Improving the Security of the Medical Images

Ahmed Mahmood
School of Engineering
University of Guelph
Guelph, ON, CANADA

Charlie Obimbo
School of Computer Science
University of Guelph
Guelph, ON, CANADA

Tarfa Hamed
School of Computer Science
University of Guelph
Guelph, ON, CANADA

Robert Dony
School of Engineering
University of Guelph
Guelph, ON, CANADA

***Abstract*—Applying security to the transmitted medical images is important to protect the privacy of patients. Secure transmission requires cryptography, and watermarking to achieve confidentiality, and data integrity. Improving cryptography part needs to use an encryption algorithm that stands for a long time against different attacks. The proposed method is based on number theory and uses Chinese remainder theorem as a backbone. This approach achieves high level of security and stands against different attacks for a long time. On watermarking part, the medical image is divided into two regions: a region of interest (ROI) and a region of background (ROB). The pixel values of the ROI contain the important information so this region must not experience any change. The proposed watermarking technique is based on dividing the medical image in to blocks and inserting the watermark to the ROI by shifting the blocks. Then, an equivalent number of blocks in the ROB are removed. This approach can be considered as lossless since it does not affect on the ROI, also it does not increase the image size. In addition, it can stand against some watermarking attacks such cropping, and noise.**

Keywords—Medical Imaging Security; Telemedicine Security; Chinese remainder theorem; Watermarking

I. INTRODUCTION

Until recently the sole responsibility of keeping patients' records in confidence was with the Physicians. This meant that the Physician was not to disclose any medical information *revealed* by a patient or *discovered* by a physician in connection with the treatment of a patient to any unauthorized person [1]. However, with the advent of recent computer technology, and it's permeation into the Medical field through E-health [2], Telemedicine [3-6], to name but a few, the challenges of confidentiality arising from the storage and transmission of medical data cannot be left to physicians alone.

Indeed, transferring medical data such as radiological results from a medical database center to another one without applying security techniques means low level of privacy for patients. Medical information transmission has increased with the use of telemedicine. Telemedicine is important because it enables consultations by remote specialists, loss-free and immediate availability of individual patient information, and improved communication between partners in a health care system [7].

Security of medical information imposes three mandatory characteristics: confidentiality, reliability and availability. Confidentiality means that only the entitled users have access to the information and this can be achieved using encryption. Reliability has two aspects; i) Integrity: the information must not been modified by unauthorized people, and, ii) Authentication: a proof that the information belongs indeed to the correct patient and is issued from the correct source and one of the techniques to achieve this is watermarking. Availability is the ability of an information system to be used by the entitled users in the normal scheduled conditions of access and exercise. For storage and transmission, encryption is a very efficient tool, but once the sensitive data is decrypted, the information is not protected anymore. Once the images are in the open (plain-text) form, the major threat is the violation of the access rights and of the daily logs by the intruder.

Watermarking is made to introduce identifiers, which, by construction, are inseparable from the document they are embedded in. They may be seen as ultimate ramparts against usurpation and fabrication. Medical tradition is very strict with the quality of biomedical images, in that it is often not allowed to alter in any way the bit field representing the image (nondestructive) [8]. Watermarking technique is based on the data modification principle. Therefore, the watermarking method must be reversible, in that the original pixel values must be exactly recovered. This limits significantly the capacity and the number of possible methods. It also constrains to have dedicated routines to automatically suppress and introduce the mark in order to prevent the transmission of unprotected documents. However, applying watermarking blindly is not acceptable in the medical imaging field where any modification in the high information area of the image is not acceptable. Dividing the medical image into two regions can solve this problem: a region of interest (ROI) and a region of background (ROB). The pixel values of the ROI contain the important information so this region must not experience any change. On the other hand, the ROB can provide a suitable place to embed the watermarking data.

In this paper next section provides background about medical imaging encryption (MIE) and its current methods in Section II. Section II also illustrates medical images watermarking (MIW) and the current approaches in the medical field. Section 3 presents the proposed approaches in the encryption and watermarking areas. Image analyzing methods that are used to measure the performance of the proposed algorithm such as histograms, correlation coefficients, and average intensity difference are described in section IV. Finally, the conclusions and the future work are presented in last section.

II. MEDICAL IMAGE ENCRYPTION & WATERMARKING

A. Medical Image Encryption

Medical images may be encrypted to ensure privacy and integrity. As known, the strength of many encryption algorithms lies in the encryption key and its length, which is a major design issue. The encryption scheme is said to be computationally secure if it meets the following criteria:

1) the cost of breaking the cipher exceeds the actual value of the encrypted information;

2) the time required to break the cipher exceeds the useful lifetime of the information.

Image encryption, using CRT is performed by Thien and Lin [9] in 2002, using lossless and lossy forms. In 2006 Meher and Patra [10] used CRT secret image sharing in a naïve way. There have been some attempts to improve the performance of these methods [11-13].

1) Encryption Types

Stream ciphers and block ciphers are the main parts of symmetric algorithms. For stream cipher methods, the procedure is to encrypt one single bit of plaintext at a time, while the block ciphers take a number of bits and encrypt them as a single unit. Stream ciphers typically execute at a higher speed than block ciphers and have a lower complexity. However, stream ciphers can be vulnerable to serious security problems if used incorrectly [14].

2) Encryption Properties

Important properties for designing encryption schemes for medical data applications are presented below [15] [16]:

- The data size of medical images is large due to lossless compression. The encryption/decryption speed of some existing ciphers is not fast enough. This is especially true of software implementation that uses the naive approach. Hence, the size of the data to be encrypted is an important consideration in the de- sign of encryption schemes for medical imaging.

