Fatma KHALLAF, Walid EL-SHAFAI, El-Sayed M. EL-RABAIE, Naglaa F. SOLIMAN, Fathi E. Abd EL-SAMIE, 2023. A novel hybrid cryptosystem based on DQFrFT watermarking and 3D-CLM encryption for healthcare services. *Frontiers of Information Technology & Electronic Engineering*, 24(7):1045-1061. https://doi.org/10.1631/FITEE.2200372

A novel hybrid cryptosystem based on DQFrFT watermarking and 3D-CLM encryption for healthcare services

Key words: Color medical image; Quaternion; Adaptive watermarking; Encryption; Fractional transform; Three-dimensional chaotic logistic map (3D-CLM)

Corresponding author: Walid EL-SHAFAI
E-mail: eng.waled.elshafai@gmail.com

ORCID: https://orcid.org/0000-0001-7509-2120

Motivation

- Securing color medical images in healthcare applications has become a challenging issue, which motivated us to design a novel hybrid cryptosystem based on discrete quaternion fractional Fourier transform (DQFrFT) watermarking and three-dimensional chaotic logistic map (3D-CLM) encryption for healthcare services.
- The proposed technique is based on a combination of high efficiency DQFrFT watermarking and the implementation of an effective medical image cryptography system based on higher-order chaos functions.
- We implement an effective medical image cryptography system based on a higher-order of chaos functions.

Multistage privacy system for color medical images based on DQFrFT, support vector machine (SVM) watermarking, and 3D-CLM encryption

System model

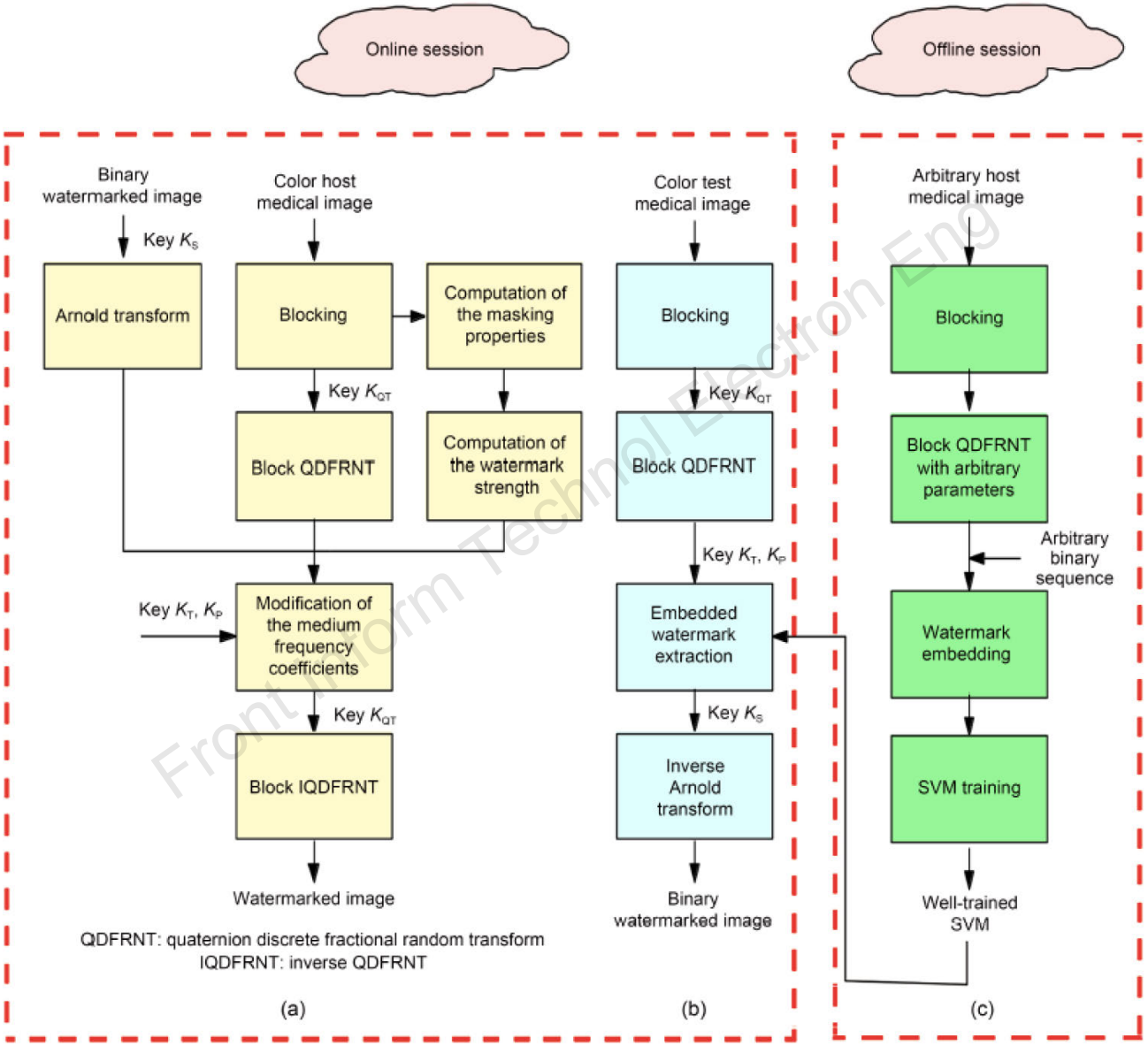


Fig. 1 Online and offline session diagrams for the proposed color medical image adaptive watermarking system: (a) watermark embedding; (b) watermark extraction; (c) support vector machine (SVM) training

Proposed color medical image watermarking scheme (stage 1)

This scheme has two parts: an online session for both watermark embedding and extraction and an offline SVM training session.

