Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 7, pp. 1949–1960
DOI : 10.47974/JDMSC-1783

Cipher block chaining-based color medical image encryption for secure transmission

Fatma Hassan Al-Rubbiay
Department of Statistics
College of Economics and Administration
University of Mustansiriyah
Baghdad
Iraq

Abstract

Research in multimedia security is devoted to medical image encryption. Cipher Block Chaining (CBC), Rotation Operations, and Random Permutations (RaPe) are proposed in this manuscript as a hybrid encryption algorithm for medical images. As a result, the RGB planes are scrambled in specified directions: horizontally, vertically, and diagonally. An exhaustive attack method is effectively protected against decryption utilizing this method since it completely erases the outline of encrypted medical images, blurs the RGB-level matrix distribution properties, and completely erases the outlines of encrypted medical images. The proposed system does not use a transform domain for deploying improved security. Various parameters can be used to test and analyze the medical image in this proposed approach to ensure its security and effectiveness. Utilizing the proposed method as an example of its effectiveness, pragmatic images are selected to demonstrate its practical application in medical image encryption.

Subject Classification: *91G20, 68P25.*

Keywords: *Cipher block chaining (CBC), Random permutation (RaPe), Rotation operation, Medical image encryption, Secret image (SctImg).*

1. Introduction

Our society lives in a technology-driven era of information that allows us to process and save enormous amounts of information in a slow-moving manner. Due to the explosion of Internet applications, communication via digital data has become commonplace. Invisible communications, data

E-mail: fatima_h@uomustansiriyah.edu.iq

security issues, and the copyright protection of digitized properties have also been investigated due to digital media utilizing. Generally speaking, these developments have not resulted in progress in information security. It is now possible to store information that was once stored on a large amount of manuscript in a form that is easily accessible and physically difficult to steal on a disk. Different aspects of information security are concerned with trust. Assurance of information is another term that is commonly utilized. There is no limit to the types of information that can be secure, whether they are in an electronic or machine-readable format. Whatever form information or data takes, it must be safeguarded and protected. If your information is threatened, lost, or misused, you need an information security chain. Data security and truth have become increasingly difficult to confirm in this era of technological innovation due to the proliferation of tools that manipulate and distort data, as well as individuals who utilize technology for malicious purposes. Keeping this in mind, we developed a system that ensures the security of all content in the images and prevents their manipulation or counterfeiting.

2. The Planned Methodology

A. Concept

Utilizing the 'scramble method', this planned system would endow with two levels of confirmation. There is no need to utilize a transformation process to accomplish this. An image is utilized here to encrypt a message that can later be decrypted for a variety of aims. The first step in encrypting a medical image is to divide it into 3- planes, such as R_Plan, G_Plan, and B_Plan. After encryption, the image is rotated. Two levels of verification are utilized in this encryption operation. Medical images are encoded in RGB by scrambling them horizontally, vertically, and diagonally.

B. Cipher Block Chaining (CBC)

A block cipher can be configured to operate utilizing CBC, which encrypts sequences of bits as a single block accompanied by a cipher key). A key feature of this system is the chaining method, which allows for the decryption of cipher text only after all preceding blocks have been decrypted. The block immediately preceding any cipher text block is valid as well. In cipher text, even a single bit slip affects all subsequent blocks. Crypt text blocks are transposed in an orderly manner, which corrupts the decryption. The cipher block chaining process basically involves XORing

each plaintext block with the previous ciphertext block and then encrypting the XORed block.

C. An Overview of Scramble Technique

Modern data communication schemes utilize scrambling methods to encode data, which can aid in retrieving information from received data and improve synchronization between transmitters and receivers. Oftentimes, receivers encounter long sequences of 1s and 0s in digital systems, making retrieval of timing information difficult. Therefore, input devices randomize data, but receivers fail to receive it consistent with their nature. A scrambling device can guarantee randomized bit sequences that will eliminate issues like adaptive equalization, clock recovery, and variations in received data. As part of this planned method, scrambling techniques are implemented to create scrambled RGB images along specified directions, such as horizontally, vertically, and diagonally. Information cannot be viewed by unauthorized persons without the secret decryption key. If the correct key is utilized, the message will be unscrambled and the contents will be visible only to the intended user.

