Computers, Materials & Continua
DOI:10.32604/cmc.2022.020454
Article

Tech Science Press

A Fractional Fourier Based Medical Image Authentication Approach

Fayez Alqahtani[1,*], Mohammed Amoon[2,3] and Walid El-Shafai[4]

[1]Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, 11451, Saudi Arabia
[2]Department of Computer Science, Community College, King Saud University, Riyadh, 11437, Saudi Arabia
[3]Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt
[4]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt
[*]Corresponding Author: Fayez Alqahtani. Email: fhalqahtani@ksu.edu.sa
Received: 25 May 2021; Accepted: 27 June 2021

Abstract: Patient medical information in all forms is crucial to keep private and secure, particularly when medical data communication occurs through insecure channels. Therefore, there is a bad need for protecting and securing the color medical images against impostors and invaders. In this paper, an optical medical image security approach is introduced. It is based on the optical bit-plane Jigsaw Transform (JT) and Fractional Fourier Transform (FFT). Different kernels with a lone lens and a single arbitrary phase code are exploited in this security approach. A preceding bit-plane scrambling process is conducted on the input color medical images prior to the JT and FFT processes to accomplish a tremendous level of robustness and security. To confirm the efficiency of the suggested security approach for secure color medical image communication, various assessments on different color medical images are examined based on different statistical security metrics. Furthermore, a comparative analysis is introduced between the suggested security approach and other conventional cryptography protocols. The simulation outcomes acquired for performance assessment demonstrate that the suggested security approach is highly secure. It has excellent encryption/decryption performance and superior security results compared to conventional cryptography approaches with achieving recommended values of average entropy and correlation coefficient of 7.63 and 0.0103 for encrypted images.

Keywords: Medical image security; encryption; JT; FFT; cryptosystem

1 Introduction

Nowadays, most of the activities in our lives are significantly dependent on communication and transmission over wired and wireless infrastructures. The transmitted digital data comprises text, image, audio, video, etc., which is named multimedia data. One of the most critical multimedia contents that carry necessary information is digital images used in various and valuable applications such as medical science, telemedicine, and healthcare systems [1–3]. With time, it has become easier to intercept medical information, unauthorized access, misuse of the data, plagiarism, etc. This malpractice cannot be done with an excellent digital signature scheme.

The development of the Internet of Medical Things (IoMT) brought about monumental changes to facilitate disease management, improve diagnostic diseases and treatment methods, and reduce medical costs and errors. However, due to the wide range of IoMT providers and products on the market and the large number of devices that wirelessly transfer sensitive medical data to the cloud, the IoMT is not immune to security and privacy breaches [4,5]. The lack of safety knowledge among healthcare users, such as patients and healthcare workers, compounds the deficiencies and can encourage attackers that threaten patient lives. Therefore, the protection and privacy of the IoMT is a critical issue that needs to be further researched and resolved [6]. Nonetheless, safety evaluation presents problems when choosing appropriate and reliable safety measures for inexperienced IoMT adopters.

IoMT suffers from a variety of difficulties, including the lack of protection and privacy controls. So, we should also highlight the importance of implementing the necessary safety measures to improve IoMT immunity from cyber-attacks. Thus, IoMT security and privacy and intelligent current security solutions are required [7]. The security measures for IoMT show a trade-off between the level of security and the efficiency of the system [8,9].

The deficiency of critical protection and security could cause numerous attacks and threats to severe disasters for networks and people. The health and management of IoMT are therefore becoming more and more critical. An authentication and data encryption process must protect a wireless network for the transmission of medical data. In IoT data security systems, the data is encrypted and encoded with a secret key before being transmitted across the network. After that, the specialist recovers secure data with a digital signature and access information [10,11]. So, due to the importance of medical data security, this paper describes a robust way of managing and securing color medical image communication for achieving reliable protection against cyber-attacks in IoT applications.

Thus, to transmit critical information such as medical images in healthcare applications, it is urgent to preclude the medical images from the risks of attacks and threats by employing effective cryptography techniques. Initially, some standard encryption techniques are used to secure textual information, like Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), and International Data Encryption Algorithm (IDEA) [12–14]. However, these techniques have nevertheless been discovered to be inappropriate for efficient image communication due to their underlying characteristics like an enormous number of iterations, high pixel redundancy, strong correlation, and big-time order. So, they minimize inclusive security performance.

The related conventional and previous security protocols have critical challenges. Thus, this inspired us to design an effective color medical image security protocol based on the JT transform and optical FFT encryption to cipher the transmitted color medical images. The proposed security protocol is far more secure from cryptanalytic attacks because of its higher permutation and diffusion features than traditional security protocols. Thence, the main contributions of this work are as follows:

a) Employing different multi-stage operations for performing an efficient encryption process rather than one operation as used in most of the literature security protocols.

b) Introducing significant attainment for the estimated entropy values for all tested color medical images, where the entropy metric is considered the primary and considerable metric for any encryption process.
c) Investigating comprehensive simulation results with different color medical images to prove its superior performance.
d) Considering the noise effect with different types to efficiently evaluate the encryption/decryption efficacy.
e) The proposed cryptosystem presents lower processing time which can be significantly recommended for real-time IoMT services.
f) Investigating the performance against more attacks and introduced robust results.
g) The proposed cryptosystem encompasses both diffusion and permutation processes.
h) The proposed cryptosystem is compared to more related works to prove its performance efficiency.

The remainder of this paper is structured as follows. Section 2 offers some related studies of recent security protocols. Section 3 presents a detailed explanation of the suggested security protocol for the secure transmission of medical images. The simulation outcomes and comparative analysis are delivered in Section 4. Section 5 concludes the works and offers some future directions.

2 Related Work

The present tendency of medical information and medical image communication over the wireless and wired networks is highly increased, especially in the recent trends of IoMT services. Thence, security plays a crucial role in the transmission of medical data via the Internet network. It is recently vital to safeguard medical data in telehealth services [15–18]. Gupta et al. [19] proposed a medical image security technique that utilizes a chaotic logistic map. Usman et al. [20] presented a steganography scheme for digital image hiding to secure its medical information content to achieve a high-level imperceptibility and clearness.

In [21], a comparative analysis between two medical image cryptography approaches of the chaos theory and elliptic curve cryptography is introduced. In [22], a hybrid system of ciphering and reversible steganography algorithms is introduced to accomplish medical image security with high performance and robustness. In [23], a hybrid security protocol of the DWT and JPEG2000 techniques is proposed for partial cryptography of medical data with low computational complexity and high ciphering performance. In [24], the authors proposed a robust chaotic logistic-based cryptosystem for efficient medical data transmission.

In [25], a real-time and robust medical cryptosystem for IoMT healthcare applications is presented. In [26], the authors suggested a chaotic sequence-based medical image cryptosystem for key generation. After that, a random two rounds-based diffusion process is utilized to produce the ciphered medical image. In [27], the authors described a new medical image security protocol based on logistic and Chebyshev maps to improve the cryptography performance. In [28], a partial medical image cryptosystem is introduced based on a hybrid of DNA encoding and chaotic map encryption.

In [29], the authors developed various medical image cryptosystems. These cryptosystems can be employed for any form of multimedia data. In [30], a cellular automata-based medical image cryptosystem is introduced based on chaos cryptography concepts. This cryptosystem achieved high security and fast performance. In [31], the authors investigated a robust security protocol for medical images. The main merit of this security protocol is that it mitigated many types of communication attacks. In [32], the authors introduced both stream-cipher-based and block-cipher-based medical image cryptosystems. These cryptosystems exceedingly provide good encryption and integrity control to secure the transmission of medical data. In [33], the authors proposed an efficient ROI-based medical color image cryptosystem. It is robust against different forms of cyber-attacks.

