Computers, Materials & Continua
DOI:10.32604/cmc.2022.018545
Article

Tech Science Press

Secure and Robust Optical Multi-Stage Medical Image Cryptosystem

Walid El-Shafai[1], Moustafa H. Aly[2], Abeer D. Algarni[3,*], Fathi E. Abd El-Samie[1,3] and Naglaa F. Soliman[3,4]

[1]Department Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt
[2]Department of Electronics and Communications Engineering, College of Engineering and Technology, Arab Academy for Science, Technology and Maritime Transport, Alexandria, 1029, Egypt
[3]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, 84428, Saudi Arabia
[4]Department of Electronics and Communications, Faculty of Engineering, Zagazig University, Zagazig, 44519, Egypt
[*]Corresponding Author: Abeer D. Algarni. Email: adalqarni@pnu.edu.sa

Received: 12 March 2021; Accepted: 07 May 2021

Abstract: Due to the rapid growth of telemedicine and healthcare services, color medical image security applications have been expanded precipitously. In this paper, an asymmetric PTFrFT (Phase Truncated Fractional Fourier Transform)-based color medical image cryptosystem is suggested. Two different phases in the fractional Fourier and output planes are provided as deciphering keys. Accordingly, the ciphering keys will not be employed for the deciphering procedure. Thus, the introduced PTFrFT algorithm comprises asymmetric ciphering and deciphering processes in contrast to the traditional optical symmetric OSH (Optical Scanning Holography) and DRPE (Double Random Phase Encoding) algorithms. One of the principal impacts of the introduced asymmetric cryptosystem is that it eliminates the one-dimensionality aspects of the related symmetric cryptosystems due to its remarkable feature of phase nonlinear truncation components. More comparisons on various color medical images are examined and analyzed to substantiate the cryptosystem efficacy. The achieved experimental outcomes ensure that the introduced cryptosystem is robust and secure. It has terrific cryptography performance compared to conventional cryptography algorithms, even in the presence of noise and severe channel attacks.

Keywords: Optical encryption; medical image security; symmetric and asymmetric encryption; OSH; DRPE; PTFrFT

1 Introduction

Digitalization is a huge part of our life today, with broad applications in health, science, engineering, media, communication, etc. A large amount of digital multimedia data is often transmitted via open networks with the widespread use of the Internet. Therefore, the security and integrity of this large amount of data are of great concern [1,2]. A type of the precious data is represented with digital images used in various beneficial applications such as military, biometric authentication, online shopping, online banking, healthcare systems, telemedicine, medical science, etc. [3–5].

The lack of powerful security and protection tools could cause various threats and attacks, leading to serious disasters for people and networks. In medical image communication through the Internet, intruders can simply retrieve the images because of the shortage in security levels. Therefore, the protection of the transmitted image information becomes a serious problem. Several papers described different multimedia encryption techniques like those found in [1–21]. There are several chaotic maps in the state-of-the-art works, such as Arnold map, Logistic map, and Cat map [12–21]. Various image security and image cryptography techniques based on chaos systems have been presented in [22–27]. The main disadvantage of the traditional chaotic-map-based cryptography procedures is that they depend on lower-order chaos functions. Therefore, it is essential to develop robust cryptography algorithms to avoid this disadvantage.

The conventional cryptography techniques [28–34] have nevertheless been found not appropriate for efficient image communication due to their underlying characteristics like large number of iterations, high pixel redundancy, strong correlation, and large computational cost. So, they minimize the inclusive security performance. Thus, it is urgent to preclude medical images from the risks of attacks and threats through employing effective cryptography techniques. Consequently, due to the importance of medical data security, this paper presents a robust way of managing and securing color medical image communication for achieving reliable security in telemedicine applications.

This motivated us, in this paper, to implement an effective and asymmetric optical color medical image cryptosystem, where two random phases are exploited as ciphering keys that are distinct from the deciphering keys. The introduced cryptosystem has an attractive advantage of nonlinear truncation of phase components for the communication of color medical images through insecure channels. Hence, it is suitable for cloud-based telemedicine and healthcare applications. Simulation results of the proposed cryptosystem on different color medical images prove better security performance with lower computational cost in the presence of different types of noise and multimedia attacks.

The paper is planned as follows. Section 2 presents some work related to medical image security. Section 3 introduces the inclusive clarification of the suggested asymmetric cryptosystem for secure color medical image communication. Simulation outcomes and comparisons are provided in Section 5. The main concluding remarks are offered in Section 6.

2 Related Work

There is a critical need for telemedicine healthcare opportunities and facilities that can be delivered through software tools. This will create a healthcare delivery system with more timeliness and efficiency. Security plays a crucial role in the transmission of medical data via the Internet. Recently, it has become a challenge to secure medical images in healthcare and telemedicine applications [35–38]. Gupta et al. [39] introduced a high-security medical image cryptosystem that depends on logstic map. In [40], the authors introduced a comparison between chaos theory and elliptic curve cryptography as tools for image security. Abdel-Nabi et al. [41] proposed an algorithm that merges reversible data steganography and ciphering approaches to achieve the required protection of stored and transmitted medical data and images.

In [42], a hybrid approach was proposed for partial encryption. It guarantees optimal and robust storage and communication of medical information. This approach has low processing time for the ciphering-deciphering processes. Bharghavi et al. [43] presented an efficient security system based on chaotic logistic map for reliable medical image transmission. In [44], a robust and fast medical image ciphering approach was suggested for real-time medical communication services. In [45], the authors presented a powerful and efficient medical image ciphering approach. Two chaotic sequences are utilized in this approach for key generation. Then, a diffusion process with two rounds is adopted to create the encrypted medical images. Dai et al. [46] explained a new technique for medical image security based on a hybrid structure of Chebyshev maps and logistic maps to enhance the ciphering performance. In [47], the authors presented a partial encryption framework based on a chaotic map and DNA encoding for securing medical images.