Implementation of Data Encrypting and Decryption Procedures

Key Generating

In order to encrypt and decrypt messages, cryptographic keys are utilized. Cryptographic images are generated utilizing the sender's key. Original images are obtained in reverse at the receiver. Keys will be generated to begin the encryption/decryption process as found in Figure 1 for encryption, and Figure 2 for decryption. Encryption of input images is required for this process. Three channels will be created from the selection of images (Red_Channel, Green_Channel, and Blue_Channel). for the purpose of key generation. When the key generation process is performed, there is a key generated for each red, green, and blue channel in the image. Binary values are stored in arrays once they have been calculated for each pixel.

Encryption Process Procedures

Phase 1: Secret Color Medical Image Reading.

Phase 2: Create RGB (Red, Green, and Blue) planes from the secret medical image.

Phase 3: The RaPe is applied to the medical image based on the pixel values. In this case, it is initiated so that a random sequence can be generated.

Phase 4: Rotate the medical image key according to the first key.

Phase 5: Medical image is shuffled. Rotate this image and convert it to binary.

Phase 6: XOR is then utilized in the first level of substantiation.

Phase 7: To complement the binary image, shuffle every bit in every pixel.

Phase 8: Implement the most common cryptographic technique, block chaining, on the resultant shuffled image.

Phase 9: Now convert each pixel back to decimal.

Phase 10: To increase the security of the image, each RGB plane is scrambled horizontally, vertically, and diagonally.

Phase 11: Green and blue planes are processed similarly as well.

Phase 12: Create an encrypted image of the resultant image.

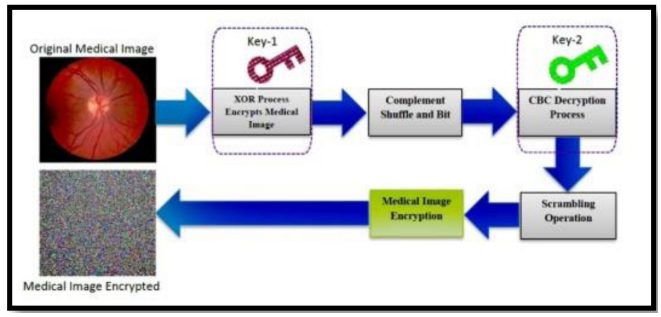

Figure 1

Encryption of Medical Images: Block Diagram

A. Decryption Process Procedures

Phase 1: Encrypted Medical Image Reading.

Phase 2: Divide The Encrypted Medical Image into RGB (Red, Green, and Blue) Planes.

Phase 3: Perform the Decryption Process first to the Red Plane.

Phase 4: The Red Plane is Utilized for Descrambling.

Phase 5: Convert key 2 into Binary Utilizing CBC Process.

Phase 6: Taking the Complement of a Binary.

Phase 7: The red plane is subjected to an XOR Operation.

Phase 8: Reconvert the binary values to decimal after shunting them as in encryption.

Phase 9: The medical image is rotated with key 1 a certain number of times.

Phase 10: The processes (Phases from 4 to 9) are also carried out on the green and blue planes.

Phase 11: The final step is to combine all the planes so that the original medical image can be obtained.

Phase 12: Save the resultant medical image as the decrypted medical image (original image).

