

Proposed Privacy Preservation Technique for Color Medical Images

Walid El-Shafai^{1,2}, Hayam A. Abd El-Hameed³, Noha A. El-Hag⁴, Ashraf A. M. Khalaf³,
Naglaa F. Soliman⁵, Hussah Nasser AlEisa^{6,*} and Fathi E. Abd El-Samie¹

¹Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt

²Security Engineering Laboratory, Department of Computer Science, Prince Sultan University, Riyadh, 11586, Saudi Arabia

³Electrical Communications Engineering Department, Faculty of Engineering, Minia University, Minia, 61111, Egypt

⁴Higher Institute of Commercial Science, Management Information Systems, El-Mahala El-Kobra, Egypt

⁵Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia

⁶Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia

*Corresponding Author: Hussah Nasser AlEisa. Email: haleisa@pnu.edu.sa

Received: 09 April 2022; Accepted: 29 June 2022

Abstract: Nowadays, the security of images or information is very important. This paper introduces a proposed hybrid watermarking and encryption technique for increasing medical image security. First, the secret medical image is encrypted using Advanced Encryption Standard (AES) algorithm. Then, the secret report of the patient is embedded into the encrypted secret medical image with the Least Significant Bit (LSB) watermarking algorithm. After that, the encrypted secret medical image with the secret report is concealed in a cover medical image, using Kekre's Median Codebook Generation (KMCG) algorithm. Afterwards, the stego-image obtained is split into 16 parts. Finally, it is sent to the receiver. We adopt this strategy to send the secret medical image and report over a network securely. The proposed technique is assessed with different encryption quality metrics including Peak Signal-to-Noise Ratio (PSNR), Correlation Coefficient (C_r), Feature Similarity Index Metric (FSIM), and Structural Similarity Index Metric (SSIM). Histogram estimation is used to confirm the matching between the secret medical image before and after transmission. Simulation results demonstrate that the proposed technique achieves good performance with high quality of the received medical image and clear image details in a very short processing time.

Keywords: LSB steganography; AES algorithm; KMCG algorithm

1 Introduction

Authentication in the medical field based on digital images has captured much attention in the recent years. This target can be achieved with image watermarking and image encryption techniques. Communication security mechanisms, such as encryption, and steganography, have been introduced into medical image communication for achieving data security and privacy [1–3]. Encryption techniques are



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

good tools for information security in open networks. However, these tools need general and private keys to recover the original information. In addition, image watermarking can be used for security in the image communication process to detect image tampering, guarantee intellectual property rights, or improve the security of transmitted data. Each modality of medical images has its own characteristics that can be exploited in the security framework, which should be designed to accommodate the challenging open communication channel impairments [4].

For image communication over unsecure networks, both active and passive attacks are encountered [5,6]. These attacks are mainly related to cryptanalysis. As there are advances in cryptography, there are advances in cryptanalysis. Cryptography is mainly related to encrypting and decrypting information, so that the user can store and transmit sensitive information within insecure networks. This information is viable to the public except for the specified recipients. With some leaks about the encryption and decryption algorithms, cryptanalysts try to break the encryption algorithms. Generally, cryptanalysis is the process of analyzing and breaking down the secure communication process adopted for image communication.

Watermarking algorithms can be used for intellectual property protection [7]. A digital watermark, which is the medical report of a medical image, can be embedded into a cover image, and then extracted afterwards to confirm the report authenticity [8]. The proposed technique in this paper hides cipher reports within the medical image with the help of LSB steganography. In addition, the KMCG algorithm [9] is used for image steganography. Steganography is used to hide the medical image with a ciphered medical report into a cover image, which makes it difficult for an observer to figure out where the message is.

The main objective of this work is to present a robust and reliable hybrid multi-level security technique for efficient medical image transmission [10]. Several factors are considered in this paper to achieve the required objective:

- **Quality of the stego-image:** The quality of the stego-image should be maintained by choosing the most suitable domain for the embedding process
- **Payload capacity in the cover image:** The cover image must contain all bits of secret data.
- **Detectability of the secret data:** This technique must prevent detection/recovery by a third party as much as possible.
- **Robustness and security:** They express the ability to preserve secret data in the presence of attempts to remove, discover or degrade it.
- **Constant bit rate:** Watermark should not increase bit rate, at least for applications that have a constant bit rate.
- **Effect on bandwidth:** Secret images should not increase the bandwidth required to transmit the cover image.
- **Fidelity:** High fidelity of the cover image should be maintained even with the embedding process.
- **Perceptual transparency:** The embedded secret image must not affect the quality of the underlying cover image.

This paper is organized as follows. Section 2 introduces some of the existing image security-related works. In Section 3, we present the proposed multi-level security technique. In Section 4, the used datasets and computer specifications are introduced. A discussion of the image quality metrics used to evaluate the proposed technique is introduced in Section 5. The simulation results and discussions are given in Section 6. Finally, Section 7 presents the main conclusions.

