Vol.63: e20180473, 2020
http://dx.doi.org/10.1590/1678-4324-2020180473
ISSN 1678-4324 Online Edition

Article - Engineering, Technology and Techniques

Fast Medical Image Security Using Color Channel Encryption

Isunuri Bala Venkateswarlu[1]
https://orcid.org/0000-0002-7671-8831

[1]IIITDM Kancheepuram, Chennai, Tamil Nadu, India.

Received: 2018.08.31; Accepted: 2020.02.27.

*Correspondence: baluatresearch@gmail.com; Tel.: +91-80-74970616

HIGHLIGHTS

- This paper implements fast medical image security scheme.
- Color channel encryption is used for medical image security.
- Proposed scheme includes both watermarking and encryption.
- Image key is used for watermarking image.

Abstract: Evolution of digital Health-care Information System established Medical Image Security as the new contemporary research area. Most of the researchers used either image watermarking or image encryption to address medical image security. However, very few proposals focused on both issues. This paper has implemented a Fast Medial Image Security algorithm for color images that uses both watermarking and encryption of each color channel. The proposed method starts with embedding of a smoothened key image (K) and patient information over the original image (I) to generate a watermarked image (W). Then, each color channel of the watermarked image (W) is encrypted separately to produce an encrypted image (E) using the same smoothened key image (K). This image can be transmitted over the public network and the original image (I) can be achieved using decryption algorithm followed by de-watermarking using the same key image (K) at the receiver. Qualitative and quantitative results of the proposed method show good performance when compared with the existing method with high Mean, PSNR and Entropy.

Keywords: Image Watermarking; Image Security; Medical Image Security; Color Channel Encryption.

INTRODUCTION

Recent advancements in digital communication increased the volume of networked multimedia systems with an accumulation of a huge number of images and videos [1,2]. Nowadays, social media applications are flooding with private images. Similarly, digital medical images of patients are shared by advanced telemedicine applications. These networked multimedia applications inflated the importance of Security. In general, image security techniques can be considered for both Gray image as well as Color images. However, most of the researchers are attracted towards gray image security as securing a one-dimensional gray image is less complex than three-dimensional color image. In general, image security techniques can be broadly classified as Image Watermarking and Image Encryption.

Image Watermarking

Digital image watermarking [3-4] is the practice of imperceptibly altering a piece of data in order to embed information about the data which is the most popular technique for low-level image security used for copyright infringements. Nowadays, rapid digitization mandated the companies to publish their multimedia data like images, animations, and videos over the network which increased the potential for re-usability. With this, proof of ownership for the multimedia data over the network becomes a critical task for the companies and hence image watermarking became the relatively new research area. The main aim of the watermarking is to superimpose a copyright label known as selective noise (like company logos or copyright information etc.) over original image to own the images. According to Tefas and coauthors [4], watermarking applications can be classified into three types:

1. Robust to resist host image manipulations and are usually employed in Intellectual Property Rights (IPR) protection applications.
2. Fragile to be vulnerable to all modifications applied in authentication scenarios.
3. Semi-fragile allows selective robustness and fragileness.