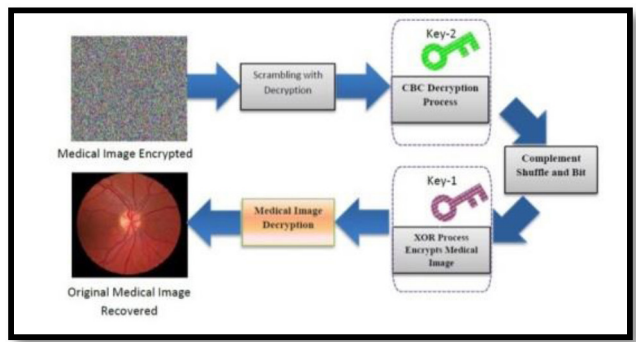

Figure 2

Decryption of Medical Images: Block Diagram

3. Performance Evaluation Measures

A. Mean Square Error Analysis (MSE)

The differences among encrypted medical images and Secret Medical Images are called MSE. These differences must be very high for the best performance as illustrated in Table 1.

$$MSE = \frac{1}{M * N * (\text{Secret Image} - \text{Encrypted Image})} \tag{1}$$

Table 1

Performance Analysis-MSE

SctImg	MSE		
	The Red_Band	The Green_Band	The Blue_Band
Retina Image	4.47E+03	3.07E+03	3.34E+03
Brain Image	2.32E+03	2.25E+03	3.16E+03

B. Peak Signal to Noise Ratio Analysis (PSNR)

The power of the peak signal divided by noise power is the ratio. The quality of the image is measured utilizing this tool. There must be a low value of PSNR for a good encrypted image as explained in Table 2 and Table 3.

$$PSNR = 10\log_{10}\frac{I_{\max}^2}{MSE}\text{dB} \quad (1)$$

Where I_{max} is Image intensity maximum.

Table 2

Display the performance of PSNR of tested medical input images for every Plan (Red_Plan, Green_Plan, and Blue_Plan)

SctImg	PSNR		
	The Red_Band	The reen_Band	The Blue_Band
Retina Image	1.29E+01	1.46E+01	1.42E+01
Brain Image	1.58E+01	1.59E+01	1.44E+01

Table 3

Display the Total Performance of PSNR of Tested medical Input Images

Medical Test Image	PSNR
Sec_Med_Img_1	6.34E+00
Sec_Med_Img_2	6.20E+00
Sec_Med_Img_3	6.97E+00
Sec_Med_Img_4	6.41E+00
Sec_Med_Img_5	6.20E+00

Bit Error Rate Analysis (BER)

BER also tells us about the errors seen in the procedure. According to this proposal, it should be approximately 0.5 for all images. Image encryption routines require an error rate of almost 50%, which is almost confirmed by this study as listed in Table 4.

Table 4

Performance Analysis - Bit Error Rate

SctImg	BIT ERROR RATE	Total No of Pixel errors
Retina Image	1.71E+00	2.62E+05
Brain Image	1.71E+00	2.62E+05

An analysis of two adjacent pixels' correlation

Correlations affect security by expressing the degree of association among pixels adjacent to each other in an image or the degree of relationship among adjacent pixels in an image. Metrics for correlating are intended to minimize redundant information within an encrypted image.

$$r_{xy} = \frac{\text{cov}(x,y)}{\sqrt{\text{var}\ (x)\sqrt{\text{var}(y)}}} \tag{4}$$

$$Cov(x,y) = E[(x_i - E[x_i])(y_i - E[y_i])] \tag{2}$$

$$E[x\} = \frac{1}{N}\sum_{i=1}^{N} x_i, E[y] = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{3}$$

$$Var(x) = \frac{1}{N}\sum_{i=1}^{N} x_i - E[x_i])^2 \tag{4}$$

$$Var(x) = \frac{1}{N}\sum_{i=1}^{N} y_i - E[y_i])^2 \tag{5}$$

Table 5

Analysis of performance - correlation coefficient

Coefficient of correlation Calculation	Medical secret image		Medical Encrypted image	
	Brain Image	Iris Image	Brain Image	Iris Image
Vertical Correlation	2.13E+00	1.96E+00	1.21E+00	1.20E+00
Horizontal Correlation	2.12E+00	2.09E+00	1.21E+00	1.21E+00
Diagonal Correlation	2.08E+00	1.91E+00	1.20E+00	1.21E+00

4. Experimental and Simulation Results

A. *Medical Image Encryption Procedure*

An Iris image and a Brain image are utilized as the SctImg in MATLAB 7-10 to verify the effectiveness of this project. The images are 256 x 256 pixels in size.

1. *Testing the images:* Images taken here are Iris and Brain with dimensions of 256*256. A JPEG file contains these SctImgs (JPG). Scrambling is applied to each of the three RGB planes (Red, Green, and Blue) of the images. As presented in Figures 3 and 4, this is the case.

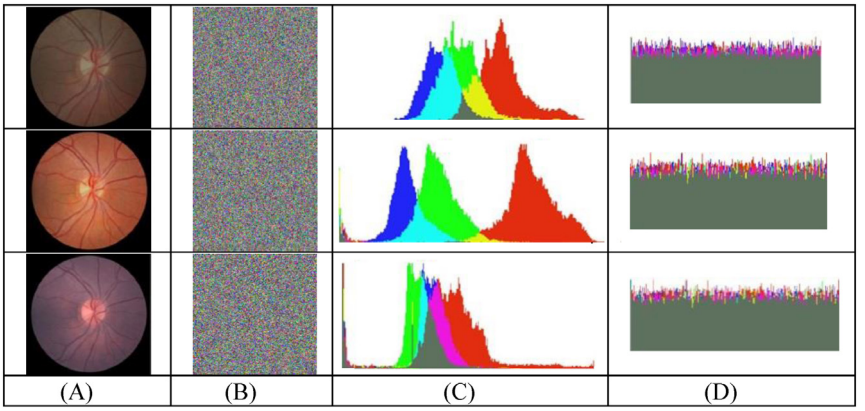

Figure 3

(A) The Secret Iris Image, (B) Medical Image Encryption, (C) Image Histogram Before Encryption, (D) Image Histogram After Encryption.

1. *Histogram Analyzing:* The statistical similarity between encrypted and original images should be avoided to prevent information from being leaked to attackers. A histogram illustrates how pixels are distributed in an image by displaying a graphical representation. The original and encrypted media histograms are compared.
2. *Performance Analyzing:* Performance analysis is utilized to evaluate and determine the effectiveness of the proposed method by analyzing

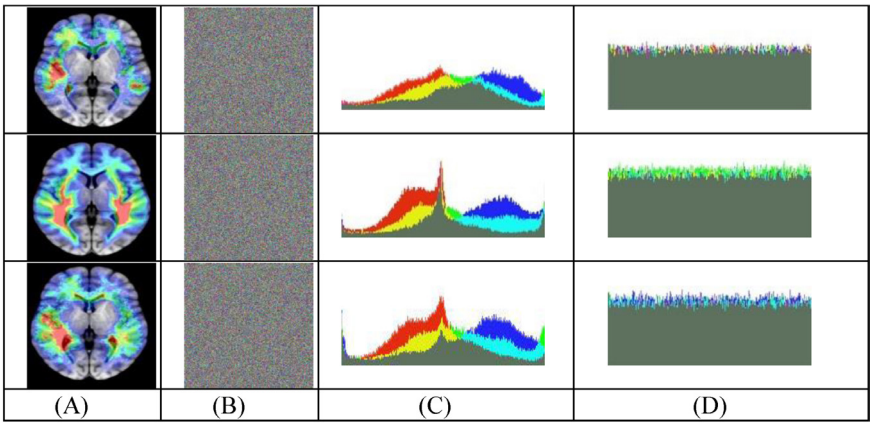

Figure 4

(A) The Secret Brain Image, (B) Medical Image Encryption, (C) Image Histogram Before Encryption, (D) Image Histogram After Encryption

its performance. There are PSNR values for the SctImg (original) in Table 2. As can be seen in Table 3, Bit Error Rates are shown. Iris and brain correlation coefficients.

B. Medical Image Decryption Procedure

Decryption is also of the utmost importance in this project in order to prove that the method also works on the receiver's end. Its retrieval is devoid of any deformation, thereby demonstrating. As a result of the algorithm, the algorithm is efficient. Only the correct keys and encryption mode can be used to recover the original image.

5. Conclusion

Our manuscript proposes a hybrid encryption technique for color medical images, combining random permutation, rotation, and CBC. As a result, RGB planes are scrambled in various directions, including horizontally, vertically, and diagonally. The decryption of encrypted medical images is effectively prevented by this method since it reduces the outline of the images, blurs the distribution characteristics of RGB-level matrixes, and prevents exhaustive attack methods from decrypting the images. Rather than incorporating the transform domain into the spatial domain, this can be accomplished within the spatial domain itself. Defining the secret key without any problems, in a rapid manner, and with ease is the purpose of the proposed scheme.

References

[1] S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102 (Oct. 2017), doi: 10.1016/j.ijleo.2017.08.028.

[2] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144 (Mar. 2018), doi: 10.1016/j.sigpro.2017.10.004.

[3] Y. Chen, C. Tang, and R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 167, p. 107286 (Feb. 2020), doi: 10.1016/j.sigpro.2019.107286.

[4] S. K.U. and A. Mohamed, "Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion," *Signal*

Processing: Image Communication, vol. 99, p. 116495 (Nov. 2021), doi: 10.1016/j.image.2021.116495.

[5] Dey, . S., and A. Mitra, "CBC Mode Based Image Encryption Technique Using Arnold Transformation," *SSRN Electronic Journal* (2022), doi: 10.2139/ssrn.4034314.

[6] S. Ashokkumar, K. Karuppasamy, B. Srinivasan, and V. Balasubramanian, "Parallel Key Encryption for CBC And Interleaved CBC," *International Journal of Computer Applications*, vol. 2, no. 1, pp. 21–25 (May 2010), doi: 10.5120/616-867./

[7] K. Yadav and T. Chaware, "Review of Joint Encoding and Encryption for Image Transmission using Chaotic Map, LDPC and AES Encryption," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC) (Oct. 2021), doi: 10.1109/ispcc53510.2021.9609351.

[8] V. Sharma, B. B. Sharma, and R. Nath, "Digital image chaotic encryption and transmission using UIO," 2017 International Conference on Computer, Communications and Electronics (Comptelix) (Jul. 2017), doi: 10.1109/comptelix.2017.8003933.

[9] K. S. R. Murthy and V. M. Manikandan, "A Reversible Data Hiding through Encryption Scheme for Medical Image Transmission Using AES Encryption with Key Scrambling," *Journal of Advances in Information Technology*, vol. 13, no. 5 (2022), doi: 10.12720/jait.13.5.433-440.

[10] R. B and N. Makhija, "Secured image storage and transmission technique suitable for IoT using Tangle and a novel image encryption technique," *Multimedia Tools and Applications* (Mar. 2023), doi: 10.1007/s11042-023-14794-3.

[11] X.-Q. Fu, B.-C. Liu, Y.-Y. Xie, W. Li, and Y. Liu, "Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos," *IEEE Photonics Journal*, vol. 10, no. 3, pp. 1–15 (Jun. 2018), doi: 10.1109/jphot.2018.2827165.

[12] M. Et al., "An analysis on image encryption for secured transmission of biomedical applications," *Information Technology in Industry*, vol. 9, no. 1, pp. 01–11 (Feb. 2021), doi: 10.17762/itii.v9i1.82.

[13] X.-Q. Fu, B.-C. Liu, Y.-Y. Xie, W. Li, and Y. Liu, "Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos," *IEEE Photonics Journal*, vol. 10, no. 3, pp. 1–15 (Jun. 2018), doi: 10.1109/jphot.2018.2827165.