- Compressibility: when compression is applied after encryption, the randomness of the cipher text will considerably decrease the amount of compression achieved. As a result, one approach is to en- crypt the content after compression; however after compression the entire compressed content needs to be encrypted. For this reason a stage within compression needs to be identified where partial encryption can be performed without affecting the compression. Consequently, there is a tradeoff needed between compression and encryption.

- The avalanche property: a good encryption algorithm should have the avalanche property where a small change in either plaintext or the key should result in a huge change in the ciphertext.

- Security and usability: medical images may stored for a long time; therefore, the encryption algorithm should result in a ciphertext that can stand against different attacks.

3) Encryption Attacks

Attacks can be classified into two basic categories. In the first type, the attacker has some knowledge of the algorithm and/or a sample of a plaintext-ciphertext pair. In the second type, the attacker has no knowledge of the algorithm; this is known as brute-force attack when every possible key on a piece of ciphertext is tried until its plaintext is obtained [17]. The different types of cryptanalytic attacks are explained in the following paragraphs.

- Ciphertext - Only Attack.

In this attack the attacker is able to get part of the ciphertext when the attacker has some medical data that are encrypted by the same encryption algorithm. The attacker’s job is to recover the plain- text of as many images as possible, or to deduce the key (or keys) used to recover the images [17] [18] [19]. An example of this attack is the jigsaw puzzle attack. The attacker first divides a cipher image into many small pieces; then, the attacker tries to break these pieces simultaneously.

As each piece is very small compared with the whole cipher image, the time needed to break each piece is less than that needed to break the entire cipher image [17].

- Known - Plaintext Attack.

This attack occurs when attacker is able to have access to some cipher images and their original images. This may help in determining the key or a part of the key [17] [18] [19].

- Chosen- Plaintext Attack.

An attacker is able to select some medical images and get the relating cipher images. This occurs when the attacker not only has access to the cipher images and the original medical images, but the attacker also has the ability to choose the image parts that get encrypted. This is more powerful than a known-plaintext attack because the cryptanalyst can choose specific image blocks to encrypt [14] [20] [17].

- Chosen - Ciphertext Attack.

In this attack, the attacker is able to get several cipher images and original images [14] [20] [17]. When an attacker is able to modify the choice between the two types of images based on the results of previous encryption.

The DICOM medical images are usually secured using classical encryption algorithms such as advanced encryption standard (AES) or triple data encryption standard (3DES) [21]. Encrypting a medical image using AES or 3DES encryption algorithms provide a high level of security, but require long processing time.

For example, encrypting an MRI brain image with dimensions of 512×512 pixels takes 521.67 s using a computer that runs on a CPU Intel Core2 Quad Q6700 [22].

B. Medical Image Watermarking

Watermarking is the process of embedding small sensitive data such as copyright and ownership identification in images; it has become a necessary component of multimedia applications that are subject to illegal use [23]. In addition, it is used for data authentication purposes to detect any changes in a medical image. The robust watermarking algorithm should be able to retrieve sensitive data after applying different image processing such as translation, resizing, and cropping, as well as different types of distortions such as filtering, and contrast. These issues are very important when creating a new design for a strong watermarking method.

The three types of watermarking methods for medical images are

1) *minimum distortion,*
2) *lossless watermarking, and*
3) *segmentation [24].*

The first method consists in using classical watermarking methods while minimizing the distortion. In this case, the watermark replaces some image details, such as the least significant bit of the image. However, embedding different watermarks may cause degradation in the watermarked medical images and this degradation in the image quality is measured with a number of metrics, such as MSE and PSNR [25]. Lossless or reversible watermarking represents the second type: the watermark can be removed from the image once the embedded data is read, allowing retrieval of the original image. This approach provides authentication without proof of ownership. The third type is implemented by segmenting the medical image using image segmentation techniques into two regions where the first is known as region of interest (ROI) and the second as region of background (ROB); the watermarked data are embedded within the ROB in order not to compromise the diagnosis capability. Image segmentation techniques that are necessary for deciding the suitable areas for using the watermarking technique.

The two main categories of digital watermarking are

1) *visible and*
2) *invisible.*

A visible watermark is similar to stamp a watermark on paper. It is seen in many digital applications such as the logos of television channels, or the data of medical images as shown in Figure 1. On the other hand, invisible watermarking is often used to identify copyright data, for example, an author or a distributor. There are different classifications of invisible watermarking algorithms. Watermarking approaches can be distinguished in terms of the watermarking host such as text, audio, images, and video. In addition, they can be classified types according to whether the extraction of the original signal is non-blind, semi-blind, or blind. In non-blind schemes, both the original image and the secret key are needed, while in semi-blind schemes, both the secret key and the watermark are needed; blind schemes need only the secret key.

The main classes of watermarking techniques are spatial domain, and transform domain. The watermark in the spatial domain technique represents the first class where it is embedded by changing the pixel values of the original image, while in the transform domain technique, the data are

Fig. 1. Visible Watermarking of a Medical Image

embedded by modulating the transform domain signal coefficients. In [26] Li uses the moment-preserving threshold, which is a pixel-based segmentation to separate the ROI from the ROB for mammogram medical images. However, ultra sound and brain images most of the time create confusion for the ROI and ROB so some researchers have tried to offer a solution. For example in [27] Cao suggests adding a digital envelope so the important data can be embedded in it. This solution increases the size of the transmitted data.

C. Watermarking Properties

Properties for an efficient watermarking system are application dependent; one of the challenges in this area is that these properties compete with each other. None of the digital watermarking techniques have yet to meet all of these properties.