Further research works are investigated in the literature that can be developed for medical image security protocols [34–39]. In [34], an optical security protocol based on Fourier analysis, RSA, projection profilometry algorithms is introduced. In [35], the authors developed a user-defined key-based digital image cryptosystem. This cryptosystem split the input image into a different number of shares that are ciphered with unique keys. The authors in [36] suggested a color image cryptosystem based on a selective DRPE algorithm. A secret key based on the FFT transform is introduced to achieve further security performance in the proposed approach.

In [37], the authors developed a hybrid encryption-compression system for efficient security and storing digital images. In [38], the authors introduced an LSB-based concealing algorithm for digital images. It conceals four digital images within a single medical image to create the stego image. After that, this resulting stego image is ciphered based on an optical cipher-based cryptosystem. In [39], the authors developed a salient ROI-based image cryptosystem to encrypt the digital images with different optical-based chaos maps.

Considering the deficiencies of the previous traditional security protocols in the literature, a cost-effective optical medical image security protocol based on the optical JT and FFT algorithms is presented in this paper for telehealth services. The color components of the medical image are separated into bit-planes. After that, an optical random shifting-based JT algorithm is employed on the resulting bit-planes of the medical image components. Then, an optical FFT-based diffusion process is performed on the image components resulted from the prior stage to generate the final ciphered medical image.

3 Proposed Optical Color Medical Image Cryptography Approach

The proposed optical security protocol composes two phases of ciphering and deciphering, as indicated in Figs. 1a and 1b. The detailed steps of the ciphering phase demonstrated in Fig. 1a are as follows:

1) The input color medical image $f(k, l)$ is divided into R, G, and B components $f_R(k, l)$, $f_G(k, l)$, and $f_B(k, l)$

$$f(k, l) = [f_R(k, l), f_G(k, l), f_B(k, l)] \tag{1}$$

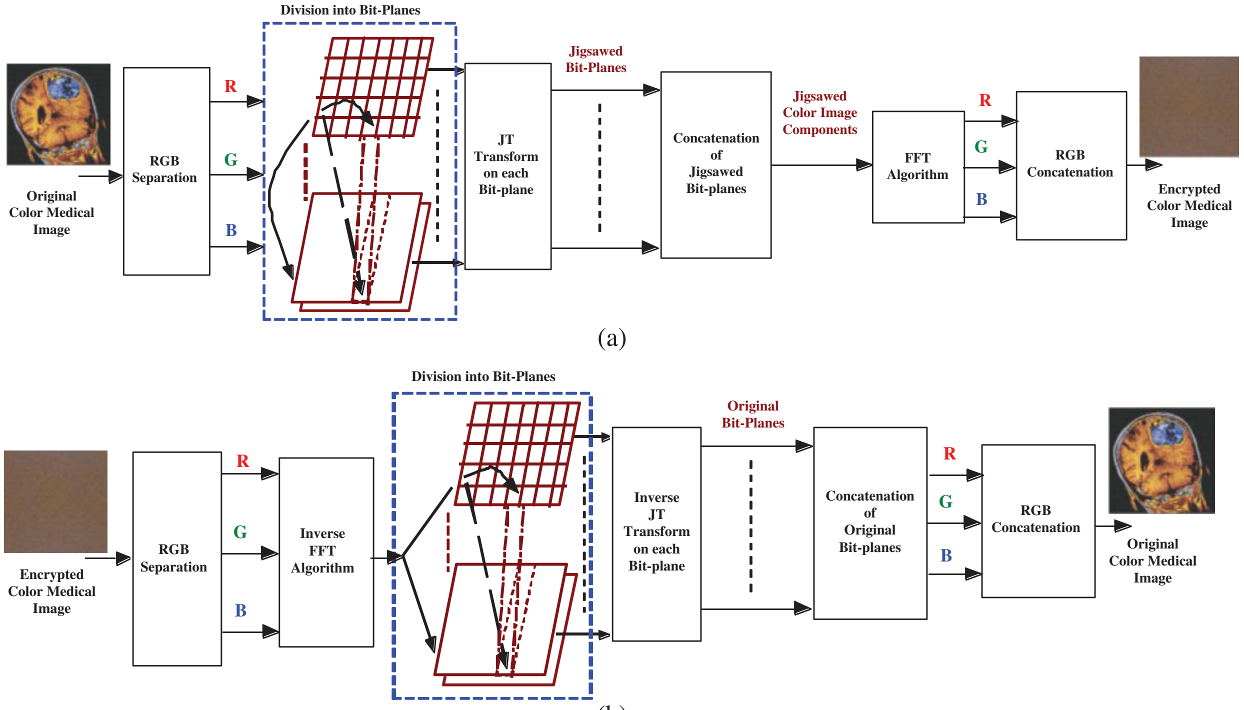
2) Each element of the three R, G, and B components of the input color medical image is separated into different bit-planes.

$$f_R(k, l) = \left[f_{R_1}(k, l), \ldots, f_{R_i}(k, l)\right] \tag{2}$$

$$f_G(k, l) = \left[f_{G_1}(k, l), \ldots, f_{G_i}(k, l)\right] \tag{3}$$

$$f_B(k, l) = \left[f_{B_1}(k, l), \ldots, f_{B_i}(k, l)\right] \tag{4}$$

3) Every separated bit-plane $f_i(k, l)$ of the three R, G, and B components is subject to the Jigsaw transform.



(a)

(b)

Figure 1: Proposed optical color medical image security protocol (a) Ciphering phase and (b) Deciphering phase

$$JT\left[f_R(k,l)\right] = \left[JT\left[f_{R_1}(k,l)\right], \ldots, JT\left[f_{R_i}(k,l)\right]\right] \tag{5}$$

$$JT\left[f_G(k,l)\right] = \left[JT\left[f_{G_1}(k,l)\right], \ldots, JT\left[f_{G_i}(k,l)\right]\right] \tag{6}$$

$$JT\left[f_B(k,l)\right] = \left[JT\left[f_{B_1}(k,l)\right], \ldots, JT\left[f_{B_i}(k,l)\right]\right] \tag{7}$$

4) The obtained Jigsaw transformed bit-planes of each element of the three R, G, and B components are combined to produce one transformed component of the R, G, and B components $Z_R(k,l)$, $Z_G(k,l)$, and $Z_B(k,l)$.

$$Z_R(k,l) = JT\left[f_R(k,l)\right] \tag{8}$$

$$Z_G(k,l) = JT\left[f_G(k,l)\right] \tag{9}$$

$$Z_B(k,l) = JT\left[f_B(k,l)\right] \tag{10}$$

5) The acquired Jigsaw transformed R, G, and B components are additionally scrambled with the optical FFT algorithm with a fractional order of (ϕ_1, ϕ_2) to obtain the final scrambled R, G, and B components $S_R(k,l)$, $S_G(k,l)$, and $S_B(k,l)$.

$$S_R(k,l) = FFT_{(\phi_1,\phi_2)}\left[Z_R(k,l)\right] \tag{11}$$

$$S_G(k,l) = FFT_{(\phi_1,\phi_2)}\left[Z_G(k,l)\right] \tag{12}$$

$$S_B(k,l) = FFT_{(\phi_1,\phi_2)}\left[Z_B(k,l)\right] \tag{13}$$

6) Concatenate the final scrambled R, G, and B components to get the final scrambled color medical image $S(k, l)$.

$$S(k, l) = [S_R(k, l), S_G(k, l), S_B(k, l)] \tag{14}$$

7) Transmit the final ciphered color medical image through a noisy communication medium.

