \) represents the composite number obtained by multiplying the prime numbers. Table 2 shows the elapsed times for factoring numbers larger and smaller than 65535. \( \Phi(n) \) is selected as the middle number of the selected prime numbers. According to the results shown in Table 2, it is clear that the factoring of the proposed algorithm using a fixed Mersenne prime number is stronger than that of two prime numbers because it has a longer mean time (1.2337 s) with three prime numbers.
numbers compared to the mean times obtained using two prime numbers (1.0712 and 1.2112 s).

Results

Figure 2 shows the test breast phantom and cryptographic system. To verify the modified RSA algorithm, we used a multi-modal breast phantom (Model 073, CIRS Inc., Norfolk, VA), as shown in Figure 1(a). The images obtained from the ultrasound machine (E-cube 12R, Alpinion Technologies Inc., Seoul) were transferred to the constructed streaming server and these data were wirelessly transmitted via a Wi-Fi channel to the wireless receiver. The data received from the wireless receiver were decoded to retrieve the image data. Figure 2(b) shows the embedded Linux system based on an ARM7 core. The role of the system is to generate prime numbers, the composite number \(n\), \(\Phi(n)\), private key, public key, and to distribute the public key. We used streaming-type encryption for the ultrasound imaging data. Two bytes represent the range from 0 to 65535 (0 x FFFF) in the \(2^{16} - 1\) digit number. Therefore, encryption is performed for each 2-byte size.

Figure 3 shows the ultrasound image obtained from the breast phantom (Model 073). To encode 2-byte data from 0 to 65535, we selected a value of \(n\) that is greater than 65535. We then encoded the cipher stream \((C)\) from the plain stream \((M)\), \(C = M^n \pmod{n}\). Here, \(n\) is a composite number that is the product of the selected prime numbers. The composite number \(n\) is the public key for encoding the data in the proposed RSA algorithm. As the composite number is large, the elapse time for factorization in prime numbers is typically longer, leading to a longer elapse time to decode the public key, and thus improving the strength of the encryption.

Table 3 shows a comparison of the encryption speed results obtained using two and three prime numbers. The elapse time using Mersenne prime numbers is slightly shorter (0.8360 s) than that using two prime numbers (0.8365 and 0.8389 s). The digital imaging and communication in medicine (DICOM) files obtained from ultrasound machines need to be extracted to separate the private information and

![Image](image1)

Figure 2. Experiment setup for verifying the modified RSA algorithm in the medical ultrasound imaging instrumentation. (a) Commercial ultrasound linear array transducers with breast phantom and (b) cryptographic system implementation to send the data wirelessly.

![Image](image2)

Figure 3. Ultrasound image obtained from the breast phantom.

Table 3. Comparison data of the encryption speed.

| Prime numbers | \(n\)          | \((e, \Phi(n)) = 1\) | \(C = M^n \pmod{n}\) | Mean Time (seconds) |
|---------------|---------------|----------------------|----------------------|---------------------|
| \(P_1 : 53\)  | 70331         | 37                   | 0.8365               |
| \(P_2 : 1237\)| 70649         | 37                   | 0.8360               |
| \(P_1 : 31\)  | 72133         | 37                   | 0.8389               |
image data. The performances of the original image and images encrypted with the conventional RSA and modified RSA algorithms using Mersenne prime numbers were compared after the encryption process. **Figure 4** shows the DICOM images when using the conventional RSA encrypting algorithm and the modified RSA encrypting algorithm using Mersenne prime numbers, respectively.

Additionally, the images were compressed to compare the performances of the conventional RSA and modified RSA encryption algorithms. After encrypting the DICOM images obtained from the ultrasound instrumentation, the mean square error (MSE), structural similarity index (SSIM), peak signal-to-noise ratio (PSNR), and root mean square error (RMSE) values were measured and compared to evaluate the capability comparison of the algorithms [2,3]. MSE is the average precision value of the mean error deviation between the modelled and processed images [21]. SSIM is the index value that shows the similarity between the original and encrypted images [22]. PSNR is the ratio between the measured maximum signal power level and the noise signal power level of the encrypted images [23]. Therefore, higher PSNR is desirable for image processing and reconstruction because the noise signal power level is the minimum detection level of the signals [24–26]. RMSE is used to measure the precision of the images between the modelled and measured environment [27]. A lower RMSE is preferable because it indicates that the encrypted images are more similar to the original images. The MSE, RMSE, and SSIM performances are measured based on error values, and the PSNR performances are measured based on the dB scales.

We compared the image compression ratios when using the conventional RSA and modified RSA algorithms using Mersenne prime numbers. The measured MSE values are 5366.5578 and 2867.0798, respectively.

We also compared the PSNR values of the encrypted ultrasound images when using RSA and modified RSA algorithms. The PSNR value when using the modified RSA encrypting algorithm (13.5564 dB) is higher than that when using the conventional RSA algorithm (10.8338 dB). The RMSE values of the encrypted ultrasound images when using the conventional RSA and modified RSA algorithms were compared. The error value when using the modified RSA encrypting algorithm (53.5451) is much lower than that when using the conventional RSA algorithm (73.2567). The SSIM values of the encrypted ultrasound images when using the RSA and modified RSA algorithms were compared. A slightly higher SSIM value was achieved when using the modified RSA algorithm (0.6174) than when using the conventional RSA algorithm (0.6073). **Table 4** summarizes the experimental results of the MSE, SSIM, PSNR, and RMSE values after encrypting the DICOM images using the conventional RSA and modified RSA algorithms.