- Robustness. Digital images commonly are subject to many types of distortions, such as filtering, resizing, and cropping. These distortions are still very common and represent an open issue with respect to the robustness of watermarking. However, the mark should be discovered if these distortions occurred.
- Capacity. The capacity of the hidden data is another important issue where the watermarking algorithm should embed a predefined number of bits that can be hidden in the host signal. This number will depend on the application and there is no general rule for this. In general, the number of bits that can be inserted in the data is limited and in the LSB method; it is between (0.125 - 0.25) of the total size.
- Invisibility. There are two types of invisibility due to the implementation method: perceptual invisibility, and statistical invisibility. In perceptual invisibility the

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

watermark is hidden in such a way that it is hardly noticed. An unauthorized person should not be able to detect the watermark by means of statistical methods. For example, the availability of a large number of digital works watermarked with the same code should not allow the extraction of the embedded mark by applying statistically based attacks. A possible solution is to use a content-dependent watermark.

D. Watermarking Attacks

The main challenges in the watermarking research area are a lack of standards and benchmarking, and a lack of comprehensive mathematical theory. The two basic types of watermarking are visible and invisible watermarking.

An image watermark may survive many attacks. The attacks related to invisible watermarking are similar to stego-attacks. Attacks on visible watermarks include an analysis of lighting and shadows, localized analysis of noise, histogram, and looking for discontinuities. Watermark attack types based on the aim of the attacker are as follows [28] [29].

Possible attacks on MIW are grouped into the followings.

- *Passive Attacks*. The attacker tries to determine whether a watermark is present but the removal of the watermark is not a goal.
- *Active Attacks*. Active attacks can be divided into three types as follows:
  - *Robustness Attack*. In this attack the attacker attempts to remove or destroy the watermark, so that the watermark detector is unable to detect watermark, and key issue in proof of ownership, fingerprinting, copy control. Types of this attack include geometrical, filtering, and noise.
  - *Collusion Attacks*. The attacker uses several copies of watermarked data (images, video etc.) to find the watermark and to construct a copy with no watermark. This is serious for fingerprinting applications.

Forgery Attacks. The attacker tries to embed a valid watermark. This has serious implications in authentication

III. PROPOSED ALGORITHM

The proposed algorithm has two parts. The first part is to perform the watermarking part and the second part is to implement strong encryption using the Chinese remainder theorem (CRT). Figure (2) presents the steps of the proposed algorithm. The watermarked data is the username of the person that requested for the medical images and a serial number between the two parties to achieve authenticity and avoid any forgery one.

This watermark that contains characters and numbers are converted to the hexadecimal representation then it is encrypted using Caesar shift cipher method. The watermark insertion place is selected near to the edge of the medical image. This method does not affect the ROI because the insertion of the watermark is in ROB, therefore this method can be considered as a lossless method.

The encryption part starts by selecting two relatively prime numbers one of them should be 256 so the encrypted pixel value does not exceed 255 which is the maximum value for an eight bit pixel. In order to have a good understanding about the CRT implementation is presented the following equations.

Consider $n \geq 2$, and m_1, m_2… m_n are positive relatively prime integers. Let the integer b_i denote the remainder of x modulo m_i for $1 \leq i \leq n$. The CRT is represented by the

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ x \equiv b_3 \pmod{m_3} \end{cases} \tag{1}$$

following system that has a unique solution x.

This by Obimbo's notation may be written as:

$$x \equiv (b_1, b_2, b_3) S (m_1, m_2, m_3) \tag{2}$$

The solution of x in equation 2 can be computed in a number of ways [30][31][33][34]. One of the approaches to solve these equations is Charlie's method. This method is selected because it has higher performance and faster than other methods [33]. The method starts by computing the value of x that satisfies the equations iteratively as shown below:

$$x_n = m_n \tag{3}$$

$$x_{n-1} = x_n + l_n \times k_n \tag{4}$$

where, $$l_{n-1} = m_{n-1} \times m_n \tag{5}$$

and $$k_n = l_{n-1} \pmod{m_{n-1}} \tag{6}$$

IV. IMAGE ANALYZING METHODS

In order to verify the security and the performance of a new algorithm, this algorithm should be analyzed and tested according to the image features. Some of the used keywords are defined.

The image mean can be defined as the average pixel value of an image, and for grey-scale medical images it is equal to the average brightness or intensity, while the image variance gives an estimate of the spread of pixel values around the image mean.

A. Histogram

The encrypted image histogram should be close to the uniform distribution to avoid statistical attacks [32]. The histogram of an image shows the number of occurrences for each grey level in the medical image. Mathematically, the histogram is a discrete function and its grey levels are in the range [0, L - 1] as in the following equation:

$$\text{hist}(r_k) = \frac{n_k}{N} \qquad (7)$$

Where r_k is the kth grey level, and n_k is the number of pixels in the image with that grey level. N is the total number of pixels in the image. It may be noted that k = 0, 1, ..., L − 1.

The histogram gives a global description of the image, so having a narrow histogram of the image means that the image is poorly visible because the difference in grey levels present in the image is generally low [35]. In the same way, a widely distributed histogram means that almost all the grey levels are present in the image, and thus the overall contrast and visibility increases.

B. Entropy

Entropy is a statistical measure of disorder and randomness. The entropy $En(d)$ of data d is measured as [34]:

$$En(d) = \sum_{i=1}^{L} p(m_i)\log\frac{1}{p(m_i)} \qquad (8)$$

Where L is the total number of pixels and $p(m_i)$ represents the probability occurrence of a pixel with value m_i. When the entropy of the encrypted image is close to log L bits, its histogram is considered sufficiently uniform.

C. Difference Between Original & Watermarked Images

This measurement is very useful to show the effect of the watermark on the image. If the input image of a system is $f(x,y)$, and the watermarked image of that system is $g(x,y)$, then the error function $e(x,y)$ can be defined as the difference between the input and the watermarked images [36].

This difference value between the two images represents the effect of watermarking, as expressed in the following equations:

$$e(x, y) = f(x, y) - g(x, y) \qquad (9)$$

The mean square error Ems (or MSE) formula is:

$$Ems = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} e(x,y)^2 \qquad (10)$$

And the peak signal to noise ratio (PSNR) formula is described below:

$$PSNR = 10\log_{10}\left[\frac{255^2}{Ems}\right] \qquad (11)$$

The algorithm used to place the encrypted watermark is illustrated below in Figure 2.