The detailed steps of the deciphering phase are the opposite of the ciphering steps mentioned above, as exhibited in Fig. 1b. The profit from employing the optical FFT algorithm is that it meaningfully enhances the security and robustness of the suggested security protocol by exploiting the advantage of the fractional orders of the secret keys of the FFT transform. Thus, the optical FFT algorithm is exceedingly advised to efficiently transmit medical images through an insecure medium in telehealth applications. For comprehensive details about the optical FFT algorithm are discovered in [40,41].

4 Results and Discussions

Various medical images in color formats with distinct characteristics are selected and investigated in the simulation work to entirely substantiate the benefits of the suggested optical security protocol. Firstly, the examined medical images are divided into their color components (R, G, and B) to be utilized as the input of the proposed security protocol. The employed color medical images and their separated R, G, and B components are exhibited in Fig. 2.

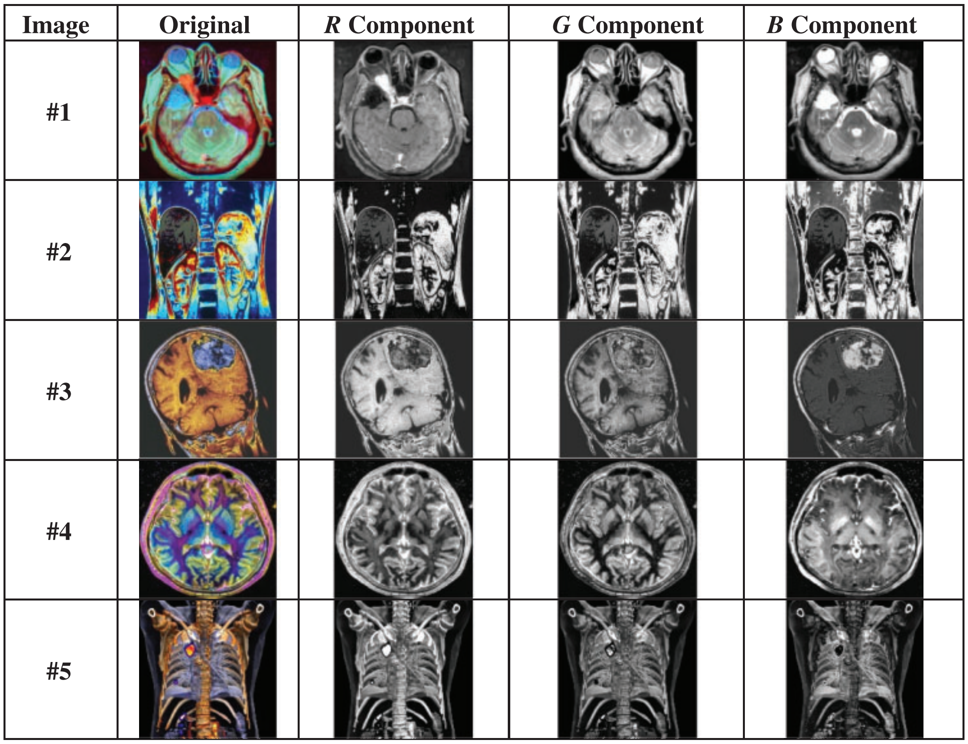


Figure 2: Examined color medical images and their RGB components

The security protocol performance is examined utilizing a laptop with i7-5000 Intel CPU and 8 GB RAM. The MATLAB R2020b is used as the execution software for performing the simulation experiments. The performance investigation of the proposed security protocol is validated through visual analysis [5], histogram security analysis [13], entropy security analysis [15], correlation security analysis [17], quality security analysis [39], differential security analysis [10,30], edge security analysis [24], key sensitivity security analysis [14], noise effect analysis [16,33], occlusion security analysis [4], and computational cost analysis [25]. Furthermore, a comprehensive comparative analysis with the recent related works is investigated.

The encryption and decryption outcomes of the examined color medical images and their encrypted *R*, *G*, and *B* components are presented in Fig. 3. These results prove the high efficacy of the ciphering and deciphering performance of the proposed optical security protocol. It is observed that all details and significant objects on the medical images are hidden using the proposed security protocol. Also, the proposed security protocol can recover the decrypted images with an appreciated performance that is completely similar to the original color medical images.

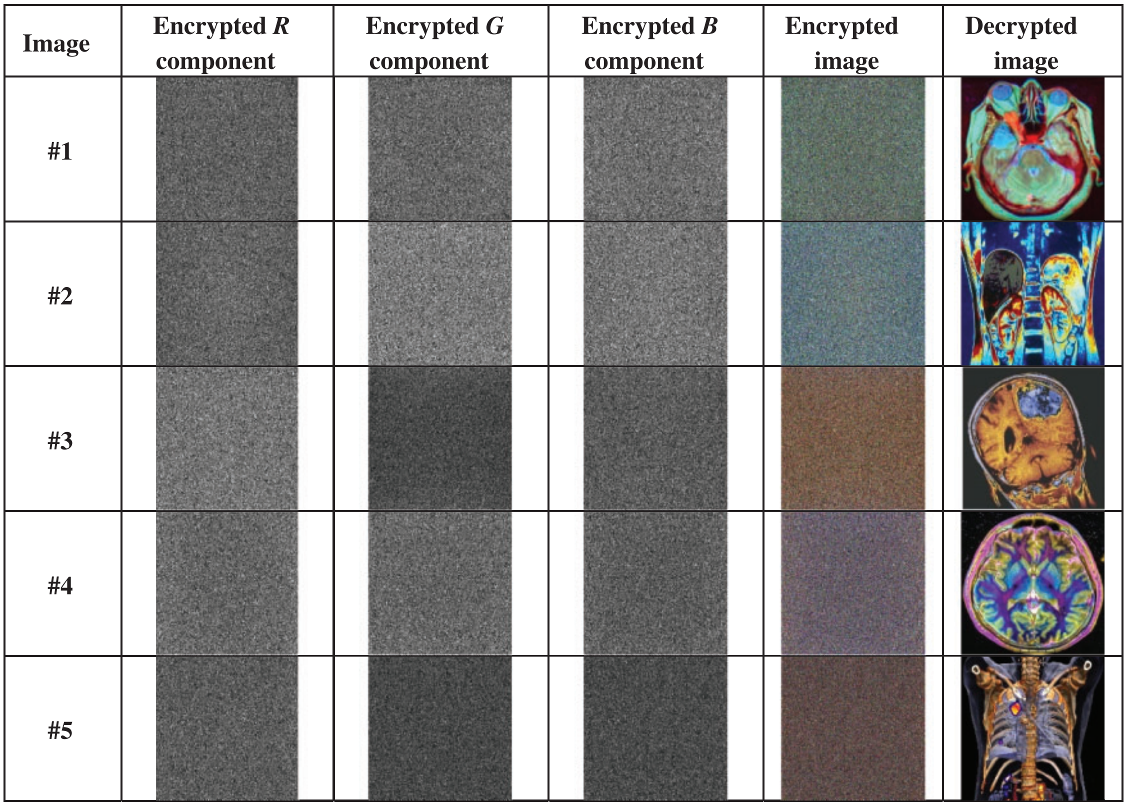


Figure 3: Encrypted color medical images, their encrypted RGB components, and their decrypted images

The outcomes of the histogram security analysis of the proposed security protocol are presented in Figs. 4 and 5. The histogram outcomes of the original images and their color components are shown in Fig. 4, while the histogram outcomes of the encrypted and decrypted images are demonstrated in Fig. 5. These histograms clarify that the original and decrypted images have identical histogram distributions, while the histograms of the encrypted images and their color components are completely dissimilar from the original images and their color components. So, the suggested optical security protocol has a tremendous ciphering/deciphering performance.