[14] A. Antariksa, "Ransomware Attack using AES Encryption on ECB, CBC and CFB Mode," *Jurnal Ilmu Komputer*, vol. 12, no. 1, p. 8 (Mar. 2019), doi: 10.24843/jik.2019.v12.i01.p06.

[15] Z. Wang, "Secure Image Transmission in Wireless OFDM Systems Using Secure Block Compression-Encryption and Symbol Scrambling," IEEE Access, vol. 7, pp. 126985–126997 (2019), doi: 10.1109/access.2019.2939266.

[16] V. A. Memos and K. E. Psannis, "Encryption algorithm for efficient transmission of HEVC media," *Journal of Real-Time Image Processing*, vol. 12, no. 2, pp. 473–482 (May 2015), doi: 10.1007/s11554-015-0509-3.

[17] Z. Wang, F. Chen, W. Qiu, S. Chen, and D. Ren, "A two layer chaotic encryption scheme of secure image transmission for DCT precoded OFDM-VLC transmission," *Optics Communications*, vol. 410, pp. 94–101 (Mar. 2018), doi: 10.1016/j.optcom.2017.09.095.

[18] J. Ramasamy and J. S. Kumaresan, "Image Encryption and Cluster Based Framework for Secured Image Transmission in Wireless Sensor Networks," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1355–1368 (Feb. 2020), doi: 10.1007/s11277-020-07106-7.

[19] J. Liang, D. Xiao, Y. Xiang, and R. Doss, "A Compressed Sensing Based Image Compression-Encryption Coding Scheme without Auxiliary Information Transmission," ICC 2022 - IEEE International Conference on Communications (May 2022), doi: 10.1109/icc45855.2022.9839131.

[20] Z. Wang, F. Chen, W. Qiu, S. Chen, and D. Ren, "A two layer chaotic encryption scheme of secure image transmission for DCT precoded OFDM-VLC transmission," *Optics Communications*, vol. 410, pp. 94–101 (Mar. 2018), doi: 10.1016/j.optcom.2017.09.095.

[21] N. Sammeta and L. Parthiban, "Data Ownership and Secure Medical Data Transmission using Optimal Multiple Key-Based Homomorphic Encryption with Hyperledger Blockchain," *International Journal of Image and Graphics* (Oct. 2021), doi: 10.1142/s0219467822400034.

[22] R. M. Dansereau, S. Jin, and R. A. Goubran, "Reducing Packet Loss in CBC Secured VoIP using Interleaved Encryption," 2006 Canadian Conference on Electrical and Computer Engineering (May 2006), doi: 10.1109/ccece.2006.277417.

[23] M. Nandi, "Fast and Secure CBC-Type MAC Algorithms," *Lecture Notes in Computer Science*, pp. 375–393 (2009), doi: 10.1007/978-3-642-03317-9_23.

[24] R. V. U. and T. V., "Image Encryption using DNA rules & Transmission of an encrypted digital image using USRP-2901 and MATLAB," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) (Mar. 2019), doi: 10.1109/vitecon.2019.8899561.

[25] R. V. U. and T. V., "Image Encryption using DNA rules & Transmission of an encrypted digital image using USRP-2901 and MATLAB," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) (Mar. 2019), doi: 10.1109/vitecon.2019.8899561.

[26] J. Liang, D. Xiao, Y. Xiang, and R. Doss, "A Compressed Sensing Based Image Compression-Encryption Coding Scheme without Auxiliary Information Transmission," ICC 2022 - IEEE International Conference on Communications (May 2022), doi: 10.1109/icc45855.2022.9839131.

[27] S. Ajili, M. A. Hajjaji, B. Bouallegue, and A. Mtibaa, "Joint Watermarking\Encryption image for safe transmission: Application on medical imaging," 2014 Global Summit on Computer; Information Technology (GSCIT) (Jun. 2014), doi: 10.1109/gscit.2014.6970110.

Received April 2023