- Online watermark embedding

1. Watermark preprocessing
2. Quaternion discrete fractional random transform (QDFRNT) block and masking characteristic calculations
3. Position selection for embedding
4. Embedding a watermark with adjustable watermark strength
5. Watermarked image generation

Proposed color medical image watermarking scheme (stage 1)

- Offline SVM training

1. Create a random binary sequential **BS** of length L. The length L should be greater than 50 to keep SVM efficient.
2. From step 2 to step 4, embed the sequence **BS** into an arbitrary host image using the embedding method, with random order α, periodicity M, random matrix $\boldsymbol{P}$, unit pure quaternion μ, and basic strength Δ_0, to produce the modifying QDFRNT coefficients $Y'_q(u_l, v_l)$ ($l = 1, 2, ..., L$).
3. Compute the set S_{u_1,v_1} for each embedding position (ul, vl), l = 1, 2,..., L using

$$S_{u_1,v_1} = \{\delta_{u_l-1,v_l-1}, \delta_{u_l-1,v_l}, \delta_{u_l-1,v_l+1}, \delta_{u_l,v_l-1}, \delta_{u_l,v_l}, \delta_{u_l,v_l+1}, \delta_{u_l+1,v_l-1}, \delta_{u_l+1,v_l}, \delta_{u_l+1,v_l+1}\}.$$

Consider each set S_{u_1,v_1} as the input to a sample and BS(l) as the output. Then, these samples are trained, and the well-trained SVM model is used as a classifier. It can be sent to the recipient, or the receiver can train the SVM model using our technique and random parameters.

Proposed color medical image watermarking scheme (stage 1)

- Online watermark extraction

1. Calculate the QDFRNT coefficients for each block of 8×8 pixels using order K_{QT_α}, unit pure quaternion K_{QT_μ}, periodicity.K_{QT_M}, and random matrix K_{QT_P}.
2. Calculate the set S_{u_1,v_1} for all embedding positions (u_l, v_l).
3. Reconfigure the bits **WS** into a 2D binary watermark image of size

$$\sqrt{\text{size}(K_p)/K_T} \times \sqrt{\text{size}(K_p)/K_T}.$$

Proposed 3D-CLM encryption scheme (stage 2)

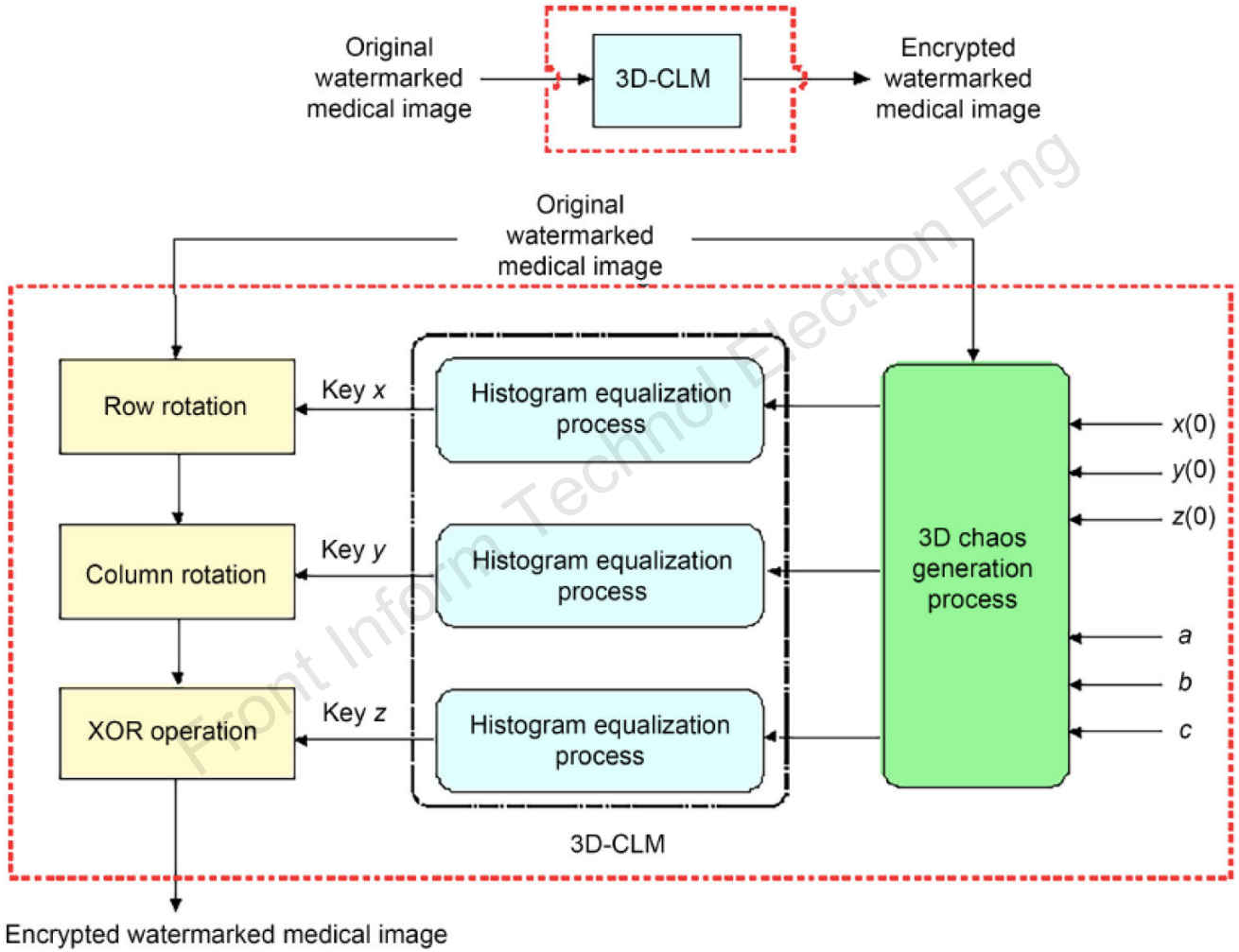


Fig. 2 Block diagram of the proposed three-dimensional chaotic logistic map (3D-CLM) encryption scheme

Δ_0

Proposed 3D-CLM encryption scheme (stage 2)

- In recent years, the chaos process has attracted much attention because its operation produces noise-like signals. The chaos-based encryption process has appreciated features of confusion, sensitivity to primary value, and diffusion. There are many chaotic maps in the most recent works, such as the Arnold map, logistic map, and cat map.