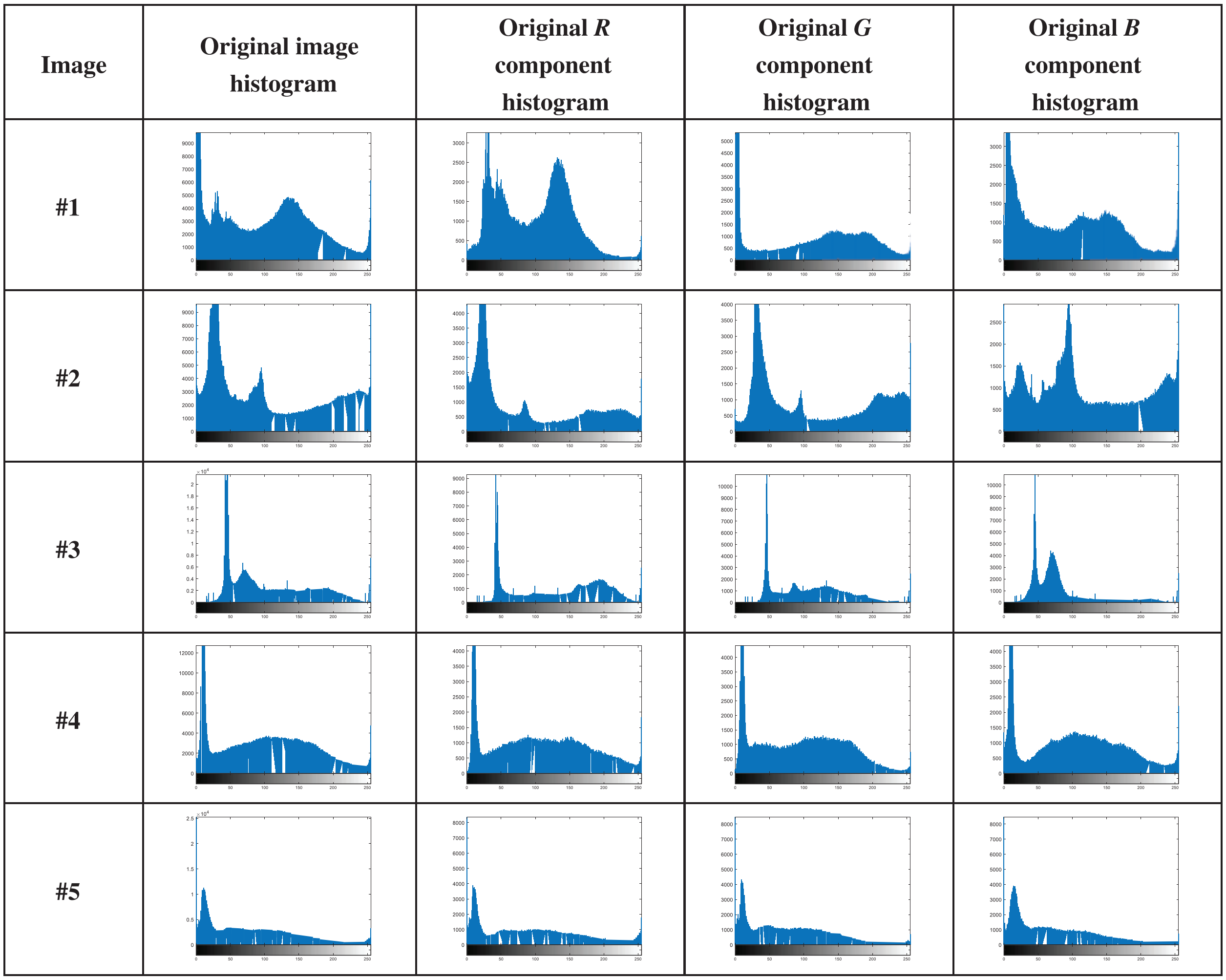


Figure 4: Histograms of the examined color medical images and their RGB components

The outcomes of the entropy security analysis of the examined images and their ciphered and deciphered images are depicted in Tab. 1. These acquired entropies prove that the suggested security protocol can efficiently mitigate the entropy attack by achieving optimum entropy values for the ciphered images. Also, it is noticed that the deciphered and original images have entirely similar entropy values, which proves the efficacy of the suggested security protocol.

The outcomes of the correlation security analysis of the examined images and their ciphered and deciphered images are depicted in Tab. 2. These acquired correlations prove that the suggested security protocol can efficiently mitigate the possible vertical, horizontal, diagonal attacks by achieving low correlation values for the ciphered images. Also, it is noticed that the deciphered and original images have entirely similar correlation values, which prove the efficacy of the suggested security protocol.