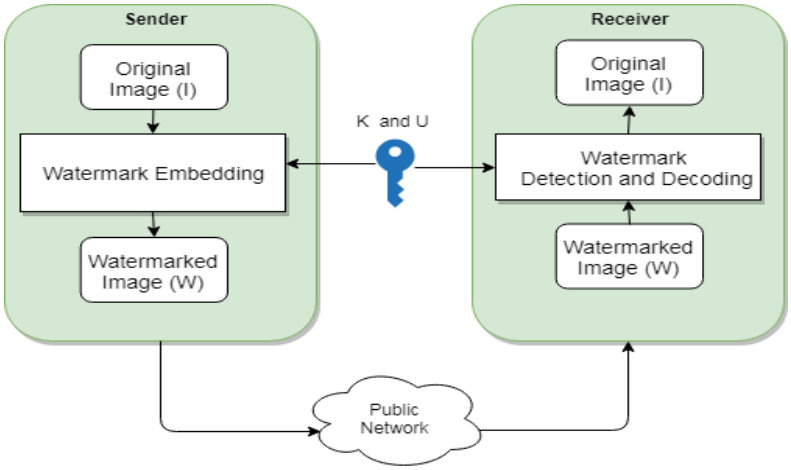


Figure 1. Watermark embedding process

Even though watermarking can be used for the variety of applications, copyright protection watermarking established itself as a unique task for image security as it enlightens the proof of ownership. High security can be achieved using key (K) while performing watermarking task. Watermarking is a three-step process including watermark embedding, detection, and decoding as shown in Figure 1. At sender side, watermark embedding is performed which is the process of superimposing key (K) over original image (I) using a set of controlling parameters (U) to produce the watermarked image (W) as shown in Equation 1. Then the watermarked image can be transmitted over the network.

$$W = \text{Embed}(I, K, U) \quad (1)$$

Now at the destination, first watermark detection will be performed to check whether the image contains watermark or not by taking W and K as input. If the image contains watermark it returns 1 otherwise it returns 0. Finally, this watermarking security ends with decoding process which reproduces the original image with K and U from the watermarked image W using Equation 2.

$$I = \text{Decode}(W, K, U) \quad (2)$$

Depending upon the visual appearance, image watermarking can be considered as two types: one will display the embedded image or information on the original image which can be used for copyright protection. The second approach will hide the image or information details over the original image with some mathematical operations known as stenography based watermarking to address content protection. Even though watermarking is the easiest method of image security, it would not be a suggestive method to achieve high-level image security. Moreover, it is unable to modify the original image structure and visual components.

Image Encryption

Contemporary image transmission applications require alteration of the image as the visual components of the original image should not be disclosed to the unauthorized parties. This motivated several researchers to focus on other alternative methods and arrived to use Image Encryption for strong security. In general,

image encryption is the process of visual scrambling of image using any encryption techniques. There are two types of encryption like Symmetric and Asymmetric. Symmetric encryption uses the same Private or Secret Key (K_{pr}) for both encryption and decryption. On the other hand, Asymmetric encryption uses the public key (K_{rpu}) for encryption while private key (K_{rpr}) will be used for decryption as shown in Figure 2.

	Application	Algorithm Used	Input	Process	Output
Symmetric	Sender and Receiver uses same Private Key(K_{pr})				
	Sender	Encryption (EA)	PT	$ET=EA_{Kpr}(PT)$	ET
	Receiver	Decryption (DA)	ET	$PT= DA_{Kpr}(ET)$	PT
Asymmetric	Sender uses Receivers Public Key(K_{rpu}) Receiver uses Receivers Private Key(K_{rpr})				
	Sender	Encryption (EA)	PT	$ET=EA_{Krpu}(PT)$	ET
	Receiver	Decryption (DA)	ET	$PT= DA_{Krpr}(ET)$	PT

Notations used: Plain Text (PT), Encrypted Text (ET), Shared Secret / Private Key used by both Sender and Receiver (K_{pr}), Receivers Public Key used by Sender (K_{rpu}), Receivers Private Key used by Receiver (K_{rpr}).
Figure 2. Types of image encryption process

Even though there are several symmetric as well as asymmetric encryption techniques for text or binary information, only symmetric techniques are useful for image encryption as they need only one private key. A survey of image encryption algorithms was published by Manju and coauthors [5]. This study presents encryption and decryption process of all possible image encryption techniques like Vigenere, AES, DES, IDEA, Blowfish, and RC along with the comparison to exhibit the pros and cons of each algorithm. However, image encryption can be performed with the following process as shown in Figure 3.