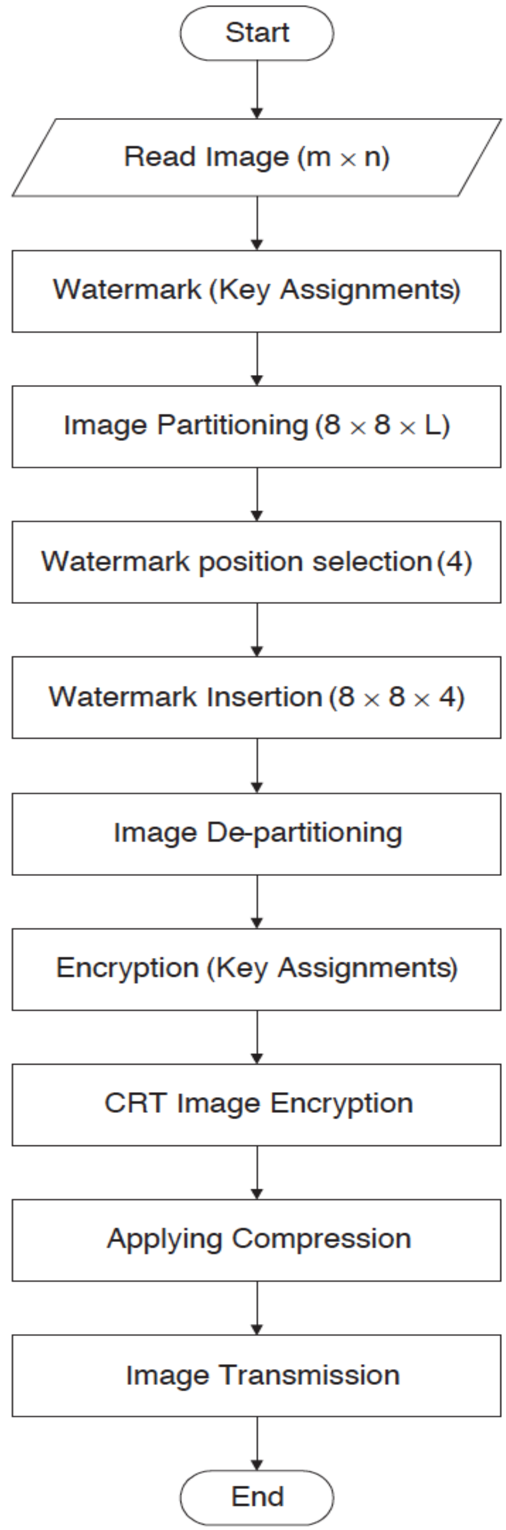

Fig. 2. Algorithm for Watermark Encryption & Placement

V. Results And Discussions

Watermarked images are shown below in Figures 3 and 4 where the watermark cannot be noticed visually.