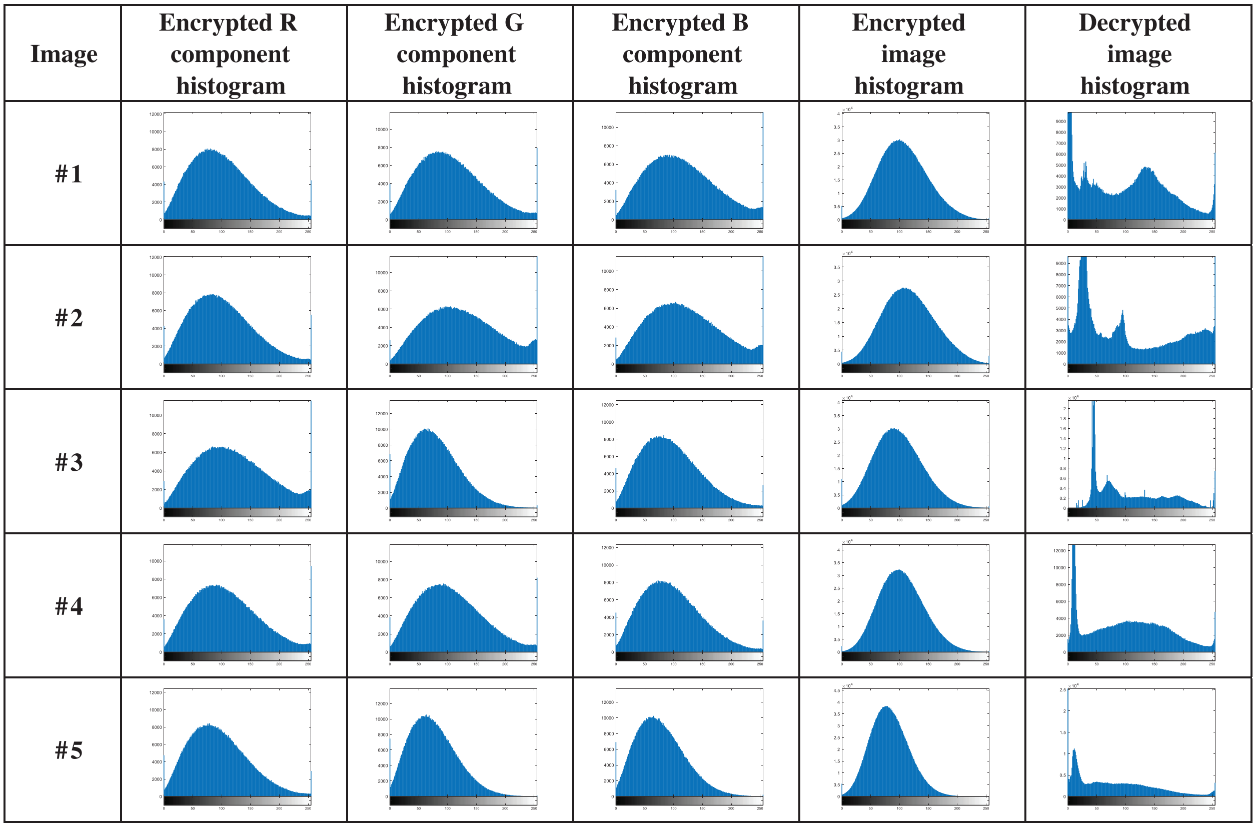


Figure 5: Histogram findings of the encrypted and decrypted images and their color components

Table 1: Information entropies of the examined images and their encrypted and decrypted images

Image	Original	Encrypted	Decrypted
#1	7.4126	7.9603	7.4126
#2	7.5147	7.9728	7.5147
#3	6.7032	7.9394	6.7032
#4	7.3117	7.9572	7.3117
#5	6.8702	7.9693	6.8702

The quality security analysis of the proposed security protocol is validated in terms of the histogram deviation (H_D) and the deviation irregularity (I_D) assessment metrics. Tab. 3 presents the values of the H_D and I_D findings. These obtained values are low, which means that the suggested security protocol achieves better deviation performance in histogram difference and irregularity among the ciphered and original images.

Table 2: Correlations of the examined images and their encrypted and decrypted images

Image	Original			Encrypted			Decrypted		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
#1	0.9807	0.9898	0.9754	0.0761	0.0652	0.1024	0.9807	0.9898	0.9754
#2	0.9720	0.9909	0.9661	0.1110	0.1134	0.0311	0.9720	0.9909	0.9661
#3	0.9794	0.9769	0.9290	0.0208	0.0732	0.0255	0.9794	0.9769	0.9290
#4	0.9918	0.9911	0.9815	0.0840	−0.3069	0.1056	0.9918	0.9911	0.9815
#5	0.9861	0.9793	0.9732	0.0585	0.0547	0.0963	0.9861	0.9793	0.9732

Table 3: Irregular and histogram deviations of the examined ciphered images

Image	H_D	I_D
#1	3.3817	0.0069
#2	5.8571	0.0072
#3	4.2084	0.0076
#4	3.7563	0.0077
#5	4.2765	0.0074

The performance of the suggested security protocol is investigated in terms of mitigating the differential cryptanalytics by estimating the values of the UACI (Unified Averaged Changed Intensity) and NPCR (Number of Changing Pixel Rate). Tab. 4 offers the NPCR and UACI outcomes for the suggested security protocol. These outcomes prove the robustness of the proposed security protocol against the differential attacks where the obtained NPCR and UACI values are near the ideal values.

Table 4: NPCRs and UACIs of the examined medical images

Image	NPCR	UACI
#1	0.99596	0.33385
#2	0.99663	0.33375
#3	0.99635	0.33432
#4	0.99649	0.33487
#5	0.99641	0.33629

Furthermore, the quality security analysis of the proposed security protocol is validated in terms of the FSIM (Feature Similarity), PSNR (Peak Signal-to-Noise Ratio), and SSIM (Structural Similarity) assessment metrics. Tab. 5 presents the values of the acquired FSIM, PSNR, and SSIM findings among the ciphered and original images. These obtained values are low, which means that the suggested security protocol achieves better security performance in hiding the details and visual objects of the medical images through the encryption process.

The efficacy of the suggested security protocol is further validated in terms of the EDR (Edge Differential Ratio) and the Laplacian boundary edges. Tab. 6 offers the EDR outcomes of the ciphered images for the proposed security protocol. These outcomes of the tested medical images are close to the optimum value of 1 for the suggested security protocol. Consequently, this assures that the ciphered and original medical images are entirely distinct. Moreover, the Laplacian edges of the deciphered, ciphered, and original images are visualized, as demonstrated in Fig. 6. It is noticed that the original and deciphered images have the same Laplacian edges, which proves the high decryption performance of the proposed security protocol. Also, the Laplacian edges among the ciphered and original images are entirely distinct, which proves the high encryption performance of the proposed security protocol.

Table 5: FSIM/PSNR/SSIM findings between the ciphered and original images

Image	PSNR (dB)	SSIM	FSIM
#1	9.8257	0.0373	0.5124
#2	8.8547	0.0266	0.4649
#3	9.3421	0.0651	0.4964
#4	8.9458	0.0282	0.4795
#5	8.6283	0.0252	0.4472

Table 6: EDR outcomes of the ciphered images

Image	EDR
#1	0.93100
#2	0.91755
#3	0.93200
#4	0.92960
#5	0.90220

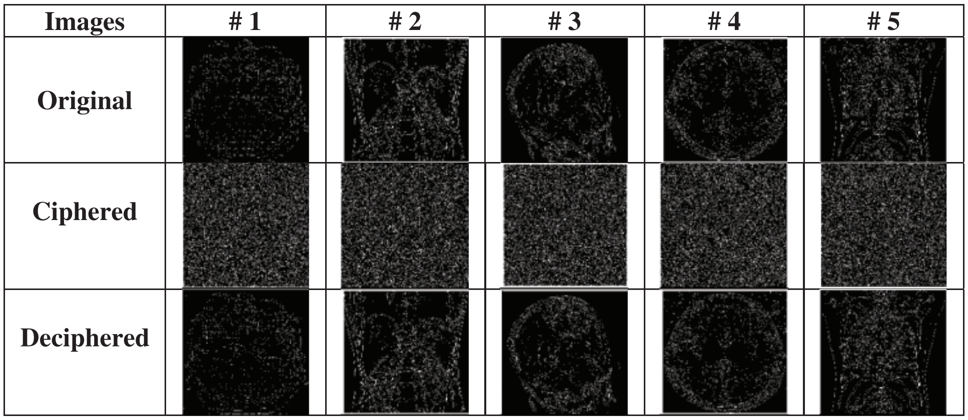


Figure 6: Laplacian edge findings of the ciphered, original, and deciphered images

The key sensitivity analysis for the proposed security protocol is examined using correct and incorrect secret keys to check the sensitivity performance against modification in control parameters. Fig. 7 demonstrates the acquired outcomes of the security sensitivity analysis in terms of the deciphered medical images and their visualized histograms using correct and incorrect security keys. It is remarked that the suggested security protocol has excessive sensitivity to minor alterations in control secret parameters.

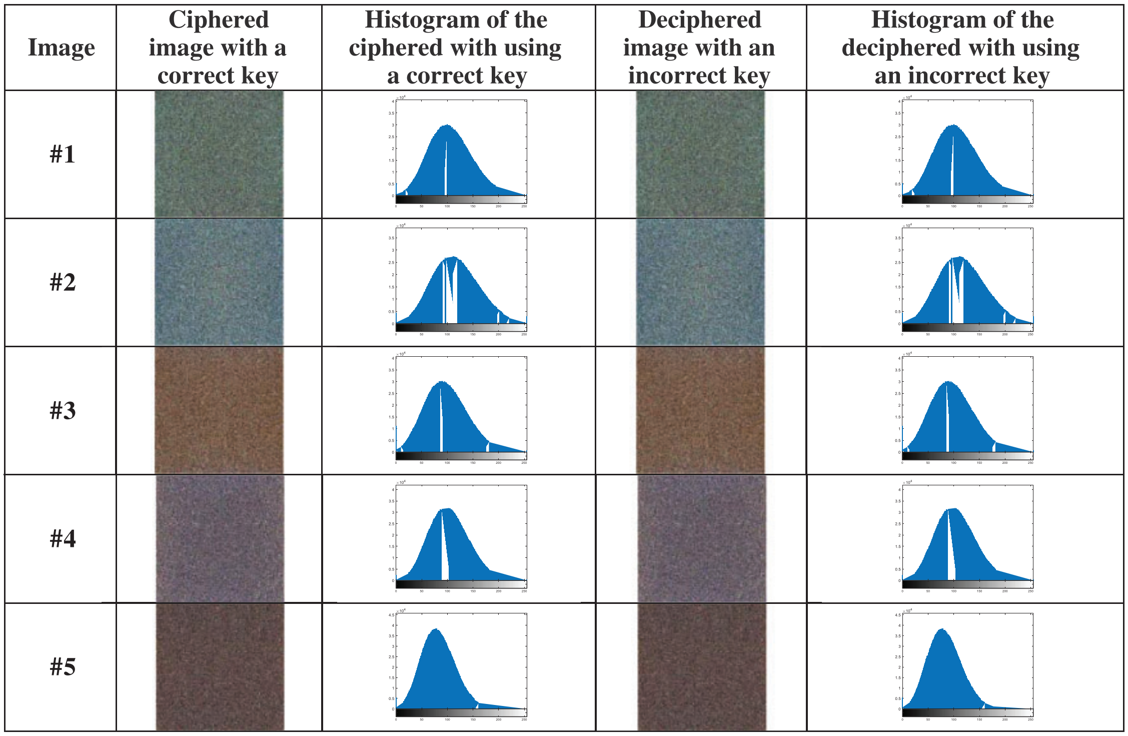


Figure 7: Findings of the key sensitivity testing for the examined medical images

The performance of the decryption procedure of the suggested security protocol is examined against various noises encompassed in the communication medium. The deciphering procedure must survive the noise impacts to achieve the respected implementation of the suggested security protocol. In these simulation experiments, the impact of the Speckle, Poisson, Salt and Pepper, and Gaussian noises are studied. Fig. 8 demonstrates the findings of decrypted images for the enciphered images displayed in Fig. 3 when they are subject to various noise variances. It is remarked that the deciphered images are discernable and detectable if the communication corruption influences the enciphered images. Hence, the suggested security protocol has a perceptible benefit in opposing the communication noise impact.

In simulation experiments, the occlusion attack analysis for the proposed security protocol is studied to prove the efficacy and robustness of the proposed protocol against cropping attacks. This is also to test the capability of the suggested security protocol in returning and deciphering the enciphered images subjected to cropping and occluding attacks. Fig. 9 demonstrates the findings of the occlusion analysis at different cropping percentages. It is observed that the color medical images are deciphered with efficient performance, although the presence of severe occlusion attacks on the enciphered color medical images. Thus, the suggested optical security protocol has outstanding robustness against possible occlusion attacks.

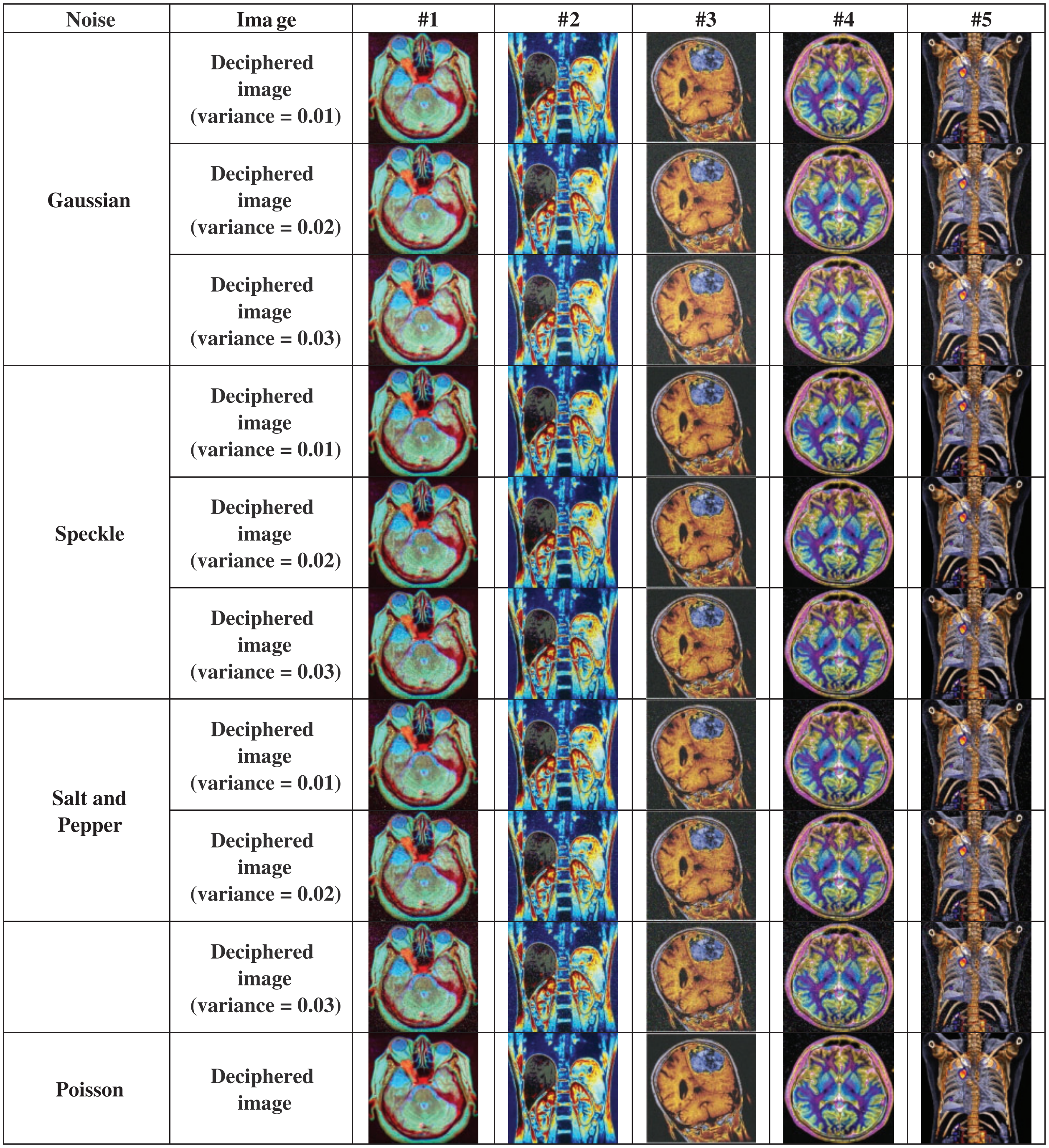

Noise
Ima ge
#1
#2
#3
#4
#5
Gaussian
Deciphered image (variance = 0.01)
Deciphered image (variance = 0.02)
Deciphered image (variance = 0.03)
Speckle
Deciphered image (variance = 0.01)
Deciphered image (variance = 0.02)
Deciphered image (variance = 0.03)
Salt and Pepper
Deciphered image (variance = 0.01)
Deciphered image (variance = 0.02)
Deciphered image (variance = 0.03)
Poisson
Deciphered image