2 Related Work

Arunkumar et al. [11] presented a technique for image security, which combines Discrete Wavelet Transforms (DCT), Singular Value Decomposition (SVD), Redundant Integer Wavelet Transform

(RIWT), and chaotic logistic map. The chaotic logistic map used for encryption provides more security for digital images and enhances the technique robustness. Thanki et al. [12] introduced a technique for secure image transmission using watermarking and encryption. The secret patient identity is embedded into the cover medical image for identification and authentication based on SVD and ridgelet transform. Before sending an image to the receiver, Arnold-scrambling-based encryption is employed. Yuvaraja et al. [13] suggested an efficient hiding technique that utilizes fuzzy logic. The construction of fuzzy rules determines the thin and thick edges in both cover and secret images. Then, the wavelet transform is applied to the edge detection results from the cover and secret images. Shanthakumari et al. [14] presented a two-layer data security scheme using LSB image steganography with an elliptic curve encryption algorithm. In this scheme, the data to be hidden is encrypted using the elliptic curve cryptography algorithm, and inserted into a cover media with the LSB inversion algorithm.

Thakur et al. [15] presented a multi-layer medical data security system through watermarking and chaotic encryption. The secret patient report is hidden into the cover medical image for better security, and the chaotic encryption algorithm is applied on the watermarked image. El-Shafai et al. [16] presented an encryption algorithm for transmitting the watermarked medical images. In their algorithm, Electronic Patient Record (EPR) is inserted as a watermark in a cover image to protect the patient information.

Hashim et al. [17] presented a performance evaluation of steganography schemes based on LSB for different image formats. In addition, the paper discussed the importance of the LSB in different image formats. Zhu et al. [18] proposed a grayscale high-definition image encryption scheme based on the AES algorithm. This scheme is based on modifications of the AES to reduce computational complexity. The first modification reduces the number of rounds to one, while the second modification replaces the S-box with a new one to decrease hardware requirements.

3 The Proposed Multi-Level Security Technique

The secret image is encrypted using the AES algorithm on the sender side, as shown in Fig. 1. The secret report is hidden using LSB-based image steganography in this encrypted secret image. Furthermore, the encrypted secret image with the secret report is hidden in the cover medical image, using the KMCG-based image steganography. The stego-image obtained is split into 16 parts, indexed, and sent to the receiver.

On the receiver side shown in Fig. 2, the sub-images are fetched one by one and merged based on their index. First, the encrypted image is obtained from the merged image. Next, by using LSBs, the secret report is extracted from the encrypted medical image. Finally, decryption is performed to extract the secret image. Thus, the receiver obtains the secret report and image from the cover image.

3.1 Encryption Scheme Based on AES

AES-128 encryption algorithm [19] can be divided into three stages, as shown in Fig. 3. The 128-bit initial key is Exclusive-ORed with the 128-bit plaintext in the initial round. Shift rows, sub bytes, mix columns, and add round keys operations are performed on the states in the final round.

- The sub bytes transformation is implemented independently on each byte of the state using a transformation table of size 256 bytes (S-Box).
- The shift rows transformation is a circular shifting on the rows towards the left with distinct bytes.
- The mix columns transformation is performed using a modulo $x^4 + 1$. In the final round, this transformation is not applied.
- The add round key transformation is the final transformation in each round. It is an XOR operation that adds a round key to the state in each iteration.

The AES decryption steps are performed in reverse order as follows:

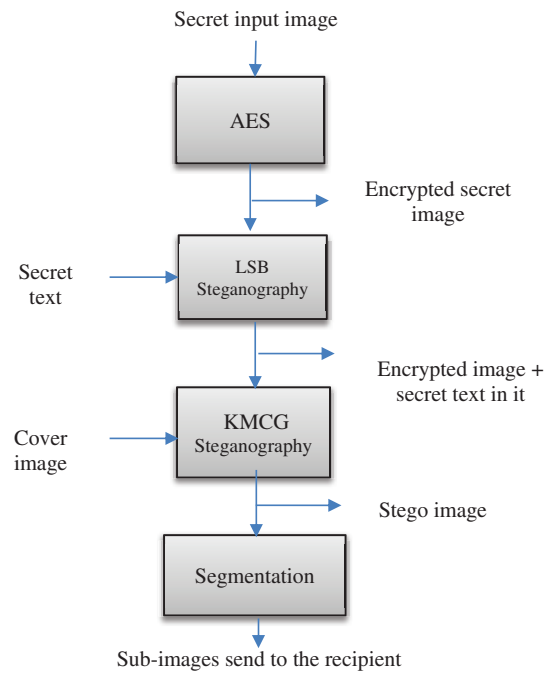


Figure 1: Steps performed by the transmitter

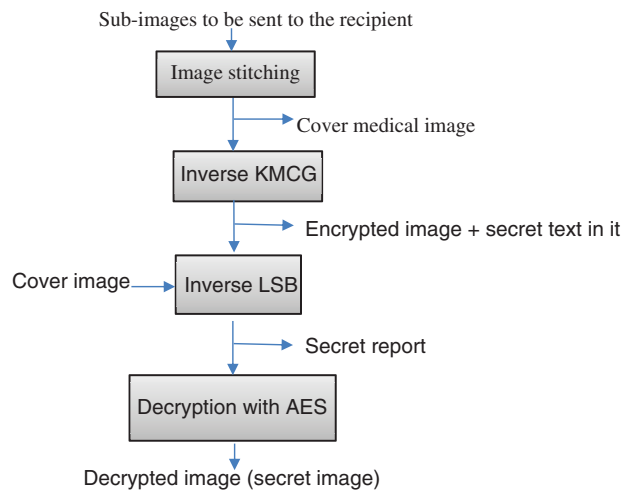


Figure 2: Steps performed by the receiver

- The new inverse S-box table is used to substitute all bytes.
- All rows are shifted circularly right.
- Inverse mix column transformation is implemented.