Simulation results

- These tests are implemented using Intel® Core™ i7-7700HQ CPU @2.80 GHz with 16 GB RAM and employing MATLAB 2020b. For 1D QDFRNT, five 512-bit 1D quaternion signals are created at random, whereas for 2D QDFRNT, five color medical images of size 512×512 are employed. The size of the color medical image is $m \times n$ in all the equations, where m represents height and n represents width.
- Here, we present only one sample.

Evaluation of the first stage of the proposed system (watermarking)

Fig. 3 Binary watermark image (a) and encrypted watermarked image (b) with the Arnold scheme

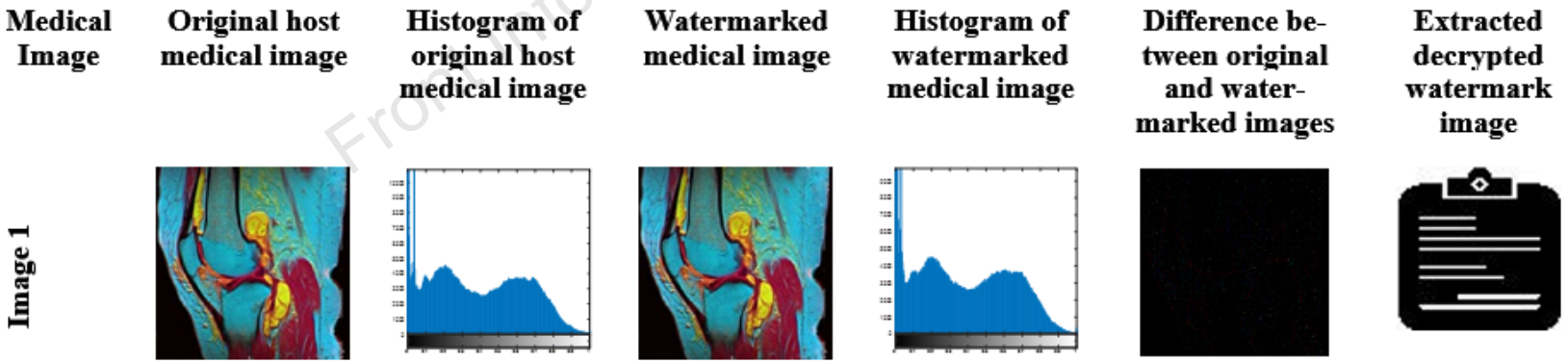


Fig. 4 Subjective results of the first stage for the examined medical images in absence of attacks

Evaluation of the first stage of the proposed system (watermarking)

Table 1 Objective results of the first stage for the examined color medical image 1 in the absence of attacks

Watermarked medical image			Extracted watermarked image			
PSNR (dB)	SSIM	FSIM	SSIM	FSIM	BER	Correlation
82.63	1.0000	0.9999	1.0000	0.9999	0.0050	0.9987

PSNR: peak signal-to-noise ratio; SSIM: structural similarity; FSIM: feature similarity; BER: bit error rate

Table 2 Objective results of the extracted watermarked images for the examined medical image 1 in the case of rotation and Gaussian noise attacks

Parameter	Rotation attack			Gaussian noise attack		
	5°	10°	20°	σ=0.02	σ=0.04	σ=0.06
SSIM	0.9462	0.9451	0.9397	0.9752	0.9738	0.9712
FSIM	0.9262	0.9207	0.9168	0.9604	0.9591	0.9564
BER	0.0098	0.0108	0.0137	0.0067	0.0073	0.0087
Correlation	0.9384	0.9337	0.9217	0.9704	0.9615	0.9553

SSIM: structural similarity; FSIM: feature similarity; BER: bit error rate

Evaluation of the first stage of the proposed system (watermarking)

Table 3 Objective results of the extracted watermarked images for the examined medical image 1 with different attacks

Parameter	Motion blur	Disk blur	Average blur	JPEG 20%	JPEG 40%	JPEG 60%	Resizing attack	Crop attack
SSIM	0.9864	0.9829	0.9860	0.9833	0.9836	0.9839	0.9907	0.9897
FSIM	0.9859	0.9831	0.9853	0.9842	0.9846	0.9849	0.9896	0.9886
BER	0.0052	0.0073	0.0064	0.0058	0.0056	0.0053	0.0053	0.0069
Correlation	0.9759	0.9727	0.9749	0.9742	0.9744	0.9747	0.9957	0.9943

SSIM: structural similarity; FSIM: feature similarity; BER: bit error rate

Table 4 Average embedding time of the first stage for the examined color medical image 1

Medical image	Average embedding time (s)
Image 1	2.52

Evaluation of the full proposed system (encryption)