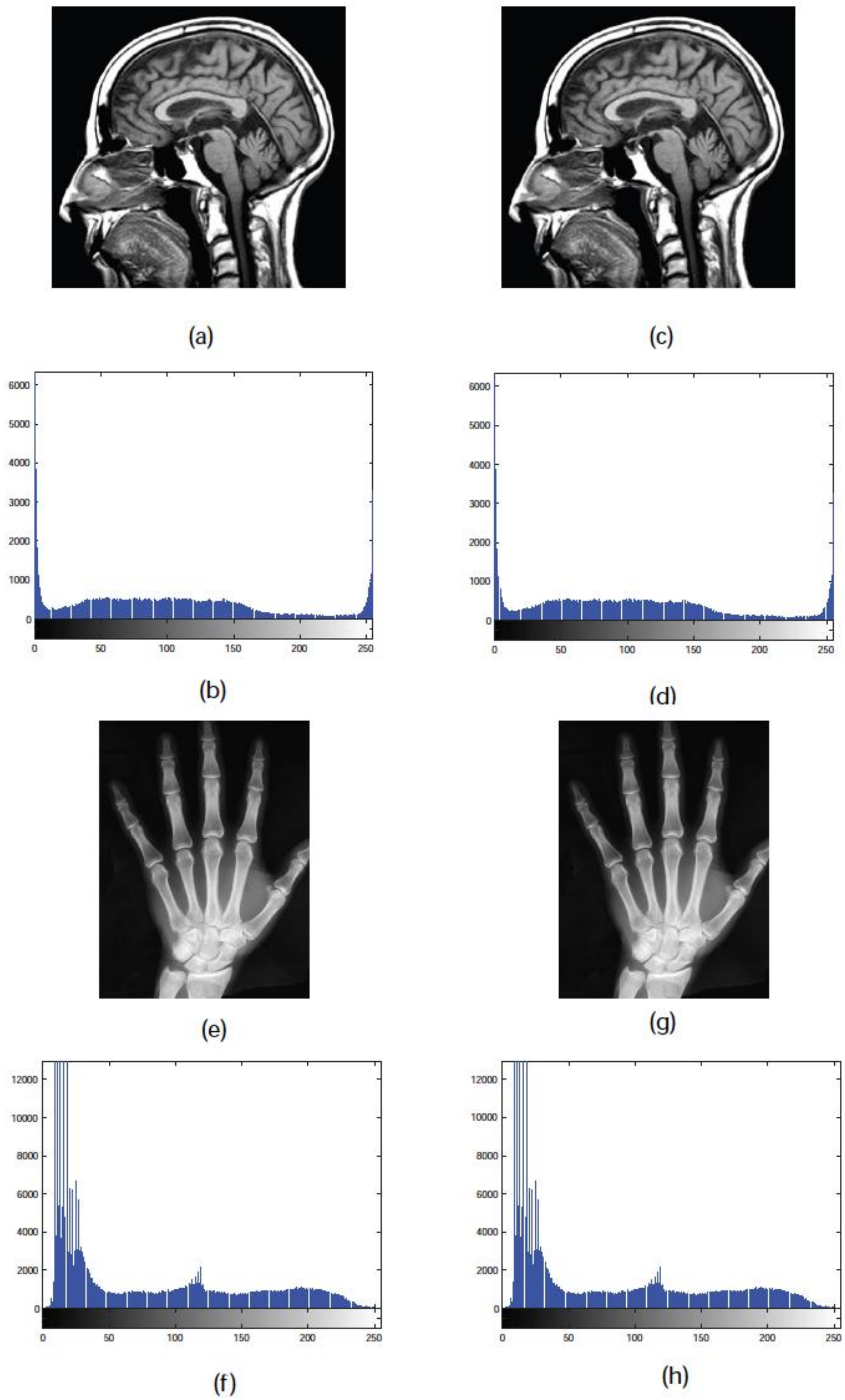

Fig. 3. Watermarked Images with Their Histograms

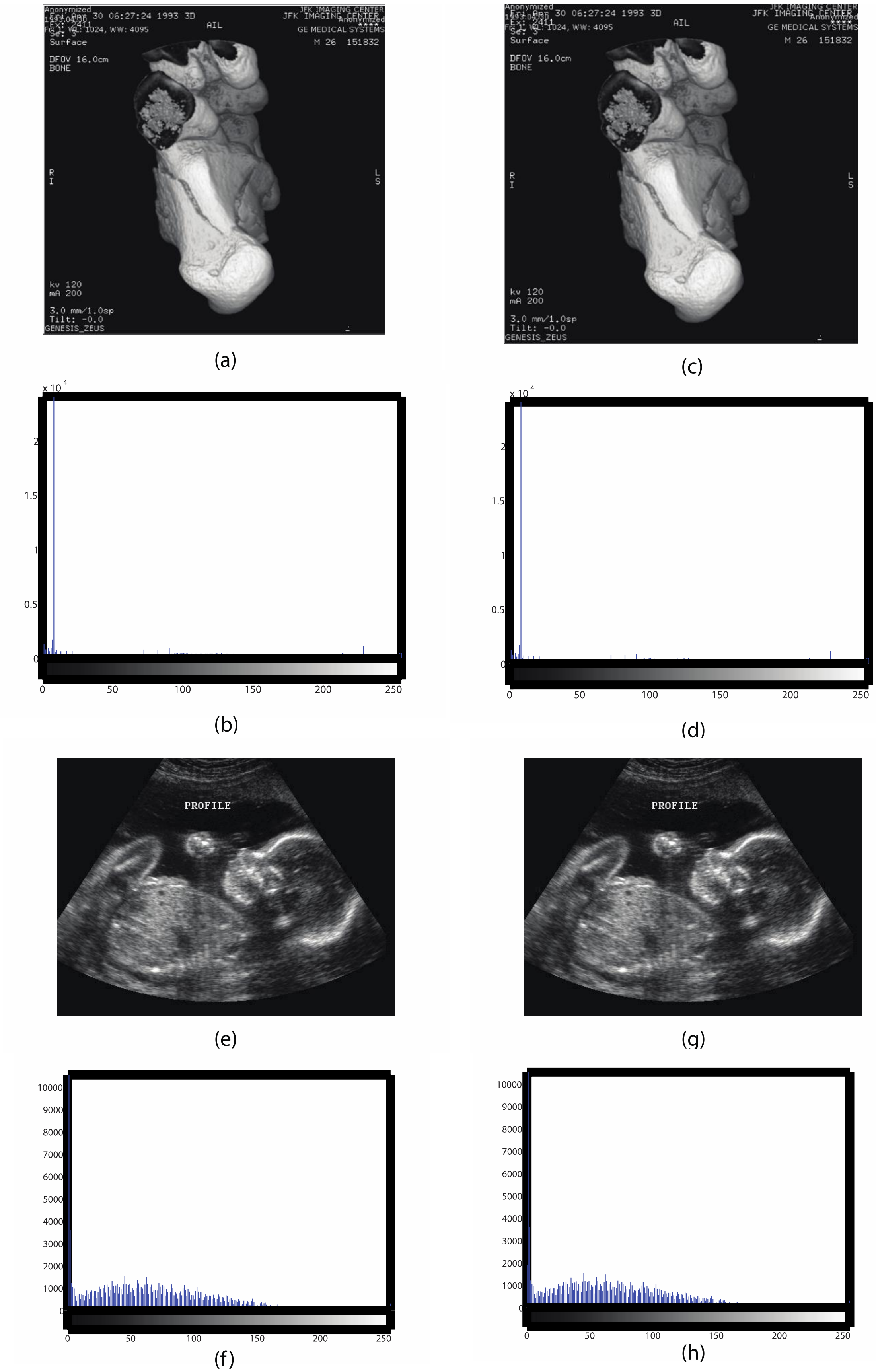

Fig. 4. Watermarked Images with Their Histogram

The Ems and PSNR calculation are shown in Table 1. It can be seen that the insertion of the watermark had a small effect on the Ems and PSNR values.

TABLE I. EMS AND PSNR FOR THE WATERMARKED IMAGES

Image	*EMS*	*PSNR*
CT Ankle	0.0688	59.7538
MRI Brain	0.0739	99.4457
X-ray Hand	0.1895	55.3553
Ultra sound	0.0331	82.9366

On the other hand, the CRT method did not show good performance to secure the medical images and this is related to characteristics of the medical images.

Table 2 shows the results of CRT encryption using two bits. The increase of bits improves the performance where the entropy was better for the four bits CRT. However, the eight bits CRT entropy was lower than the four bits value.