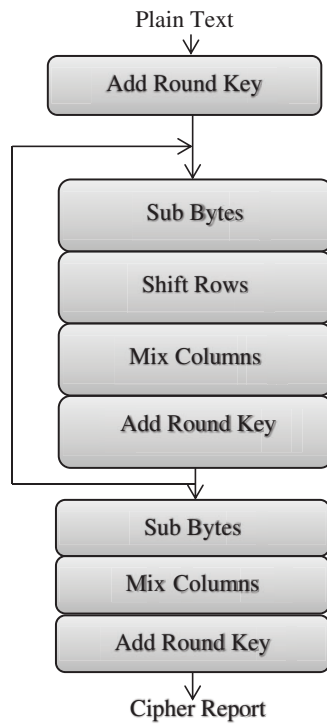


Figure 3: AES encryption steps

3.2 LSB-Based Steganography Scheme

The LSB steganography is simple and easy to implement. It has an important advantage. The original image and the stego image are very similar and can not be observed by human eyes [20]. The LSB steganography comprises an LSB encoder and an LSB decoder as shown in Figs. 4 and 5, respectively.

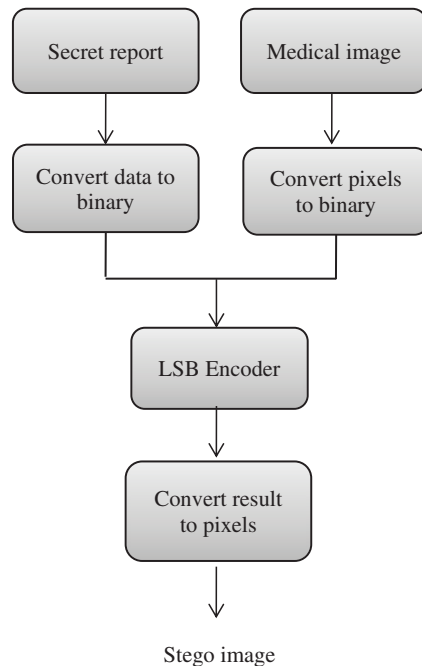


Figure 4: LSB encoder

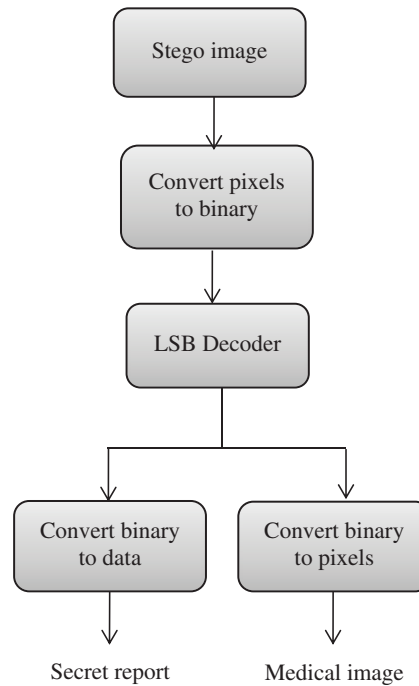


Figure 5: LSB decoder

a) Steps for LSB Encoder:

Step 1: Input the secret message that needs to be hidden.

Step 2: Input the secret medical image.

Step 3: Convert the secret message and the secret medical image to binary numbers.

Step 4: LSB encoder is applied.

Step 5: The stego image is obtained by converting the resultant binary numbers to pixel values.

b) Steps for LSB Decoder:

Step 1: Read stego image.

Step 2: Convert the stego image to binary numbers.

Step 3: LSB decoder is applied to obtain the secret message.

Step 4: The secret message and image are separated.

3.3 Image Steganography Based on KMCG Algorithm

In this step, the KMCG algorithm is implemented for image steganography [8] to hide the secret image in the cover image. In this step, the image is segmented and converted into vectors of a suitable size. The secret image is hidden in the cover image using the KMCG algorithm, and the resulting image is sent over the communication channel.

Steps for the KMCG Algorithm:

Step 1: The image is divided into blocks of size 2×2 pixels.

Step 2: Each row of the image is converted to a vector. These vectors are called the training set.

Step 3: The training set is classified according to the first column, and then divided into two parts.

Step 4: The previous step is repeated on the second column to obtain the median value.

Step 5: The sorting process is replicated until the codebook reaches the desired size.

3.4 Image Segmentation

The final step at the transmitter side is the image segmentation. Image segmentation is the process of dividing an image into multiple segments. The goal of segmentation is to modify the representation of the image to make it hard for the attacker to decode all image parts. The image is segmented into 16 blocks to be transmitted over the communication channel in this step.