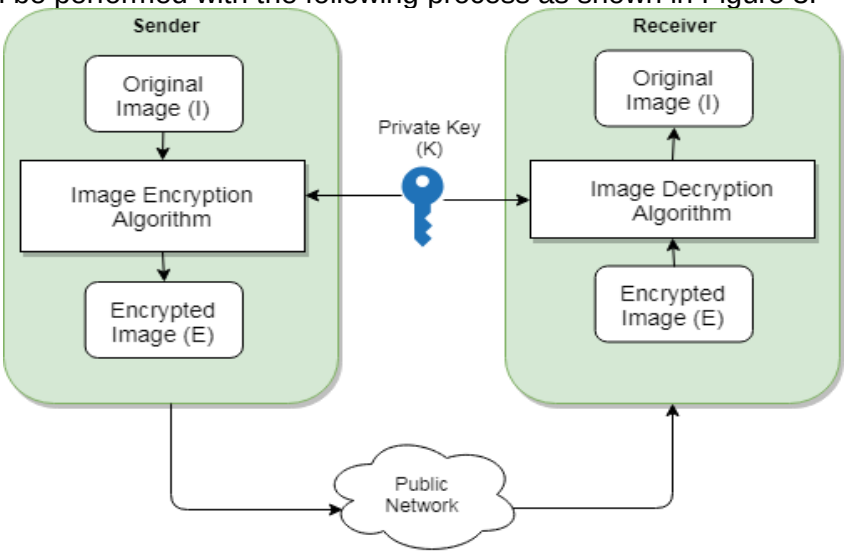


Figure 3. Image encryption process

The encryption process is also similar to watermarking, which starts with the encryption of the original image (I) using a private key (K) to produce an encrypted image (E) at the sender side. Then, encrypted image (E) is ready for transmission over the public network and can be decrypted to get the original image (I) using a decryption algorithm with the help of same private key (K) at receivers side.

Literature review

With the above discussion, it is found that the importance of image security is inevitable. Moreover, the evolution of digital health-care information system established a new research area known as Medical Image Security due to the critical and sensitive nature of patient's medical images [6]. Even though image security immersed with the number of research proposals, medical image security encompasses a considerable

number of proposals. Tirkel and coauthors [7] introduced digital watermarking and then several proposals focused on image watermarking to address various types of security issues along with copyright protection. A wavelet analysis based adaptive blind grayscale image watermarking algorithm was presented by Qing and coauthors [8] which has higher robustness to random noise attack, Shabir and coauthors [9] implemented of intermediate significant bit embedding (ISBE) based digital image watermarking to achieve copyright protection and content authentication. Neural network-based watermarking scheme presented by Kalaivani [10] to address unauthenticated attacks. A variety of proposals found like Yu-Hsum and coauthors [11] proposed digital blind watermarking for depth-image-based rendering (DIBR) 3D image for content protection. Khalil and coauthors [12] presented an efficient just perceptual weighting (JPW) model for wavelet-based fingerprint image watermarking.

Huge number of proposals intensified medical image encryption like a lossless approach known as EdgeCrypt implemented by Yicong and coauthors [13] which can fully protect the selected objects/regions within medical images or the entire medical images. Qian and coauthors [14] combined the biological characteristics of DNA and the improved sequence of logistic mapping method for image encryption. Joshua and coauthors [15] used discrete wavelet transform (DWT) based image encryption. On the other hand, Sokouti and coauthors [16] presented an improved padding based GGH encryption algorithm. A framework for the chaos-based quantum encryption has been proposed by Ahmed and coauthors [17]. Abdmouleh and coauthors [18] presented a new approach of partial encryption based on the Discrete Wavelet Transform (DWT). Abdel-Nabi and coauthors [19] implemented a simple and efficient joint reversible data hiding and encryption algorithm. Rajendra and coauthors [20] presented a diverse approach that interleaves patient information with medical images to reduce storage and transmission overheads. Similarly, Bouslimi and coauthors [21] proposed another joint encryption/watermarking system for protecting medical images. Kester and coauthors [22] implemented fully recoverable encrypted and watermarked image technique.

