mathematics

MDPI

Article

Development of Public Key Cryptographic Algorithm Using Matrix Pattern for Tele-Ultrasound Applications

Seung-Hyeok Shin [1], Won-Sok Yoo [1] and Hojong Choi [2,*]

[1] Department of Applied Mathematics, Kumoh National Institute of Technology, Gumi 39177, Korea
[2] Department of Medical IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39253, Korea
* Correspondence: hojongch@kumoh.ac.kr; Tel.: +82-54-478-7782

Received: 3 August 2019; Accepted: 13 August 2019; Published: 17 August 2019

Abstract: A novel public key cryptographic algorithm using a matrix pattern is developed to improve encrypting strength. Compared to the Rivest–Sharmir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) algorithms, our proposed algorithm has superior encrypting strength due to several unknown quantities and one additional sub-equation during the encrypting process. Our proposed algorithm also provides a faster encoding/decoding speed when the patient's images for tele-ultrasound applications are transmitted/received, compared to the RSA and ECC encrypting algorithms, because it encodes/decodes the plain memory block by simple addition and multiplication operations of n terms. However, the RSA and ECC algorithms encode/decode each memory block using complex mathematical exponentiation and congruence. To implement encrypting algorithms for tele-ultrasound applications, a streaming server was constructed to transmit the images to the systems using ultrasound machines. Using the obtained ultrasound images from a breast phantom, we compared our developed algorithm, utilizing a matrix pattern, with the RSA and ECC algorithms. The elapsed average time for our proposed algorithm is much faster than that for the RSA and ECC algorithms.

Keywords: cryptographic algorithm; matrix pattern; tele-ultrasound

1. Introduction

Ultrasound is a non-expensive, non-invasive, and non-ionizing medical imaging modality compared to positron emission tomography (PET), single photo emission tomography (SPECT), and X-ray or computer tomography (CT) [1–4]. Ultrasound machines have been widely used in a variety of diagnostic areas, such as intravascular, esophageal, and intra-cardiac applications, and therapeutic areas, such as prostate cancer, uterine fibroid treatment, and breast cancer applications [5–10]. Ultrasound imaging or therapeutic machines have also been combined with other medical imaging modalities, such as magnetic resonance imaging (MRI), PET, and CT [11–13]. However, examination of the ultrasound images is operator-dependent, limited to trained medical specialists only [14,15].

Tele-ultrasound is a specific type of tele-medicine using commercial ultrasound machines [16–18]. When ultrasound examinations are performed remotely, the patient's images obtained from the ultrasound machine are transferred to other computers or terminal devices, including cellular phones and tablet devices, for further diagnosis and treatment [16]. Over the past 10 years, tele-ultrasound research has been widely involved with a variety of clinical applications, such as emergency diagnosis and surgery, intensive care units, and remote education or consultation [18]. For emergency diagnosis, ultrasound machines have recently been used as a diagnostic tool in ambulances for emergency

diagnosis cases with non-physicians before patients arrive at the hospital or medical center [16]. In the case of an emergency situation, the patient's image data, obtained from the ultrasound machine in the ambulance or emergency room, must be transferred though high-speed communication channels to other workstations or computers should a medical clinician need to advise further diagnosis for the immediate treatment and appropriate care of the patient [19].

Due to the development of the semiconductor industry, the manufacturing and fabrication costs of the application-specific integrated circuit (ASIC), one of the main components of the portable ultrasound scanner, have reduced [20–22]. Therefore, for intensive care applications, portable ultrasound scanners, particularly, have been used to check the chests and abdomens of severely-injured patients or children in emergency departments [17,23]. Remotely monitoring patients' conditions with portable ultrasound scanners provides real-time guidance for non-physicians through the acquisition of high-quality images [24]. An example of a remote consultation application is the focused assessment sonography for trauma (FAST) exam, operated by non-physicians, which has been utilized to check the free intraperitoneal fluid in the abdomen area [25,26]. Therefore, an accurate consultation from a primary doctor must be performed remotely in hospitals. By utilizing the FAST exam remotely, clinicians can estimate the suspected abdomen area and may reduce any intra-abdominal bleeding in the liver or cardiac area for the emergent situation before patients arrive at hospitals [27].

There are security issues when transferring and accessing patients' data for tele-ultrasound applications [28,29]. Recently, research has increased into technological approaches concerning the security issues that surround the transmission and sharing of medical imaging data, as well as into the development of tele-ultrasound applications [29]. Cryptographic algorithms for the encryption of medical images in the tele-ultrasound areas are one of the fundamental mechanisms used for patient confidentiality. A Kobayasi encrypting algorithm was introduced to extract the patients' images and security data for tele-medicine applications [30]. However, this encryption must extract the pixel data and security data together to achieve the appropriate algorithms. Double chaotic layer encryption was proposed for electroencephalograms (EEG), tele-medicine applications, which are effective for low-frequency and low-size EEG data [31]. A cryptosystem based on the chaotic theory was proposed for large data tele-ophthalmology applications and requires the production of pseudorandom sequences and a highly-uniform histogram together [32]. The RSA algorithm, with 2-D discrete wavelet transform watermarking procedures, was utilized for MRI, CT, and ultrasound medical images [33]. However, these methods require the extraction of patients' image data with the help of a private key in the wavelet domain and, hence, require a large database and wavelet domain conversion process. Owing to its higher security, elliptic curve cryptography (ECC) was used in wireless healthcare systems for ultrasound machines instead of the RSA algorithms [34]. There are many encrypting algorithms for tele-medicine applications, including tele-ultrasound applications. However, our developed public key cryptographic algorithm using a matrix pattern may have a strong encrypting capability with a faster transmit speed.

Digital imaging and communication in medicine (DICOM) is a standard of transmitting medical images which are protected by digital signature algorithms and watermarking, both of which are security mechanisms for medical image protection [35]. However, there are many terminal devices for tele-ultrasound applications, such as cellular phones, personal digital assistants, tablets, and readers. These terminal devices favor the use of other image formats, such as the tagged image file format (TIFF), graphics interchange format (GIF), portable network graphics (PNG), joint photographic experts group (JPEG) and JPEG-2000, independent JPEG (IJG), and Lempel–Ziv–Welch (LZW), because they have limited data spaces and memory for efficient data transmission [16,36]. In other words, it is essential that medical image transmission is compressed and encrypted. Therefore, our system structure for tele-ultrasound applications must be tested using one of these compressed image formats to demonstrate its encoding/decoding capabilities.

Figure 1 shows the flow chart of the proposed tele-ultrasound system with commercial ultrasound systems. The patients' DICOM or BMP images, obtained from the ultrasound system, are stored in a

web server, then the encoding JPEG process is performed in the transmission system. The encoded JPEG images are then transmitted through high-speed communication channels, such as Wi-Fi channels, to the receiving system to de-code the compressed images.

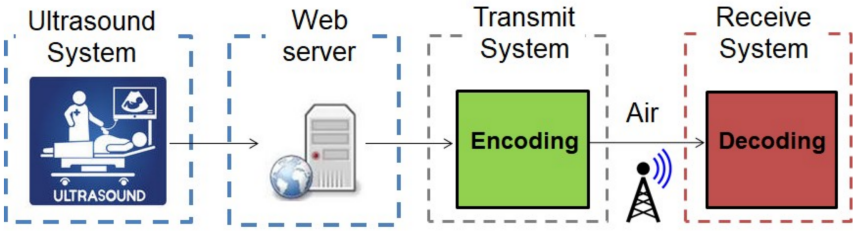


Figure 1. Flow chart of proposed tele-ultrasound system methodology.