3.5 Image Stitching

At the receiver side, all parts of the segmented image are merged to obtain the output cover image that contains a secret image inside it to extract a secret image and secret message from it.

4 Datasets and Computer Specifications

All images were tested on core i3 1.8 GHz-4 GB memory using MATLAB 2019a for all algorithms. The database comprises Magnetic resonance imaging (MRI) normal brain, brain tumor, normal chest X-ray, COVID-19, and retinal images. These images are acquired from some public healthcare datasets [21–24], as shown in Fig. 6.

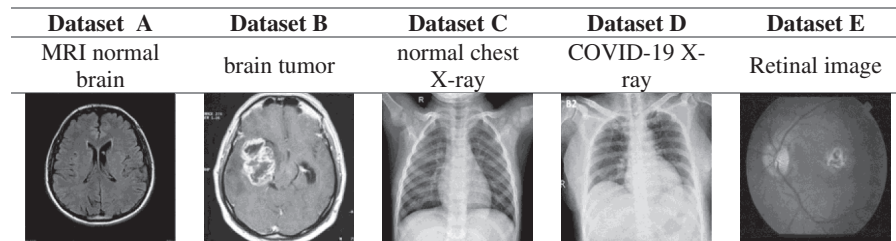


Figure 6: Samples of the used datasets for MRI normal brain, brain tumor, normal chest X-ray, COVID-19 X-ray, and retinal images

5 Evaluation Metrics

5.1 Peak Signal-to-Noise Ratio

It is a quantitative quality metric based on the maximum pixel gray level value, and it is calculated with Eq. (1):

$$PSNR = 10 \log \left(\frac{(f_m)^2}{RMSE^2} \right) \quad (1)$$

where f_m represents the maximum pixel gray level value in the image and $RMSE$ is the root mean square error.

5.2 Correlation Coefficient

The correlation coefficient is one of the best tools to calculate the degree of closeness between two images. The correlation coefficient between the secret encrypted medical image at the transmitter side and the output medical decrypted image at the receiver side is used as a tool for encryption quality evaluation. The low correlation between them reflects the strength of the encryption algorithm. The correlation coefficient is estimated as in Eq. (2):

$$R = \frac{\text{cov}(f(x, y)\Psi(x, y))}{\sqrt{D(f(x, y))} \sqrt{D(\Psi(x, y))}} \quad (2)$$

where

$$\text{cov}(f, \Psi) = \frac{1}{L} \sum_{l=1}^L (f_l(x, y) - E(f(x, y)))(\Psi_l(x, y) - E(\Psi(x, y))) \quad (3)$$

$$D(f(x, y)) = \frac{1}{L} \sum_{l=1}^L (f_l(x, y) - E(f(x, y)))^2 \quad (4)$$

$$E(f(x, y)) = \frac{1}{L} \sum_{l=1}^L f_l(x, y) \quad (5)$$

where $f(x, y)$ and $\Psi(x, y)$ are the gray-scale values of the secret image and the encrypted image, respectively. L is the number of pixels.

5.3 Feature Similarity Index Metric (FSIM)

FSIM is used for image quality assessment. Let f_1 be the recovered secret medical image, f_2 be the secret medical image and their phase congruencies be PC_1 and PC_2 , respectively. The magnitude gradient maps G_1 and G_2 are extracted from images f_1 and f_2 . FSIM can be calculated depending on PC_1 , PC_2 , G_1 , and G_2 , as shown from Eqs. (6) to (8) [25].

The similarity of these two images can be calculated using phase congruency as:

$$S_{PC} = \frac{(2PC_1PC_2 + T_1)}{(PC_1^2 + PC_2^2 + T_1)} \quad (6)$$

where T_1 is a constant. Similarly, the similarity is calculated from magnitude gradient maps G_1 and G_2 as in [25]:

$$S_G = \frac{(2G_1G_2 + T_1)}{(G_1^2 + G_2^2 + T_1)} \quad (7)$$

The similarity S_L between f_1 and f_2 is calculated by combining PC s and G s. It can be defined as in (8):

$$S_L(x) = [S_{PC}(x)]^\alpha \cdot [S_G(x)]^\beta \quad (8)$$

where α and β are the parameters used to adjust the relative importance of PC and G values.

5.4 Structural Similarity Index Metric (SSIM)

The SSIM is a perception-based model that considers image degradation as a perceived change in structural information. The SSIM measure between two windows is [25]:

$$S(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{x,y} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (9)$$

where μ_x is the average of x , μ_y is the average of y , σ_x^2 is the variance of x , σ_y^2 is the variance of y , and $\sigma_{x,y}$ is the covariance of x and y . C_1 and C_2 are two variables, where $C_1 = (K_1L)^2$ and $C_2 = (K_2L)^2$. L is the dynamic range of the pixel values. $K_1 = 0.01$ and $K_2 = 0.03$ by default

5.5 Histogram Evaluation

Histogram acts as a graphical representation of the brightness distribution of an image. The histogram reflects the number of pixels on the vertical axis for a particular brightness in the image.

6 Simulation Results and Discussions

The most important step in this technique is the first step, which is the encryption of the secret medical image to be transmitted, securely. The AES algorithm does the encryption and decryption processes. AES encryption is done in rounds, where we process 16 pixels in each round. The results of image encryption are shown in Fig. 7.

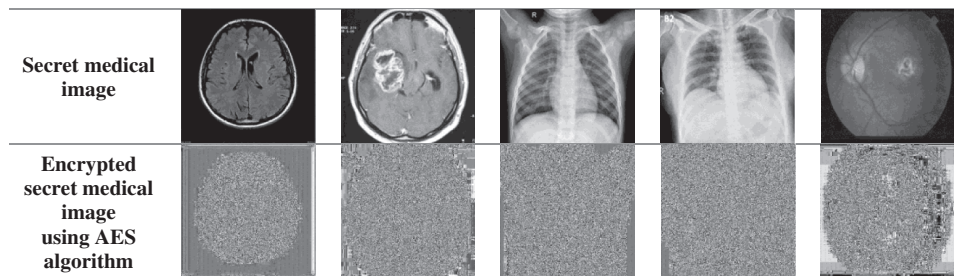


Figure 7: Encrypted secret medical image using AES algorithm

After encrypting the secret image, the LSB-based image steganography is performed to hide the secret message in the secret image. We append a null character with the secret report to denote the end of text. LSB-based image steganography involves hiding data in the LSBs of an image. First, the secret message is converted into its American Standard Code for Information Interchange (ASCII) representation. Then, these ASCII values are converted into their 8-bit binary representation. Finally, the LSBs of the pixel values of the secret image are replaced with these bits in order. Hence, the secret report is successfully hidden inside the secret image. The resulting images are encrypted secret medical images with their secret reports, as shown in Fig. 8. From the obtained results, the encrypted secret medical image after the embedding process of the secret report is quite close to the encrypted secret medical image according to the human perception vision.

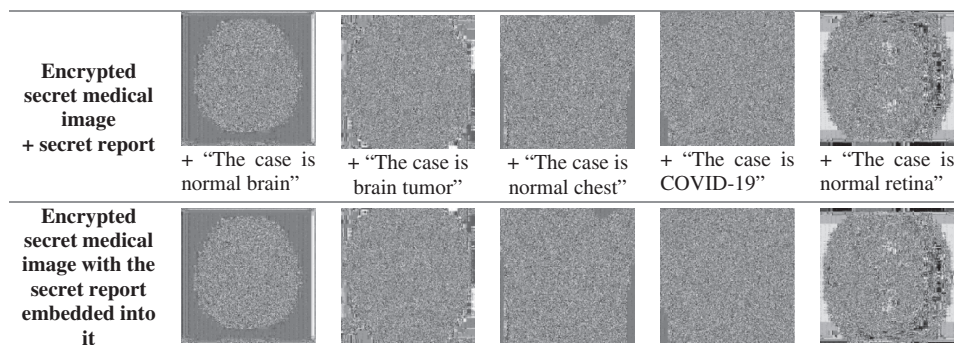


Figure 8: Encrypted secret medical image with the secret report embedded into it

Similar to the method of LSB-based image steganography that involves hiding the secret report into the secret image, the encrypted secret image containing the secret report is hidden inside the cover image using

the same technique. The binary representation of the pixel values of the encrypted image with the secret report in it is hidden first in the red component, followed by the blue and the green components of the cover image, as shown in Fig. 9. Next, we segment the cover image with the ciphered secret medical image and the secret report embedded in it into multiple parts (16 to be specific), as shown in Fig. 10. Each part is then separately sent to the receiver. This segmentation makes it very difficult to obtain the total image, and it makes obtaining the information inside the image difficult.