Most of the proposals implemented gray image security except Kester and coauthors [22]. Moreover, very few proposals addressed both watermarking along with encryption and only Rajendra and coauthors [20] addressed embedding of patient information. This motivated us to implement a combined approach of watermarking and encryption to raise the level of image security for color images along with patient information. Moreover, this proposed method uses simple operations like XOR for watermarking and RC4 for encryption to achieve fast Medical image security along with embedding of patient information.

METHODS

The proposed method encrypts each color channel of the color image to produce a scrambled image and hence named as Color Channel Encryption (CCE). Even though image encryption is the main objective of the proposed CCE method, watermarking is also added to achieve high level of security. In addition to this, patient information has attached to the original image for saving additional space required to store patient information like Patient Name, Address, Gender, and Age. At the sender system, encryption of the proposed CCE method performs two steps including watermarking and encryption as shown in Figure 4.

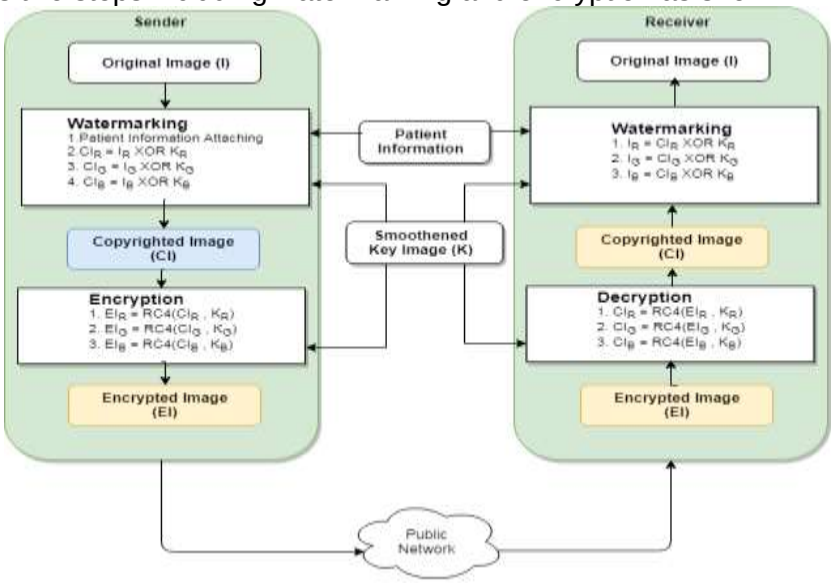


Figure 4. Color Channel Encryption process

Image watermarking requires original color image (I) and Key image (K) as shown in Figure 5(a) and (b) along with Patient Information text (PI). It is mandatory to select key image such that original image size is greater than the key image size as key image need to be embedded into original image. This step generates Copyrighted image (CI) as follows.

1. Initially, patient information from the file/text will be attached to the original image at the desired location (like the top right corner). It can be attached in different ways; one simple way is by superimposing PI text over the medical image as shown in Figure 5(c). It is a lossy approach that removes some of the pixel values of the original image and displays PI text on the image. Second lossy approach is replacing single color channel values by PI text character codes to preserve privacy of PI text and will not display any PI text on the image. Another lossless approach is to include a separate strip of PI text over the original image which increases the resulting copyrighted image size.
2. Then, the watermarking process will be started by modifying the key image using some filter to get the smoothened key image (SK) as shown in Figure 5(d). This filtration increases complexity for key attackers. Any user-defined filter can be used to modify the key image and the proposed method uses Gaussian function for smoothing the key image using Equation 3.

$$G(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-x^2}{2\sigma^2}} \quad (3)$$

3. Now, the smoothened image is embedded into the original color image using bit-wise XOR ($\oplus$) of each color channel of original image with respective color channels of key image using Equation 4. Set of parameter (P) including location and orientation of SK image will be used for image watermarking. If M1xN1 and M2xN2 are the sizes of original and smoothened key images respectively then the default parameters can be P $=\left[\left(\frac{M1-M2}{2}, \frac{N1-N2}{2}\right), 0^o\right]$. This step produces the copyrighted color image (CI) as shown in Figure 5(e).