TABLE II. ENTROPY FOR THE ENCRYPTED IMAGES

Image	*Entropy after Watermark*	*Entropy after Encryption*
CT Ankle	3.6834	4.3804
MRI Brain	6.2493	6.4751
X-ray Hand	6.4386	6.9569
Ultra sound	5.7701	6.3961

The results of CRT encryption using base 2 are shown below in Figure 5.

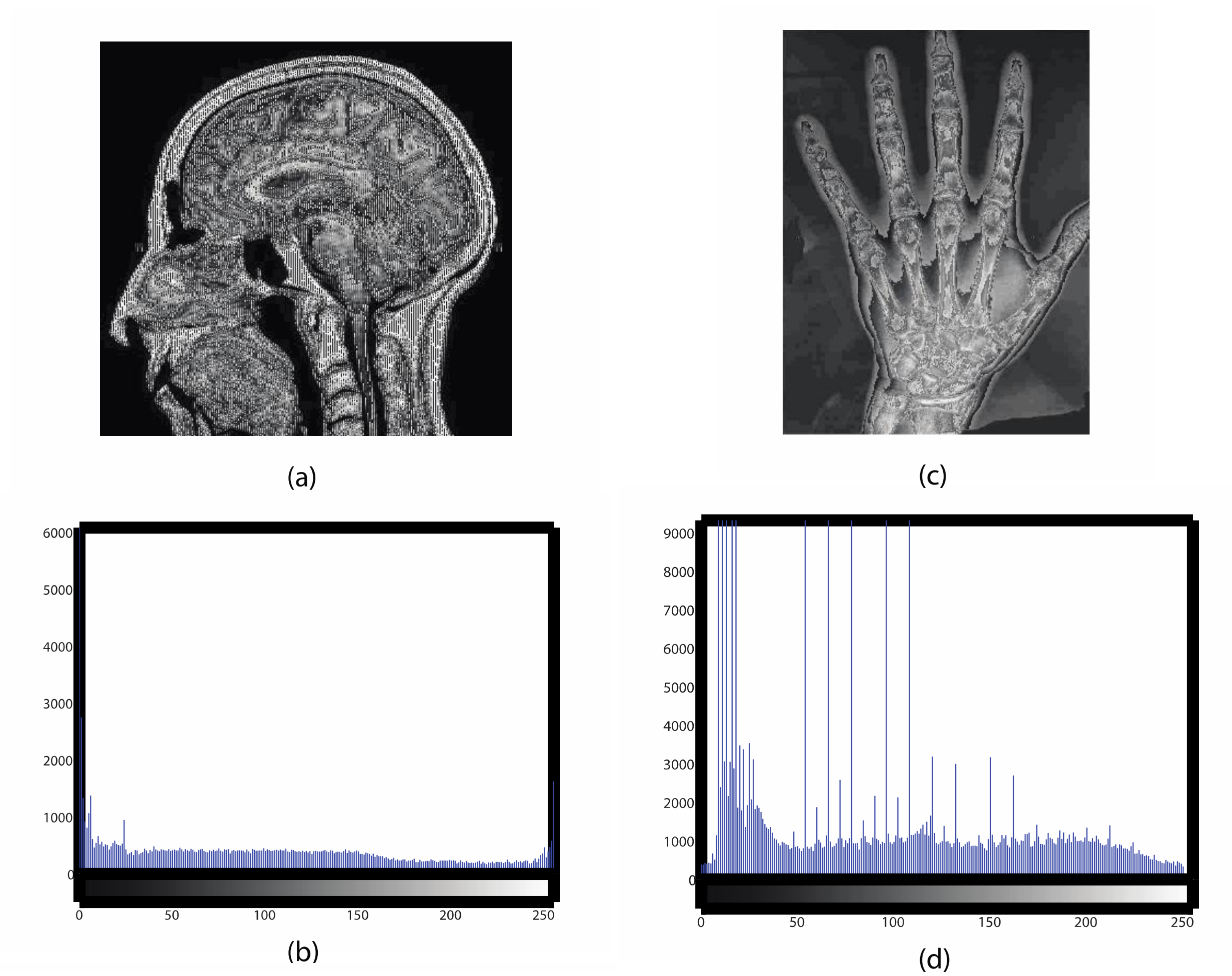

Fig. 5. Encrypted Images with Their Histograms

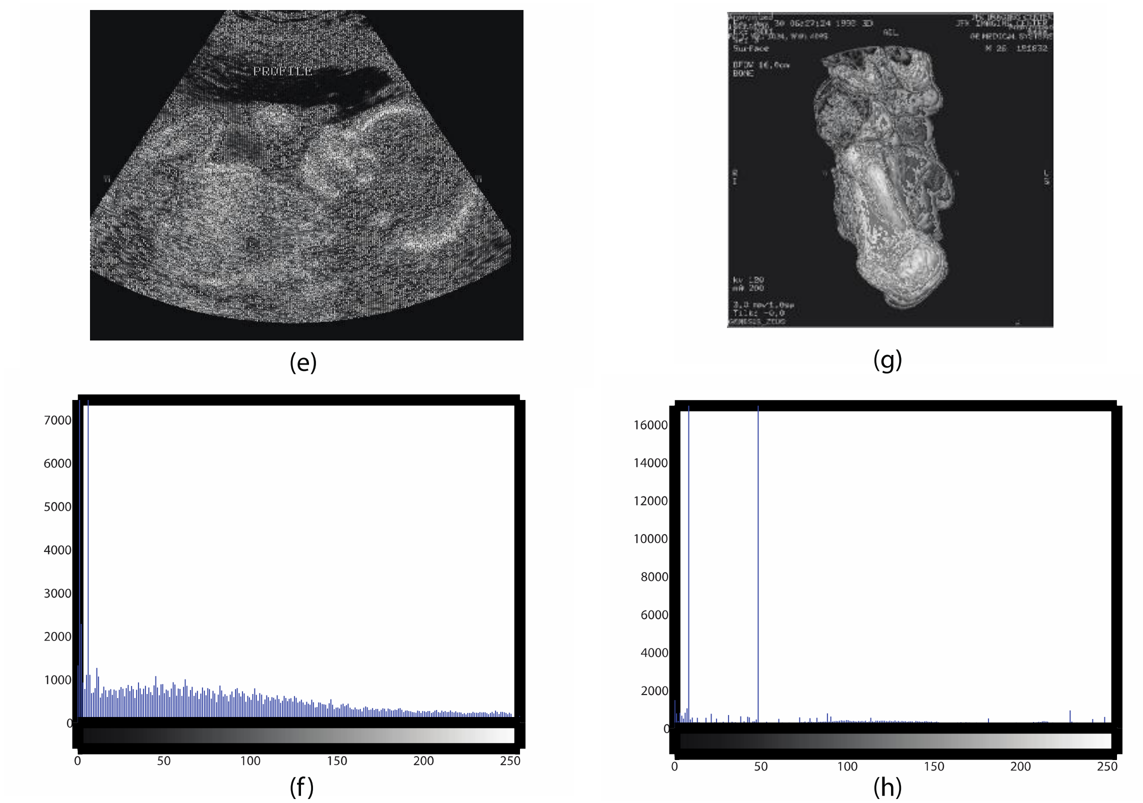

Fig. 5. (cont.): Encrypted Images with Their Histograms

The algorithm used was found to be considerably faster than the one for encryption for both AES and triple-DES. Figure 6 shows the processing time of proposed algorithm compared with AES and 3DES encryption algorithms. AES and 3DES are the adopted algorithms for securing medical images. The processing time was obtained using a MATLAB 7.10 code in a computer runs on a CPU Intel i7 820.

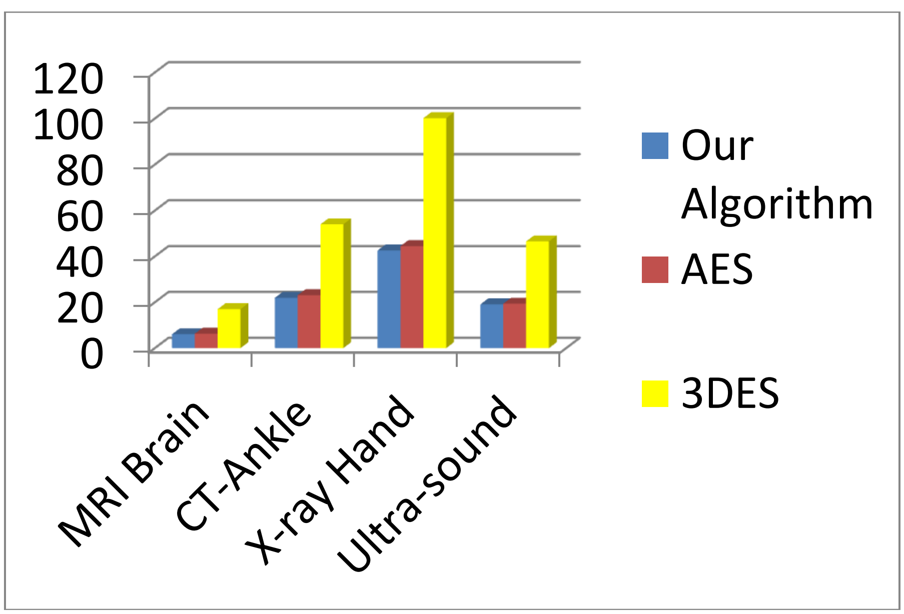

Fig. 6. Encryption Time of Different Algorithms

VI. Conclusion

Security techniques become more complex as the speed of computers increases. Providing a secure algorithm to protect medical images is complicated because of the special concerns of the medical community. First, the algorithm must recover the exact image with no change in any pixel value. Second, the algorithm should have a short processing time with high security that can stand for a long time.

Since the use of CRT as an encryption method for Medical images is novel, it can still be improved to work better with in this area. The proposed security algorithm tries to obtain better performance by reducing the encryption processing time compared