Cyber Security for Medical Image Encryption using Circular Blockchain Technology Based on Modify DES Algorithm

https://doi.org/10.3991/ijoe.v19i03.37569

Abeer Salim Jamil[1(✉)], Abdul Monem S. Rahma[2]
[1]Department of Computer Technology Engineering, Al-Mansour University College, Baghdad, Iraq
[2]Department of Computer Sciences, Al-Maarif University College, Anbar, Iraq
abeer.salim@muc.edu.iq

Abstract—Recently, with the requirement for protecting the privacy of images transferred over the internet and media networks. The need to protect these images from hacking by unauthorized persons and from the manipulation of these images has become very important in this research, Block chain technology was used for its importance in cybersecurity. To maintain the confidentiality of the patient's medical data, as a result, to solve this problem requires increasing the strength of the key used in the encryption process, which is responsible for ensuring the security of the image. In this paper, it is proposed to use block chain technology with the Data Encryption Standard (DES) algorithm for the purpose of increasing the degree of security of the transmitted images by enhancing the key during the process of encrypting the transmitted images as well as increasing the degree of authentication between the sender and receiver. Experimental outcomes manifested that the security of encryption image that gained via the suggested algorithm is higher, performing the goal of protecting the information of medical image, as presented by the results obtained in Entropy, MSE, and PSNR.

Keywords—medical image encryption, cyber security, encryption model, decryption model, block chain technology, DES algorithm

1 Introduction

Blockchain technology has become an important technology in latest years, and it is used in a variety of applications, such as record keeping, Bitcoin transactions, file transfer, healthcare system, and others. It is accomplished through the use of hash functions, which are used to connect two blocks to each other [1]. This process works well in large networks where it is difficult to attack during data transfer, but it is easily breached by a hacker in smaller networks. In this case, the data can be secured by using one of the encryption algorithms such as the DES algorithm to secure the data transfer from hacking [2–4]. In general, there are two types of encryption methodologies: First, Symmetric key encryption and second, a symmetric key encryption [5, 6]. The symmetric encryption algorithms include (2) categories: First, block codes and second, streaming codes. Each encrypted bit in the streaming code is encrypted separately via

supplementing a bit from a key of stream to a plain text (bit). But, a block of bits (plain text) is encrypted at the same time with the same keys, which represent the block codes. Block codes use the Feistel network like the DES, and block codes that do not use the Feistel network like the Advanced Encryption System (AES) [7, 8]. DES is a block encryption, running on plain text blocks of a certain size (64 bits) and returning blocks of encrypted text of the same size, as shown in Figure 1 [9–11]. As shown in Figure 2, the hash function is a code generated by the sender, but it cannot protect the file's content (text or image). This generated hash code can merely ensure the transferred file authenticity, not its confidentiality [3]. The remainder of this research is structured as following: Previous studies are represented in section (2). Section (3) discusses the circular blockchain technology. Section (4) depicts the DES algorithm. Section (5) illustrates the proposed method. Section (6) represents the implementation and result discussion. The final section presents the conclusions to a close.

2 Related works

Privacy and security in security institutions are important topics to study; at the moment, the blockchain technology is a significant technology in ensuring the data security during the files (medical images) transfer. Below are previous and recent studies related to cyber security for medical image encryption and block chain technology. In research [1, 12], blockchain technology was used in the file transfer system. But, blockchain technology only has the potential to provide authentication. To protect the data security and confidentiality, the AES algorithm was used before the hashing was performed. The results did not give high confidence in ensuring the security of data to users during its transmission. The researchers proposed a private block chain network to be used to reduce the file size and secure the file sharing application [7]. A high level of security was achieved by encrypting the file (text) with the ASE and RSA algorithms from the field of cryptography. The researchers of [9] proposed an algorithm that can encrypt blockchain-based e-commerce platform data using an asymmetric key algorithm which was based on the attraction of a chaotic neural network, as well as an asymmetric encryption algorithm depending on the chaotic sequence of the neural network, to achieve good application results. In work of [13], a secure and decentralized application for file transfer using blockchain technology has been proposed, where the application was based on file sharing through the use of a secret block chain network that can be utilized by smaller institutions. In [14–16], the Crypto-Stegno model for securing IOT medical information was proposed, where this model was applied to healthcare information groups, and good results were obtained with a good confidentiality on the IoTM platform. In [17], the researchers proposed how to store and retrieve files using blockchain technology by employing artificial intelligence algorithms, such as swarm and whisper, which enable the provision of a secure guarantee for decentralized file storage and retrieval. In [18], the AES algorithm was updated for data protection while also providing high speed and reducing the volume of data transmitted through unlocked channels. In [19], the researchers proposed how to used block chain technology with cyber security for healthcare medical by using the (LGE-HES) algorithm for the cybersecurity of block chain in healthcare networks. In [20],

the authors reviewed the developments of the healthcare field by using blockchain as a model, and discussed the applications of block chain and challenges.

3 Data encryption standard (DES) algorithm

The DES method is widely employed in a variety of applications [21, 22], which include commercial, military, and security communications systems [23]. DES is a symmetrical encryption method developed by IBM in 1972 that is employed to both encrypt and decrypt data [21]. Block ciphers utilize the same key for encrypting the whole plaintext block at a period of time. The Feistel network could be used to generate block ciphers. Feistel networks' primary purpose is to multiply the number of rounds required for repeating the similar processes as a bit-shuffling and a logical operation (XOR process). The following is a summary of DES encryption/decryption performance: Plain text input on a (64-bit) block that is processed using an initial switch (P), following that, 16 rounds of plain text and key (56 bit) are applied, and finally reverse permutations are applied [23]. The DES algorithm structure divided the plain text block of the input (64-bit) into two sub-blocks: Left (32-bit) and right (32-bit), as shown in Figure 1.

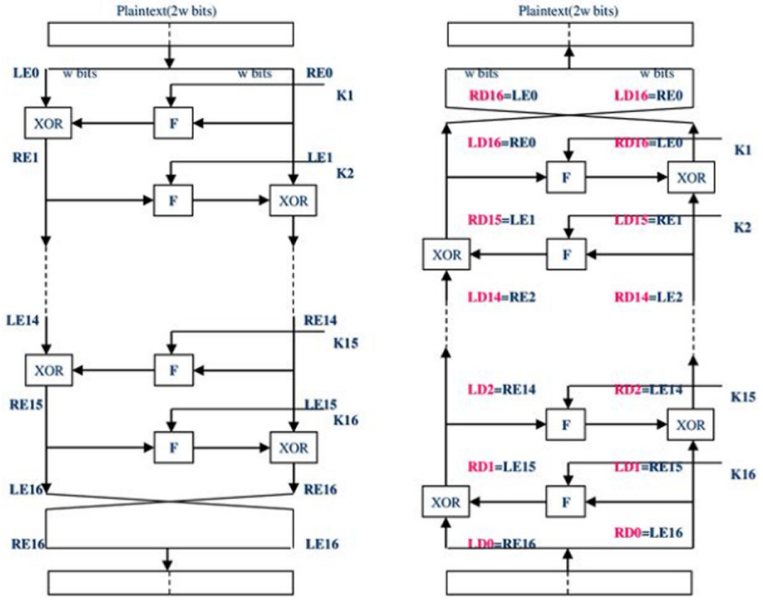

Fig. 1. DES algorithm: (a) encryption data and (b) decryption data

4 Blockchain cryptography

Blockchain has witnessed the most recent developments and potential in financial and inter-organizational transactions in the form of blockchain. To build blockchain-based solutions for their customers, organizations use Blockchain technology to manage cybersecurity, distributed databases, healthcare, and digital transactions [11, 23].

The main advantage of using blockchain technology is that it ensures the transaction security due to its encryption, decentralization, and consensus principles. Sequential block technology uses structured distributed blocks in the blockchain network to store and process data [24]. The whole new block contains a transaction or a set of transactions that is connected to every one of previous blocks by an encryption chain, as illustrated in Figure 2 [25, 26].

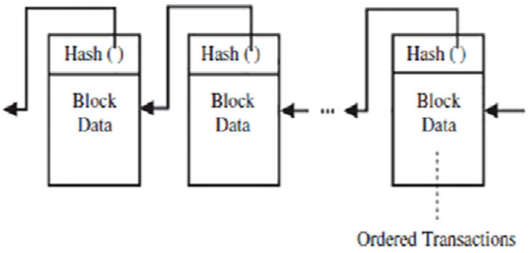

Fig. 2. Block chain implementation

A hash value must be assigned to each block in the blockchain. These blocks are connected by their previous hash. When an attacker attempts to change the data [27, 28], the hash will be changed. It will possess an influence upon the whole series. Consequently, sensitive information or data will be more secure [28, 29]. To establish trust, the blockchain employs cryptography [30, 31]. Cryptography is used to store information on the blockchin on the ledger. Blockchain makes use of some cryptography building blocks, such as public key, private key, and hash function [12, 31–34].

5 Proposed model of image encryption

The proposed model secured the medical image while transferring images from send to receive using the concept of blockchain technology, as well as encryption algorithm. The two phases of this proposal are as follows: in the first phase,the data in the desired file (medical image) is encrypted and decrypted using the DES encryption algorithm and decrypted based on blockchain technology, but the second phase represents the measurement of encryption.

A. Image encryption and decryption phase. The proposed model presents a medical image encryption and decryption. The idea of this proposal is encrypting a digital image (color image) by using circular blockchain technology based on DES algorithm. Data Encryption Standard (DES) is regarded unsafe for numerous uses for several causes. It's principally based upon merely one bit (zero) or (one). Likewise, it utilizes merely single function (XOR), because it doesn't have sufficient arbitrariness as well as being prone to the attacks. As a result, for addressing such problems, in the present section, Blockchain technology will be used for improving the performance of DES encryption while making the algorithm further complicated to attacks. And, this can be done via changing the key generation process of using various keys. For each, a key was created individually. And, the initial key was the input key that's utilized to encrypt and decrypt the first block. The second block was encrypted by a key created from the result of the first round of the first block. On this basis, the process of generating the

keys will continue as mentioned above during the healing process until finishing the process of encrypting the all blocks, as depicted in Figures 3 and 4. The digital image was divided into a number of blocks, and after that, it was encrypted with Eq. (1).

$$\boldsymbol{C}_i = \boldsymbol{P}_i \oplus \boldsymbol{K}_i \tag{1}$$

Where, C_i represents the cipher of image, and denotes the ith original image. As well, K_i is the 56-bit block at iteration i employed for the image of encryption as well as decryption. To return the original image, the image was decrypted by using Eq. (2).

$$\boldsymbol{P}_i = \boldsymbol{C}_i \oplus \boldsymbol{K}_i \tag{2}$$

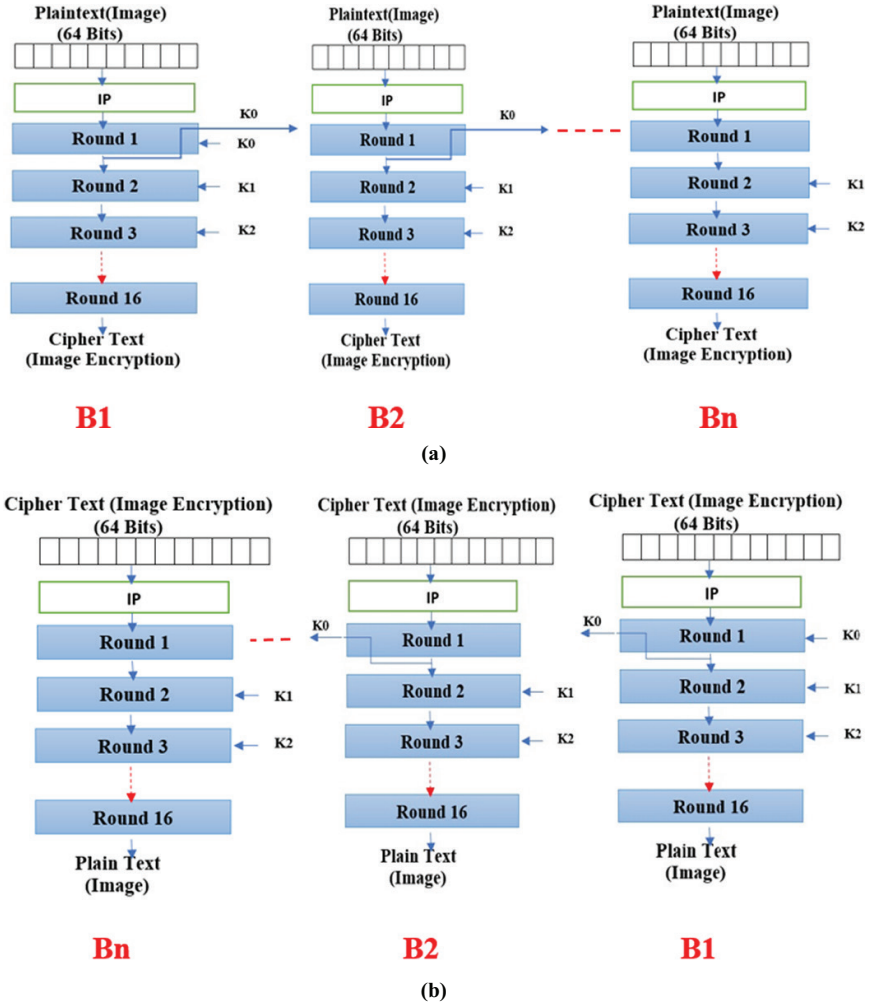

Fig. 3. Modification of the DES algorithm: (a) encryption using block chain based on DES algorithm and (b) decryption using block chain based on DES algorithm decryption

Input: Medical image
Output: Image encryption

Step (1): Begin
Step (2): Read the image (original).
Step (3): Convert into gray image.
Step (3): Split the input into N. of blocks (64 bits), Left (32) as well as Right (32).
Step (4): Create the key (56 bits).
Step (5): For 16 rounds, do the following:
- Each Block (64 bits) divided into 2 part (L, R).
- Encryption operation do by apply Eq. (1) and compute the value of hash function and key for another block encryption (result of 1 round).
Step (6): Repeat the step 5 until the N. blocks are encrypted.
Step (7): Brows the image encryption.
Step 8: End

(a)

Input : Image encryption
Output : Medical image (original)

Step (1): Begin
Step (2): Read the image (Encryption).
Step (3): Split the input into N. of blocks (64 bits).
Step (4): As same key used (56 bits).
Step (5): For 16 rounds, do the following:
-Each Block (64 bits) divided into 2 part (L, R).
-Decryption operation do by apply Eq. (2) and compute the value of hash function and key for another block encryption (result of 1 round).
Step (6): Repeat the step 5 until the N. blocks are decrypted.
Step (7): Brows the Result (image original).
Step (8): End

(b)

Fig. 4. The suggested face encryption algorithm: (a) encryption algorithm and (b) decryption algorithm

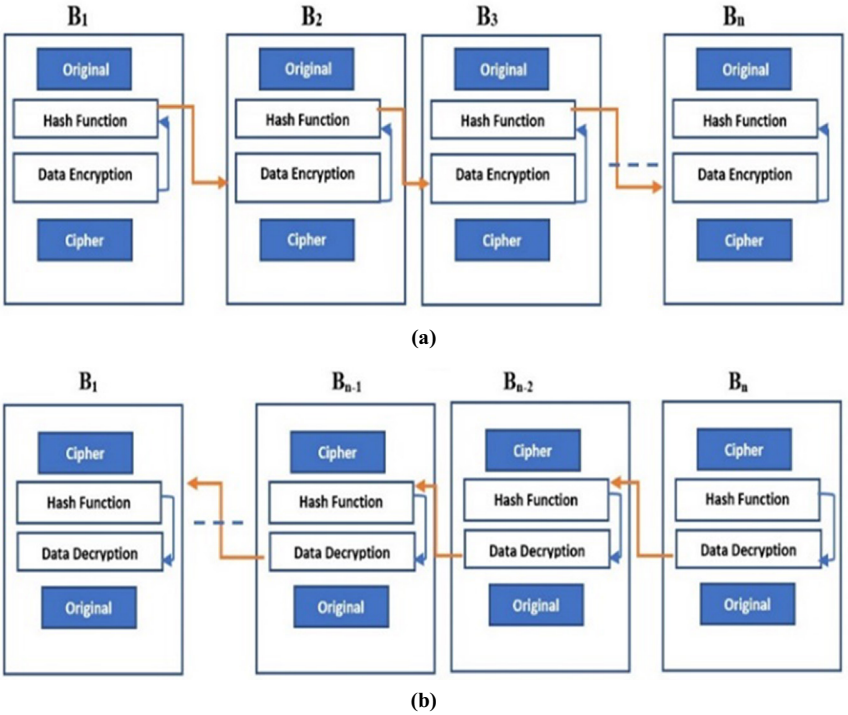

Fig. 5. Hash function authentication: (a) encryption & hash function phase and (b) decryption & hash function phase

And, the encrypted file as manifestoed in Figure 5a was delivered on the receipt end, as well as the hash code was validated. When a hash code match process occurs, it means that no hackers have changed or accessed the data file. Following authentication, the received data file will be decrypted using the same key that was used for encryption, as manifested in Figure 5b.

B. Evaluations of result. Three metrics were used to assess the performance of the decryption operation: Peak signal to noise ratio (PSNR), Entropy, and mean square error (MSE). And, MSE is the ultimate error measure between two images (initial image and encryption image) for encrypted images, whereas the PSNR the cumulative squared error measure between two images. To calculate the PSNR, the mean square error was first computed employing the following equations:

$$MSE = \frac{\sum_{i=0}^{M} \sum_{j=0}^{N} [X_1(i,j) - X_2(i,j)]^2}{M * N} \tag{3}$$

$$PSNR = 10 log_{10} \left(\frac{R^2}{sqrt(MSE)} \right) \tag{4}$$

Entropy is an important test for determining the degree of randomness in information. Equation (5) can be used to calculate the entropy. $P(I_n)$ denotes the probability of the

image, and X represents the image (X_n). For grayscale images, the maximum entropy value is eight.

$$E(X) = -\sum_{n=1}^{256} P_n\ (X_n) log_2 P(X_n) \tag{5}$$

6 Results of experiment and discussion

The proposed method can be used to encrypted any size or type of medical images.

And, as evinced in the Figure 6, the suggested method has been implemented to three different samples (medical images).

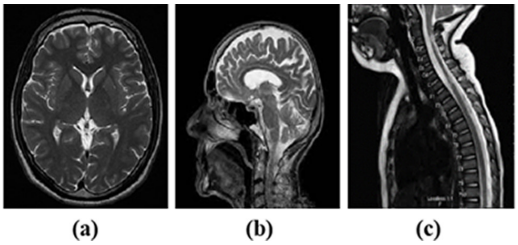

Fig. 6. Original three samples (medical images)

The images histogram is elucidated in Figure 7, and this histogram represents the medical images before and after the encryption (traditional method and proposed model). The histogram of the three sample images, as displayed in Figures 7 and 8, proved that the proposed model presented achieved accurate outcomes after the encryption.

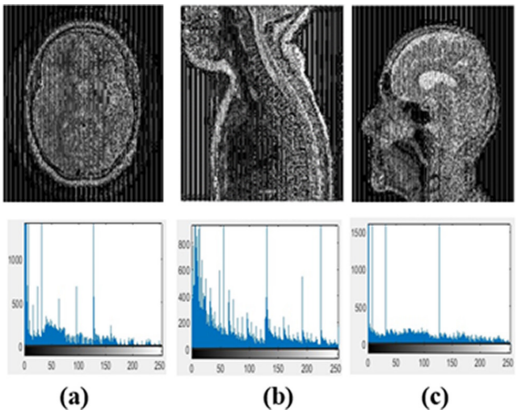

Fig. 7. Histogram of three encryption medical images (traditional method) for samples (a, b, and c)

As exhibited in the Figure 8, the keys were used to encrypt the original image, so, for the first block, the key was generated at a random number, and then after completing the

first round, the output from the first round represented the input (first) key to the second block. This has given strong results in encoding the images, as portrayed in this figure.

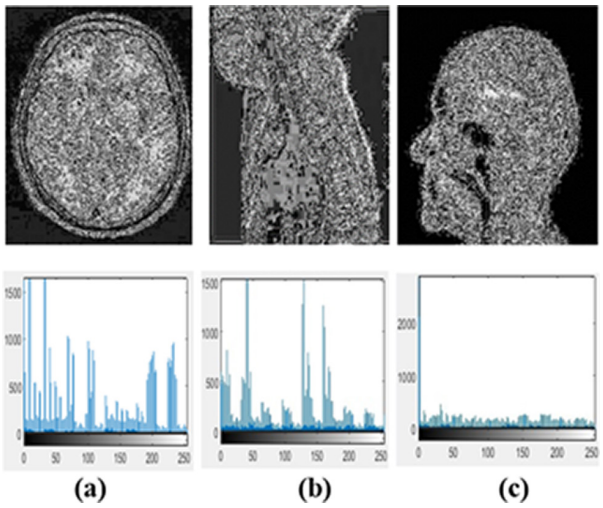

Fig. 8. Histogram of three encryption medical images (proposed model) for samples (a, b, and c)

In the Figure 9, to compare between encrypted medical images, (a) is the image that is encrypted via the traditional DES algorithm which one can recognize, but (b) is the image that is encrypted by the proposed model, when the randomness (keys) being augmented, and the image features are disappeared, as well, it becomes more difficult for identifying the original image.

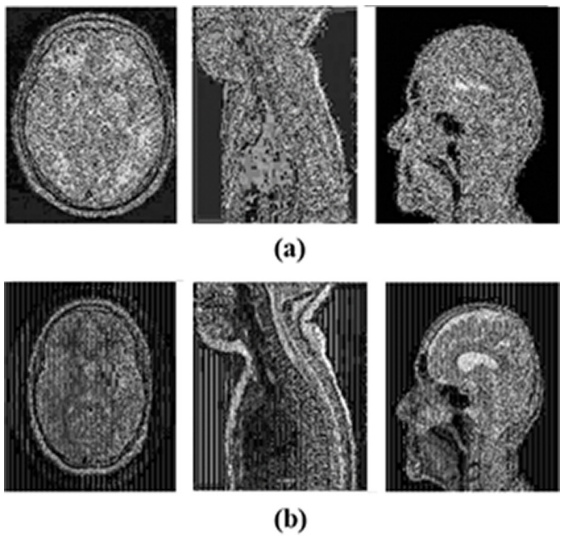

Fig. 9. Comparison of the encryption and decryption for three medical images: (a) traditional algorithm and (b) proposed algorithm

For the original images, encryption images, using the proposed model makes them not possible identify the images and increase the encrypted images' distortion as well as randomness, decrypting the images without losing any information, as demonstrated in Figure 10.