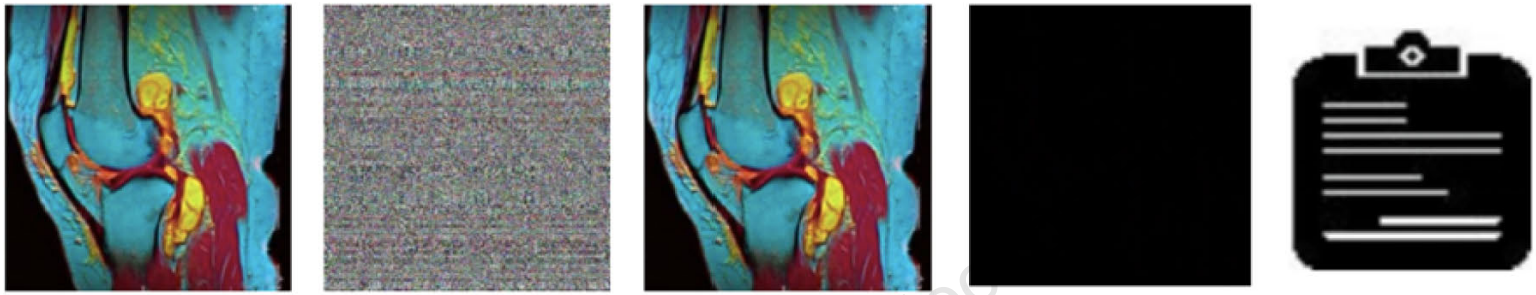


Fig. 5 Subjective results of the second stage for the examined medical image 1: (a) original watermarked medical image; (b) encrypted watermarked medical image; (c) decrypted watermarked medical image; (d) difference between the original and decrypted watermarked images; (e) extracted decrypted watermarked image after the decryption process

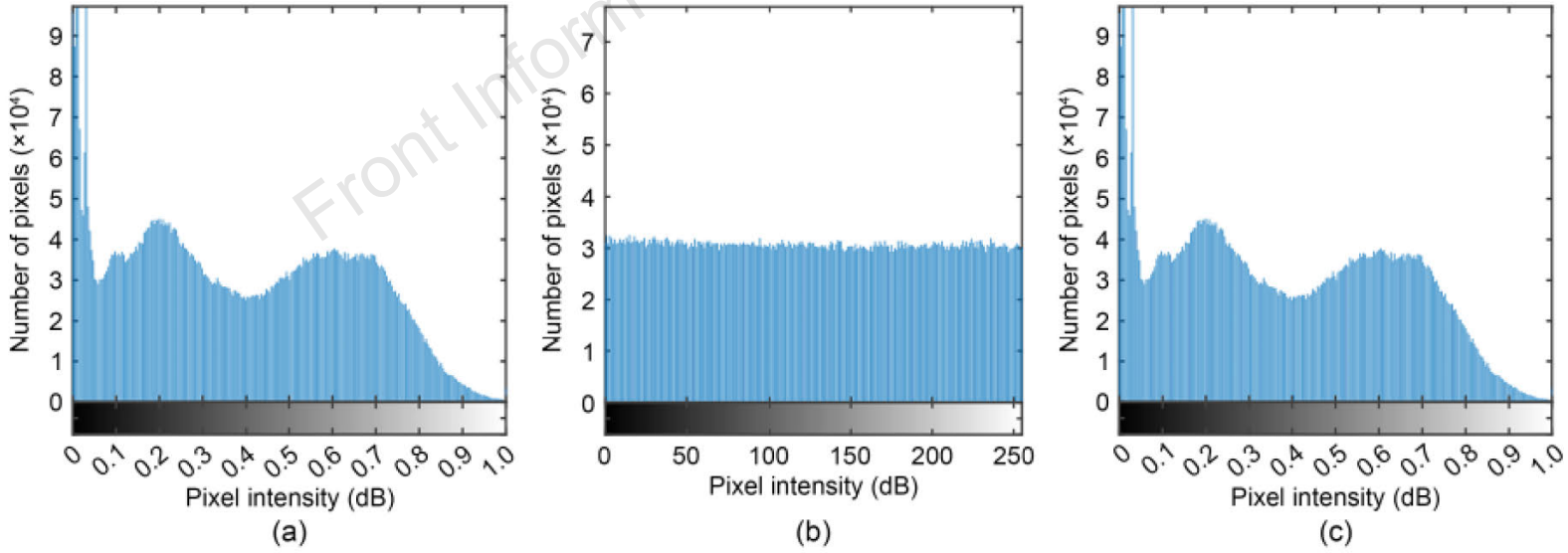


Fig. 6 Histogram of the original (a), encrypted (b), and decrypted (c) watermarked medical image 1

Evaluation of the full proposed system (encryption)