Figure 8: Deciphered images in the presence of Speckle, Poisson, Salt and Pepper, and Gaussian noises

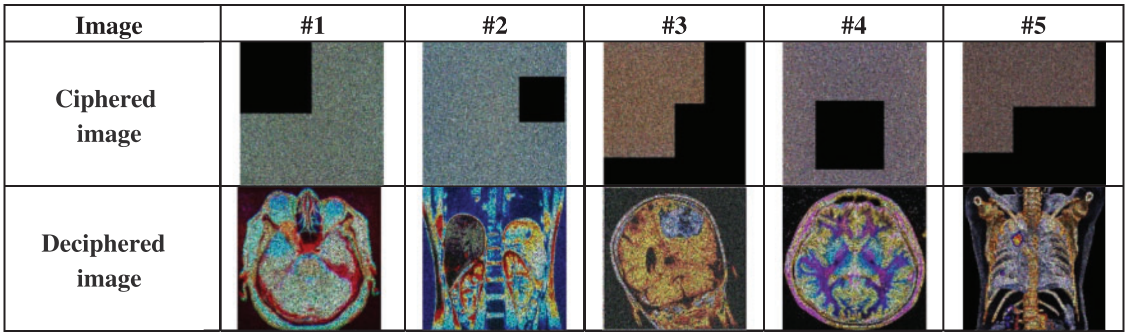


Figure 9: Outcomes of the enciphered and deciphered medical images at different ratios of occlusion attack

Table 7: Ciphering/deciphering times for the proposed security protocol

Image	Time (s)
#1	4.9037
#2	4.8246
#3	4.6437
#4	4.6904
#5	4.2734

Table 8: Security analysis of the proposed security protocol and related conventional security protocols

Protocol	Entropy	PSNR (dB)	Correlation	NPCR	UACI
[19]	7.9878	–	0.0578	0.9941	0.3397
[20]	7.9952	–	0.0069	–	–
[21]	7.9983	31.57	0.04267	0.9954	0.3311
[22]	7.9896	30.50	0.0004	0.9967	0.3346
[23]	7.9970	–	0.0042	0.9962	0.3352
[24]	7.9987	–	0.0011	0.9925	0.3330
[25]	7.9895	–	0.003768	0.9963	0.3347
[26]	7.9927	–	0.0037	0.9959	0.3351
[27]	7.9972	–	−0.0025	0.9963	0.3360
[28]	7.9975	33.87	0.0011	0.9951	0.3358
[29]	7.9893	32.42	0.0053	0.9928	0.3325
[30]	7.9973	30.84	0.0088	0.9960	0.3357
[31]	7.9909	–	0.0025	–	–
[32]	7.9971	32.31	0.0130	0.9961	0.3342
[33]	7.9972	–	0.0116	0.9946	0.3341
[34]	7.9896	33.57	0.0023	0.9961	0.3347
[35]	7.9984	–	0.0032	0.9952	0.3368
[36]	–	–	0.0274	0.9937	0.3328
[37]	7.9927	–	0.0081	0.9927	0.3342
[38]	7.9980	–	0.0000327	0.9975	0.3345
Proposed	7.99826	37.29	−0.00173	0.99613	0.33417

It is advocated for any security protocol to have less computational complexity besides high efficacy and security. Tab. 7 offers the estimated ciphering/deciphering execution times for the proposed security protocol. These attained ciphering/deciphering execution times indicate that the proposed security protocol is exceedingly suitable for real-time telehealth systems in IoMT applications.

For evaluating the privacy efficacy of the suggested security protocol, comprehensive comparisons are investigated for the proposed security protocol contrasted to the latest security protocols [19–38]. These comparisons are in terms of the average entropy, PSNR, correlation, NPCR, and UACI values for the ciphered color Lena image, as depicted in Tab. 8. It is observed that the proposed security protocol achieves superior outcomes compared to other studies in the literature for the whole tested security metrics.

5 Conclusion and Suggestions for Future Work

An efficient optical security protocol was suggested for robust transmission of color medical images for telehealth services. This protocol was based on the deployment of optical JT and FFT transforms. Two scrambling and diffusion stages were employed in the suggested security protocol to safeguard the transmitted color medical images against possible attacks and modifications. The scrambling stage was performed on the color components of the input medical image before the JT transform and FFT transform to achieve a remarkable level of security and robustness. Different secret kernels were exploited using a single arbitrary phase code and a single lens in the second diffusion stage. Comprehensive simulation assessments on various color medical images with distinct features are analyzed based on several statistical security metrics; to confirm the efficiency of the suggested security protocol for secure color medical image communication. Also, a comparative analysis was established between the suggested optical security protocol and other conventional cryptography protocols in the literature. The acquired outcomes demonstrated that the suggested security protocol was highly secure and robust against intruder attempts. It accomplished excellent encryption/decryption performance and superior security results compared to conventional cryptography protocols with attaining excellent average NPCR and UACI values of 0.99613 and 0.33417, respectively. In future work, the security analysis on different modalities of 3D medical images could be investigated. A hybrid of optical and digital cryptography protocols could be utilized to combine their foremost benefits for attaining a secure transmission of medical images through insecure channels. Furthermore, a hybrid multi-stage security protocol for secure medical image communication could be developed, combining steganography, ciphering, and watermarking protocols.

Acknowledgement: The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research group No. (RG-1441-456).

Funding Statement: This research was funded by the Deanship of Scientific Research at King Saud University through research group No. (RG-1441-456) (Grantee: MA, https://dsrs.ksu.edu.sa/).

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

References

[1] W. El-Shafai, F. Khallaf, E. El-Rabaie and F. Abd El-Samie, "Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 5, pp. 1–29, 2021.

[2] F. Abd El-Samie, R. Nassar, M. Safan, M. Abdelhamed, A. Khalaf *et al.,* "Efficient implementation of optical scanning holography in cancelable biometrics," *Applied Optics*, vol. 60, no. 13, pp. 3659–3667, 2021.

[3] I. Elashry, W. El-Shafai, E. Hasan, S. El-Rabaie, A. Abbas *et al.,* "Efficient chaotic-based image cryptosystem with different modes of operation," *Multimedia Tools and Applications*, vol. 79, no. 29, pp. 20665–20687, 2020.

[4] 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.

[5] J. Yaacoub, M. Noura, H. Noura, O. Salman, E. Yaacoub *et al.,* "Securing internet of medical things systems: Limitations, issues and recommendations," *Future Generation Computer Systems*, vol. 105, no. 5, pp. 581–606, 2020.

[6] 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.