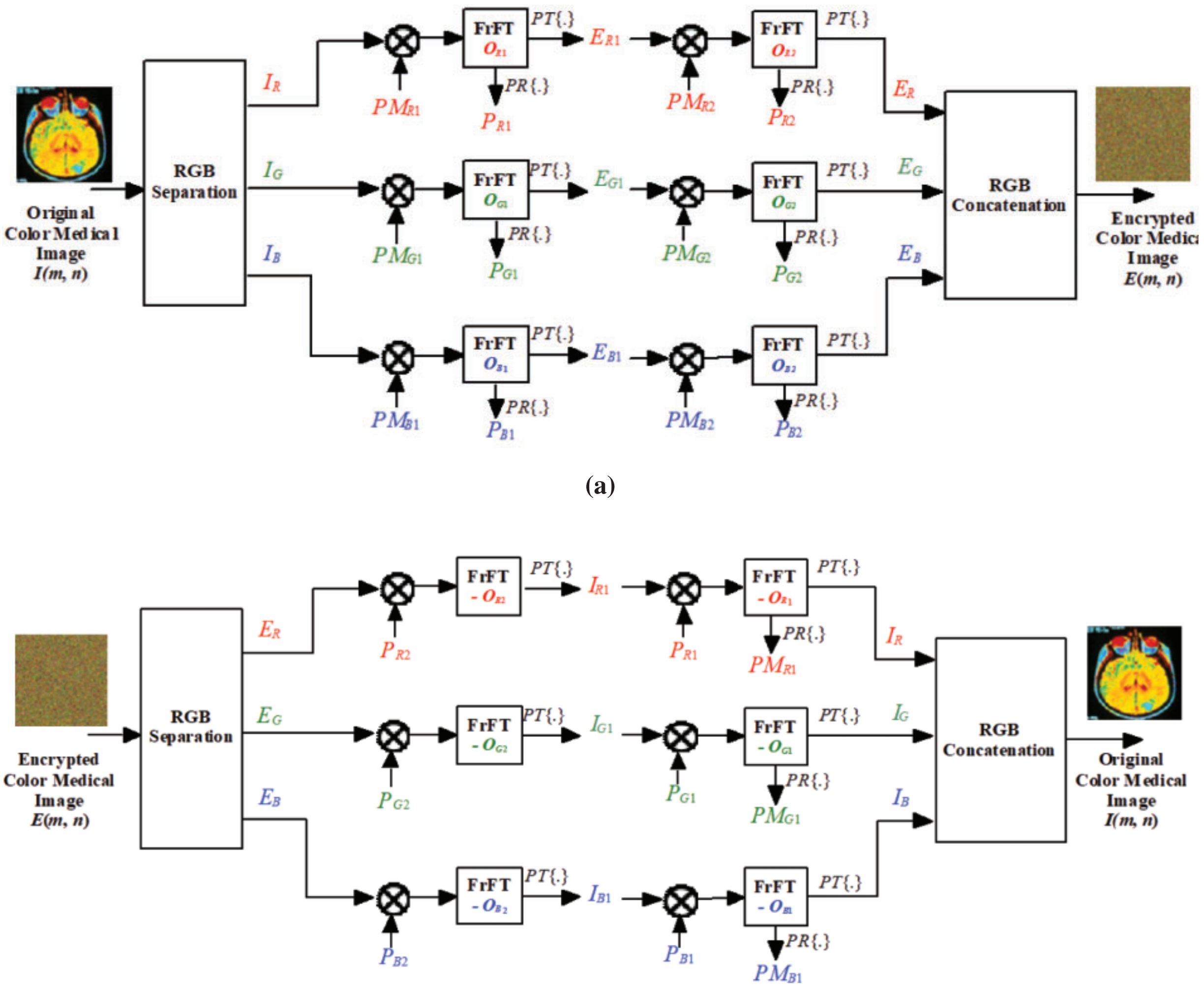
Puech et al. [48] investigated different ciphering techniques for medical image communication. The advantage of these techniques is that they can be employed for images, videos, and 3D objects. In [49], corresponding to cellular automata chaotic features, the authors proposed an efficient medical image ciphering algorithm. The simulation findings showed that this algorithm offers more security and speed. Saraswathi et al. [50] introduced an efficient medical image crptosystem based on an asymmetric stream cipher security technique. It has been concluded that this cryptosystem is robust against various types of cyberattacks. Suganya et al. [51] proposed a hybrid cryptosystem that depends on stream-based and block-based ciphering algorithms. This cryptosystem highly provides integrity control and encryption of medical images. Zhou et al. [52] suggested a security technique that is capable of full protection of chosen regions/objects in medical images.

Moreover, several image security systems [53–58] can be exploited in medical imaging services. In [53], the authors introduced an optical image security algorithm using fringe projection profilometry and Fourier fringe analysis. Das et al. [54] developed an image security system in which the input image is ciphered based on a user-defined key. Jain et al. [55] proposed a partial-random-phase-encoding-based color image ciphering and deciphering framework. Li et al. [56] suggested an effective hybrid image ciphering/compression framework. Ramaraju et al. [57] proposed a least-significant-bit-based image hiding technique. It hides four images inside a single image to generate a stego-image that is then ciphered with a secret key. Wen et al. [58] proposed a robust optical salient region ciphering method, in which the salient regions are pre-ciphered by employing a chaotic optical ciphering technique.

Although the statistical security analysis of the previous related works [1–58] showed numerous differences, most of the presented methods have significant challenges with ciphering and deciphering processes. The traditional encryption methods do not achieve the required quality level in the presence of multimedia assaults. Consequently, the presented state-of-the-art methods have low performance levels in the presence of multimedia attacks and channel noise. Additionally, the state-of-the-art methods have not been assessessed with enough evaluation metrics and in-detail statistical security analysis. In addition, they necessitate additional calculations in the ciphering and deciphering procedures, and hence, they have large computational cost. Therefore, considering the shortcomings of the previous encryption methods in the literature, an efficient optical color medical image cryptosystem based on the asymmetric PTFrFT encryption algorithm is suggested in this paper for telemedicine and healthcare security applications. The security examination of the presented algorithm is investigated through visual results, differential analysis, histograms, encryption quality analysis, information entropy, communication noise analysis, and security analysis. Therefore, several statistical tests on different samples of color medical images are performed.

3 Proposed Optical PTFrFT-Based Color Medical Image Cryptosystem

The proposed optical cryptosystem consists of two stages of encryption and decryption as illustrated in Figs. 1a and 1b. The encryption keys of the medical images comprise the generated optical keys of arbitrary phase masks (PMs) of the employed asymmetric PTFrFT algorithm.



(a)

(b)

Figure 1: Suggested multi-stage PTFrFT-based color medical image cryptosystem (a) Encryption stage (b) Decryption stage

The precious aspect of the employed asymmetric PTFrFT cryptosystem is that there are two distinct ciphering/deciphering secret keys. This tremendous trait has encouraged us to utilize it for building a secure and robust color medical image cryptosystem. The PTFrFT is estimated with the FrFT of the plain color medical image with the truncation operation of phase components, where the amplitude modular part of the FrFT spectrum is merely exploited, and the phase part of the FrFT spectrum is separated. The ciphering methodology of the introduced cryptosystem is executed with the steps demonstrated in Fig. 1a.

1) Separate the input color medical image into the R, G, and B color components $I_R(m,n)$, $I_G(m,n)$, and $I_B(m,n)$ as offered in Eq. (1).

$$I(m,n) = [I_R(m,n),\ I_G(m,n),\ I_B(m,n)] \tag{1}$$

2) Multiply the separated color components by the first phase masks PM_{R1}, PM_{G1}, and PM_{B1}, and then apply the first FrFT operation with the first fractional orders O_{R1}, O_{G1}, and O_{B1} to produce the primary encrypted image components. Each of these components can be decomposed into two parts: phase retaining part as in Eqs. (2)–(4) and phase truncated part as in Eqs. (5)–(7).

$$E_{R_1}(m,n) = PT\{\mathrm{FrFT}^{O_{R_1}}\left[I_{R_1}(m,n).PM_{R_1}(m,n)\right] \tag{2}$$

$$E_{G_1}(m,n) = PT\{\mathrm{FrFT}^{O_{G_1}}\left[I_{G_1}(m,n).PM_{G_1}(m,n)\right] \tag{3}$$

$$E_{B_1}(m,n) = PT\{\mathrm{FrFT}^{O_{B_1}}\left[I_{B_1}(m,n).PM_{B_1}(m,n)\right] \tag{4}$$

$$P_{R_1}(m,n) = PR\{\mathrm{FrFT}^{O_{R_1}}\left[I_{R_1}(m,n).PM_{R_1}(m,n)\right] \tag{5}$$

$$P_{G_1}(m,n) = PR\{\mathrm{FrFT}^{O_{G_1}}\left[I_{G_1}(m,n).PM_{G_1}(m,n)\right] \tag{6}$$

$$P_{B_1}(m,n) = PR\{\mathrm{FrFT}^{O_{B_1}}\left[I_{B_1}(m,n).PM_{B_1}(m,n)\right] \tag{7}$$

where $PR\{.\}$ and $PT\{.\}$ are the phase reservation and truncation operators, respectively. The $PM_{R_1}(m,n)$, $PM_{G_1}(m,n)$, and $PM_{B_1}(m,n)$ are the primary encryption phase masks that are randomly generated by the 2D Arnold map [3].