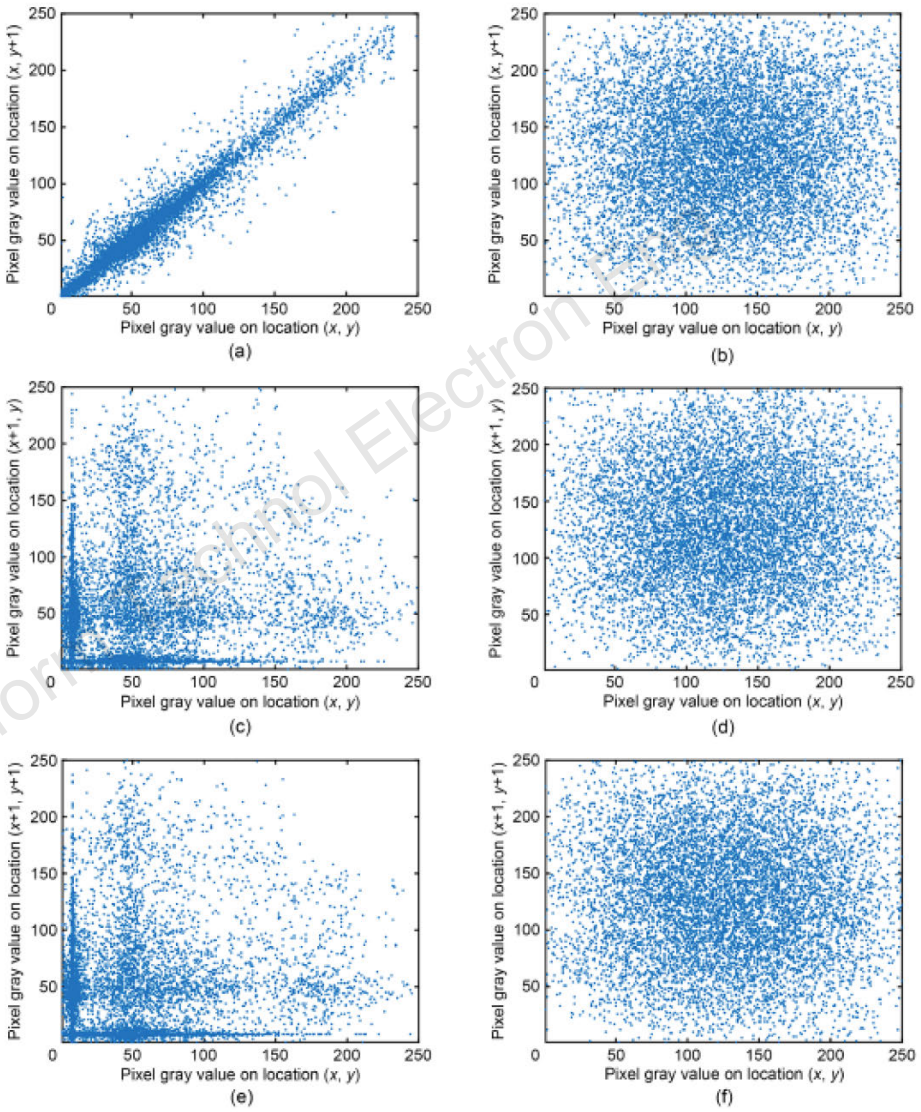


Fig. 7 Horizontal (H), vertical (V), and diagonal (D) correlation results of two adjacent pixels in the original and encrypted watermarked medical images of the tested medical image 1: (a) H direction in the original watermarked medical image; (b) H direction in the encrypted watermarked medical image; (c) V direction in the original watermarked medical image; (d) V direction in the encrypted watermarked medical image; (e) D direction in the original watermarked medical image; (f) D direction in the encrypted watermarked medical image

Evaluation of the full proposed system (encryption)

Table 5 Correlation coefficients in the original, encrypted, and decrypted watermarked medical image 1

Image	Correlation coefficient		
	Horizontal	Vertical	Diagonal
Original	0.9413	0.9819	0.9262
Encrypted	0.1666	0.0445	0.0892
Decrypted	0.9413	0.9819	0.9262

Table 6 Information entropies of the tested plain, ciphered, and deciphered watermarked medical image 1

Image	Information entropy
Original	7.6715
Encrypted	7.7849
Decrypted	7.6715

Evaluation of the full proposed system (encryption)

Table 7 PSNR, SSIM, and FSIM results between plain and ciphered watermarked medical image 1

PSNR (dB)	SSIM	FSIM
8.7738	0.0107	0.5506

PSNR: peak signal-to-noise ratio; SSIM: structural similarity; FSIM: feature similarity

Table 8 Results of ciphered watermarked medical image 1

NPCR	UACI	H_D	D_I	EDR
0.9960	0.3346	6.1023	0.0076	0.9095

NPCR: number of pixel change rate; UACI: unified average changing intensity; EDR: edge detection ratio

Evaluation of the full proposed system (encryption)

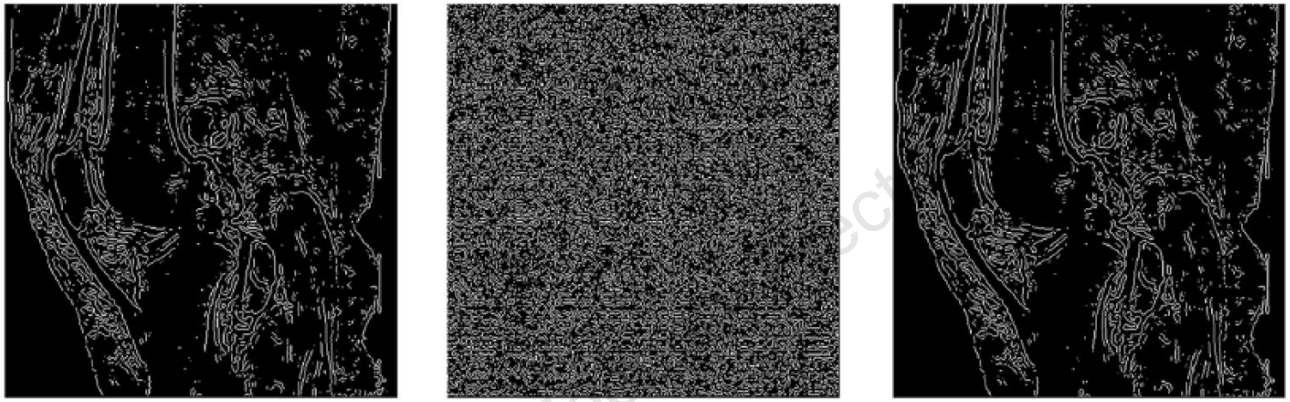


Fig. 8 Laplacian of Gaussian edge detection results of watermarked medical image 1: (a) original; (b) encrypted; (c) decrypted

Evaluation of the full proposed system (encryption)