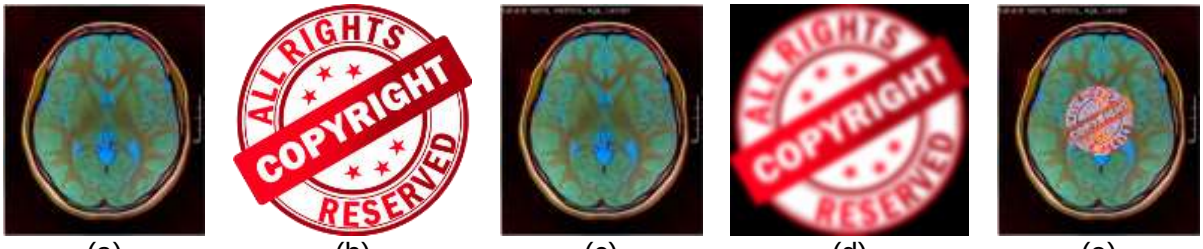
$$CI(R, G, B) = [\ CI_R, CI_G, CI_B\ ] = [\ I_R \oplus SK_R, I_G \oplus SK_G, I_B \oplus SK_B\ ] \quad (4)$$

Image encryption

Now, the copyrighted color image will be encrypted using a fast and secure encryption algorithm. Study of Manju and coauthors [5] reveals that RC4 is the fast algorithm with high visual scrambling, PSNR, and Entropy. Hence, the proposed method considers RC4 algorithm to achieve desired fast medical image security. Image encryption will be performed using RC4 to encrypt each color channel of the copyrighted image (CI) using smoothed key image (SK). This will produce an encrypted color image (EI) using Equation 5.

$$EI(R, G, B) = [\ EI_R, EI_G, EI_B\ ] = [\ RC4(CI_R, SK_R), RC4(I_G, SK_G), RC4(I_B, SK_B)\ ] \quad (5)$$

Privacy and confidentiality of the medical image can be achieved by the visual scrambling of original image to unveil the structural component of the image. Now, the encrypted color image is ready for transmission over the public network.



(a) (b) (c) (d) (e)

Figure 5. Proposed Image watermarking (a) Original image; (b) Key image; (c) Image with patient information; (d) Smoothened key image; (e) Copyrighted image

At the receiver side, firstly the encrypted color image is decrypted using RC4 with the same smoothened key image (SK) to generate reconstructed copyrighted image (CI). Then, the copyrighted image is bit-wise XOR with the same SK image to regain original image with patient information. If we need lossless original image after decryption we need to use separate strip of patient information text.

RESULTS AND DISCUSSION

The proposed method has simulated using MATLAB R2018b. Four types of medical images including Magnetic Resonance Imaging (MRI), Positron Emission Tomography (PET), X-ray and Ultrasound has considered to demonstrate the strength of proposed Color Channel Encryption (CCE) method. All of these images have considered in lossless PNG format. Figure 6(a), (b), (c) and (d) shows original images of head MRI, chest PET, chest X-ray, and fetal Ultrasound color images respectively. This study has included two major types of analysis including qualitative and quantitative.