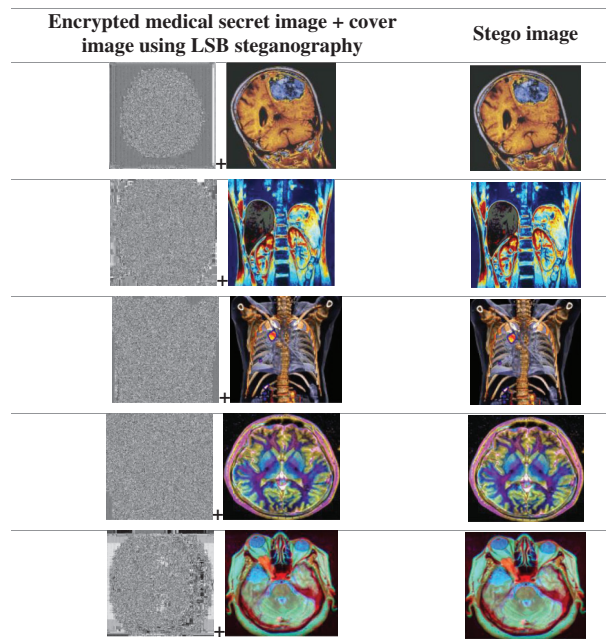


Figure 9: Resulting stego images

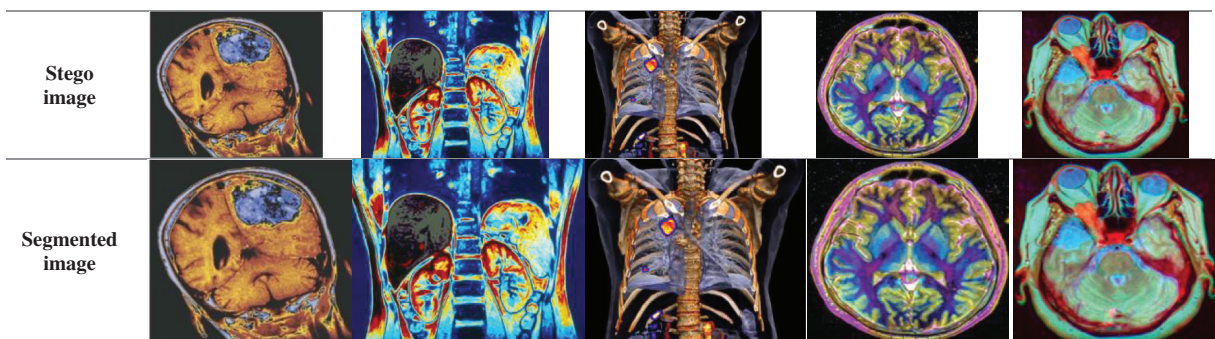


Figure 10: Segmented image for each cover image

The sub-images are stitched back based on their index values (0 to 15) to regain the original cover image at the receiver side. The LSBs of the image components are extracted 8-bits at a time for the entire size of the secret image. Now, we obtain the encrypted secret image with the secret report embedded in it. From this secret image, the LSBs are extricated, 8 bits at once, until we hit a number representing a zero. These 8-bit binary numbers obtained are converted to their decimal representations. These decimal representations represent the ASCII values of the characters. They are then converted back to their character representation to obtain the secret report, as shown in Fig. 11. The process of decryption of secret images

using AES is similar to the encryption process, but its order is reversed. It is described at the beginning of this paper. On repeating the process of AES, we obtain the secret image at the receiver size, as shown in Fig. 11, which gives the output of the extraction process at the receiver side. The decrypted medical images are very clear with excellent visual perception.

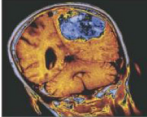
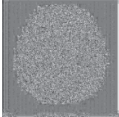
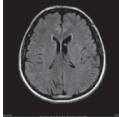
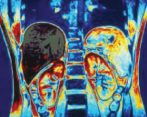
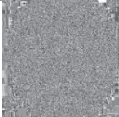
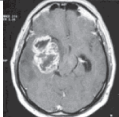
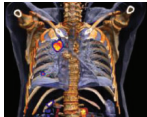


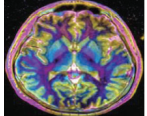


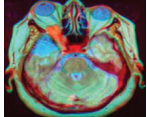
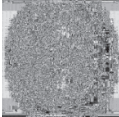
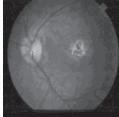
Merged image containing the secret image	Extracted secret image	Extracted report	Decrypted medical image
		“the case is normal brain”	
		“the case is brain tumor”	
		“the case is normal chest”	
		“the case is COVID-19”	
		“the case is normal retinal”	

Figure 11: Output of the extraction process at the receiver output

Tab. 1 tabulates the values of PSNR, C_r , SSIM, and FSIM for the received stego images. They are checked for five types of medical images. As shown from the results, the quality of the extracted image is very good for all images, as PSNR values are large and reasonable to a large extent. The high correlation values reflect the similarity between the cover image with the secret medical image and secret report and the cover image only. The maximum value of C_r is 1. As shown in Tab. 1, all C_r values are close to 1. In addition, it is clear from Tab. 1 that SSIM and FSIM are approximately 1, meaning that the cover image with a secret medical image and without are very close to each other. The difference between the two images is not observed by human eyes. As shown in Fig. 12, the histograms of the cover images with and without embedding are similar.

Table 1: PSNR, C_r , SSIM, and FSIM for the decrypted images at the receiver

Parameter	Normal brain	Brain tumor	Normal chest	COVID-19	Normal retina
PSNR	38.637	36.574	37.265	35.873	32.605
C_r	0.9981	0.9986	0.9986	0.9974	0.9851
SSIM	0.9942	0.9932	0.9936	0.9894	0.9879
FSIM	0.9970	0.9963	0.9947	0.9935	0.9826