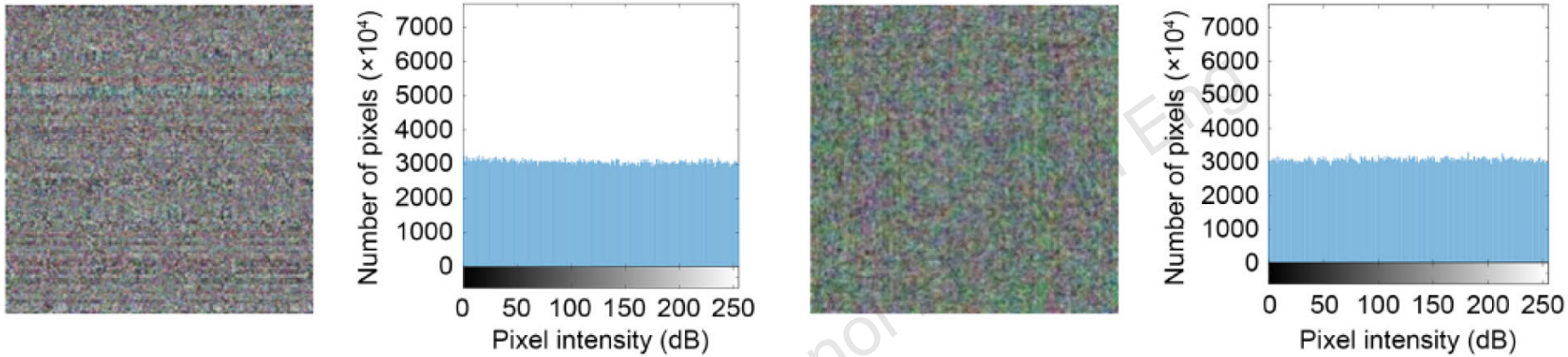


Fig. 9 Key sensitivity results for the examined medical image 1: (a) encrypted image using the correct key; (b) histogram of the encrypted image using the correct key; (c) decrypted image using an incorrect key; (d) histogram of the decrypted image using an incorrect key

Table 9 Processing time of encrypted watermarked medical image 1

Medical image	Time (s)
Image 1	3.92

Noise attack analysis

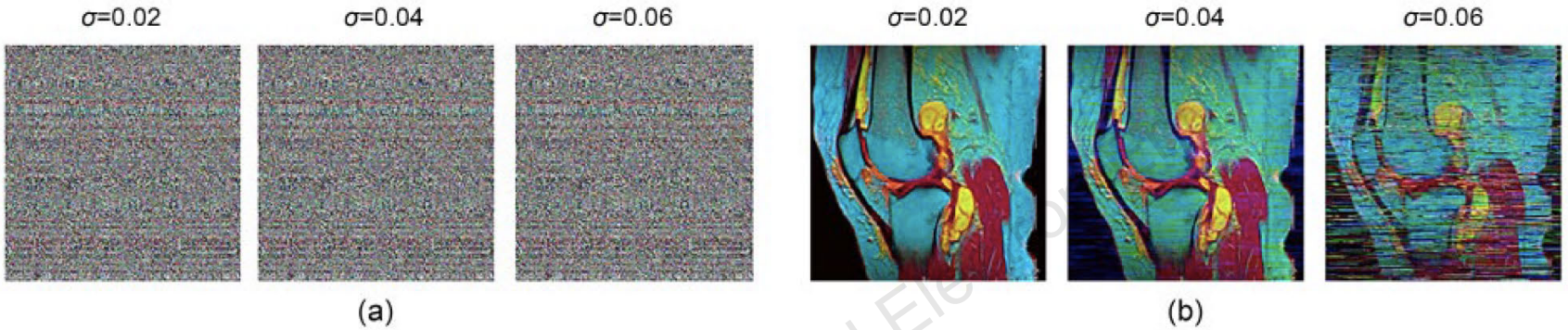


Fig. 10 Encrypted (a) and decrypted (b) watermarked medical image 1 in the presence of Gaussian noise with different noise variances (μ=0)

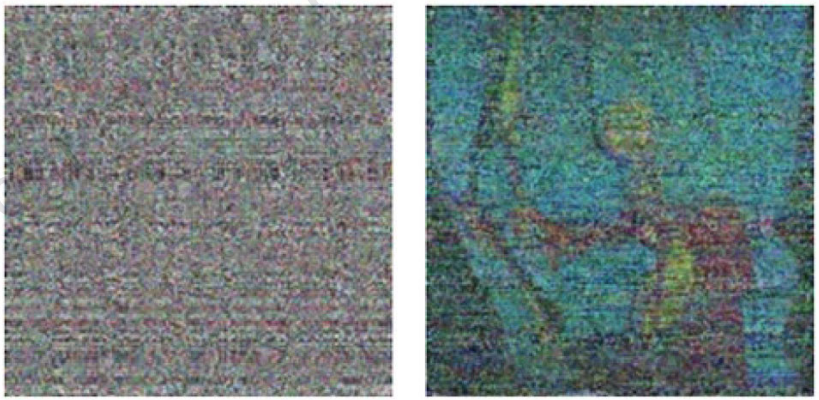


Fig. 11 Encrypted (a) and decrypted (b) watermarked image 1 in the presence of Poisson noise

Noise attack analysis

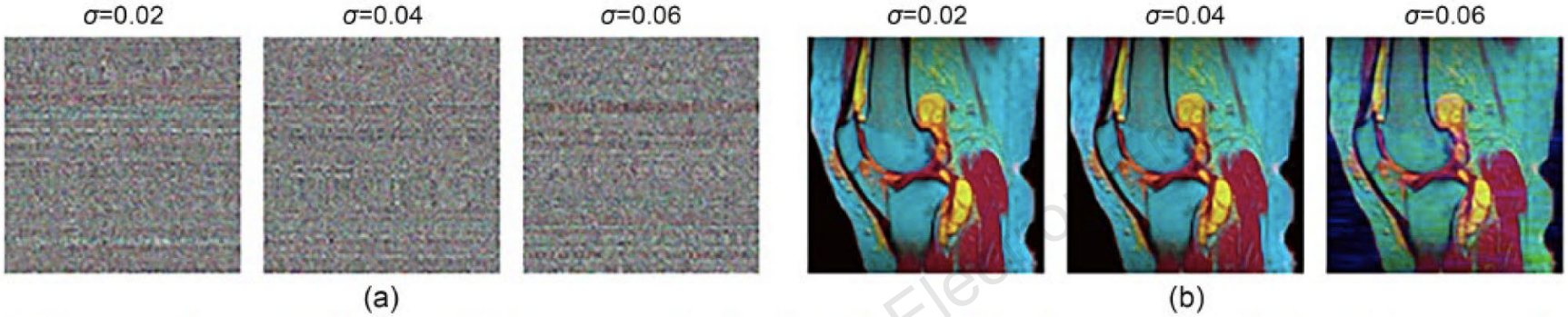


Fig. 12 Encrypted (a) and decrypted (b) watermarked medical image 1 in the presence of salt-and-pepper noise with different noise variances