This paper is structured as follows. In Section II, we describe how to construct the RSA and ECC algorithms and prove the algorithms mathematically. In Section III, we describe how to construct our proposed algorithm and prove the algorithm mathematically. The proposed algorithm introduced in this section is novel and it is obtained by the improvement of public key cryptosystem and vector orthogonality. In Section IV, we show the measurement and comparison experimental results of our proposed algorithm with other algorithms to evaluate the encrypting strength and the encoding/decoding speed of each encrypting algorithm. Section V provides the concluding remarks of this study.

2. Preliminary

We used the basic theory of Euler's totient function, Euler's theorem, and Euclid's theorem for constructing the cryptographic algorithms [37,38]. Euler's totient function is defined below [39]. Euclid's theorem can be expressed as a linear combination of the integers [40].

2.1. RSA Algorithm

The RSA algorithm is a famous cryptographic algorithm used by modern computers and communications to encrypt and decrypt messages [41]. It is a kind of asymmetric and public key cryptographic algorithm based on number theories [42]. The RSA algorithm is derived from Euler's totient function, Euler's theorem, and Euclid's theorem [43]. For any natural number n, Euler's totient function symbol is $\Phi(n)$, which refers to the number of positive integers that are less than n and coprime with n. For the RSA algorithm, factorization of composite numbers that comprise sufficiently large two prime numbers is too difficult. The key generation and the encoding and decoding steps for the RSA algorithm are described as follows [44].

2.1.1. Key Generation Step

(A) Randomly choose two prime number integers p and q,

$$(p, q) = 1, \tag{1}$$

where (p, q) is the greatest common divisor of p and q.

(B) Compute $n = p \times q$, where n is used as modulo for both the public and private key.

(C) Compute Euler's function $\Phi(n)$ using the two prime numbers p and q.

$$\Phi(n) = \Phi(p \cdot q) = \Phi(p) \cdot \Phi(q) = (p - 1) \cdot (q - 1). \tag{2}$$

(D) Choose an integer e such that

$$(\Phi(n), e) = 1, \tag{3}$$

where $1 < e < \Phi(n)$.

(E) Since $(\Phi(n), (e)=1$ by Equation (3), there exist integers d and t such that $ed + \Phi(n)t = 1$. Thus, we can compute d by using Euclid's theorem so that the product of e and d is as follows:

$$e \cdot d \equiv 1 \pmod{\Phi(n)}. \tag{4}$$

(F) Select the integers n and e as the public key, then, select the integers p, q, and d as the private key.

2.1.2. Encoding Step

(A) M is a separated memory block which is stored into the $M_1, M_2, \ldots, M_n$ such that it represents a value in the range of 1 to n.

$$M = (M_1, M_2, \ldots, M_n). \tag{5}$$

(B) Encode to cipher block using the public key n and e to obtain M_i:

$$M_i{}^e \equiv C_i \pmod{n}, \tag{6}$$

where $i = 1, 2, \ldots$.

2.1.3. Decoding Step

(A) The cipher block C_i is decrypted into M_i.

(B) Decode to plain block using the key p, q, and d.

$$C_i{}^d \equiv M_i \pmod{n}. \tag{7}$$

2.2. Elliptic Curve Cryptographic Algorithm

The elliptic curve cryptography (ECC) system is based on a discrete logarithm problem of finite fields defined on the elliptic curve group and is a public key cryptographic algorithm proposed independently by Miller and Koblitz in 1985 [45]. This algorithm has been intensively researched for number theories and algebraic geometry fields for 150 years and was also used to prove Fermat's last theorem [46]. Recently, the ECC theory has been used for factorization, primality test, and public key cryptographic algorithms, which are the basic crypto-system [37]. The elliptic curve on a finite field is a set such that

$$E = \left\{(x, y) \in F \times F \middle| \, y^2 = x^3 + ax + b\right\}, \tag{8}$$

where E is a set of the point (x, y) that satisfies the following equation: $y^2 = x^3 + ax + b$. However, the characteristics of a finite field F are assumed as over 0 or 4. If the multiple root of the equation $y^2 = x^3 + ax + b$ does not exist, then

$$4a^3 + 27b^2 \neq 0. \tag{9}$$

In the case of Equation (9), the sum of the set is the following: $E(F) = E \cup O$, where the set E and infinite origin O are to the commutative group, as shown in Equations (10) and (11). We also call the $E(F)$ a group over elliptic curve. An additional theorem of a group over elliptic curve $E(F)$ is described below.

$$P + O = O + P = P, \tag{10}$$

where $\exists P \in E(F)$.

In Equation (10), P is a point on the E and the O is an identity element to satisfy the commutative group.

$$(x, y) + (x, -y) = 0, \text{ i.e., } -\mathrm{P} = (x, -y), \tag{11}$$

where $P = (x, y) \in E(F)$.

$P = (x, y)$ is a point on the symmetry curve E. In the case: $P \neq Q$, $Q \neq O$, $Q \neq -P$

(2) $P \neq Q$,

Point K is an intersection point of $\overline{PQ}$ and E. The symmetry point K is defined to be $P + Q$.

(ii) $P = Q$,

Point K is an intersection point tangent to P and E. The symmetry point K is defined to be $P + Q$.

Figure 2 explains the elliptic curve. Let Equation (12) be the equation of the line through the points P and Q.

$$y = \alpha x + \beta, \tag{12}$$

$$\alpha = (y_2 - y_1)/(x_2 - x_1), \tag{13}$$

$$\beta = y_1 - \alpha x_1, \tag{14}$$

$$(\alpha x + \beta)^2 = x^3 + ax + b. \tag{15}$$

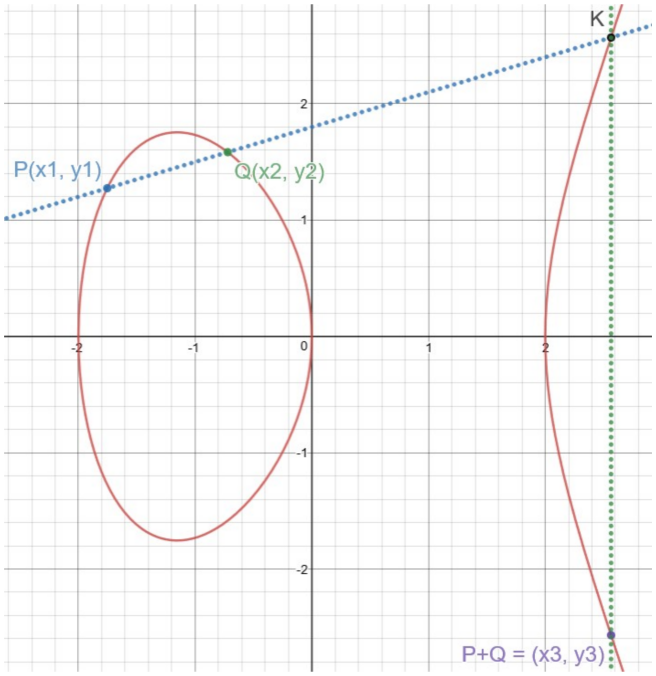


Figure 2. Addition of a group over elliptic curve.