[7] S. Ibrahim, M. Egila, H. Shawky, M. Elsaid, W. El-Shafai *et al.,* "Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption," *Multimedia Tools and Applications*, vol. 79, no. 19, pp. 14053–14078, 2020.

[8] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Processing*, vol. 113, no. 1, pp. 104–112, 2015.

[9] X. Wang, Y. Zhao, H. Zhang and K. Guo, "A novel color image encryption scheme using alternate chaotic mapping structure," *Optics and Lasers in Engineering*, vol. 82, no. 1, pp. 79–86, 2016.

[10] O. Faragallah, A. Afifi, W. El-Shafai, H. El-Sayed, M. Alzain *et al.,* "Efficiently encrypting color images with few details based on rc6 and different operation modes for cybersecurity applications," *IEEE Access*, vol. 8, pp. 103200–103218, 2020.

[11] R. Enayatifar, A. Abdullah, I. Isnin, A. Altameem and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Optics and Lasers in Engineering*, vol. 90, pp. 146–154, 2017.

[12] X. Chai, Y. Chen and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 88, no. 2, pp. 197–213, 2017.

[13] X. Chai, K. Yang and Z. Gan, "A new chaos-based image encryption algorithm with dynamic key selection mechanisms," *Multimedia Tools and Applications*, vol. 76, no. 7, pp. 9907–9927, 2017.

[14] C. Li, G. Luo, K. Qin and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[15] S. Oueida, Y. Kotb, M. Aloqaily, Y. Jararweh and T. Baker, "An edge computing based smart healthcare framework for resource management," *Sensors*, vol. 18, no. 12, pp. 1–22, 2018.

[16] 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.

[17] 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.

[18] J. Liu, Y. Ma, S. Li, J. Lian and X. Zhang, "A new simple chaotic system and its application in medical image encryption," *Multimedia Tools and Applications*, vol. 77, no. 17, pp. 22787–22808, 2018.

[19] R. Gupta, R. Pachauri and A. Singh, "An effective approach of secured medical image transmission using encryption method," *Molecular and Cellular Biomechanics*, vol. 15, no. 2, pp. 63–83, 2018.

[20] M. Usman and M. Usman, "Using image steganography for providing enhanced medical data security," in *Proc. IEEE Annual Consumer Communications & Networking Conf.*, Las Vegas, NV, USA, pp. 1–4, 2018.

[21] M. Benssalah, Y. Rhaskali and M. Azzaz, "Medical images encryption based on elliptic curve cryptography and chaos theory," in *Proc. IEEE Int. Conf. on Smart Communications in Network Technologies*, El Oued, Algeria, pp. 222–226, 2018.

[22] H. Abdel-Nabi and A. Al-Haj, "Medical imaging security using partial encryption and histogram shifting watermarking," in *Proc. IEEE 8th Int. Conf. on Information Technology*, Amman, Jourdan, pp. 802–807, 2017.

[23] M. Abdmouleh, A. Khalfallah and M. Bouhlel, "A novel selective encryption DWT-based algorithm for medical images," in *Proc. IEEE 14th Int. Conf. on Computer Graphics, Imaging and Visualization*, Marrakesh, Morocco, pp. 79–84, 2017.

[24] G. Bharghavi, P. Kumar, K. Geetha and N. Devi, "An implementation of SLICE algorithm to enforce security for medical images using DNA approach," in *Proc. IEEE Int. Conf. on Communication and Signal Processing*, Chennai, India, pp. 0984–0988, 2018.

[25] J. Dagadu, J. Li, F. Shah, N. Mustafa and K. Kumar, "DWT based encryption technique for medical images," in *Proc. IEEE 13th Int. Computer Conf. on Wavelet Active Media Technology and Information Processing*, Chengdu, China, pp. 252–255, 2016.

[26] J. Dagadu, J. Li and F. Shah, "An efficient di-chaotic diffusion based medical image cryptosystem," in *Proc. IEEE 14th Int. Computer Conf. on Wavelet Active Media Technology and Information Processing*, Chengdu, China, pp. 206–210, 2017.

[27] Y. Dai and X. Wang, "Medical image encryption based on a composition of logistic maps and chebyshev maps," in *Proc. IEEE Int. Conf. on Information and Automation*, Shenyang, China, pp. 210–214, 2012.

[28] B. Parameshachari, H. Panduranga and S. Naveenkumar, "Partial encryption of medical images by dual DNA addition using DNA encoding," in *Proc. IEEE Int. Conf. on Recent Innovations in Signal Processing and Embedded Systems*, Bhopal, India, pp. 310–314, 2017.

[29] W. Puech, "Image encryption and compression for medical image security," in *Proc. IEEE First Workshops on Image Processing Theory, Tools and Applications*, Sousse, Tunisia, pp. 1–2, 2008.

[30] I. Ranaee, M. Nia, R. Jahantigh and A. Gharib, "Introducing a new algorithm for medical image encryption based on chaotic feature of cellular automata," in *Proc. IEEE Int. Conf. for Internet Technology and Secured Transactions*, London, UK, pp. 582–587, 2013.

[31] P. Saraswathi and M. Venkatesulu, "A novel stream cipher using pesudo random binary sequence generator for medical image encryption," in *Proc. IEEE Int. Conf. on Trends in Electronics and Informatics*, Tirunelveli, India, pp. 425–429, 2017.

[32] G. Suganya and K. Amudha, "Medical image integrity control using joint encryption and watermarking techniques," in *Proc. IEEE Int. Conf. on Green Computing Communication and Electrical Engineering*, Coimbatore, India, pp. 1–5, 2014.

[33] Y. Zhou, K. Panetta and S. Agaian, "A lossless encryption method for medical images using edge maps," in *Proc. IEEE Annual Int. Conf. of the Engineering in Medicine and Biology Society*, Minneapolis, MN, USA, pp. 3707–3710, 2009.

[34] A. Chatterjee, J. Dhanotia, V. Bhatia, S. Rana and S. Prakash, "Optical image encryption using fringe projection profilometry, Fourier Fringe analysis, and RSA algorithm," in *Proc. IEEE 14th IEEE India Council Int. Conf.*, Roorkee, India, pp. 1–5, 2017.

[35] R. Das, S. Manna and S. Dutta, "Cumulative image encryption approach based on user defined operation, character repositioning, text key and image key encryption technique and secret sharing scheme," in *Proc. IEEE Int. Conf. on Power, Control, Signals and Instrumentation Engineering*, Chennai, India, pp. 748–753, 2017.

[36] S. Jain and A. Khunteta, "Color image encryption by component based partial random phase encoding," in *Proc. IEEE Int. Conf. on Inventive Research in Computing Applications*, Coimbatore, India, pp. 144–148, 2018.

[37] P. Li and K. Lo, “Lo Joint image compression and encryption based on alternating transforms with quality control,” in *Proc. IEEE Visual Communications and Image Processing*, Singapore, pp. 1–4, 2015.

[38] P. Ramaraju, G. Raju and P. Krishna, “Image encryption after hiding (IEAH) technique for color images,” in *Proc. Int. Conf. on Signal Processing, Communication, Power and Embedded System*, Paralakhemundi, India, pp. 1202–1207, 2016.

[39] W. Wen, Y. Zhang, Y. Fang and Z. Fang, “A novel selective image encryption method based on saliency detection,” in *Proc. IEEE Visual Communications and Image Processing*, Chengdu, China, pp. 1–4, 2016.

[40] 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.

[41] 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. 80, no. 3, pp. 1–35, 2020.