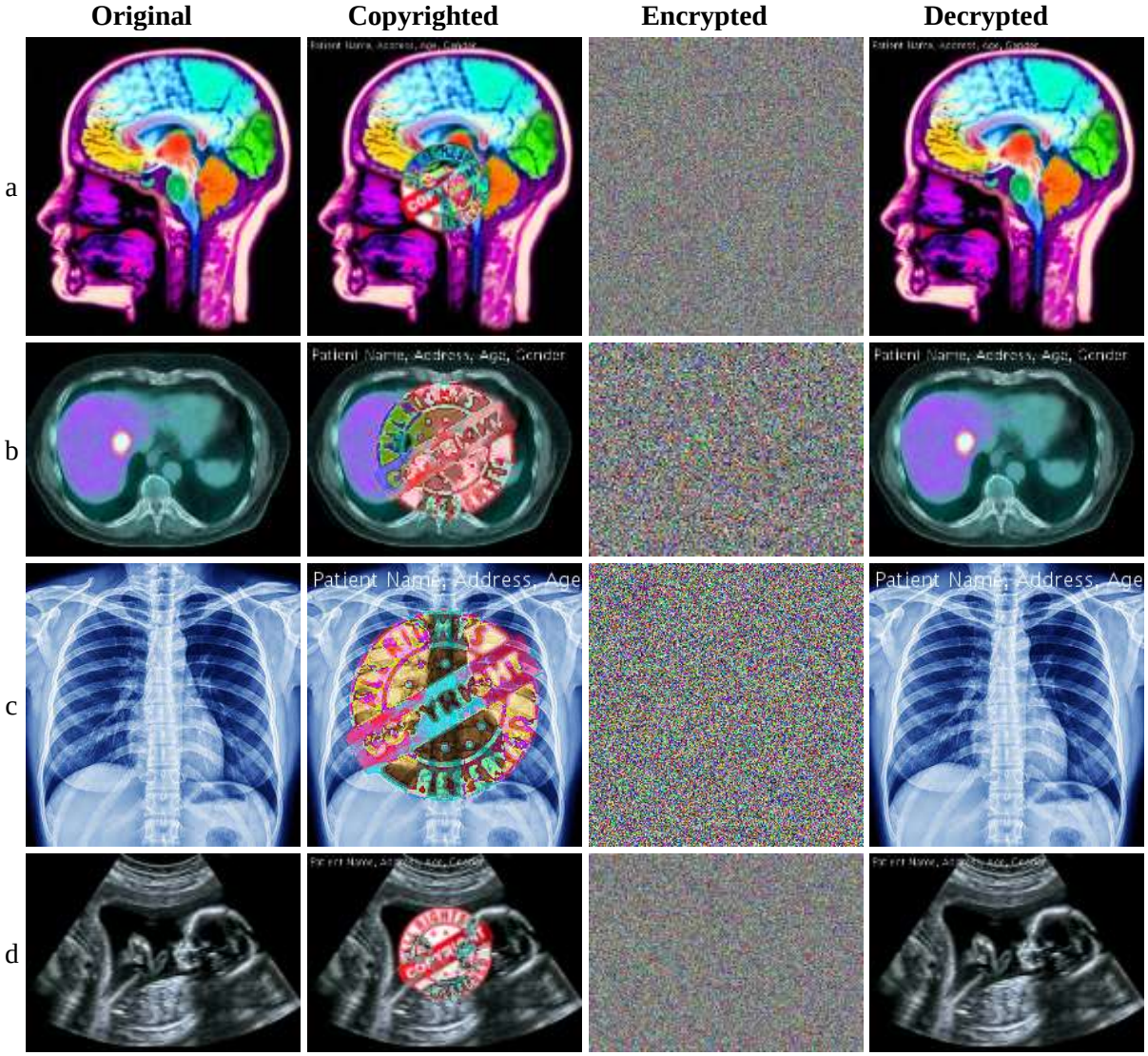


Figure 6. CCE results (a) MRI image of the head; (b) PET image of the chest; (c) X-**ray** image of the chest; (d) Ultrasound image of the fetal.

Qualitative analysis

The proposed method uses superimposing of PI text as it is the fastest approach while adding PI text to original image. Results of copyrighted images can be seen from the second column of Figure 6. The proposed CCE method has distracted structure of the original images completely and can be observed from the third column of Figure 6. Finally, fourth column depicts decrypted color images that are similar to original images. Thus, the proposed method recovers the original image with patient information (PI) without any loss of image. Original image without patient information can be achieved when we use separate PI text image approach instead of superimposing PI text approach while adding patient information.