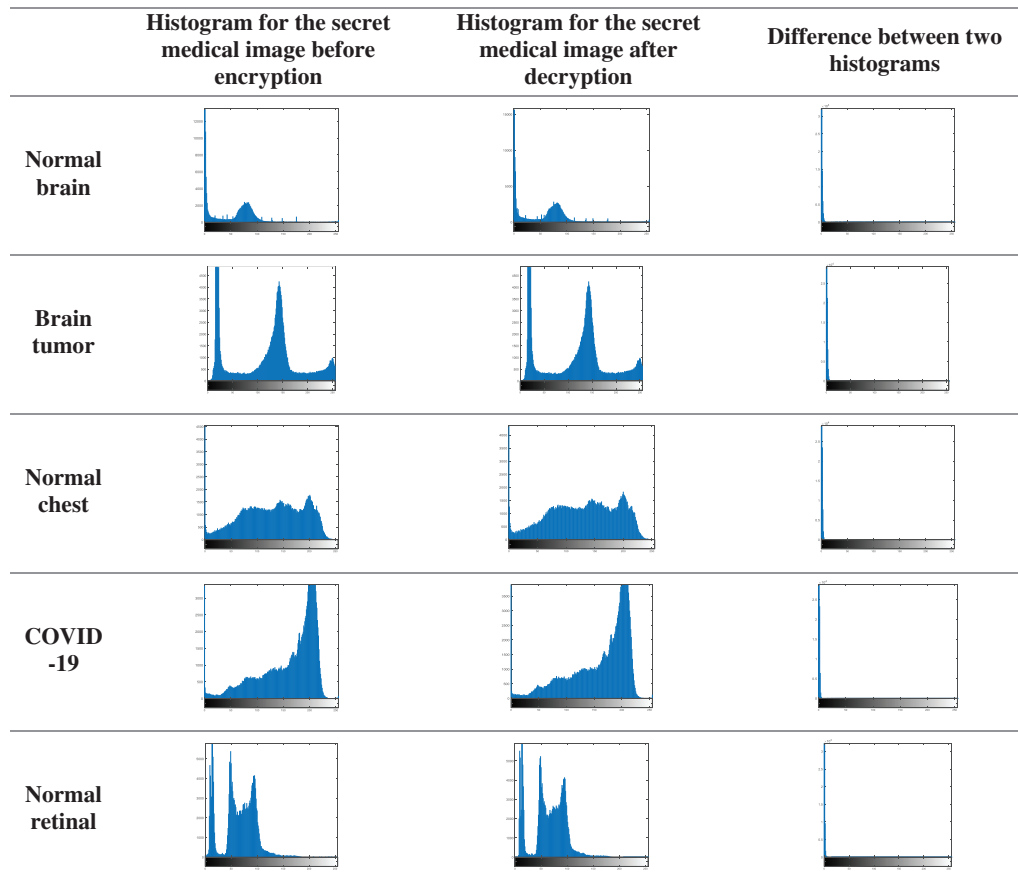


Figure 12: Difference between histograms for the cover medical image before and after embedding

Tab. 2 demonstrates the comparison outcomes between the suggested technique and state-of-the-art schemes [12–16]. The proposed technique achieves higher SSIM and higher C_r than those introduced by Thanki et al. [12], but the latest achieves higher PSNR values than those of the proposed technique. The proposed technique achieves higher PSNR and C_r values than those of Yuvaraja et al. [13], Thakur et al. [15], and El-Shafai et al. [16]. Shanthakumari et al. [14] have higher PSNR values than those of the proposed technique, but SSIM values for the proposed technique are higher than those of Shanthakumari et al. [14].

Table 2: Performance comparison in terms of PSNR, C_r , and SSIM between the proposed technique and the schemes in [12–16]

Schemes	Year	Proposed algorithm	PSNR	C_r	SSIM
Thanki et al. [12]	2021	FRT, SVD	57.3996	0.9641	–
Yuvaraja et al. [13]	2019	DWT + Fuzzy logic	36.1020	–	–
Shanthakumari et al. [14]	2020	ECC + LSB	47.5130	–	0.9579
Thakur et al. [15]	2019	DWT, DCT, SVD + Chaotic encryption	35.5399	0.9980	0.9973
El-Shafai et al. [16]	2019	IWT + Chaotic encryption	35.3101	0.9819	–
Proposed technique	2021	LSB, KMCG + AES	38.6378	0.9981	0.9942

7 Conclusions and Future Work

This paper produced a new algorithm in which AES encryption is combined with LSB steganography to provide a highly secure method for the transmission of each medical image with its report between the sender and the receiver. The AES algorithm is used to encrypt the secret image, and the LSB steganography is used to hide the secret report. The secret image and report are hidden inside the cover medical image using the KMCG algorithm. It becomes difficult for the intruder to get access to the secret medical image or secret report as the cover medical image sent is segmented into 16 parts. All results demonstrate the effectiveness of the algorithm and confirm the extent of its success in our electronic world. Applications of this proposed technique may include financial services (banking), agencies, medical images, hiding passwords and encryption keys, and transporting highly private documents. The proposed technique needs a small processing time. Therefore, it is suitable for image transmission over wireless channels for real-time applications. In the future work, the machine learning algorithms like support vector machines and neural networks can be used for image segmentation. Additionally, in the future, more suggestions related to deep learning can be introduced to enhance the performance of the proposed technique.