Using Equations (8) and (12), we can obtain Equations (13), (14), and (15). Therefore, we can obtain the three valuables, x_1, x_2, and x_3, in Equation (16).

$$x_3 = \alpha^2 - x_1 - x_2. \tag{16}$$

In addition, point (x_3, y_3) is on the straight line in Equation (12) such that we can obtain Equation (17).

$$-y_3 = \alpha x_3 + (y_1 - \alpha x_1) = y_1 + \alpha(x_3 - x_1). \tag{17}$$

Therefore, from (16) and (17), the coordinates (x_3, y_3) of $P + Q$ can be represented by Equations (18) and (19).

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \tag{18}$$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3). \tag{19}$$

The key generation and the encoding and decoding steps for the ECC algorithm are described as follows [47].

2.2.1. Key Generation Step

(A) Select an elliptic curve group $E(F)$ of a finite field F and select a maximum characteristic element P of $E(F)$.

(B) Select any integer $\alpha \in Z$ and calculate the element Q.

$$Q = \alpha P. \tag{20}$$

(C) Select (F, $E(F)$), elements P and Q as a public key, then select an integer α as a private key.

2.2.2. Encoding Step

(A) Prepare a plain memory block for the encoding of $E(F)$.

(B) Select any integer k ∈ Z and encode the plain memory block M to cipher like a (C_1, C_2).

$$C_1 = kP, C_2 = M + KQ. \tag{21}$$

2.2.3. Decoding Step

(A) Decode the cipher block.

$$C_2 - \alpha C_1 = (M + KQ) - \alpha(kP) = (M + kQ) - k\,Q = M. \tag{22}$$

The security of modern ECC depends on the intractability of determining α from $Q = \alpha\, P$ given known values of Q and P if α is sufficiently large ($\alpha \geq 500$). This is because the addition of two points on an elliptic curve (or the addition of one point to itself) yields a third point on the elliptic curve whose location has no obvious relationship to the locations of the first two, and repeating this many times over yields a point αP that may be essentially anywhere.

3. Proposed Algorithm

The proposed algorithm uses an $n \times n$ matrix, three pairs of private/public keys, and a salt matrix that makes it quite difficult to find the private keys [48]. The strength of the proposed algorithm is given by the cipher changing by the salt matrix every encoding step.

3.1. Key Generation Algorithm

(A) Select a positive integer n and select the $1 \times n$ matrix A to use as a first private key. The matrix A is a super-increasing sequence [48,49].

$$A = (a_1, a_2, \ldots, a_{\mathrm{n}}),$$

where $a_1, a_2, \ldots, a_{\mathrm{n}}$ are positive integers, such that we can obtain

$$a_i > \sum_{j=1}^{i-1} a_j, \ for\ I = \ 2, \ldots, n. \tag{23}$$

(B) Select a positive integer m such that

$$(a_1 + a_2 + \ldots, a_{\mathrm{n}}) < m, \tag{24}$$

where m is used as a modulus of congruence.

(C) Select a $1 \times n$ matrix K in Z_m to use as a second private key.

$$K = (k_1, k_2, \ldots, k_n), \tag{25}$$

where $Z_m = \{0, 1, 2, \ldots, m-1\}$ is the least complete residue class modulo m.

(D) Select Si $(1 \le i \le n)$ in Z_m such that

$$(k_1 S_1 + k_2 S_2 + \ldots + k_n S_n) \equiv O \pmod{m}, \tag{26}$$

where k_i $(1 \le I \le n)$ are the integers selected in (C).

(E) S is described as an $n \times n$ matrix to use as a first public key.

$$S = \begin{bmatrix} s_1 & s_1 & \ldots & s_1 \\ s_2 & s_2 & \ldots & s_2 \\ . & . & \ldots & . \\ s_n & s_n & \ldots & s_n \end{bmatrix}, \tag{27}$$

where Si $(1 \le i \le n)$ are the integers selected in (D).

(F) Select an $n \times n$ matrix B in Z_m to use as a second public key such that

$$\mathrm{KB} \equiv (a_1, a_2, \ldots, a_n) \pmod{m}, \tag{28}$$

where a_i and Si $(1 \le i \le n)$ are the integers selected in (A) and (C), respectively.

(G) Use as public keys n, m, S, and B.

3.2. Encoding Algorithm

(A) Select an $n \times n$ random matrix P to use the element p_{ij} as a salt:

$$P = (P_{ij}), \tag{29}$$

where $p_{ij} \in Z_m$, $1 \le i, j \le n$.

(B) The plain memory block M to binary memory block:

$$M = (m_1, m_2, \ldots, m_n), \tag{30}$$

where $m_i \in \{0,\ 1\}$, $j = 1,2, \ldots, n$.

(C) Encoding the plain memory block M:

$$(SP + B) \times MT \equiv CT \pmod{m}, \tag{31}$$

where C is a cipher block, S is a matrix using Equation (27), B is a matrix using Equation (28), P is a matrix using Equation (29), and M^T and C^T are matrix transforms.

3.3. Decoding Algorithm

(A) Find a positive integer α such that

$$KC^T \equiv \alpha \pmod{m}, \tag{32}$$

where $\alpha \equiv (k_1 m_1 + k_2 m_2 + \ldots + k_n m_n) \pmod{m}$. Notice that $\alpha \equiv (\alpha_1 m_1 + \alpha_2 m_2 + \ldots + \alpha_n m_n) \pmod{m}$.

(B) Find a plain memory block.

$$m_n = \begin{cases} 0 : \alpha < a_n \\ 1 : \alpha \geq a_n \end{cases} \quad and \; m_i = \begin{cases} 0 : \alpha - \sum_{j=i+1}^{n} a_j m_j < a_i \\ 1 : \alpha - \sum_{j=i+1}^{n} a_j m_j \geq a_i \end{cases}, (i = 1, 2, \ldots, n-1) \tag{33}$$

According to the conditions, Deffuant models propose how to decide the threshold of the opinion in the social networks [50,51]. However, this paper describes how to decide the plain memory block value according to the conditions.

<Example of proposed algorithm>

1. Key Generation Step Let $n = 4$, the super-increasing sequence $A = (1, 3, 5, 15)$ and let $m = 30$. Select

$$K = \begin{bmatrix} 2 & 8 & 3 & 11 \end{bmatrix}, S = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 4 & 4 & 4 & 4 \end{bmatrix}, and \; B = \begin{bmatrix} 0 & 4 & 1 & 2 \\ 0 & 1 & 0 & 1 \\ 3 & 2 & 1 & 1 \\ 2 & 1 & 0 & 0 \end{bmatrix}.$$

   Then, $KS \equiv O \pmod{30}$ and $KB \equiv A \pmod{30}$.
2. Public Keys: n, m, S, B and Private Keys: A, K
3. Encoding Step Let the plain text.

$$\mathrm{M} \equiv [m_1 \; m_2 \; m_3 \; m_4] = [1 \; 0 \; 1 \; 1].$$

   Choose any 4×4 matrix

$$P = \begin{bmatrix} 5 & 1 & 3 & 1 \\ 1 & 0 & 1 & 4 \\ 3 & 1 & 0 & 3 \\ 4 & 1 & 2 & 7 \end{bmatrix}.$$

   The plain text M is encrypted by computing.

$$(SP + B) \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 7 \\ 5 \\ 13 \\ 18 \end{bmatrix} (\mathrm{mod}\; 30)$$

   The cipher text is $C = [7 \; 5 \; 13 \; 18]$.
4. Decoding Step
   Compute

$$KC^T = \begin{bmatrix} 2 & 8 & 3 & 11 \end{bmatrix} \begin{bmatrix} 7 \\ 5 \\ 13 \\ 8 \end{bmatrix} = 291 \equiv 21 \; (\mathrm{mod}\; 30)$$

   This yields $m_1 + 3m_2 + 5m_3 + 15m_4 = 21$. Therefore, the cipher text C is decrypted as

$$[m_1 \; m_2 \; m_3 \; m_4] = [1 \; 0 \; 1 \; 1].$$

Table 1 shows the decoding procedure for the proposed public key cryptographic algorithm process using matrix patterns. Using Equation (31) and private key A, the cipher memory is decoded into matrix R. The initial α value is generated from Equation (32). After determination of $sumA$, which satisfies α value from the elements of the matrix K, we store 1 or 0 as a result of matrix R using Equation (33). If the row and column size of the matrix R reach zero, the decoding process is complete. The value "α" is the same valuable in Equation (32). "Alpha-sumk" means that alpha minus sumK. "row and column" are a row and a column of the matrix A or R, respectively.

Table 1. Decoding procedure of proposed algorithm.

Algorithm. Find a plain memory

INPUT: matrix A, α
OUTPUT: matrix R
alpha = α
procedure Decoding()
  WHILE row > 0 **DO**
    WHILE column > 0 **DO**
      Set sumA to sum from $A_{(1,1)}$ to $A_{(row, column)}$
      IF alpha >= sumK **THEN**
        Compute alpha **as** alpha - sumK
        Set $R_{(row,column)}$ **to** 1
      ELSE
        Set $R_{(row,column)}$ **to** 0
      ENDIF
      Compute column as column - 1
    ENDWHILE
    Compute row as row - 1
  ENDWHILE
RETURN with error code

We prove the proposed algorithm mathematically as shown below from Equation (34) to Equation (38).

Figure 3 explains the sequence diagram regarding the key management of this study. To send the coded message, Alice (sender) and Bob (receiver) are selected. Alice generates the super-increasing subsequence matrix A and modulo m using Equations (23) and (24), then, the S and B public key using Equations (26), (27), and (28) to pass them to Bob. Bob generates matrix S' and B', respectively, based on the size of n and modulo m, and exchanges the public keys between Alice and Bob. Alice generates a random matrix P to send a message M, encoding the message using Equation (31), then, sends that to Bob. Bob decodes the received encrypted message using Equation (32).

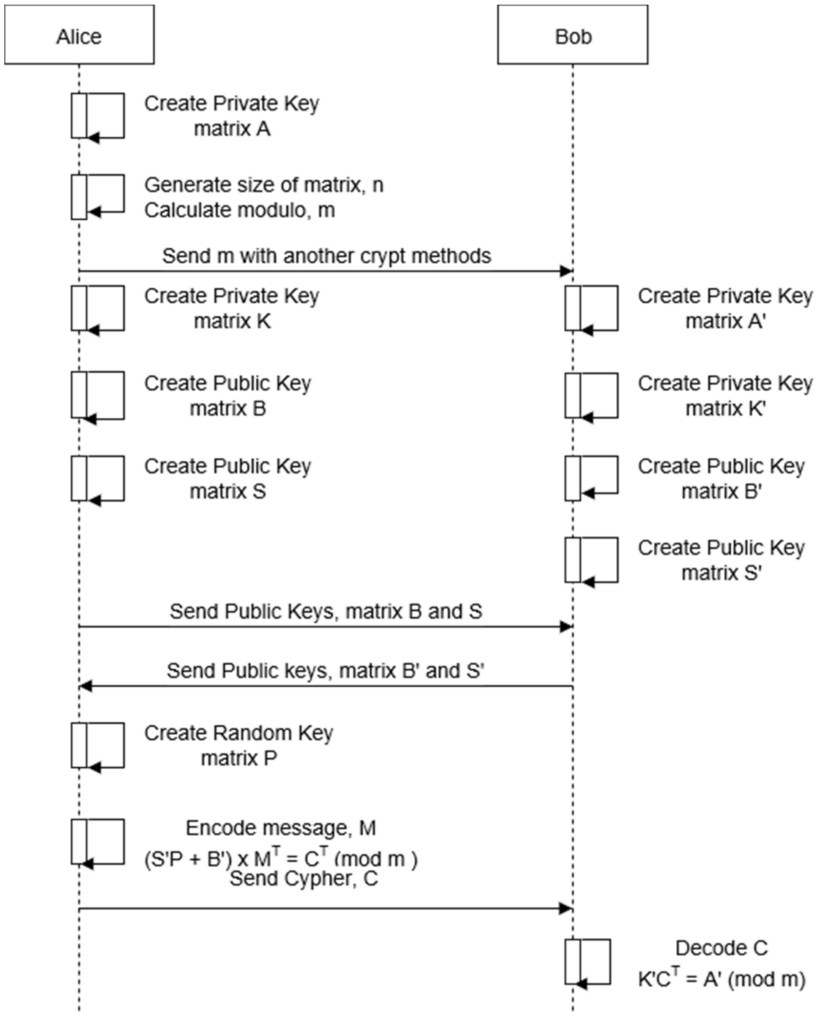


Figure 3. Key generation, exchange, and message encoding/decoding sequence.

3.4. Proof of the Algorithm

(A) We already know private key K when using Equation (25), cipher C^T, and Equation (31).

$$\alpha \equiv KC^{\mathrm{T}} \pmod{m}. \tag{34}$$

(B) We can transfer C^T to Equation (37) when using Equation (31).

$$C^T \equiv \left\{ (SP + B) \times M^T \right\} (\mathrm{mod}\ m). \tag{35}$$

(C) We can calculate Equation (36).

$$K\left\{ (SP + B) \times M^T \right\} \equiv \left\{ (KS) \times PM^T + (KB) \times M^T \right\} (\mathrm{mod}\ m). \tag{36}$$

(D) (KS) equals to the matrix O when using Equation (26). Therefore, we obtain the following equation:

$$\left\{ O + (KB) \times M^T \right\} \equiv (KB) \times M^T (\mathrm{mod}\ m). \tag{37}$$

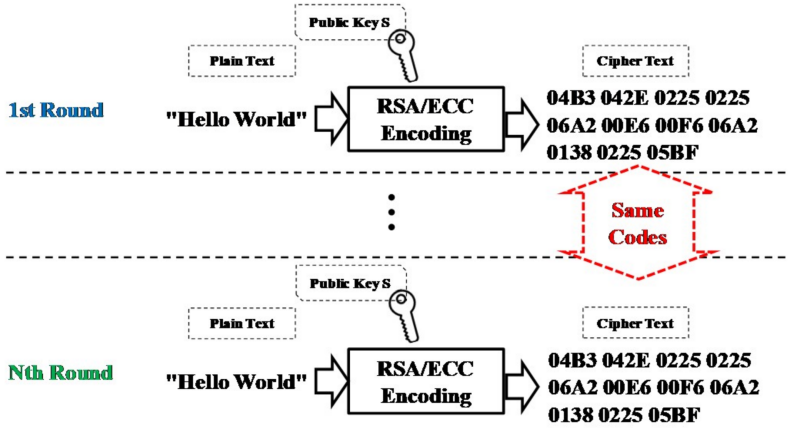
(E) (KB) represents Equation (38) when using Equation (28).

$$(KB) \times M^T \equiv (a_1, a_2, \ldots, a_n) \begin{pmatrix} m_1 \\ m_2 \\ . \\ . \\ . \\ m_n \end{pmatrix} (\text{mod } m). \tag{38}$$

(F) In Equation (39), we re-write Equation (32) to Equation (38).

$$\begin{aligned} \alpha \equiv KC^T \equiv K\{(SP+B) \times M^T\} \equiv (KS) \times PM^T + (KB) \times M^T \equiv O + (KB) \times M^T \\ \equiv (KB) \times M^T \equiv (a_1, a_2, \ldots, a_n) \begin{pmatrix} m_1 \\ m_2 \\ . \\ . \\ . \\ m_n \end{pmatrix} \equiv (a_1 m_1 + a_2 m_2 + \ldots a_n m_n) \ (\text{mod } m) \end{aligned} \tag{39}$$

As most of the public key cryptographic algorithm uses the same key in its encryption process, it is vulnerable to attacks when analysis of character frequency is used [52]. However, the public key cryptographic algorithm proposed in this paper is much safer from these attack types because users select the matrix at random aside from the public key when they encrypt plain memory. Figure 4 explains the differences between the RSA, ECC, and the proposed algorithms. Compared to the RSA and ECC algorithms, our proposed algorithm used an additional matrix pattern, which could increase the strength of the cryptographic capability as different codes can be created for every round compared to the RSA and ECC algorithms, which make the same codes.



(a)

Figure 4. *Cont.*

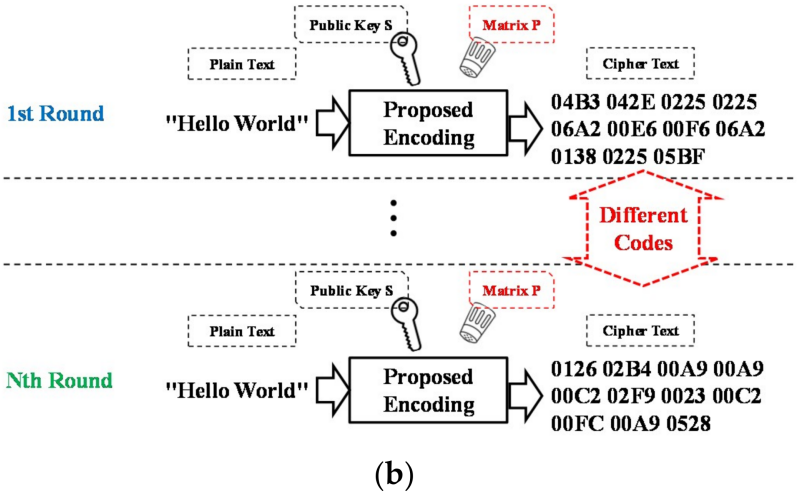


Figure 4. Encoding processes of (**a**) RSA and (**b**) proposed algorithms.

4. Results and Discussion

For the case of the RSA algorithm, there is a disadvantage that the same cipher text can be generated in all rounds if the plain text is encoded with the same pattern. However, for the case of our proposed algorithms, the matrix P, defined in Equation (28), can be generated randomly in all rounds of encoding time when using Equation (31). Therefore, there is an advantage that different cipher texts can be generated each time when the plain text of the same pattern is encoded with same public key.

Tele-medical transmission applications have been used to verify capability of the encrypting algorithms using the time to find the private keys [53,54]. The probability P of finding the private keys A and K from the proposed algorithm can be calculated by Equation (40). The probability of finding each element in private key A in Equation (23) is used in Equation (40).

$$P = \frac{1}{\prod_{i=0}^{n-1} \frac{m}{2^i}}, \tag{40}$$

where any integer $n > 1$ and $m > 1$.

For example, the calculated probability to find matrix A if integers $n = 8$ and $m = 1024$ are 1/17,592,186,044,416. It will take 557,844 years to find one matrix per second. For the larger integer m, the probability is further reduced.

The private key K can be calculated as a matrix multiplication with the public key S using Equation (26). However, it is impossible to find private keys for calculation because there are eight unknown quantities and one additional subequation. For the RSA algorithm, it takes a long time to factorize the prime numbers for a composite number over 100 digits [44]. Recent research has shown that the RSA cryptosystem is rapidly breaking down when using quantum computers [55]. However, our proposed algorithm increases encryption strength using private key A, which is less likely to be found, and private key K, which cannot be computed mathematically, at the same time. Equation (41) describes the public key and private key generation algorithm of the ECC:

$$y = g^x \pmod{p}, \tag{41}$$

where any integer $x > 1$, $g > 1$, and p are prime.

We will describe how to perform the experimental results to estimate the encrypting strength.

RSA: We measured the elapsed fractional decomposition of the composite number 10,967,909 against the prime number 4,613,169.

ECC: The p and x prime numbers in Equation (31) are fixed to 3461, 3169, and 1024. Then, the x prime number that satisfies a private key y is sequentially retrieved to measure the elapsed time.

Proposed: After we set the matrix A for the private key (16,644; 34,543; 205,415; 307,306; 702,750; 1,388,246; 2,794,512; and 5,504,370) and set modulo m to 10,955,976 by Equation (24), we measured the time to find the matrix elements searched for each element by Equation (33). The time complexity of encoding is O ($N \times \log m$) in Equation (31) and the space complexity of encoding is $4 \times N^2$ from the N $\times$ N matrix S, P, B, and A.

In Table 2, the average elapsed time for searching the private key when using our proposed algorithm (42.41753 ms) is much longer than those using the RSA and ECC encrypting algorithms, respectively (2.80888 and 0.72106 ms). As a result, we observed that the search speed of the proposed algorithm using a small value is much longer than that of the RSA and ECC algorithms, such that the stability of the key is experimentally confirmed.

Table 2. Elapsed time (ms) to find private keys when using RSA, ECC, and the proposed algorithms.

Number of Experiments	RSA	ECC	Proposed
1	2.8101	0.7209	42.4272
2	2.8092	0.7211	42.4146
3	2.8101	0.7214	42.4151
4	2.8078	0.7219	42.4147
5	2.8106	0.7166	42.4159
6	2.8089	0.7218	42.4216
7	2.8036	0.7212	42.4183
8	2.8092	0.7222	42.4131
9	2.8095	0.7218	42.4194
10	2.8098	0.7217	42.4154

Figure 5 shows the elapsed time to search the private key versus the number of experiments to compare the encrypting strength for the RSA, ECC, and proposed algorithms. To show the encrypting strength consistency for the algorithms, we repeated the test 10 times.

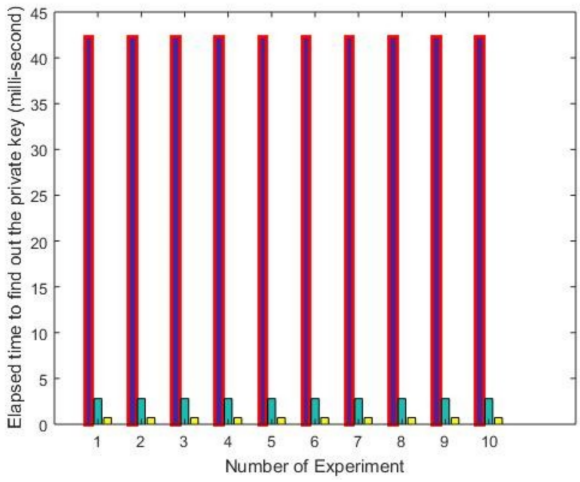


Figure 5. Elapsed time to find out private key vs. number of experiments to compare encrypting strength when using RSA (yellow color), ECC (light blue color), and proposed algorithms (purple color).

The RSA algorithm searches the private key based on mathematical theory, therefore, it takes a long time to decompose smaller numbers [44]. The ECC and proposed algorithms are the method of probability to find each key element [47]. For the case of the ECC and proposed algorithms, we consider the characteristics of this cryptographic algorithm, which assumes that the private key was

known in advance. Therefore, we performed experiments with similar values in a range smaller than the composite number used for the RSA.

To apply the encrypting algorithms for tele-ultrasound applications, the ultrasound images of the multimodal breast phantom (Model 073, CIRS Inc., Norfolk, VA, USA) were obtained using a commercial ultrasound machine (E-cube 12R, Alpinion Technology Inc., Seoul, South Korea). Figure 6 shows the setup of the commercial ultrasound machine with the breast phantom and its image.

(**a**)

(**b**)

Figure 6. (**a**) Commercial ultrasound machine with breast phantom and (**b**) breast phantom image.

In the experiment, libjpeg 9b version is used [56]. Using the libjpeg process, DICOM images were obtained from the commercial ultrasound machine with the breast phantom and were converted to JPEG images to reduce the image data size, because the tele-ultrasound applications have limited bandwidths when using wireless channels, such as Wi-Fi [29]. Afterwards, the images were tested using the RSA, ECC, and the proposed algorithms to check the encoding/decoding speeds, as communication speed is an important merit for tele-ultrasound applications [16]. In this paper, we used an RSA and ECC algorithm in the OpenSSL cryptographic library, which is an open license [56]. A Linux stand-alone system composed of an Intel core i5 3.20 GHz, 6144 KB cache size, and 8 GB memory was used to test the encrypting strength capability of the RSA, ECC, and our proposed algorithms. Figure 7 shows the encoding/decoding procedure of the RSA, ECC, and the proposed algorithms. The procedure details are described as below.

1. The DICOM image is converted to a JPEG image that is then reduced in size.
2. The JPEG image splits pixel data into plain memory by the encoder.
3. The encoding procedure performs the encoding process from the pixel data to the encoded data.
4. The decoding procedure performs the decoding process from the encoded data to the decoded data.
5. A JPEG image is produced by the decoder.

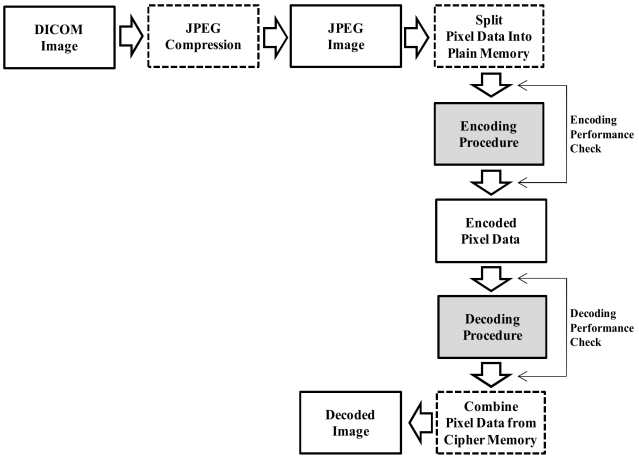


Figure 7. Block diagram for encoding/decoding procedures of the RSA/ECC/proposed algorithms.

Table 3 shows the measured elapsed time to check the encoding speed when using the RSA, ECC, and our proposed algorithms. To demonstrate the consistency in the algorithms, we repeated the test 10 times. The average elapsed time (0.0195 ms) when using our proposed algorithm is much faster than those when using the RSA and ECC encrypting algorithms (4.4311 ms and 7.3931 ms, respectively). Table 3 shows the measured elapsed time to check the encoding speed when using the RSA, ECC, and our proposed algorithms. To demonstrate the consistency in the algorithms, we repeated the test 10 times. The average elapsed time (0.0195 ms) when using our proposed algorithm is much faster than those when using the RSA and ECC encrypting algorithms (4.4311 ms and 7.3931 ms, respectively).

Table 3. Elapsed time (ms) to check the encoding speed when using the RSA, ECC, and proposed algorithms.

Number of Experiments	RSA	ECC	Proposed
1	4.4304	7.3606	0.0185
2	4.4315	7.3862	0.0184
3	4.4320	7.3959	0.0185
4	4.4315	7.3779	0.0185
5	4.4314	7.4165	0.0185
6	4.4317	7.4220	0.0184
7	4.4316	7.4005	0.0184
8	4.4306	7.4154	0.0299
9	4.4301	7.3790	0.0183
10	4.4309	7.3773	0.0183

Figure 8 shows the elapsed time to the check encoding speeds when using the RSA, ECC, and our proposed algorithms. To show consistency in the encrypting algorithms, we repeated the test 10 times.

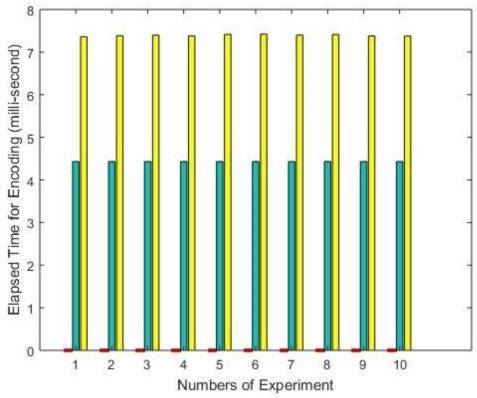


Figure 8. Elapsed time vs. number of experiments to compare encoding speeds when using RSA (green color), ECC (yellow color), and proposed algorithms (red color).

Table 4 shows the measured elapsed time to check the decoding speed when using the RSA, ECC, and our proposed algorithms. The average elapsed time for the decoding speed when using our proposed algorithm (0.0184 ms) is much faster than those when using the RSA and ECC encrypting algorithms (4.4316 ms and 7.3891 ms, respectively). Therefore, we can conclude that our proposed public key cryptographic algorithm using a matrix pattern could outperform, regarding the encoding and decoding speeds, compared to the RSA and ECC algorithms.

Table 4. Elapsed time (ms) to check decoding speed when using RSA, ECC, and proposed algorithms.

Number of Experiments	RSA	ECC	Proposed
1	4.4316	7.3736	0.0185
2	4.4320	7.3836	0.0185
3	4.4309	7.3850	0.0184
4	4.4312	7.3900	0.0184
5	4.4329	7.4220	0.0185
6	4.4315	7.3790	0.0185
7	4.4318	7.3886	0.0184
8	4.4320	7.3830	0.0183
9	4.4318	7.4070	0.0187
10	4.4312	7.3798	0.0184

Figure 9 shows the elapsed time to check the decoding speeds of the RSA, ECC, and our proposed algorithms.

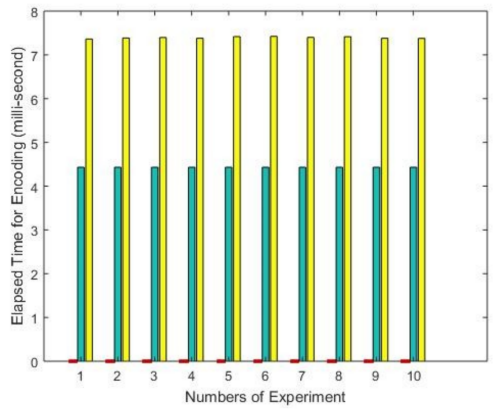


Figure 9. Elapsed time vs. number of experiments to compare decoding speeds when using RSA (green color), ECC (yellow color), and proposed algorithms (red color).

In this paper, we did not address the entire information security system for the ultrasound machines. Distributed multi-agent is a technique for securing the information integrity held by each agent. A security system mechanism using distributed multi-agent was recently proposed [57,58]. A strong security system can be constructed with an encryption algorithm with distributed multi-agent security system technology.

5. Conclusions

In addition to the hardware development for ultrasound machines, wireless internet technology development will boost the usage of tele-ultrasound applications because tele-ultrasound requires a fast internet access speed for immediate diagnosis and remote treatment. For our proposed algorithm, it is impossible to find the private keys for the calculation because there are 8 unknown quantities and one additional subequation. The average elapsed time to search the private key when using our proposed algorithm (42.41753 ms) is much longer than those when using RSA and ECC encrypting algorithms, respectively (2.80888 ms and 0.72106 ms). Therefore, our proposed algorithm shows more difficulty in the search of private keys such that it has a superior performance for the encrypting strength of the image data compared to the RSA and ECC algorithms, which are widely used for tele-ultrasound applications. In addition, our proposed algorithm encodes/decodes the plain memory block by the addition and multiplication of n terms. However, the RSA and ECC encode/decode each memory block with complex mathematical exponentiation and congruence. The average elapsed encoding time (0.0195 ms) for our proposed algorithm is much faster than the RSA and ECC algorithms (4.4311 ms and 7.3931 ms, respectively). The average elapsed decoding time (0.0184 ms) for our proposed algorithm is also much faster than the RSA and ECC algorithms (4.4316 ms and 7.3891 ms, respectively). As a result, our proposed algorithm encoding/decoding speed is faster than the RSA and ECC encoding/decoding speeds. Therefore, our proposed public key cryptographic algorithm using a matrix pattern could be an alternative solution for tele-ultrasound applications due to its superior encrypting strength and faster encoding/decoding time. The overall security system for medical information systems, such as PACS, is considered to be a stable system if a cryptographic algorithm is applied.

Author Contributions: Conceptualization, S.-H.S., W.-S.Y., and H.C.; methodology, S.-H.S., W.-S.Y., and H.C.; software, S.-H.S.; validation, S.-H.S., W.-S.Y.; data curation, S.-H.S., W.-S.Y., and H.C.; writing—original draft preparation, S.-H.S., W.-S.Y., and H.C.

Funding: This research was financially supported by the Ministry of Small and Medium-sized Enterprises(SMEs) and Startups(MSS), Korea, under the "Regional Enterprise linked with National-Innovation-Cluster Development Program(R&D, P0009964)" supervised by the Korea Institute for Advancement of Technology(KIAT).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Postema, M. *Fundamentals of Medical Ultrasound*; Taylor and Francis: New York, NJ, USA, 2011.
2. Choi, H.; Yeom, J.-Y.; Ryu, J.-M. Development of a Multiwavelength Visible-Range-Supported Opto–Ultrasound Instrument Using a Light-Emitting Diode and Ultrasound Transducer. *Sensors* **2018**, *18*, 3324. [CrossRef] [PubMed]
3. Choi, H.; Ryu, J.; Kim, J. A Novel Fisheye-Lens-Based Photoacoustic System. *Sensors* **2016**, *16*, 2185. [CrossRef] [PubMed]
4. Choi, H.; Ryu, J.-M.; Yeom, J.-Y. Development of a Double-Gauss Lens Based Setup for Optoacoustic Applications. *Sensors* **2017**, *17*, 496. [CrossRef] [PubMed]
5. Choe, S.-W.; Choi, H. Suppression Technique of HeLa Cell Proliferation Using Ultrasonic Power Amplifiers Integrated with a Series-Diode Linearizer. *Sensors* **2018**, *18*, 4248. [CrossRef] [PubMed]
6. Choi, H.; Woo, P.C.; Yeom, J.-Y.; Yoon, C. Power MOSFET Linearizer of a High-Voltage Power Amplifier for High-Frequency Pulse-Echo Instrumentation. *Sensors* **2017**, *17*, 764. [CrossRef] [PubMed]
7. Jeong, J.J.; Choi, H. An impedance measurement system for piezoelectric array element transducers. *Measurement* **2017**, *97*, 138–144. [CrossRef]