3) Similarly, repeat Step (2) through multiplying by the second phase masks PM_{R_2}, PM_{G_2}, and PM_{B_2}, and performing the second FrFT operation with the second fractional orders O_{R_2}, O_{G_2}, and O_{B_2} to produce the final encrypted image components. Each of these components has two parts: phase retaining part as in Eqs. (8)–(10) and the phase truncated part as in Eqs. (11)–(13).

$$E_R(m,n) = PT\{\mathrm{FrFT}^{O_{R_2}}\left[E_{R_1}(m,n).PM_{R_2}(m,n)\right] \tag{8}$$

$$E_G(m,n) = PT\{\mathrm{FrFT}^{O_{G_2}}\left[E_{G_1}(m,n).PM_{G_2}(m,n)\right] \tag{9}$$

$$E_B(m,n) = PT\{\mathrm{FrFT}^{O_{B_2}}\left[E_{B_1}(m,n).PM_{B_2}(m,n)\right] \tag{10}$$

$$P_{R_2}(m,n) = PR\{\mathrm{FrFT}^{O_{R_2}}\left[E_{R_1}(m,n).PM_{R_2}(m,n)\right] \tag{11}$$

$$P_{G_2}(m,n) = PR\{\mathrm{FrFT}^{O_{G_2}}\left[E_{G_1}(m,n).PM_{G_2}(m,n)\right] \tag{12}$$

$$P_{B_2}(m,n) = PR\{\mathrm{FrFT}^{O_{B_2}}\left[E_{B_1}(m,n).PM_{B_2}(m,n)\right] \tag{13}$$

where the obtained P_{R_2}, P_{G_2}, and P_{B_2} are then utilized as the decrypted keys. The $PM_{R_2}(m,n)$, $PM_{G_2}(m,n)$, and $PM_{B_2}(m,n)$ are the final encryption phase masks that are given by Eqs. (14)–(16) comprising the phase function $exp[j\psi(m,n)]$.

$$PM_{R_2}(m,n) = P_{R_1}(m,n) \times exp[j\psi_R(m,n)] \tag{14}$$

$$PM_{G_2}(m,n) = P_{G_1}(m,n) \times exp[j\psi_G(m,n)] \tag{15}$$

$$PM_{B_2}(m,n) = P_{B_1}(m,n) \times exp[j\psi_B(m,n)] \tag{16}$$

where $\psi(m,n) \in [0,\ 2\pi]$.

The benefit from using two FrFT stages is significantly improving the robustness and security of the introduced medical image cryptosystem based on the fractional orders and scaling factors of the FrFT. Due to these advantages, it is highly recommended in the proposed cryptosystem. More detailed discussions about the FrFT are found [4,5]. The deciphering steps are the inverse of the above-mentioned ciphering steps, as demonstrated in Fig. 1b. Consequently, the deciphering procedure can be implemented by exploiting the private deciphering secret keys $P_2(m,n)$ and $P_1(m,n)$, where the PTFrFT is an asymmetric transform.

4 Results and Discussions

Different color medical images that have different features are chosen and examined to substantiate the profits of the suggested optical color medical image cryptosystem. The utilized color medical images are primarily decomposed into their R, G, and B components to be used as the cryptosystem input. The simulation experiments are performed using a laptop with 8 GB RAM, and i7-5200 Intel CPU. The utilized software in the simulation tests is the MATLAB R2020b.

4.1 Visual Results

The visual analysis is the most important assessment tool utilized to appraise the security strength and efficiency of the suggested cryptosystem. The examined color medical images and their encrypted versions with the suggested optical asymmetric cryptosystem and the conventional optical symmetric DRPE and OSH cryptosystems [7,9,10,22] are displayed in Fig. 2. It is obvious that the suggested cryptosystem is more beneficial compared to other cryptosystems in concealing and diminishing the significant objects contained within the studied color medical images.

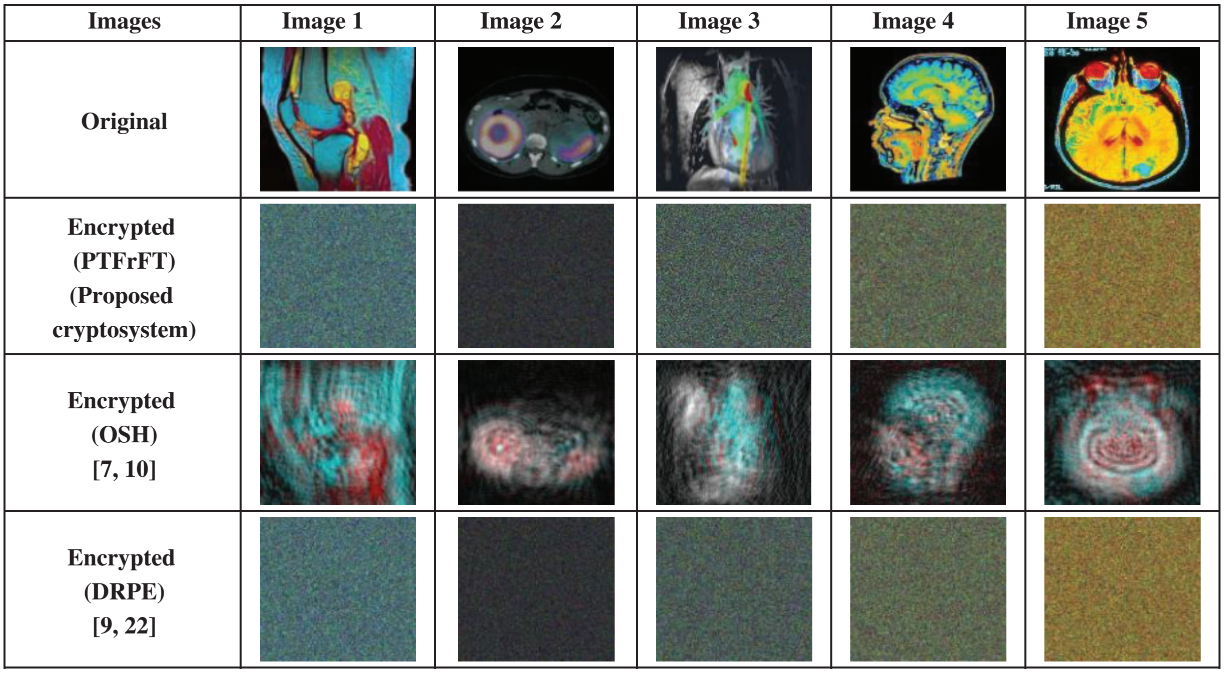


Figure 2: Original color medical images and their encrypted versions with the PTFrFT, OSH, and DRPE cryptosystems

4.2 Histogram Results

The pixel distributions of the original and ciphered images can be demonstrated through histogram analysis [16]. Both histograms of the original and ciphered images must be different to illustrate good encryption. Fig. 3 indicates the histogram security analysis of the examined original and ciphered images with the suggested and conventional cryptosystems. It is obvious that the original image histograms are entirely different from the ciphered image histograms. This proves the reliability of the suggested cryptosystem and the conventional ones.

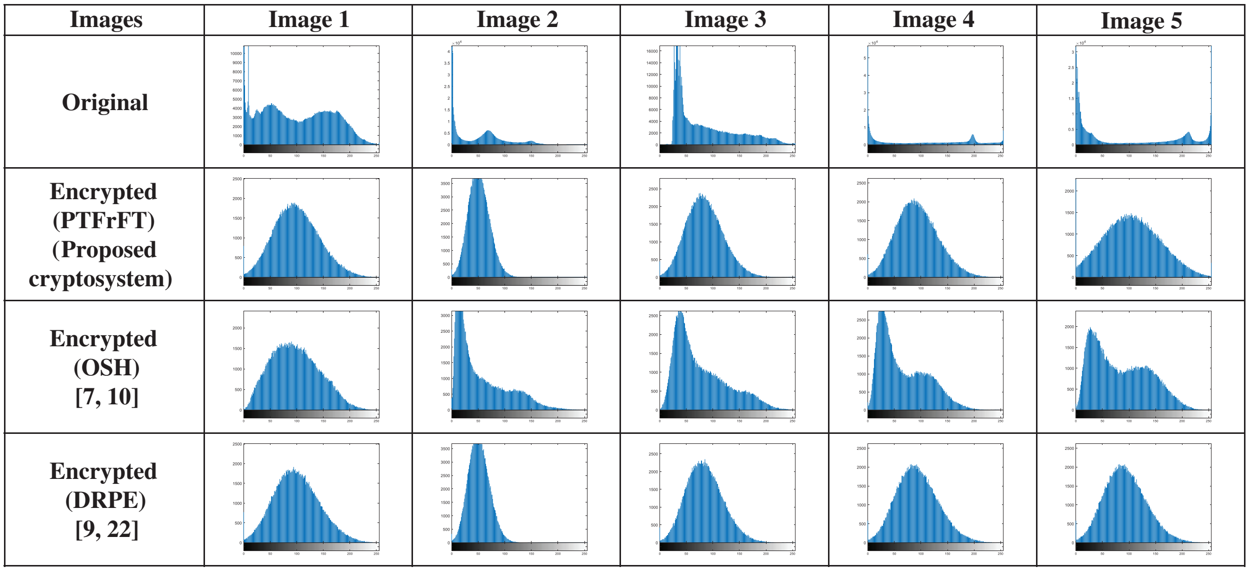


Figure 3: Histogram outcomes for the PTFrFT, OSH, and DRPE cryptosystems

4.3 Entropy Results

The entropy metric is exploited to describe the unpredictability degree of the ciphered color medical image. The proposed cryptosystem is close to achieving an ideal entropy value of 8 [23]. Tab. 1 offers the entropy outcomes of the analyzed original, encrypted, and decrypted color medical images for the suggested optical PTFrFT cryptosystem and the conventional optical cryptosystems. The obtained superior entropy values for the suggested cryptosystem prove its robustness and reliability compared to other cryptosystems through achieving better values close to the desired optimal value.

Table 1: Entropy outcomes for the PTFrFT, OSH, and DRPE cryptosystems

Image	Original image	Encrypted image (DRPE) [9,22]	Encrypted image (OSH) [7,10]	Encrypted image (proposed cryptosystem)	Decrypted image (All algorithms)
Image 1	7.422	7.615	7.488	7.821	7.422
Image 2	5.380	6.333	7.073	7.436	5.380
Image 3	6.864	7.130	7.391	7.694	6.864
Image 4	5.083	7.304	7.231	7.798	5.083
Image 5	6.055	7.668	7.536	7.807	6.055

4.4 Correlation Results

Remarkable cryptosystems are supposed to eliminate any relationship among color medical image pixels to protect the color medical image content from statistical channel attacks [20]. Tabs. 2–4 demonstrate the diagonal (D), horizontal (H), and vertical (V) correlation outcomes for the studied original, enciphered, and deciphered color medical images with the proposed cryptosystem compared to DRPE and OSH cryptosystems. The obtained D, H, and V correlation values are enormously low for the ciphered images obtained by the proposed cryptosystem compared to the traditional cryptosystems. This proves its superior security performance.

Table 2: Correlation outcomes of the DRPE cryptosystem [9,22]

Image	Original			Encrypted			Decrypted		
	H	V	D	H	V	D	H	V	D
Image 1	0.9369	0.9868	0.9483	0.0038	−0.0022	0.0363	0.9369	0.9868	0.9483
Image 2	0.9939	0.9921	0.9784	0.0027	0.0083	0.0056	0.9939	0.9921	0.9784
Image 3	0.9822	0.9948	0.9658	0.0046	−0.0095	0.0088	0.9822	0.9948	0.9658
Image 4	0.9786	0.9601	0.9479	0.0403	0.0461	0.0210	0.9786	0.9601	0.9479
Image 5	0.9625	0.9691	0.9407	0.0951	0.0734	0.0979	0.9625	0.9691	0.9407

Table 3: Correlation outcomes of the OSH cryptosystem [7,10]

Image	Original			Encrypted			Decrypted		
	D	H	V	D	H	V	D	H	V
Image 1	0.9369	0.9868	0.9483	0.9652	0.9842	0.9543	0.9369	0.9868	0.9483
Image 2	0.9939	0.9921	0.9784	0.9924	0.9927	0.9860	0.9939	0.9921	0.9784
Image 3	0.9822	0.9948	0.9658	0.9774	0.9898	0.9673	0.9822	0.9948	0.9658
Image 4	0.9786	0.9601	0.9479	0.9564	0.9539	0.9164	0.9786	0.9601	0.9479
Image 5	0.9625	0.9691	0.9407	0.9820	0.9832	0.9731	0.9625	0.9691	0.9407

Table 4: Correlation outcomes of the proposed PTFrFT cryptosystem

Image	Original			Encrypted			Decrypted		
	D	H	V	D	H	V	D	H	V
Image 1	0.9369	0.9868	0.9483	−0.0295	−0.0281	0.0637	0.9369	0.9868	0.9483
Image 2	0.9939	0.9921	0.9784	0.0003	0.0599	0.0063	0.9939	0.9921	0.9784
Image 3	0.9822	0.9948	0.9658	0.0552	0.0227	0.0426	0.9822	0.9948	0.9658
Image 4	0.9786	0.9601	0.9479	0.0464	0.1100	0.0868	0.9786	0.9601	0.9479
Image 5	0.9625	0.9691	0.9407	0.1483	0.1006	0.0991	0.9625	0.9691	0.9407

4.5 Encryption Quality Security Analysis

The deviation irregularity (I_D) and the histogram deviation (H_D) metrics [53] can be used to assess the quality performance and ciphering efficacy of the proposed optical cryptosystem. They are utilized to determine the deviation percentage of the irregularity and histogram difference between the original and ciphered medical images. Tab. 5 demonstrates the estimated I_D and H_D outcomes, where lower values are obtained for both, which is recommended for achieving superior ciphering efficacy. Consequently, the larger the decorrelation between the original and ciphered images is, the improved the operation of the suggested cryptosystem compared to the conventional DRPE and OSH cryptosystems.

Table 5: Histogram and irregular deviation results of the encrypted color medical images

Image	DRPE [9,22]		OSH [7,10]		PTFrFT (proposed cryptosystem)	
	H_D	I_D	H_D	I_D	H_D	I_D
Image 1	2.0185	0.0056	1.6903	0.0051	2.0282	0.0057
Image 2	3.3104	0.0052	2.6224	0.0048	3.3021	0.0053
Image 3	2.9012	0.0052	1.5813	0.0042	2.9103	0.0056
Image 4	3.6629	0.0059	3.5748	0.0060	3.6642	0.0060
Image 5	3.6386	0.0063	3.5924	0.0069	3.6400	0.0062

4.6 Differential Security Analysis

The differential security cryptanalysis in terms of the NPCR (Number of Changing Pixel Rate) and UACI (Unified Averaged Changed Intensity) [44] is employed to verify the robustness of the proposed cryptosystem in the presence of slight modifications of the encrypted images. For good security and robustness, it is required to achieve NPCR and UACI values of 0.996 and 0.33, respectively [9]. It is observed that the obtained UACI and NPCR values in Tab. 6 for the proposed cryptosystem are astonishingly close to the desired values in contrast to the conventional cryptosystems.

Table 6: NPCR and UACI outcomes of the tested color medical images

Image	DRPE [9,22]		OSH [7,10]		PTFrFT (proposed cryptosystem)	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
Image 1	0.9953	0.3346	0.9921	0.3347	0.9954	0.3367
Image 2	0.9950	0.3328	0.9926	0.3392	0.9952	0.3348
Image 3	0.9943	0.3339	0.9845	0.3308	0.9949	0.3353
Image 4	0.9971	0.3362	0.9973	0.3372	0.9968	0.3374
Image 5	0.9884	0.3382	0.9972	0.3359	0.9889	0.3369

4.7 SSIM, FSIM and PSNR Analysis

The SSIM (Structural Similarity), PSNR (Peak Signal-to-Noise Ratio), and FSIM (Feature Similarity) metrics [12,17] are exploited to assess the cryptosystem performance. In our security analysis, these metrics are calculated between the enciphered and plain medical images. They need to have small values for a proper enciphering process. Tab. 7 demonstrates the obtained results of the proposed and the conventional DRPE and OSH cryptosystems, where superior values are delivered by the proposed cryptosystem in contrast to the traditional cryptosystems.

Table 7: SSIM, FSIM and PSNR outcomes between the plain and encrypted medical images for the PTFrFT, OSH, and DRPE cryptosystems

Image	DRPE [9,22]			OSH [7,10]			PTFrFT (present work)		
	SSIM	FSIM	PSNR (dB)	SSIM	FSIM	PSNR (dB)	SSIM	FSIM	PSNR (dB)
Image 1	0.0103	0.5129	10.5681	0.0571	0.5882	13.6879	0.0143	0.4920	10.6102
Image 2	0.0190	0.5210	13.7794	0.0925	0.6643	17.6268	0.0225	0.5203	13.8057
Image 3	0.0120	0.5007	11.7526	0.1181	0.6205	16.7375	0.0119	0.5003	11.7475
Image 4	0.0017	0.4459	8.4068	0.0160	0.5031	11.4350	0.0024	0.4450	8.3806
Image 5	0.0016	0.4386	7.8848	0.0305	0.5226	9.7338	0.0030	0.4371	7.9084

4.8 Edge Security Analysis

The metric of EDR (Edge Differential Ratio) is employed to evaluate the misrepresentations in the boundaries and borders that result from the encryption process in the color medical images [24]. Tab. 8 reveals that the EDR outcomes of the examined color medical images are close to 1 for the proposed PTFrFT cryptosystem. Thus, this guarantees that the encrypted and plain images are totally different. Fig. 4 shows the Laplacian edge Gaussian results of the original and enciphered images with the proposed cryptosystem compared to those of the conventional algorithms. These visual outcomes confirm the amazing benefit of the proposed cryptosystem in concealing the most important aspects and features within the transmitted medical images.

Table 8: EDR values of the encrypted images for the DRPE, OSH, and PTFrFT cryptosystems

Image	EDR		
	DRPE	OSH	PTFrFT
Image 1	0.89333	0.91071	0.88889
Image 2	0.90347	0.90227	0.89853
Image 3	0.88289	0.91091	0.88208
Image 4	0.88858	0.88431	0.88351
Image 5	0.89861	0.91836	0.89977

4.9 Key Sensitivity Security Analysis

It is required for a cryptosystem to be susceptible to the control and initial values [17]. This can be validated by investigating the key security analysis. The suggested cryptosystem provides different outcomes, when the control parameters are changed. Fig. 5 offers the key sensitivity outcomes in the form of decrypted images and their histograms using incorrect key values. It is observed that the suggested cryptosystem and the tested DRPE and OSH cryptosystems have high sensitivity to slight changes in control parameters.

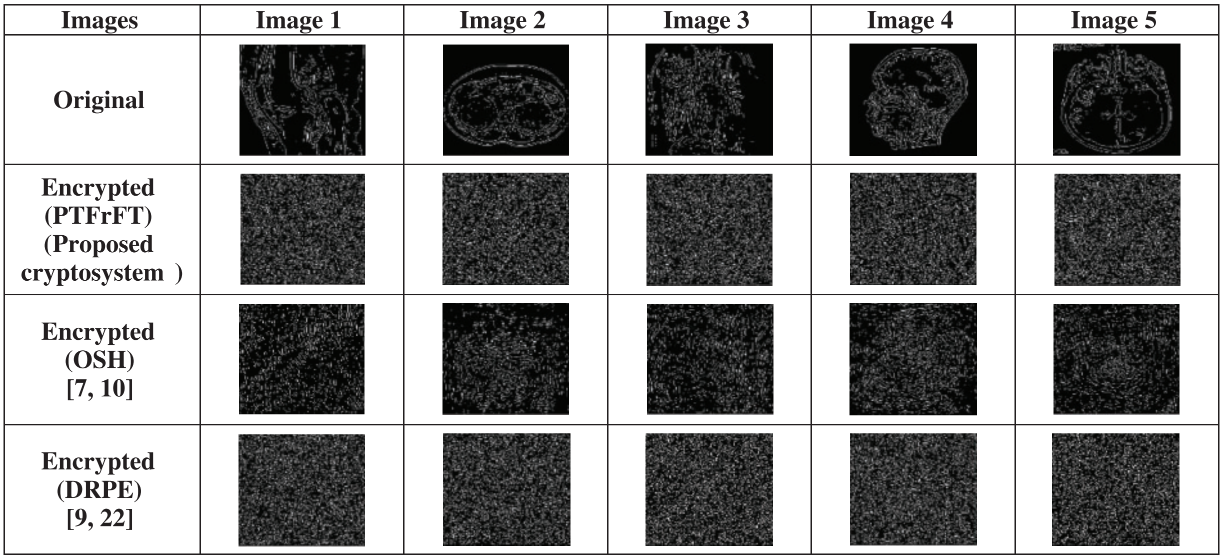


Figure 4: Laplacian edge Gaussian results for the plain and enciphered medical images with the DRPE, OSH, and PTFrFT cryptosystems

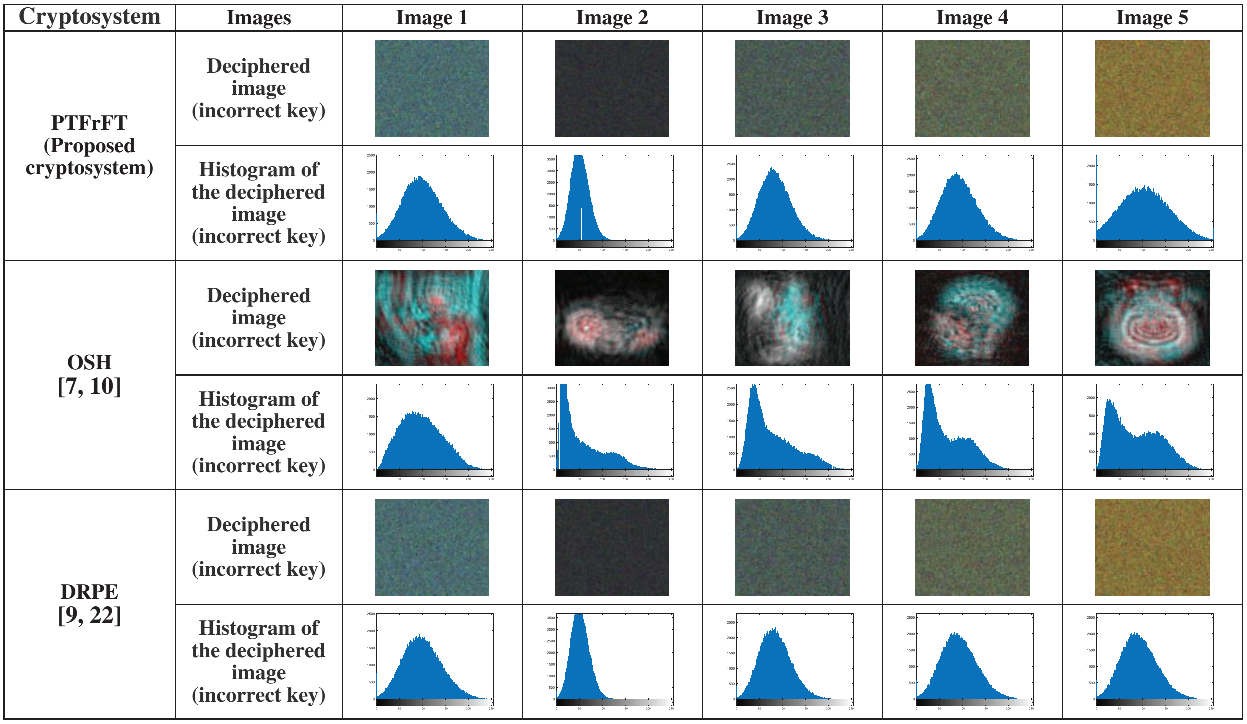


Figure 5: Results of key sensitivity analysis for the DRPE, OSH, and PTFrFT cryptosystems

4.10 Effect of Channel Noise

The transmission network commonly encompasses different types of noise. The proposed decryption process should survive the impact of noise. The effects of Salt and Pepper, Gaussian, and Speckle noise [14,22,47] are investigated in the simulation experiments. Figs. 6–8 display the outcomes of deciphered medical images for the encrypted images presented in Fig. 2 in the presence of noise with different amounts with the proposed PTFrFT and the conventional DRPE and OSH cryptosystems. It is observed that the deciphered color medical images are measurable and discernable if the transmission noise affects the enciphered color medical images. Hence, the proposed cryptosystem has a noticable advantage of resisting the effect of transmission noise compared to the conventional DRPE and OSH cryptosystems.

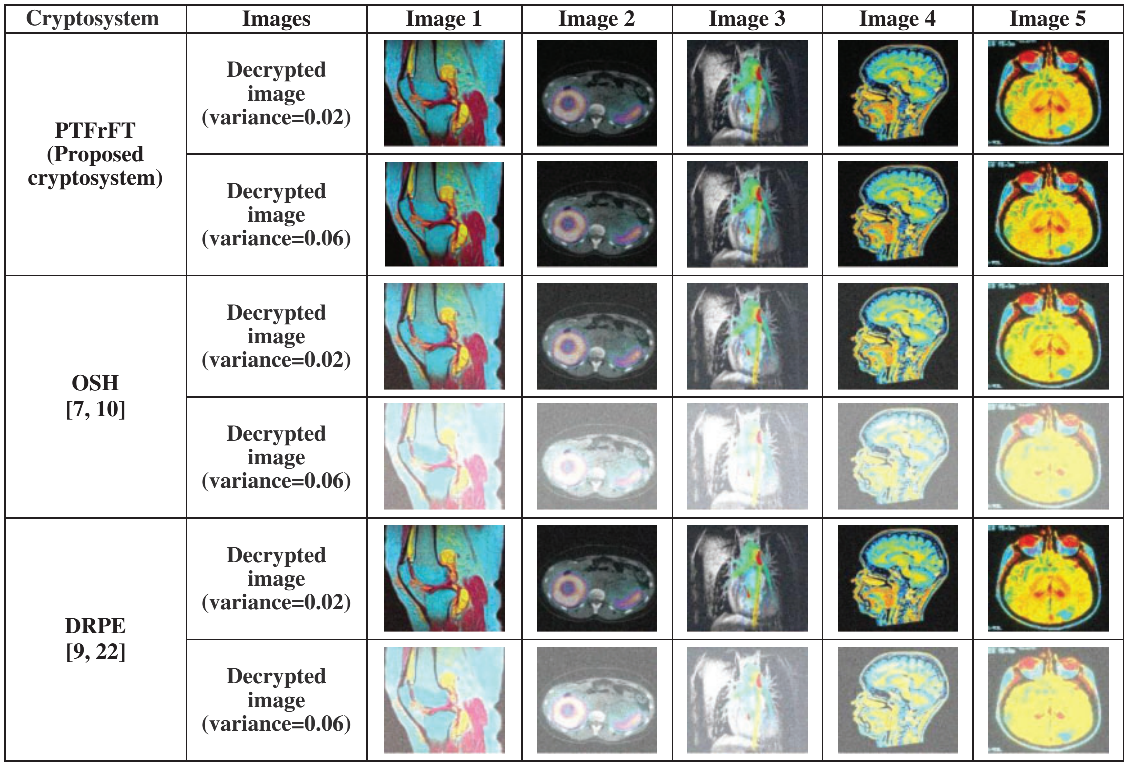

Cryptosystem
Images
Image 1
Image 2
Image 3
Image 4
Image 5
PTFrFT (Proposed cryptosystem)
Decrypted image (variance=0.02)
Decrypted image (variance=0.06)
OSH [7, 10]
Decrypted image (variance=0.02)
Decrypted image (variance=0.06)
DRPE [9, 22]
Decrypted image (variance=0.02)
Decrypted image (variance=0.06)

Figure 6: Decrypted images in the presence of Gaussian noise with the DRPE, OSH, and PTFrFT cryptosystems

4.11 Computational Processing Analysis

It is recommended for any cryptosystem to have less computations in addition to high security and efficacy. Tab. 9 presents the estimated values of the encryption/decryption times for the DRPE, OSH, and PTFrFT cryptosystems. The estimated encryption/decryption computation times provide evidence that the suggested cryptosystem is highly appropriate for real-time telemedicine services compared to other conventional cryptosystems.

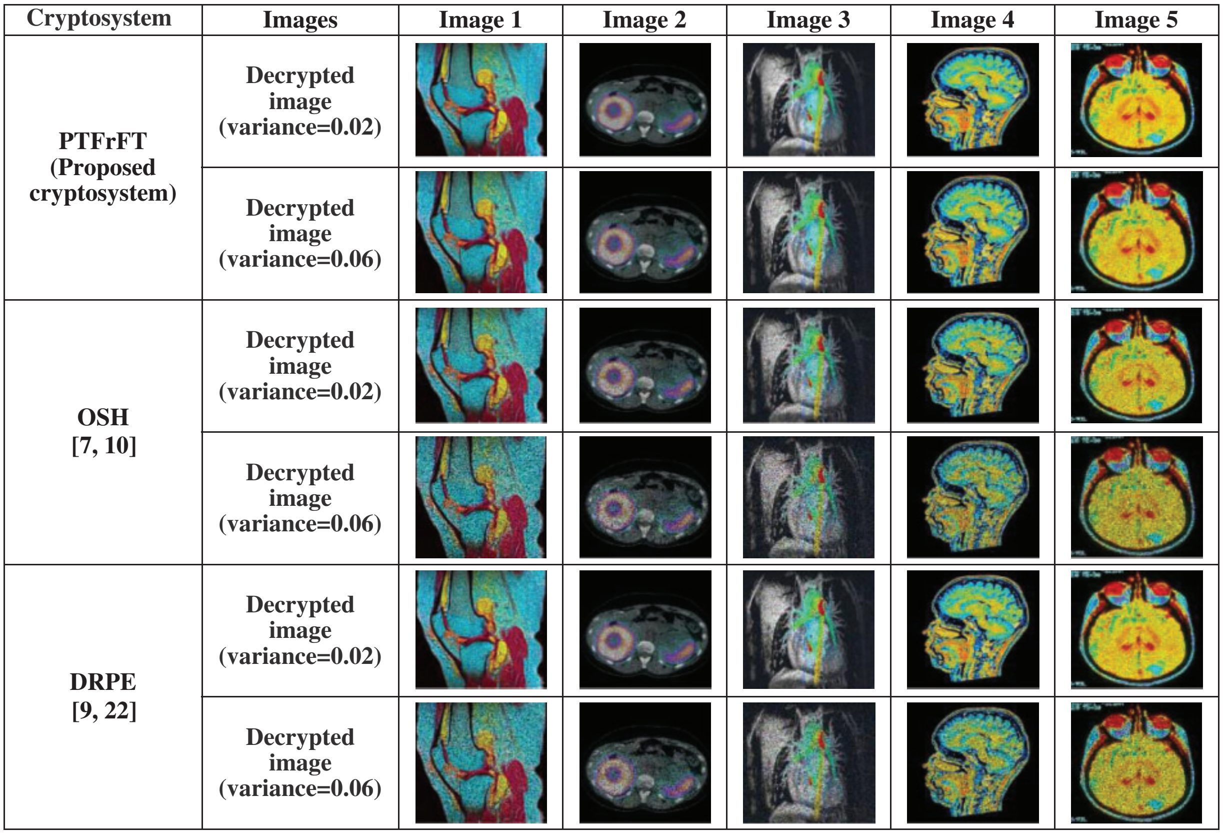

Cryptosystem
Images
Image 1
Image 2
Image 3
Image 4
Image 5
PTFrFT (Proposed cryptosystem)
Decrypted image (variance=0.02)
Decrypted image (variance=0.06)
OSH [7, 10]
Decrypted image (variance=0.02)
Decrypted image (variance=0.06)
DRPE [9, 22]
Decrypted image (variance=0.02)
Decrypted image (variance=0.06)

Figure 7: Decrypted images in the presence of Speckle noise with the DRPE, OSH, and PTFrFT cryptosystems

4.12 Comparative Study

In this section, we introduce a comprehensive comparative study for evaluating the performance of the proposed cryptosystem for confident color medical image transmission compared to the recent studies [3–6,8,11–21,29,30,32,34] using the color Lena image. The outcomes of the average UACI, correlation, entropy, PSNR, and NPCR values for the enciphered color image are demonstrated in Tab. 10. It is noticed that all security evaluation metrics of the proposed cryptosystem are close or superior to those of the previous studies. Thus, the proposed optical cryptosystem can survive various types of multimedia attacks due to its robustness and reliability compared to related cryptosystems. It also achieves a higher level of confusion efficacy. The obtained outcomes reveal that the proposed optical cryptosystem has minimal complications and good resistance to various types of attacks compared to the conventional cryptosystems. In summary, the proposed cryptosystem provides more robustness and security and higher speed.

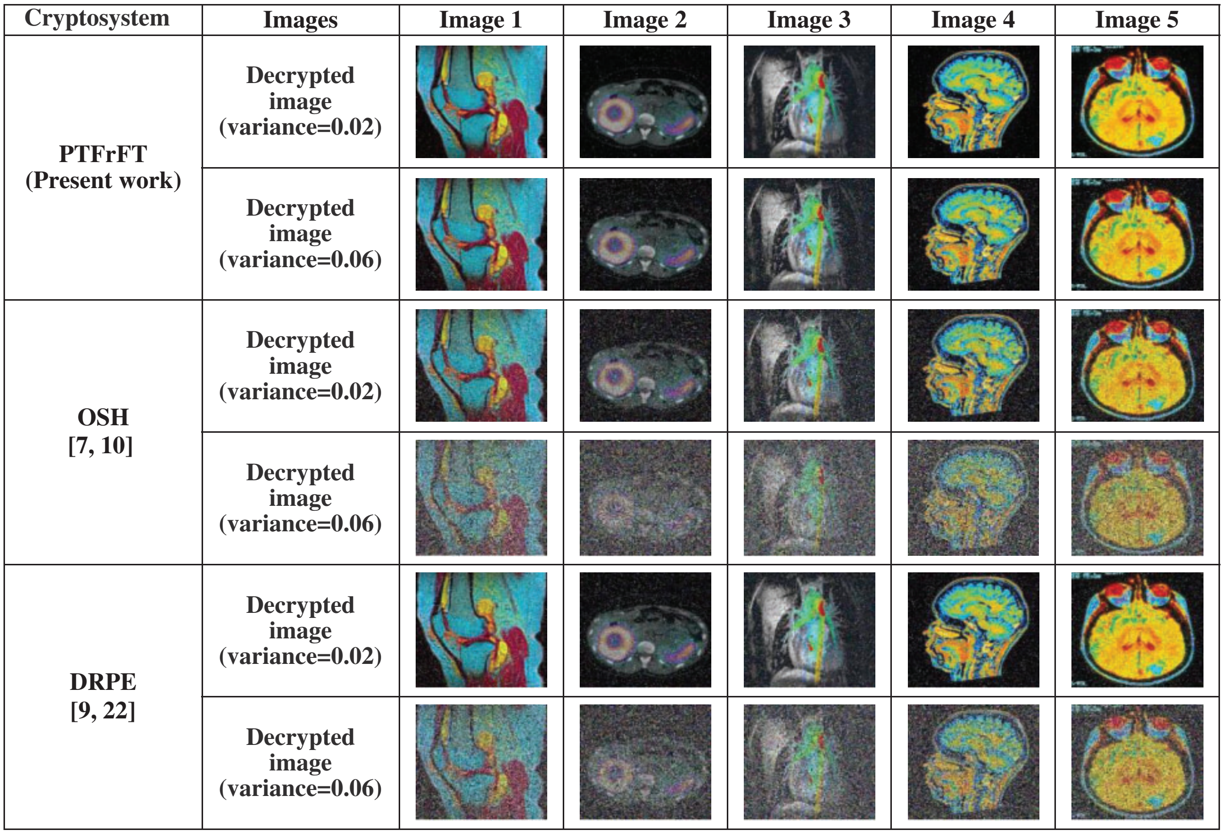

Cryptosystem
Images
Image 1
Image 2
Image 3
Image 4
Image 5
PTFrFT (Present work)
Decrypted image (variance=0.02)
Decrypted image (variance=0.06)
OSH [7, 10]
Decrypted image (variance=0.02)
Decrypted image (variance=0.06)
DRPE [9, 22]
Decrypted image (variance=0.02)
Decrypted image (variance=0.06)

Figure 8: Decrypted images in the presence of Salt and Pepper noise with the DRPE, OSH, and PTFrFT cryptosystems

Table 9: Encryption/decryption times for the DRPE, OSH, and PTFrFT cryptosystems

Image	Computational time (s)		
	DRPE [9,22]	OSH [7,10]	PTFrFT (proposed cryptosystem)
Image 1	3.2934	4.6586	3.2527
Image 2	3.4528	4.8272	3.1596
Image 3	3.4294	4.4495	3.2047
Image 4	3.6364	5.6271	3.3576
Image 5	3.8982	5.7937	3.2129

Table 10: Comparative study of the proposed cryptosystem and recent related cryptosystems

Cryptosystem	PSNR (dB)	Correlation	Entropy	UACI	NPCR
[3]	–	0.0578	7.9878	0.3397	0.9941
[4]	–	0.0069	7.9952	–	–
[5]	31.57	0.04267	7.9983	0.3311	0.9954
[6]	30.50	0.0004	7.9896	0.3346	0.9967
[8]	–	0.0042	7.9970	0.3352	0.9962
[11]	–	0.0037	7.9927	0.3351	0.9959
[12]	–	−0.0025	7.9972	0.3360	0.9963
[13]	33.87	0.0011	7.9975	0.3358	0.9951
[14]	32.31	0.0130	7.9971	0.3342	0.9961
[15]	32.42	0.0053	7.9893	0.3325	0.9928
[16]	30.84	0.0088	7.9973	0.3357	0.9960
[17]	–	0.0025	7.9909	–	–
[18]	–	0.0116	7.9972	0.3341	0.9946
[19]	33.57	0.0023	7.9896	0.3347	0.9961
[20]	–	0.0032	7.9984	0.3368	0.9952
[21]	–	0.0000327	7.9980	0.3345	0.9975
[29]	–	0.0011	7.9987	0.3330	0.9925
[30]	–	0.003768	7.9895	0.3347	0.9963
[32]	–	0.0274	–	0.3328	0.9937
[34]	–	0.0081	7.9927	0.3342	0.9927
Present work	35.69	−0.00248	7.99837	0.33284	0.99628

5 Conclusion and Suggestions for Future Work

A secure optical cryptosystem was suggested for efficient color medical image communication. It is based on the utilization of the optical asymmetric PTFrFT algorithm. In the proposed cryptosystem, a multi-stage FrFT with different fractional orders is exploited for allowing a secure and robust color medical image transmission for telemedicine applications. The suggested asymmetric cryptosystem depends on two-phase distributions in the fractional Fourier and output planes as decryption keys. Comparison and simulation experiments have been carried out to compare the proposed optical cryptosystem with other optical and digital cryptosystems. The obtained results confirmed the exciting success of the proposed optical cryptosystem in meritoriously ciphering the transmitted color medical images. Subsequently, it is highly appreciated for safeguarding medical image telemedicine services rather than the conventional optical and digital cryptosystems. In the future work, we plan to test the proposed cryptosystem on 3D medical images with different modalities. A hybrid cryptosystem of digital and optical encryption algorithms could be introduced to merge their main advantages for achieving high robustness and security of medical image communication.

Acknowledgement: The authors would like to thank the support of the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University.

Funding statement: This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-track Research Funding Program to support publication in the top journal (Grant no. 42-FTTJ-12).

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

References

[1] M. Chen, G. Ma, C. Tang and Z. Lei, “Generalized optical encryption framework based on shearlets for medical image,” *Optics and Lasers in Engineering*, vol. 128, pp. 1–10, 2020.

[2] H. Nematzadeh, R. Enayatifar, H. Motameni, F. Guimarães and V. Coelho, “Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices,” *Optics and Lasers in Engineering*, vol. 110, pp. 24–32, 2018.

[3] 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.

[4] 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.

[5] 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.

[6] X. Wu, H. Kan and J. Kurths, “A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps,” *Applied Soft Computing*, vol. 37, pp. 24–39, 2015.

[7] L. Zhang, X. Zhou, D. Wang, N. Li, X. Bai *et al.,* “Multiple-image encryption based on optical scanning holography using orthogonal compressive sensing and random phase mask,” *Optical Engineering*, vol. 59, no. 10, pp. 1–13, 2020.

[8] X. Wang and H. Zhang, “A color image encryption with heterogeneous bit-permutation and correlated chaos,” *Optics Communications*, vol. 342, pp. 51–60, 2015.

[9] J. Vilardy, M. Millán and E. Pérez-Cabré, “Experimental optical encryption scheme for the double random phase encoding using a nonlinear joint transform correlator,” *Optik*, vol. 217, pp. 1–7, 2020.

[10] P. Tsang, A. Yan, T. Poon and H. Lam, “Asymmetrical and biometric encrypted optical scanning holography (ABE-OSH),” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1094–1101, 2019.

[11] 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, pp. 79–86, 2016.

[12] X. Wang, H. Zhang and X. Bao, “Color image encryption scheme using CML and DNA sequence operations,” *Biosystems*, vol. 144, pp. 18–26, 2016.

[13] 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.

[14] X. Chai, Z. Gan, K. Yang, Y. Chen and X. Liu, “An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations,” *Signal Processing: Image Communication*, vol. 52, pp. 6–19, 2017.

[15] 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, pp. 197–213, 2017.

[16] 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.

[17] 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.

[18] A. Niyat, M. Moattar and M. Torshiz, “Color image encryption based on hybrid hyper-chaotic system and cellular automata,” *Optics and Lasers in Engineering*, vol. 90, pp. 225–237, 2017.

[19] X. Wu, K. Wang, X. Wang, H. Kan and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Processing*, vol. 148, pp. 272–287, 2018.

[20] J. Wu, X. Liao and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11–23, 2018.

[21] P. Sneha, S. Sankar and A. Kumar, "A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold-Tent maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1289–1308, 2020.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] O. Faragallah, M. AlZain, H. El-Sayed, J. Al-Amri, W. El-Shafa *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.

[27] 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.

[28] 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, pp. 1–26, 2020.

[29] W. Auyporn and S. Vongpradhip, "A robust image encryption method based on bit plane decomposition and multiple chaotic maps," *International Journal of Signal Processing Systems*, vol. 3, no. 1, pp. 8–13, 2015.

[30] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Processing*, vol. 113, pp. 104–112, 2015.

[31] E. Lee and K. Park, "Image restoration of skin scattering and optical blurring for finger vein recognition," *Optics and Lasers in Engineering*, vol. 49, no. 7, pp. 816–828, 2011.

[32] S. Banerjee, S. Mukhopadhyay and L. Rondoni, "Multi-image encryption based on synchronization of chaotic lasers and iris authentication," *Optics and Lasers in Engineering*, vol. 50, no. 7, pp. 950–957, 2012.

[33] N. Saini and A. Sinha, "Biometrics based key management of double random phase encoding scheme using error control codes," *Optics and Lasers in Engineering*, vol. 51, no. 8, pp. 1014–1022, 2013.

[34] G. Verma, M. Liao, D. Lu, W. He, X. Peng *et al.,* "An optical asymmetric encryption scheme with biometric keys," *Optics and Lasers in Engineering*, vol. 116, pp. 32–40, 2019.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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. 984–988, 2018.

[44] 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.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] P. Li and K. 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.

[57] 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.

[58] 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.