Acknowledgement: Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2022R66), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding Statement: Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2022R66), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] A. Alarifi, S. Sankar, T. Altameem, K. Jithin, M. Amoon *et al.*, “A novel hybrid cryptosystem for secure streaming of high efficiency H. 265 compressed videos in IoT multimedia applications,” *IEEE Access*, vol. 8, pp. 128548–128573, 2020.
- [2] O. Faragallah, H. El-sayed, A. Afifi and W. El-Shafai, “Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform,” *Optics and Lasers in Engineering*, vol. 137, pp. 1–15, 2021.
- [3] A. Alarifi, M. Amoon, M. Aly and W. El-Shafai, “Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system,” *IEEE Access*, vol. 8, pp. 221246–221268, 2020.
- [4] O. Faragallah, M. Alzain, H. El-Sayed, J. Al-Amri, W. El-Shafai *et al.*, “Block-based optical color image encryption based on double random phase encoding,” *IEEE Access*, vol. 7, pp. 4184–4194, 2018.
- [5] K. Al-Afandy, W. El-Shafai, E. El-Rabaie, F. Abd El-Samie, O. Faragallah *et al.*, “Robust hybrid watermarking techniques for different color imaging systems,” *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25709–25759, 2018.
- [6] W. El-Shafai, S. El-Rabaie, M. El-Halawany and F. Abd El-Samie, “Security of 3D-HEVC transmission based on fusion and watermarking techniques,” *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 27211–27244, 2019.
- [7] W. El-Shafai, S. El-Rabaie, M. El-Halawany and F. Abd El-Samie, “Efficient hybrid watermarking schemes for robust and secure 3D-MVC communication,” *International Journal of Communication Systems*, vol. 31, no. 4, pp. 1–23, 2018.
- [8] O. Faragallah, M. AlZain, H. El-Sayed, J. Al-Amri, W. El-Shafai *et al.*, “Secure color image cryptosystem based on chaotic logistic in the FrFT domain,” *Multimedia Tools and Applications*, vol. 79, no. 3, pp. 2495–2519, 2020.
- [9] O. Faragallah, A. Afifi, W. El-Shafai, H. El-Sayed, E. Naeem *et al.*, “Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications,” *IEEE Access*, vol. 8, pp. 42491–42503, 2020.
- [10] A. Mahmoud, W. El-Shafai, T. Taha, S. El-Rabaie, O. Zahran *et al.*, “A statistical framework for breast tumor classification from ultrasonic images,” *Multimedia Tools and Applications*, vol. 80, no. 4, pp. 5977–5996, 2021.

- [11] S. Arunkumar, V. Subramaniaswamy, V. Vijayakumar and R. Logesh, "SVD-Based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images," *Measurement*, vol. 139, no. 3, pp. 426–437, 2019.
- [12] R. Thanki and A. Kothari, "Multi-level security of medical images based on encryption and watermarking for telemedicine applications," *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 4307–4325, 2021.
- [13] T. Yuvaraja and R. Sabeenian, "Performance analysis of medical image security using steganography based on fuzzy logic," *Cluster Computing*, vol. 22, no. 2, pp. 3285–3291, 2019.
- [14] R. Shanthakumari and S. Malliga, "Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography algorithm," *Multimedia Tools and Applications*, vol. 79, no. 5, pp. 3975–3991, 2020.
- [15] S. Thakur, A. Singh, S. Ghrera and M. Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3457–3470, 2019.
- [16] W. El-Shafai, E. El-Rabaie, M. El-Halawany and F. Abd El-Samie, "Efficient multi-level security for robust 3D color-plus-depth HEVC," *Multimedia Tools and Applications*, vol. 77, no. 23, pp. 30911–30937, 2018.
- [17] M. Hashim, M. Rahim, F. Johi, M. Taha and H. Hamad, "Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats," *International Journal of Engineering & Technology*, vol. 7, no. 4, pp. 3505–3514, 2018.
- [18] X. Zhu, H. Liu, Y. Liang and J. Wu, "Image encryption based on kronecker product over finite fields and DNA operation," *Optik*, vol. 224, no. 2, pp. 164–175, 2020.
- [19] W. El-Shafai, S. El-Rabaie, M. El-Halawany and F. Abd El-Samie, "Encoder-independent decoder-dependent depth-assisted error concealment algorithm for wireless 3D video communication," *Multimedia Tools and Applications*, vol. 77, no. 11, pp. 13145–13172, 2018.
- [20] W. El-Shafai, "Pixel-level matching based multi-hypothesis error concealment modes for wireless 3D H. 264/MVC communication," *3D Research*, vol. 6, no. 3, pp. 1–11, 2015.
- [21] A. Algarni, G. El Banby, S. Ismail, W. El-Shafai, F. El-Samie *et al.*, "Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security application," *Entropy*, vol. 22, no. 12, pp. 1–24, 2020.
- [22] S. Ibrahim, M. Egila, H. Shawky, M. Elsaid, W. El-Shafa *et al.*, "Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption," *Multimedia Tools and Applications*, vol. 5, pp. 1–26, 2020.
- [23] N. Soliman, M. Khalil, A. Algarni, S. Ismail, R. Marzouk *et al.*, "Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication," *Multimedia Tools and Applications*, vol. 7, pp. 1–35, 2020.
- [24] W. El-Shafai, F. Mohamed, H. Elkamchouchi, M. Abd-Elnaby and A. ElShafee, "Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm," *IEEE Access*, vol. 9, pp. 1–25, 2021.
- [25] W. El-Shafai, I. Almomani and A. Alkhayer, "Optical bit-plane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication," *IEEE Access*, vol. 9, pp. 35004–35026, 2021.