8. Choi, H. Prelinearized Class-B Power Amplifier for Piezoelectric Transducers and Portable Ultrasound Systems. *Sensors* **2019**, *19*, 287. [CrossRef]
9. Choi, H.; Choe, S.-W. Acoustic Stimulation by Shunt-Diode Pre-Linearizer Using Very High Frequency Piezoelectric Transducer for Cancer Therapeutics. *Sensors* **2019**, *19*, 357. [CrossRef]
10. Choi, H.; Park, C.; Kim, J.; Jung, H. Bias-Voltage Stabilizer for HVHF Amplifiers in VHF Pulse-Echo Measurement Systems. *Sensors* **2017**, *17*, 2425. [CrossRef]
11. Grüll, H.; Langereis, S. Hyperthermia-triggered drug delivery from temperature-sensitive liposomes using MRI-guided high intensity focused ultrasound. *J. Control. Release* **2012**, *161*, 317–327. [CrossRef]
12. Jolesz, F.A. MRI-guided focused ultrasound surgery. *Annu. Rev. Med.* **2009**, *60*, 417–430. [CrossRef] [PubMed]
13. Szabo, T.L. *Diagnostic Ultrasound Imaging: Inside Out*; Elsevier Academic Press: London, UK, 2013.
14. Choi, H.; Choe, S.-W. Therapeutic Effect Enhancement by Dual-Bias High-Voltage Circuit of Transmit Amplifier for Immersion Ultrasound Transducer Applications. *Sensors* **2018**, *18*, 4210. [CrossRef] [PubMed]
15. Hoskins, P.R.; Martin, K.; Thrush, A. *Diagnostic Ultrasound: Physics and Equipment*; Cambridge University Press: Cambridge, UK, 2010.
16. Daniels, J.M.; Hoppmann, R.A. *Practical Point-of-Care Medical Ultrasound*; Springer: New York, NJ, USA, 2016.
17. Su, M.-J.; Ma, H.-M.; Ko, C.-I.; Chiang, W.-C.; Yang, C.-W.; Chen, S.-J.; Chen, R.; Chen, H.-S. Application of tele-ultrasound in emergency medical services. *Telemed. E Health* **2008**, *14*, 816–824. [CrossRef] [PubMed]
18. Moore, C.L.; Copel, J.A. Point-of-care Ultrasonography. *N. Engl. J. Med.* **2011**, *364*, 749–757. [CrossRef] [PubMed]
19. David Cone, J.H.B.; Theodore, R.; Delbridge, J.; Brent, M. *Emergency Medical Services: Clinical Practice and Systems Oversight*; Wiley Online Library: Hoboken, NJ, USA, 2015.
20. Lee, T.H. *The Design of CMOS Radio-Frequency Integrated Circuits*; Cambridge University Press: Cambridge, UK, 2006.
21. Choi, H. Class-C Linearized Amplifier for Portable Ultrasound Instruments. *Sensors* **2019**, *19*, 898. [CrossRef]
22. Choi, H.; Yoon, C.; Yeom, J.-Y. A Wideband High-Voltage Power Amplifier Post-Linearizer for Medical Ultrasound Transducers. *Appl. Sci.* **2017**, *7*, 354. [CrossRef]
23. Zennaro, F.; Neri, E.; Nappi, F.; Grosso, D.; Triunfo, R.; Cabras, F.; Frexia, F.; Norbedo, S.; Guastalla, P.; Gregori, M. Real-Time Tele-Mentored Low Cost "Point-of-Care US" in the Hands of Paediatricians in the Emergency Department: Diagnostic Accuracy Compared to Expert Radiologists. *PLoS ONE* **2016**, *11*, e0164539. [CrossRef]
24. Levine, A.R.; McCurdy, M.T.; Zubrow, M.T.; Papali, A.; Mallemat, H.A.; Verceles, A.C. Tele-intensivists can instruct non-physicians to acquire high-quality ultrasound images. *J. Crit. Care* **2015**, *30*, 871–875. [CrossRef]
25. Brooks, A.; Price, V.; Simms, M. FAST on operational military deployment. *Emerg. Med. J.* **2005**, *22*, 263–265. [CrossRef]
26. Wagner, M.S.; Garcia, K.; Martin, D.S. Point-of-care Ultrasound in Aerospace Medicine: Known and Potential Applications. *Aviat. Space Environ. Med.* **2014**, *85*, 730–739. [CrossRef]
27. Emery, M.; Flannigan, M. How useful are clinical findings in patients with blunt abdominal trauma? *Ann. Emerg. Med.* **2014**, *63*, 463–464. [CrossRef]
28. Kim, C.; Cha, H.; Kang, B.S.; Choi, H.J.; Lim, T.H.; Oh, J. A feasibility study of smartphone-based telesonography for evaluating cardiac dynamic function and diagnosing acute appendicitis with control of the image quality of the transmitted videos. *J. Digit. Imaging* **2016**, *29*, 347–356. [CrossRef]
29. Eren, H.; Webster, J.G. *Telemedicine and Electronic Medicine*; CRC Press: Boca Ration, FL, USA, 2015.
30. Kobayashi, L.O.M.; Furuie, S.S.; Barreto, P.S.L.M. Providing integrity and authenticity in DICOM images: A novel approach. *IEEE Trans. Inf. Technol. Biomed.* **2009**, *13*, 582–589. [CrossRef]
31. Murillo-Escobar, M.; Cardoza-Avendaño, L.; López-Gutiérrez, R.; Cruz-Hernández, C. A Double Chaotic Layer Encryption Algorithm for Clinical Signals in Telemedicine. *J. Med. Syst.* **2017**, *41*, 59. [CrossRef]
32. Mehta, G.; Dutta, M.K.; Kim, P.S. *An Efficient and Lossless Cryptosystem for Security in Tele-Ophthalmology Applications Using Chaotic Theory. Ophthalmology: Breakthroughs in Research and Practice: Breakthroughs in Research and Practice*; Information Resources Management Association: Hershey, PA, USA, 2018; Volume 189.
33. Kishore, P.; Venkatram, N.; Sarvya, C.; Reddy, L. Medical Image Watermarking Using RSA Encryption in Wavelet Domain. In Proceedings of the 2014 First International Conference on Networks & Soft Computing (ICNSC2014), Guntur, India, 19–20 August 2014; pp. 258–262.

34. Kanakis, A. Implementations of Wireless and Wired Intelligent Systems for Healthcare with Focus on Diabetes and Ultrasound Applications. Ph.D. Thesis, University of Sheffield, Sheffield, UK, 2013.
35. Huang, H. *PACS and Imaging Informatics: Basic Principles and Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2011.
36. Slone, R.M.; Muka, E.; Pilgram, T.K. Irreversible JPEG compression of digital chest radiographs for primary interpretation: Assessment of visually lossless threshold. *Radiology* **2003**, *228*, 425–429. [CrossRef] [PubMed]
37. Paar, C.; Pelzl, J. *Understanding Cryptography: A Textbook for Students and Practitioners*; Springer Science & Business Media: New York, NJ, USA, 2009.
38. Strang, G. *Differential Equations and Linear Algebra*; Wellesley-Cambridge Press: Welleslely, MA, USA, 2014.
39. Lehmer, D. On Euler's totient function. *Bull. Am. Math. Soc.* **1932**, *38*, 745–751. [CrossRef]
40. Hendy, M. Euclid and the fundamental theorem of arithmetic. *Hist. Math.* **1975**, *2*, 189–191. [CrossRef]
41. Menezes, A.J.; Katz, J.; Van Oorschot, P.C.; Vanstone, S.A. *Handbook of Applied Cryptography*; CRC Press: Boca Raton, FL, USA, 1996.
42. Stallings, W. *Cryptography and Network Security: Principles and Practice*; Pearson Education: London, UK, 2003.
43. Bach, E.; Shallit, J.O. *Algorithmic Number Theory: Efficient Algorithms*; MIT Press: Cambridge, MA, USA, 1996; Volume 1.
44. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
45. Hankerson, D.; Menezes, A.J.; Vanstone, S. *Guide to Elliptic Curve Cryptography*; Springer Science & Business Media: New York, NJ, USA, 2006.
46. Stallings, W. *Network Security Essentials: Applications and Standards*; Pearson Education: London, UK, 2000.
47. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
48. Lenstra, H. Integer programming and cryptography. *Math. Intell.* **1984**, *6*, 14–21. [CrossRef]
49. Chor, B.; Rivest, R.L. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE Trans. Inf. Theory* **1988**, *34*, 901–909. [CrossRef]
50. Shang, Y. Deffuant model with general opinion distributions: First impression and critical confidence bound. *Complexity* **2013**, *19*, 38–49. [CrossRef]
51. Shang, Y. Deffuant model of opinion formation in one-dimensional multiplex networks. *J. Phys. A Math. Theor.* **2015**, *48*, 395101. [CrossRef]
52. Forouzan, B.A.; Mukhopadhyay, D. *Cryptography and Network Security (Sie)*; McGraw-Hill Education: New York, NJ, USA, 2011.
53. Boniface, K.S.; Shokoohi, H.; Smith, E.R.; Scantlebury, K. Tele-ultrasound and paramedics: real-time remote physician guidance of the Focused Assessment with Sonography for Trauma examination. *Am. J. Emerg. Med.* **2011**, *29*, 477–481. [CrossRef]
54. Al-Haj, A.; Abandah, G.; Hussein, N. Crypto-based algorithms for secured medical image transmission. *IET Inf. Secur.* **2015**, *9*, 365–373. [CrossRef]
55. Bernstein, D.J. *Introduction to Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009.
56. OpenSSL Cryptography and SSL/TLS Tookit. Available online: https://www.openssl.org/ (accessed on 16 April 2018).
57. Shang, Y. Resilient multiscale coordination control against adversarial nodes. *Energies* **2018**, *11*, 1844. [CrossRef]
58. Shang, Y. Resilient consensus of switched multi-agent systems. *Syst. Control Lett.* **2018**, *122*, 12–18. [CrossRef]