### Discussion

To verify the encryption security performances, the encryption capability was evaluated using the elapsed time. The elapsed time when using three prime numbers is longer than that using two prime numbers. Therefore, our proposed modified RSA algorithm using one fixed Mersenne prime number could be useful for...
encrypting DICOM images. As shown in Table 3, we can conclude that the proposed cryptographic method using Mersenne prime numbers increases the strength of the encryption key while slightly reducing the elapse time for streaming-type encryption by selecting the number closest to 65535.

To compare the DICOM image qualities when using the conventional RSA and modified RSA algorithms using one fixed Mersenne prime number for image encrypting capability, we calculated the MSE, SSIM, PSNR, and RSME values. As shown in Table 4, lower MSE and RSME error rates and higher PSNRs were achieved using our proposed algorithm. The modified RSA encryption algorithms have substantially smaller MSE error values. The proposed encryption algorithm has a better image capability. However, we can conclude that the proposed modified RSA algorithm using fixed Mersenne prime numbers still has reasonable SSIM values.

Conclusion
The proposed modified RSA algorithm using Mersenne numbers was successfully implemented for medical ultrasound imaging instrumentation. The encryption capability between two prime numbers and three prime numbers including a Mersenne number were compared to show the improvement in security performances. We confirm that the proposed algorithm using fixed Mersenne prime numbers improves the encryption capability of the developed algorithm compared to the algorithm using factoring of two prime numbers while providing almost the same elapsed time. Therefore, this developed modified RSA algorithm could be useful to access patient ultrasound images securely both on and off site.

Acknowledgements
This research was supported by Kumoh National Institute of Technology.

Disclosure statement
No potential conflict of interest was reported by the authors.

References
[1] Yan F, Li X, Jin Q, et al. Therapeutic ultrasonic microbubbles carrying paclitaxel and LyP-1 peptide: preparation, characterization and application to ultrasound-assisted chemotherapy in breast cancer cells. Ultrasound Med Biol. 2011;37:768–779.
[2] Hoskins PR, Martin K, Thrush A. Diagnostic ultrasound: physics and equipment. Cambridge (UK): Cambridge University Press; 2010.
[3] Postema M. Fundamentals of medical ultrasound. New York (NY): Taylor and Francis; 2011.
[4] Shung KK. Diagnostic ultrasound: imaging and blood flow measurements. Boca Raton (FL): Taylor & Francis; 2015.
[5] He Z, Zheng F, Ma Y, et al. A sidelobe suppressing near-field beamforming approach for ultrasound array imaging. J Acoust Soc Am. 2015;137:2785–2790.
[6] Weibao Q, Yanyan Y, Fu Keung T, et al. A multifunctional, reconfigurable pulse generator for high-frequency ultrasound imaging. IEEE Trans Ultrason Ferroelect Freq Control. 2012;59:1558–1567.
[7] Zhu B, Han J, Shi J, et al. Lift-off PMN-PT thick film for high frequency ultrasonic biomicroscopy. J Am Ceram Soc. 2010;93:2929–2931.
[8] Eren H, Webster JG. Telemedicine and electronic medicine. Boca Ration (FL): CRC Press; 2015.
[9] Cao F, Huang HK, Zhou XQ. Medical image security in a HIPAA mandated PACS environment. Comput Med Imaging Graph. 2003;27:185–196.
[10] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21:120–126.
[11] Rivest RL, Shamir A, Adleman LM, inventors; U.S. Patents, assignee. Cryptographic communications system and method. United States Patent US 4,405,829. 1983 Sep 20.
[12] Isvari NMS, editor. Key generation algorithm design combination of RSA and ElGamal algorithm. Proceedings of the 2016 8th International Conference on Information Technology and Electrical Engineering; 2016 Oct 5; Yogyakarta, Indonesia. 2016.
[13] Patidar R, Bhartiya R, editors. Modified RSA cryptosystem based on offline storage and prime number. Proceeding of the IEEE Computational Intelligence and Computing Research; 2013 Dec 23; Tamilnadu, India. 2013.
[14] Thangavel M, Varalakshmi P, Murali M, et al. An enhanced and secured RSA key generation scheme (ESRKGS). J Inf Secur Appl. 2015;20:3–10.
[15] Kobayashi LOM, Furuie SS, Barreto P. Providing integrity and authenticity in DICOM images: a novel approach. IEEE Trans Inform Technol Biomed. 2009;13:582–589.
[16] Acharya U R, Subbanna Bhat P, Kumar S, et al. Transmission and storage of medical images with patient information. Comput Biol Med. 2003;33:303–310.
[17] Bouslimi D, Coatireux G, Roux C. A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echographic images. Comput Methods Programs Biomed. 2012;106:47–54.
[18] Halmann MN, Unness MS, inventors; US Patent, assignee. Methods and systems for managing distribution of protected information on a medical display. United States Patent Application US 14/866,252. 2017 May 30.
[19] Crandall R, Pomerance CB. Prime numbers: a computational perspective. Berlin (Germany): Springer; 2006.
[20] Benjamin AT, Brown E. Biscuits of number theory. Washington (DC): Mathematical Association of America; 2009.

[21] Proakis JG. Digital signal processing: principles algorithms and applications. London: Pearson Education; 2001.

[22] Antoniou AD. Signal processing. New York (NY): McGraw-Hill; 2016.

[23] Kremkau FW, Forsberg F. Sonography principles and instruments. Amsterdam (Netherlands): Elsevier Health Sciences; 2015.

[24] Razavi B. RF microelectronics. Upper Saddel River (NJ): Prentice Hall; 2011.

[25] Friis HT. Noise figures of radio receivers. Proc IRE. 1944;32:419–422.

[26] Haykin S, Van Veen B. Signals and systems. Hoboken (NJ): Wiley; 2007.

[27] Seegelke C, Weigelt M. Anticipating different grips reduces bimanual end-state comfort: a tradeoff between goal-related and means-related planning processes. PLoS One. 2018;13:e0190586.