Quantitative analysis

Quantitative strength of image encryption algorithm can be specified using two primary statistical measures: Entropy and Arithmetic mean. Entropy represents the disorder of image and high entropy causes

more visual scrambling of the image. Quantitative results of above four encrypted images are tabulated in Table 1 and proposed method shows good performance when compared to Kester and coauthors [22] method which addressed color image security like the proposed method. Moreover, the proposed method shows outstanding performance in case of MRI and Ultrasound images. Arithmetic mean of Kester and coauthors [22] differs with image type and proposed CCE method produces the same mean irrespective of image type. As the proposed method uses RC4 encryption, the results depend on smoothened key image.

Table 1. Quantitative results of primary measures

Image	Entropy		Arithmetic Mean	
	Kester *et al.* [22]	Proposed CCE	Kester *et al.* [22]	Proposed CCE
Head MRI	4.6894	7.9998	39.0415	127.4772
Chest PET	-	7.9991	-	127.7357
Chest X-ray	7.1726	7.9987	143.5284	127.3215
Fetal Ultrasound	3.7603	7.9996	18.5810	127.6001

Similarly, Peak Signal to Noise Ratio (PSNR) and Correlation coefficient are the set of secondary measures. PSNR represents peak error and can be computed with maximum possible pixel value (M) and Mean Square Error (MSE) of image. PSNR reflects noise of the image and hence high PSNR represents more security. Correlation represents how original and encrypted images are similar. Thus, the average correlation should be far from zero which indicates exactly similar. The proposed CCE method produces satisfactory results in terms of secondary measures as listed in Table 2. These quantitative measures prove the strength of the high-level security of proposed CCE method.

Table 2. Quantitative results of secondary measures

Image	PSNR (dB)	$Corr_R$	$Corr_G$	$Corr_B$	$Corr_{Avg}$
Head MRI	61.5313	-0.0015	-0.0017	0.0013	-0.0006
Chest PET	67.5107	0.0065	-0.0039	0.0009	0.0012
Chest X-ray	78.3544	0.0005	0.0008	-0.0066	-0.0018
Fetal Ultrasound	63.4154	0.0011	-0.0007	0.0041	0.0015

Moreover, the proposed method has good resistance to key guessing attacks. Guessing of a key is the major security attacks for security algorithms. In order to guess key image, brute force method causes M2 * N2 * 3 * 28 combinations if size of key image is M2xN2 and each pixel takes 8-bits for three color channels. Filtration of key image adds more complexity. In addition to this, another difficult task for crackers is guessing of watermarking parameters. Location of watermark parameter has M1 * N1 possibilities if M1xN1 is size of original image and angle of watermark has 0 to 360 possibilities.

CONCLUSIONS

Medical Image Security became the contemporary research area due to the evolution of Digital Health-care Information System. The proposed CCE method consists of two steps to achieve Fast Medical Image Security. Proposed method starts with the embedding of patient information and smoothened key image over the original image. Finally, generates the encrypted image using RC4 encryption. Strengths of this proposed method are only one key image whose size is less than or equal to the size of the original image is sufficient, RC4 encryption achieves high visual scrambling with less time complexity. Moreover, watermarking causes copyright protection and embedding of patient information reduces additional space. Both qualitative and quantitative results of the CCE method showed the best performance than the existing method in achieving high security. Moreover, the proposed method has good resistance to key guessing attacks.

Conflicts of Interest: Declare conflicts of interest or state “The authors declare no conflict of interest.”

REFERENCES

1. Usman MA, Usman MR. Using image steganography for providing enhanced medical data security. 15th IEEE Annual Consumer Communications & Networking Conference (CCNC); 2018; USA.
2. Wolfgang RB, Delp III EJ. Overview of image security techniques with applications in multimedia systems. Proceedings of Multimedia Networks: Security, Displays, Terminals, and Gateways; United States; 1998; 3228.
3. Cox I, Miller M, Bloom J, Fridrich J, Kalker T: Digital Watermarking and Steganography. 2nd ed. Morgan Kaufmann Publishers; 2007.
4. Tefas A, Nikolaidis N, Pitas I: Image Watermarking: Techniques and Applications. 2nd ed. The Essential Guide to Image Processing. 2009.
5. Kumari M, Gupta S, Sardana P. A Survey of Image Encryption Algorithms. Springer 3D Display Research Center. 2017; 8(4):37.
6. Al-Haj A, Abdel-Nabi H. Digital Image Security Based on Data Hiding and Cryptography. 3rd International Conference on Information Management; 2017; China.
7. Tirkel AZ, Rankin GA, Van Schyndel RM, Ho WJ, Mee NR, Osborne CF: Electronic Water Mark. Digital Image Computing, Technology and Applications (DICTA); Macquarie University. 1993.
8. Liu Q, Ying J. Grayscale image digital watermarking technology based on wavelet analysis. IEEE Symposium on Electrical & Electronics Engineering (EEESYM); 2012; Malaysia.
9. Parah SA, Sheikh JA, Bhat GM. Fragility evaluation of intermediate significant bit embedding (ISBE) based digital image watermarking scheme for content authentication. International Conference on Advances in Electronics Computers and Communications; 2014; India.
10. Kalaivani K. An Efficient Watermarking Scheme for Medical Data Security with the Aid of Neural Network. Brazilian Archives of Biology and Technology. 2016; 59:e161070.
11. Lin YH, Wu JL. A Digital Blind Watermarking for Depth-Image-Based Rendering 3D Images. IEEE Transactions on Broadcasting. 2011; 57(2):602-11.
12. Zebbiche K, Khelifi F. Efficient wavelet-based perceptual watermark masking for robust fingerprint image watermarking. IET Image Processing. 2014; 8(1):23-32.
13. Zhou Y, Panetta K, Agaian S. A lossless encryption method for medical images using edge maps. Annual International Conference of the IEEE Engineering in Medicine and Biology Society; 2009; USA.
14. Wang Q, Zhang Q, Wei X. Image Encryption Algorithm based on DNA Biological Properties and Chaotic Systems. IEEE Fifth International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA); 2010; China.
15. Dagadu JC, Li JP, Shah F, Mustafa N, Kumar K. DWT based encryption technique for medical images. 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP); 2016; China.
16. Sokouti M, Zakerolhosseini A, Sokouti B. Medical Image Encryption: An Application for Improved Padding Based GGH Encryption Algorithm. The Open Medical Informatics Journal. 2016; 10:11.
17. Abd El-Latif AA, Abd-El-Atty B, Talha M. Robust Encryption of Quantum Medical Images. IEEE Access. 2017; 6:1073-81.
18. Abdmouleh MK, Khalfallah A, Bouhlel MS. A Novel Selective Encryption DWT-Based Algorithm for Medical Images. 14th International Conference on Computer Graphics, Imaging and Visualization; 2017; Morocco.
19. Abdel-Nabi H, Al-Haj A. Medical imaging security using partial encryption and histogram shifting watermarking. 8th International Conference on Information Technology (ICIT); 2017; Jordan.
20. Acharya UR, Acharya D, Bhat PS, Niranjan UC. Compact storage of medical images with patient information. IEEE Transactions on Information Technology in Biomedicine. 2001; 5 (4): 320-3.
21. Bouslimi D, Coatrieux G, Cozic M, Roux C. A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images. IEEE Transactions on Information Technology in Biomedicine. 2012; 16 (5): 891-9.
22. Kester QA, Nana L, Pascu AC, Gire S, Eghan JM, Quaynor NN. A Cryptographic Technique for Security of Medical Images in Health Information Systems. Procedia Computer Science. 2015; 58: 538-43.