with the current methods such as AES. At the same time, the time needed to break this method is still very big. In addition, the watermarking approach does not affect on the ROI of the medical image, therefore it can be considered as lossless

References

[1] Patient Confidentiality. American Medical Society. Available from: http://www.ama-assn.org//ama/pub/physician-resources/legal-topics/patient-physician-relationship-topics/patient-confidentiality.page. Retrieved 2013-23-09.

[2] "National E-Health Transition Authority: About Us". National E-Health Transition Authority. 2013. Retrieved 2013-23-09.

[3] Berman, Matthew; Fenaughty, Andrea (June 2005). "Technology and managed care: patient benefits of telemedicine in a rural health care network". Health Economics 14 (6). Wiley. p. 559-573. doi:10.1002/hec.952.

[4] Van't Haaff, Corey (March/April 2009). "Virtually On-sight". Just for Canadian Doctors. p. 22.

[5] Saylor, Michael (2012). The Mobile Wave: How Mobile Intelligence Will Change Everything. Perseus Books/Vanguard Press. p. 153.

[6] Conde, Jose G.; De, Suvranu; Hall, Richard W.; Johansen, Edward; Meglan, Dwight; Peng, Grace C. Y. (January/February 2010). "Telehealth Innovations in Health Education and Training". Telemedicine and e-Health 16 (1). p. 103-106. doi:10.1089/tmj.2009.0152.

[7] W. Yu-zeng, G. Shi-chao, F. Yu-jun, and F. Zhi- quan, "Research the Compression and Transmis- sion Technology of Medical Image Base on the Remote Consultation," in The 2nd International Conference on Bioinformatics and Biomedical En- gineering (ICBBE), Shanghai, China, 2008, pp. 2142–2145.