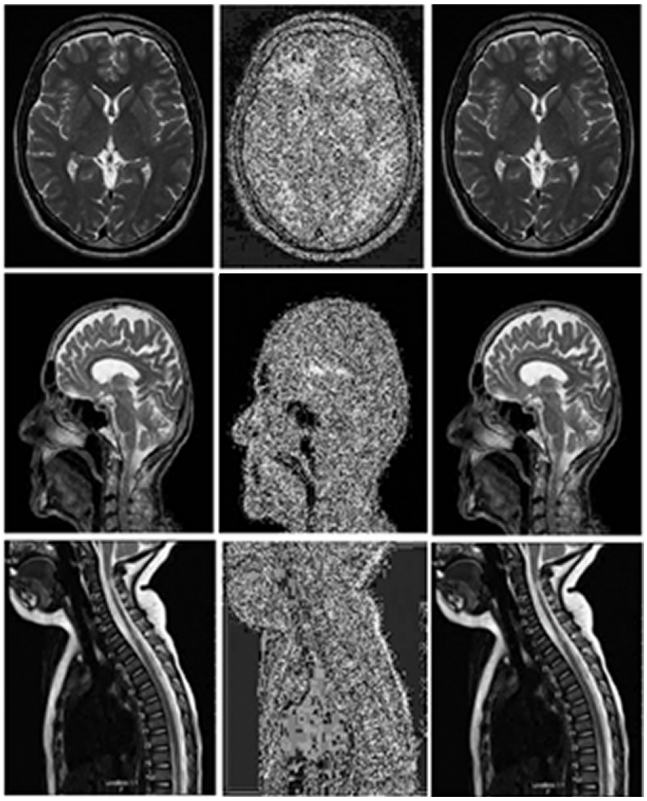

Fig. 10. Images encrypted and decrypted by the proposed model

In this paper, three randomness tests were applied on three samples of medical images, the proposed key generator produced a good robustness and a high security that can be depicted when comparing the result between the traditional method and the proposed model, as evinced in Table 1. The serial, runs, and frequency tests can be noted in Table 1.

Table 1. Three randomness tests for medical images

Test	Traditional (Key)	Proposed (Key)
Serial Test	1.89	1.67
Frequency Test	0.257	0.739
Runs Test	5.398	6.312

Table 2 shows the results of performances from the traditional algorithm and proposed model. The MSE (105.253) value of the encrypted image in the new model increased, but the PSNR (27.885) value of the encrypted image in the new model decreased, when compared with traditional method, and this represents higher error of noise. That's, the quality as well as the noise error is the reason of the increasing of encrypted image distortion in the new model, and the last value in this table is the value of entropy (7.998) that augmented the encrypted image.

Table 2. Values of entropy, PSNR and MSE for encryption images by traditional methods and proposed model

Images	Traditional Method			Proposed Model		
	MSE	**PSNR**	**Entropy**	**MSE**	**PSNR**	**Entropy**
Sample a	89.594	25.392	6.898	104.345	27.880	7.933
Sample b	90.736	23.190	6.659	103.987	27.870	7.965
Sample c	89.939	25.210	7.013	103.675	27.890	7.988

7 Conclusions

This paper aims to ensure the safety of transferred images over networks (large or small networks), because the blockchain technology has the ability to achieve authentication between the sender and the receiver by using the hash function, but in this case, it does not have the ability to provide full protection for these transferred images from hacking or fraud. To protect these images, the process of encrypting them was carried out using one of the encryption algorithms. The DES algorithm is considered strong and effective in encoding texts and also it is possible to use it in the encrypted of digital images. But, after the process of encrypting images, it was shown through the results and measurements that the algorithm does not give high accuracy in encryption due to the lack of the full encryption of the image. This leads to the identification of the image easily, so the blockchain technology was used with the DES algorithm for the purpose of increasing the degree of key strength during the encryption process. From the results obtained during the application of the proposed model in the encoding of images, it was found that the values of Entropy, MSE, PSNR are the best when compared with the old values obtained when applying the traditional algorithm and high accuracy. There is also an obvious discrepancy between the images encrypted employing the traditional algorithm as well as the proposed model for the whole images utilized, as elucidated in the Table 2. According to the proposed method, the problem of the blockchain in terms of protecting transferred image from occupation and hacking has been solved by making the encrypted image in the proposed model more secure than the traditional method.

8 References

[1] P. Nivethini, S. Meena, V. Krithikaa, and G. Prethija, "Data security using blockchain technology," *Int. J. Adv. Netw. & Appl.(IJANA)*, 2019.

[2] T. H. Obaida, A. S. Jamil, and N. F. Hassan, "Improvement of rabbit lightweight stream cipher for image encryption using Lévy flight."

[3] F. Maqsood, M. Ahmed, M. M. Ali, and M. A. Shah, "Cryptography: A comparative analysis for modern techniques," *International Journal of Advanced Computer Science and Applications,* vol. 8, no. 6, 2017. https://doi.org/10.14569/IJACSA.2017.080659

[4] A. H. M. Alaidi, R. a. M. Al_airaji, A. Aljazaery, and S. H. Abbood, "Dark web illegal activities crawling and classifying using data mining techniques," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 10, 2022. https://doi.org/10.3991/ijim.v16i10.30209

[5] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial Internet of Things," *Entropy,* vol. 22, no. 2, p. 175, 2020. https://doi.org/10.3390/e22020175

[6] S. H. Abbood and M. S. Rahim, "DR-LL Gan: Diabetic retinopathy lesions synthesis using generative adversarial network," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28005

[7] H. T. T. Truong, M. Almeida, G. Karame, and C. Soriente, "Towards secure and decentralized sharing of IoT data," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019: IEEE, pp. 176–183. https://doi.org/10.1109/Blockchain.2019.00031

[8] N. Alseelawi and H. T. Hazim, "A novel method of multimodal medical image fusion based on hybrid approach of NSCT and DTCWT," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[9] M. N. M. Bhutta *et al.*, "A survey on blockchain technology: Evolution, architecture and security," *IEEE Access,* vol. 9, pp. 61048–61073, 2021. https://doi.org/10.1109/ACCESS.2021.3072849

[10] F. Gao, "Data encryption algorithm for e-commerce platform based on blockchain technology," *Discrete & Continuous Dynamical Systems – S,* vol. 12, no. 4&5, p. 1457, 2019. https://doi.org/10.3934/dcdss.2019100

[11] H. Alrikabi, "Enhanced data security of communication system using combined encryption and steganography," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[12] I. A. Aljazaery and A. H. M. Alaidi, "Encryption of color image based on DNA strand and exponential factor," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[13] G. N. Nguyen, N. H. Le Viet, M. Elhoseny, K. Shankar, B. Gupta, and A. A. Abd El-Latif, "Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model," *Journal of Parallel and Distributed Computing,* vol. 153, pp. 150–160, 2021. https://doi.org/10.1016/j.jpdc.2021.03.011

[14] R. O. Ogundokun, J. B. Awotunde, E. A. Adeniyi, and F. E. Ayo, "Crypto-Stegno based model for securing medical information on IOMT platform," *Multimedia Tools and Applications,* vol. 80, no. 21, pp. 31705–31727, 2021. https://doi.org/10.1007/s11042-021-11125-2

[15] I. A. Aljazaery and M. R. Aziz, "Combination of hiding and encryption for data security," *International Journal of Interactive Mobile Technologies,* vol. 14, no. 9, pp. 34–47, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[16] M. K. Abdul-Hussein and H. Alrikabi, "Evaluation of the interference's impact of cooperative surveillance systems signals processing for healthcare," *International Journal of Online and Biomedical Engineering (iJOE),* vol. 18, no. 3, pp. 43–59, 2022. https://doi.org/10.3991/ijoe.v18i03.28015

[17] Y. Ranka, J. Bagrecha, K. Gandhi, B. Sarvaria, P. Chawan, and U. Student, "A survey on file storage & retrieval using blockchain technology," *Int Res J Eng Technol,* vol. 5, no. 10, pp. 763–766, 2018.

[18] B. N. Rao, D. Tejaswi, K. A. Varshini, K. P. Shankar, and B. Prasanth, "Design of modified AES algorithm for data security," *International Journal for Technological Research in Engineering,* vol. 4, no. 8, pp. 1289–1292, 2017.

[19] D. Miriam, D. Hephzibah, D. Dahiya, Nitin, and C. Robin, "Secured cyber security algorithm for healthcare system using blockchain technology," *Intelligent Automation and Soft Computing,* vol. 35, no. 2, pp. 1889–1906, 2023. https://doi.org/10.32604/iasc.2023.028850

[20] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," *Cryptography,* vol. 3, no. 1, p. 3, 2019. https://doi.org/10.3390/cryptography3010003

[21] P. Patil, P. Narayankar, D. Narayan, and S. M. Meena, "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Computer Science,* vol. 78, pp. 617–624, 2016. https://doi.org/10.1016/j.procs.2016.02.108

[22] H. Salim and H. T. Hazim, "Secure Chaos of 5G wireless communication system based on IOT applications," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 12, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[23] S. Kandar, D. Chaudhuri, A. Bhattacharjee, and B. C. Dhara, "Image encryption using sequence generated by cyclic group," *Journal of Information Security and Applications,* vol. 44, pp. 117–129, 2019. https://doi.org/10.1016/j.jisa.2018.12.003

[24] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services,* vol. 14, no. 4, pp. 352–375, 2018. https://doi.org/10.1504/IJWGS.2018.095647

[25] A. M. Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," *Cryptography and Network Security,* vol. 16, pp. 1–11, 2017.

[26] B. F. Cruz, K. N. Domingo, F. E. De Guzman, J. B. Cotiangco, and C. B. Hilario, "Expanded 128–bit data encryption standard," *Int. J. Comput. Sci. Mob. Comput,* vol. 68, no. 8, pp. 133–142, 2017.

[27] M. A. Hameed, A. I. Jaber, J. M. Alobaidy, and A. A. Hajer, "Design and simulation DES algorithm of encryption for information security," *American Journal of Engineering Research (AJER),* vol. 7, no. 4, pp. 13–22, 2018.

[28] P. K. Kushwaha, M. Singh, and P. Kumar, "A survey on lightweight block ciphers," *International Journal of Computer Applications,* vol. 96, no. 17, 2014. https://doi.org/10.5120/16883-6923

[29] L. A. Ajao, J. Agajo, E. A. Adedokun, and L. Karngong, "Crypto hash algorithm-based blockchain technology for managing decentralized ledger database in oil and gas industry," *J,* vol. 2, no. 3, pp. 300–325, 2019. https://doi.org/10.3390/j2030021

[30] S. Nuta, J. C. Schuldt, and T. Nishide, "Forward-secure public key encryption without key update from proof-of-stake blockchain," in *International Conference on Cryptology in India*, 2021: Springer, pp. 436–461. https://doi.org/10.1007/978-3-030-92518-5_20

[31] D. D. Salman, R. A. Azeez, and A. M. Hossen, "Key generation from multibiometric system using meerkat algorithm," *Engineering Technology Journal,* vol. 38, no. 3, pp. 115–127, 2020. https://doi.org/10.30684/etj.v38i3B.652

[32] N. H. M. Ali, A. M. S. Rahma, and A. S. Jamil, "Text hiding in color images using the secret key transformation function in GF (2 n)," *Iraqi Journal of Science,* vol. 56, no. 4B, pp. 3240–3245, 2015.
[33] A. S. J. A. Muhammed, and N. F. Hassan, "Partial face encryption based on CAT swarm optimization," presented at the 2nd International Conference on Advances in Engineering Science and Technology, 2022.
[34] A. S. Jamil and A. M. S. Rahma, "Image encryption based on multi-level keys on RC5 algorithm," *International Journal of Interactive Mobile Technologies (iJIM),* vol. 16, no. 17, p. 101, 2022. https://doi.org/10.3991/ijim.v16i17.34335

9 Authors

Assist. Prof. Dr. Abeer Salim Jamil received the MSc. and PhD. in Computer Science from University of Technology, Iraq, 2004 and 2015 respectively. She has around 24 years of teaching experience and 11 years teaching in Cisco Network Academic (CISCO). Her areas of interests are Digital Image Processing, Video Processing, Security, software Engineering, Networking and artificial intelligence applications. She can be contacted at email: abeer.salim@muc.edu.iq.

Prof. Abdul Monem S. Rahma has an extensive background in the field of Cryptography and Information Security. In 1984, he received his PhD in Computer Science from the Loughborough University of Technology in the United Kingdom, and become a professor in Computer Science since 2008. his main work experience involves teaching at Iraqi universities and supervising postgraduate students. Also, he was the Deputy Dean of the Department of Computer Science, University of Technology, Baghdad, Iraq from 2005 to 2013; and then from 2013 to 2015 become the Dean of the department. Now Prof. Rahma the head of the Department of Computer Science, Al-Maarif University College, Iraq. Prof. Rahma published 240 Papers, 4 Books in the field of Computer Science; supervised 41 PhD and 76 M.Sc. He can be contacted at email: monem.rahma@uoa.edu.iq.

Article submitted 2022-12-12. Resubmitted 2023-01-20. Final acceptance 2023-01-23. Final version published as submitted by the authors.