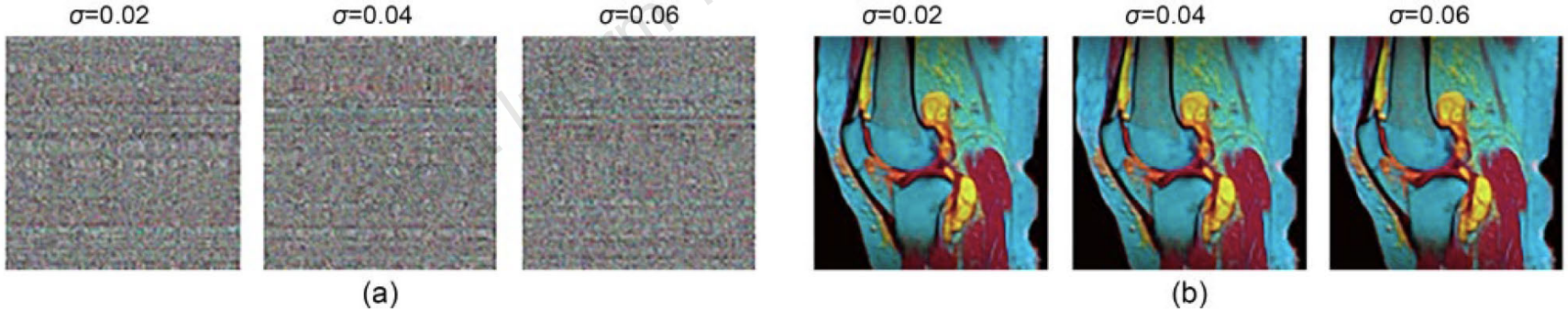
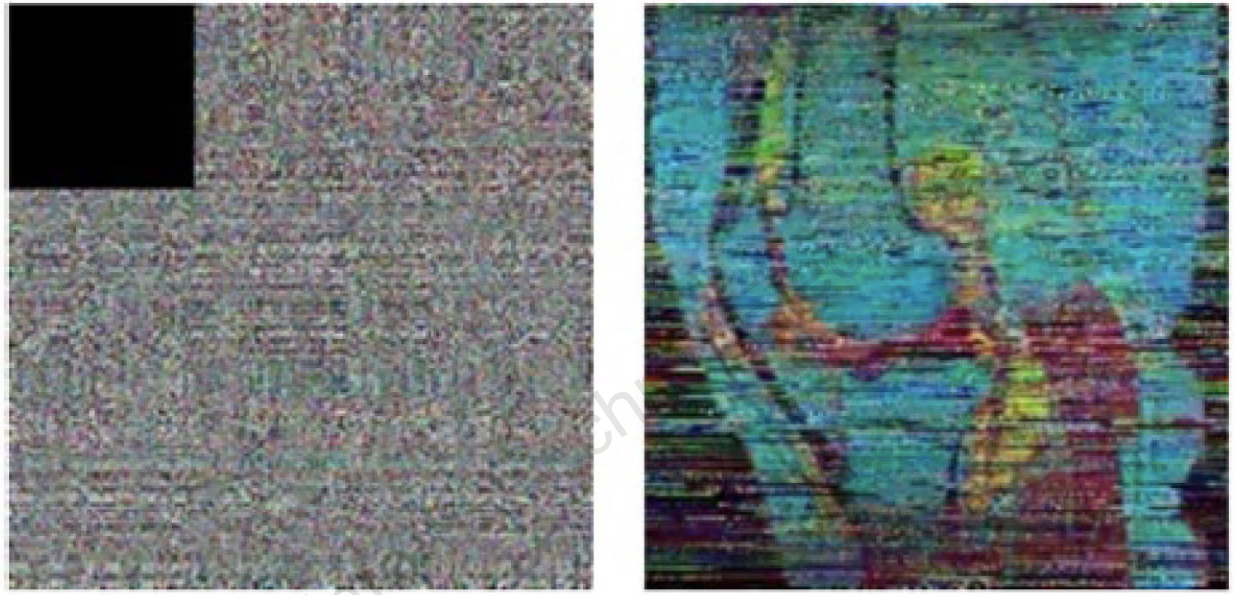


Fig. 13 Encrypted (a) and decrypted (b) watermarked medical image 1 in the presence of speckle noise with different noise variances

Noise attack analysis



(a) (b)

Fig. 14 Encrypted (a) and decrypted (b) watermarked medical images in the presence of occlusion attack on the encrypted images

Competitive study

Furthermore, more simulation tests are carried out to compare the proposed security algorithm with state-of-the-art techniques to validate the security and robustness efficiency of the multilevel security algorithm.

Table 10 presents the evaluation results of the full proposed system (encryption) in comparison with the related work without the presence of attacks. Comparison results show that the suggested security work achieves lower average runtime values for the examined color medical images than the conventional techniques. Moreover, it shows that this paper studies all evaluation metrics with and without noise attack, unlike other papers.