[8] Y. Tomioka, N. Aida, K. Kakehi, K. Nagami, H. Juzoji, and I. Nakajima, "Recent survey on patent applications for medical communications and telemedicine in Japan, USA and Europe," in Proceedings of the 7th International Workshop on Enterprise Networking and Computing in Health, pp 79 – 82.

[9] C. Thien and J. Lin, "Secret image sharing," Computers & Graphics, vol. 26, no. 5, pp. 765–770, 2002.

[10] P. Meher and J. Patra, "A new approach to secure distributed storage, sharing and dissemination of digital image," Island of Kos, Greece, 2006, pp. 373–376.

[11] V. Jagannathan, A. Mahadevan, R. Hariharan, and E. Srinivasan, "Number theory based image com- pression encryption and application to image mul- tiplexing," Chennai, India, 2007, pp. 59 – 64.

[12] S. J. Shyu and Y.-R. Chen, "Threshold secret image sharing by Chinese Remainder Theorem," Piscataway, NJ, USA, 2008, pp. 1332 – 1337.

[13] S. Hou and T. Uehara, "A Content Providing System With Privacy Protection," Nanjing, Jiangsu, China, 2010, pp. 912 – 917.

[14] W. Stallings, Cryptography and Network Security: Principles and Practice. Boston, MA: Prentice Hall, 2011.

[15] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J. Quisquater, "Overview On Selective Encryption Of Image And Video: Challenges And Perspectives," EURASIP Journal on Information Security, vol. 2008, pp. 1–18, 2008.

[16] N. Kulkarni, B. Raman, and I. Gupta, "Multimedia Encryption: A Brief Overview," Recent Advances In Multimedia Signal Processing And Communications, pp. 417–449, 2009.

[17] B. Schneier, Applied Cryptography: Protocols, Algorithms, And Source Code In C. New York, NY: John Wiley & Sons, Inc., 1996.

[18] S. Li, C. Li, K.-T. Lo, and G. Chen, "Cryptanalyzing - An Encryption Scheme Based On Blind Source Separation," IEEE Transactions On Circuits And Systems-I: Fundamental Theory And Applications, vol. 55, no. 4, pp. 1055 – 1063, 2008.

[19] S. Li, C. Li, Lo, and G. Chen, "Cryptanalysis Of An Image Scrambling Scheme Without Bandwidth Expansion," IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 3, pp. 338– 349, 2008.

[20] S. Vaudenay, A Classical Introduction To Cryptography: Applications For Communications Security. Boston, MA: Springer, 2006.

[21] A. B. Mahmood and R. D. Dony, "Segmentation based encryption method for medical images," in Proceedings of the 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates, 2011, pp. 596 – 601.

[22] Y. Zhou, K. Panetta, and S. Agaian, "A lossless encryption method for medical images using edge maps," in Proceedings of the 31st Annual International Conference of the IEEE Engineering in Medicine and Biology Society: Engineering the Future of Biomedicine, EMBC 2009, Minneapolis, MN, 2009, pp. 3707 – 3710.

[23] I. Cox, L. Matthew, A. Jeffrey et al., Digital Watermarking and Steganography. Burlington, MA: Morgan Kaufmann Publishers), 2007.

[24] G. Coatrieux, L. Lecornu, B. Sankur, and C. Roux, "A Review Of Image Watermarking Applications In Healthcare," in International Conference IEEE Engineering in Medicine and Biology Society, New York, NY, 2006, pp. 4691 – 4694.

[25] B. Planitz and A. Maeder, "Medical Image Watermarking: A Study On Image Degradation," in Proceedings of the Workshop on Digital Image Computing: Techniques and Applications, 2005, pp. 3–8.

[26] C.-T. Li, Y. Li, and C.-H. Wei, "Protection of Digital Mammograms on PACSs Using Data Hiding Techniques," International Journal of Digital Crime and Forensics, vol. 1, no. 1, pp. 75 – 88, 2009.

[27] F. Cao, H. Huang, and X. Zhou, "Medical Image Security In A HIPAA Mandated PACS Environment," Computerized Medical Imaging and Graphics, vol. 27, no. 2-3, pp. 185–196, 2003.

[28] L. Perez-Freire, P. Comesana, J. Troncoso- Pastoriza, and F. Perez-Gonzalez, "Watermarking Security: A Survey," in LNCS Transactions on Data Hiding and Multimedia Security, Heidelberg, Germany, 2006, pp. 41–72.

[29] T. Kalker et al., "Considerations on watermarking security," in Proceedings of the IEEE Workshop on Multimedia Signal Processing, Cannes, France, 2001, pp. 201–206.

[30] Donald Knuth. The Art of Computer Programming, Volume 2: Seminumerical Algorithms, Third Edition. Addison-Wesley, 1997. ISBN 0-201-89684-2. Section 4.3.2 (pp. 286–291), exercise 4.6.2–3 (page 456).

[31] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0-262-03293-7. Section 31.5: The Chinese remainder theorem, pp. 873–876.

[32] Laurence E. Sigler (trans.) (2002). Fibonacci's Liber Abaci. Springer-Verlag. pp. 402–403.

[33] C. Obimbo, "An Algorithm To Solve The Chinese Remainder Problem," in The 2001 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'2001), Las Vegas, Nevada, USA, 2001, pp. 2246–2250.

[34] K. Wong, "Image Encryption Using Chaotic Maps," Intelligent Computing Based on Chaos, pp 333–354, 2009.

[35] Y. Mao and G. Chen, "Chaos-based image encryption," Handbook of Geometric Computing, pp. 231–265, 2005.

[36] R. Gonzalez and R. Woods, "Digital Image Processing," Upper Saddle River, N.J., 2008.