Competitive study

Table 10 Comparisons with related works

Reference	Correlation coefficient*			PSNR (dB)	Entropy**	NPCR
	Horizontal	Vertical	Diagonal			
Daoui et al. (2022)	0.0082	−0.0035	−0.0036	–	–	–
Faragallah et al. (2019)	–	–	–	54.2100	–	–
Khafaga et al. (2022)	–	–	–	–	–	–
Yamni et al. (2021)	–	–	–	20.8050	–	–
This paper (image 2)	0.0466	0.0599	−0.0413	6.3120	7.9410	0.9962

Reference	UACI	SSIM	FSIM	H_D	D_I	EDR	Average runtime (s)
Daoui et al. (2022)	–	–	–	–	–	–	5.4653
Faragallah et al. (2019)	–	–	–	–	–	–	–
Khafaga et al. (2022)	–	–	–	–	–	–	11.7690
Yamni et al. (2021)	–	–	–	–	–	–	13.4568
This paper (image 2)	0.3352	0.0088	0.4317	2.9431	0.0075	0.8938	4.1700

* Encrypted watermarked medical image. ** Encrypted image. PSNR: peak signal-to-noise ratio; NPCR: number of pixel change rate; UACI: unified average changing intensity; SSIM: structural similarity; FSIM: feature similarity; EDR: edge detection ratio

Conclusions

- This paper presents a new privacy scheme for color medical images that combines DQFrFT watermarking and 3D-CLM encryption.
- The QDFRNT is developed to extend DFRNT to quaternion signal processing.
- The QDFRNT of a quaternion signal can be easily obtained by taking the DFRNT of each component, reducing computational complexity compared to the direct method.
- The proposed approach for color image adaptive watermarking using QDFRNT outperforms other systems by directly examining masking characteristics on the color host image and processing all three channels using a quaternion-based method.
- The security of the suggested technique is enhanced by incorporating random matrix and fractional order elements into the QDFRNT.
- Simulation results demonstrate the effectiveness of the proposed system against various types of channel noise attacks.
- Future work aims to expand the application of the suggested technique to other signals to further validate its security and explore hardware implementation using GPUs.

Fatma KHALLAF received her MSc and BSc (with highest honors) degrees in electronics and electrical communications engineering from Menoufia University, Menouf, Egypt, in 2021 and 2017, respectively. She is currently a full-time assistant lecturer at Ahram Canadian University (ACU). Her current research interests include multimedia security and cybersecurity applications, IoT, IIoT, image processing, encryption algorithms, cancellable biometrics, and deep learning in signal processing and communication systems.

Walid EL-SHAFAI was born in Alexandria, Egypt. He received the BSc degree (Honors) in electronics and electrical communication engineering from the Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt, in 2008, the MSc degree from the Egypt-Japan University of Science and Technology (E-JUST), in 2012, and the PhD degree from the Faculty of Electronic Engineering, Menoufia University, in 2019. Since January 2021, he has been joined as a researcher at the Security Engineering Lab (SEL), Prince Sultan University (PSU), Riyadh, Saudi Arabia. He is currently working as a lecturer and an assistant professor with the Electronics and Communication Engineering (ECE) Department, FEE, Menoufia University. His research interests include wireless mobile and multimedia communications systems, image and video signal processing, efficient 2D video/3D multi-view video coding, multi-view video plus depth coding, 3D multi-view video coding and transmission, quality of service and experience, digital communication techniques, cognitive radio networks, adaptive filters design, 3D video watermarking, steganography, encryption, error resilience and concealment algorithms for H.264/AVC, H.264/MVC, and H.265/HEVC video codecs standards, cognitive cryptography, medical image processing, speech processing, security algorithms, software defined networks, the Internet of Things, medical diagnoses applications, FPGA implementations for signal processing algorithms and communication systems, cancellable biometrics and pattern recognition, image and video magnification, artificial intelligence for signal processing algorithms and communication systems, modulation identification and classification, image and video super-resolution and denoising, cybersecurity applications, malware and ransomware detection and analysis, deep learning in signal processing, and communication systems applications. He has several publications in the above research areas in several reputable international and local journals and conferences. Also, he serves as a reviewer for several international journals.

Naglaa F. SOLIMAN received the BSc, MSc, and PhD degrees from the faculty of Engineering, Zagazig University, Egypt in 1999, 2004, and 2011, respectively. She worked at faculty of computer science at PNU, KSA. since 2015 up till now. She has been a teaching staff member with the Department of Electronics and Communications Engineering, Faculty of Engineering, Zagazig University, Egypt. Her current research interests include digital image processing, Information security, multimedia communications, medical image processing, optical signal processing, big data, and cloud computing..

EL-SAYED M. EL-RABAIE received the BSc degree (Honors) in radio communications from Tanta University, Tanta, Egypt, in 1976, the MSc degree in communication systems from Menoufia University, Menouf, Egypt, in 1981, and the PhD degree in microwave device engineering from the Queen's University of Belfast, Belfast, UK, in 1986. In his doctoral research, he has constructed a computer-aided design (CAD) package used in nonlinear circuit simulations-based on the harmonic balance techniques. Until February 1989, he was a postdoctoral fellow with the Department of Electronic Engineering, Queen's University of Belfast. He was invited as a research fellow with the College of Engineering and Technology, Northern Arizona University, Flagstaff, in 1992, and a visiting professor with Ecole Polytechnique de Montréal, Montreal, QC, Canada, in 1994. He is a reviewer of *Accreditation and Quality Assurance* of Egyptian Higher Education and a member of the Scientific Committee for the promotion of professors and assistant professors, from 2019 to 2022. He has authored or coauthored more than 500 papers and 21 text books. His current research interests include device characterization, digital communication systems, and digital image processing. He acts as a reviewer and a member of the editorial board of several scientific journals.

Fathi E. Abd EL-SAMIE received the BSc (Honors), MSc, and PhD from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. He joined the teaching staff of the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2005. He has received the most cited paper award from *Digital Signal Processing* journal in 2008. His current research areas of interest include image enhancement, image restoration, image interpolation, super resolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications.