Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.037655
Article

A Multi-Stage Security Solution for Medical Color Images in Healthcare Applications

Walid El-Shafai[1,2,*], Fatma Khallaf[2,3], El-Sayed M. El-Rabaie[2], Fathi E. Abd El-Samie[2] and Iman Almomani[1,4]

[1]Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh, 11586, Saudi Arabia
[2]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt
[3]Department of Electrical Engineering, Faculty of Engineering, Ahram Canadian University, Giza, Egypt
[4]Computer Science Department, King Abdullah II School of Information Technology, The University of Jordan, Jordan, 11942, Jordan
*Corresponding Author: Walid El-Shafai. Email: welshafai@psu.edu.sa

Received: 12 November 2022; Accepted: 02 February 2023

Abstract: This paper presents a robust multi-stage security solution based on fusion, encryption, and watermarking processes to transmit color healthcare images, efficiently. The presented solution depends on the features of discrete cosine transform (DCT), lifting wavelet transform (LWT), and singular value decomposition (SVD). The primary objective of this proposed solution is to ensure robustness for the color medical watermarked images against transmission attacks. During watermark embedding, the host color medical image is transformed into four sub-bands by employing three stages of LWT. The resulting low-frequency sub-band is then transformed by employing three stages of DCT followed by SVD operation. Furthermore, a fusion process is used for combining different watermarks into a single watermark image. This single fused image is then ciphered using Deoxyribose Nucleic Acid (DNA) encryption to strengthen the security. Then, the DNA-ciphered fused watermark is embedded in the host medical image by applying the suggested watermarking technique to obtain the watermarked image. The main contribution of this work is embedding multiple watermarks to prevent identity theft. In the presence of different multimedia attacks, several simulation tests on different color medical images have been performed. The results prove that the proposed security solution achieves a decent imperceptibility quality with high Peak Signal-to-Noise Ratio (PSNR) values and high correlation between the extracted and original watermark images. Moreover, the watermark image extraction process succeeds in achieving high efficiency in the presence of attacks compared with related works.

Keywords: Medical images; DNA encryption; digital image watermarking; fusion; healthcare applications

1 Introduction

Nowadays, digital multimedia watermarking is heavily used to solve many issues related to media security, privacy, and copyright. Digital watermarking is a method by which a marker is inconspicuously hidden in a noise-tolerant signal, such as an image, audio, or video. In other words, it is used for hiding some data related to the signal in the signal itself. The hidden message imparts a digital signature to the digital content and identifies the owner or the authorized distributor, whichever is the case. This concept is similar to steganography, the difference being in their goals. In steganography, any secret message can be hidden, and the cover signal is simply there to hide this message. On the other hand, in watermarking, the message is related to the actual content of the cover signal [1]. Data watermarking or hiding is an efficient and important scheme in the case of multimedia communication. Many watermarking techniques have been suggested in the literature for different security applications and services, such as copyright protection and authentication, broadcast monitoring, law enforcement, and medical diagnosis.

The security efficiency of any watermarking scheme is a tradeoff between three main watermarking requirements: embedding capacity, imperceptibility, and robustness against communication attacks [2]. Many related works of watermarking schemes were introduced in the literature [1–14]. Zhou et al. [1] suggested a color watermarking scheme that employed two levels of Discrete Wavelet Transform (DWT) on the original and watermark images after separating Red/Green/Blue (RGB) components. This scheme achieved good PSNR and correlation coefficient (CC) results. The disadvantage of this scheme was its low efficiency, when employing higher levels of the DWT. In addition, more attacks like rotation and cropping attacks were not tested. Kumar et al. [2] suggested a blind hybrid gray-scale watermarking approach that is based on fast Haar and redundant wavelet transforms to decompose the original and watermark images. This approach was examined against attacks like Poisson, salt-and-pepper, and speckle noise. The advantage of the suggested technique was introducing good PSNR and C_r values, but at the price of high complexity.

Al-Haj et al. [3] presented a medical image watermarking scheme that is based on the region of interest (ROI) and region of non-interest (RONI) classification process. A multi-level DWT process is employed in this scheme on the RONI. It works on three different watermark images: integrity, authentication, and tampering watermarks. The main advantage of this scheme is that it introduces appreciated security and imperceptibility. Ghosh et al. [4] introduced hybrid watermarking and cryptography schemes to efficiently transmit digital images. Their main work is based on the Hamming code, XOR process, and the least significant bit (LSB) methods. This scheme has good robustness and imperceptibility, but it was employed in the spatial domain, not in the transform domain.

Kumar et al. [5] suggested a block-based copyright protection and authentication technique based on the LSB insertion process for digital image communication. It guarantees good perceptibility results with high watermark robustness, but its efficiency was not tested and evaluated against the communication attacks. Malonia et al. [6] introduced a color image watermarking scheme that employed arithmetic progression and DWT processes. It presented higher robustness and good perceptibility.

Recently, different DCT and LWT-based image watermarking techniques have been introduced. Chen et al. [7] suggested a robust and secure copyright protection technique based on the LWT process. Tomar et al. [8] presented a hybrid structure of DCT and LWT image watermarking schemes. Mishra et al. [9] introduced an efficient LWT-based color video watermarking technique that applied machine learning and deep neural network methods. This technique performance was evaluated against various image processing attacks. Lalitha et al. [10] presented a hybrid secure approach for high-capacity audio and image watermarking based on LWT, SVD, DWT, and DCT. The disadvantage of this hybrid approach is its complexity without achieving higher robustness against attacks.

DNA encoding and chaos-based image ciphering techniques were recently introduced for efficient cryptography performance [11,12]. Wang et al. [13] proposed an algorithm that consists of two parts. The first part comprises the piecewise linear chaotic map and other chaos methods to generate an image key. The second part is the key and plain image encoding using the DNA rules and logistic map. Preet et al. [14] developed a mixture of multiple image watermarking and ciphering algorithms using LWT, DCT, and Arnold transformation.

Many research works discussed medical security, IoT, and data hiding. Huang et al. designed a healthcare system (HES) that depends on wireless body area networks (WBANs) to collect medical data. Then, the medical data is transmited through a wireless sensor network and published via a gateway [15]. Huang et al. [16] introduced a hybrid approach that considers encryption and data hiding. The image becomes secure by focusing on compressed sensing (CS). During the quantization stage, the sign bits of the CS are encrypted based on a semantic-secure stream cipher. In addition, the hiding scheme is implemented by using a non-separable histogram-shifting. Baran et al. in [17] studied DCT compression and decompression techniques. A bubble sorting technique selects the highest signal strength coefficients obtained from DCT. Kamili et al. in 2020 [18] presented a framework of industrial image communication with dual watermarking, one of the watermarks for content authentication and the other for tamper localization. DCT coefficients and energy compaction properties have been used for achieving robust embedding.

Of late, Wang et al. [19] proposed a watermarking defense algorithm to identify linear divergence attacks in the cyber-physical system (CPS) using a Kullback-Leibler (K-L) divergence detector. Guo et al. in [20] provided an efficient scheme in order to find the nearest neighbor over encrypted medical image exactly. Moreover, they computed the lower bound of the Euclidean distance with rejected candidates for medical diagnosis.

As a result of the shortcomings of the existing works, this paper aims to introduce a solution for securing medical color images. The proposed solution ensures the integrity and authenticity of the medical images by providing cover image reconstruction and complete watermark recovery. Additionaly, it improves the security and ciphering performance by reducing the ciphering time. Recently, securing medical images in telemedicine applications has become a challenging issue, which motivated this research to design a robust multi-level security framework based on fusion, encryption, and watermarking processes to transmit color medical images with high efficiency. The proposed watermarking technique depends on the mixture of DCT, LWT, and SVD.

The most important contributions of this work are multi-fold and are summarized as follows:

- Employing both DNA encoding and watermarking stages as a secure solution. Each stage comprises sub-stages to accomplish high levels of privacy, integrity, and security.
- Examining the security efficacy performance of the introduced solution by testing several security measures on various medical images with distinct characterstics.
- Exploring the impact of different noise types and the computational processing overhead of the proposed solution.
- Analyzing the robustness and security performance of the proposed solution against several types of attacks.
- Conducting a comprehensive comparative analysis with recent related works to prove the proposed solution dominance.

The rest of the paper is structured as follows. The proposed multi-level security solution is introduced in Section 2. Section 3 presents the simulation results and security assessment. Also, it gives a discussion and comparison of some related algorithms. Finally, Section 4 gives the concluding remarks of the paper and some future directions.

2 Proposed Color Medical Image Multi-Level Security Solution

This section introduces the proposed multi-level security solution composed of watermarking, encryption, and fusion schemes is introduced in this section. First, the LWT, SVD, DCT-based watermarking process is employed for color medical image copyright protection to improve the capacity of watermark embedding while preserving the imperceptibility of the watermarked color medical images. Next, the fusion process is performed in the suggested security algorithm based on the DWT transform to create the fused watermark image. Finally, this resulting fused image is encrypted using the DNA-based ciphering algorithm before being embedded inside the host color medical image to generate the watermarked color medical image. Fig. 1 shows the main three stages of the suggested multi-level security algorithm. In the receiver side, the inverse processes of these three stages are performed. Thus, the watermark extraction process is accomplished using the fused watermark image extraction, the deciphering procedure, and the anti-fusion procedure to obtain the first and second watermarks.

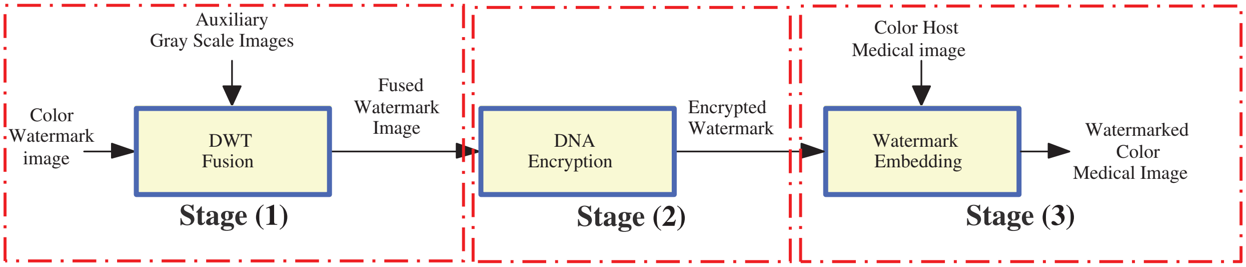


Figure 1: The general diagram of the suggested fusion-encryption-watermarking algorithm

2.1 Fusion Stage

In the fusion process, the suggested DWT-based fusion algorithm is exploited to merge the main features of the first and second watermark images. The main concept of the suggested DWT-based fusion algorithm is that the first and second watermarks are decomposed using DWT. After that, the procedure of average fusion is performed, and then the Inverse DWT (IDWT) is utilized to create the final fused image. Fig. 2 shows the main steps of the suggested DWT-based fusion algorithm.

2.2 Encryption Stage

In the encryption process, the DNA-based ciphering scheme [11] is employed to cipher the watermark fused image to increase the security level of the transmitted images. After that, the ciphered image is inserted into the host image. Figs. 3 and 4 show the flowcharts of the proposed row and column rotation steps for encrypting the fused watermark image, respectively.

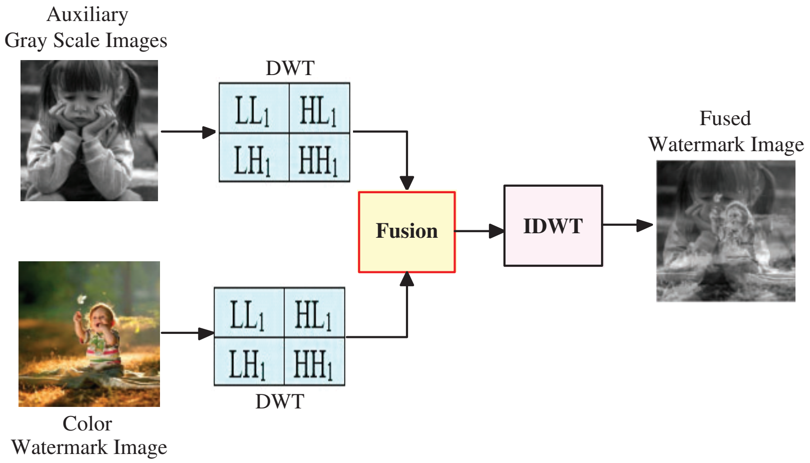


Figure 2: The main steps of two watermarks DWT-based fusion process

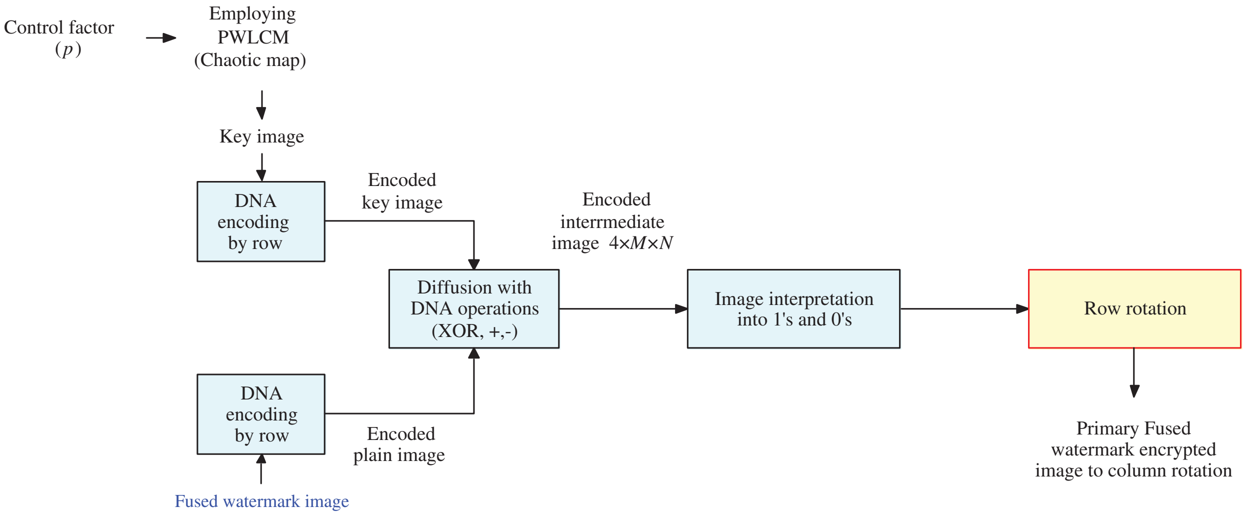


Figure 3: Block diagram of row rotation steps of the suggested cryptosystem

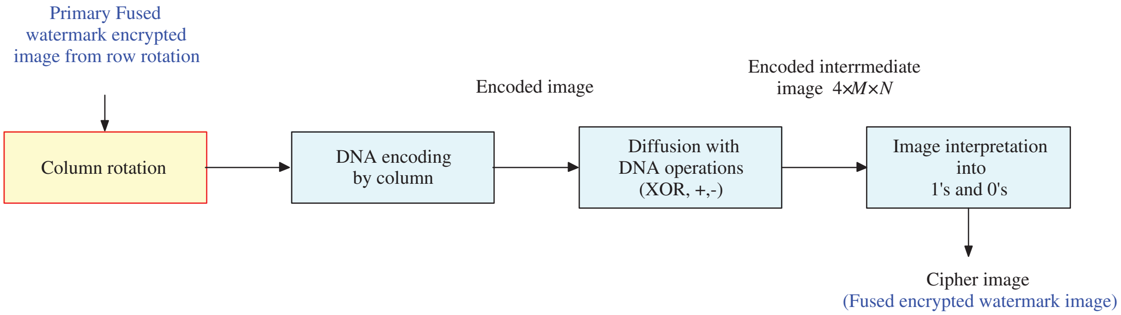


Figure 4: Column rotation steps of the suggested cryptosystem

2.3 Watermarking Stage

The proposed multi-level security algorithm inserts the encrypted image into the cover image (medical image) utilizing the proposed watermarking algorithm of the three-level LWT, DCT, and SVD. We need to remember that the main properties while performing medical image watermarking are imperceptibility and robustness. The watermarking procedure is required to achieve a tradeoff between these two features. The embedding of an image in the perceptually significant components of an image may ensure robustness, but it may be perceptible by the naked eye. Otherwise, robustness may be compromised if the watermark is hidden in perceptually unimportant components. The balance between these two factors needs to be achieved.

The proposed hybrid watermarking technique employs the LWT on the cover color medical image to split it into four sub-bands: LH_1, LL_1, HH_1, and HL_1. Then, the LWT is employed on the LL_1 sub-band to split it into LH_2, LL_2, HH_2, and HL_2. Moreover, the LWT is performed on the LL_2 sub-band to split it further into LL_3, LH_3, HL_3, and HH_3. After that, the three levels of SVD and DCT are performed on the LL_3 sub-band. The extraction steps are the reversal of the embedding steps. As it is a non-blind watermarking algorithm, the original cover image will be needed to extract the watermark. Therefore, the proposed watermarking algorithm composes two major phases: the embedding phase and the extraction phase, which are demonstrated in Figs. 5 and 6, respectively, and are discussed as follows:

2.3.1 Embedding Steps

The in-detail steps of the suggested embedding process are shown in Fig. 5 and can be summarized as follows:

1. The colored watermark image is divided into three RGB components (Red, Green, and Blue).
2. Each of the RGB components of the color watermark image is fused with a different gray-scale image individually using the proposed wavelet procedure. This generates fused watermark image 1 for the R component, fused watermark image 2 for the G component, and fused watermark image 3 for the B component.
3. The DNA-based encryption process is performed on the three fused watermark images image 1, image 2, and image 3 to produce the three ciphered fused watermark images: encrypted fused watermark 1, encrypted fused watermark 2, and encrypted fused watermark 3.
4. Three levels of LWT are applied to the resulting encrypted fused watermark images, and finally, the LL_3 sub-bands of the watermark images are selected to be embedded in the host medical image.
5. Three levels of DCT are applied on the selected LL_3 sub-bands of the watermark images to obtain the coefficient matrices.
6. The SVD is repeatedly performed on the resulting DCT coefficient matrices of the ciphered fused watermark images.

$$\mathbf{A}_j = \mathbf{U}_j\mathbf{S}_j\mathbf{V}_j^T \tag{1}$$

where j is equal to 3 to refer to the DCT frequency components of the $\{HH_3, LL_3, LH_3, HL_3\}$.

7. The host color medical image is divided into three RGB components: red, green, and blue.
8. Three levels of the LWT are performed on the host color image components, and finally, the LL_3 sub-band is selected for the original host image, where the watermark image is supposed to be embedded.

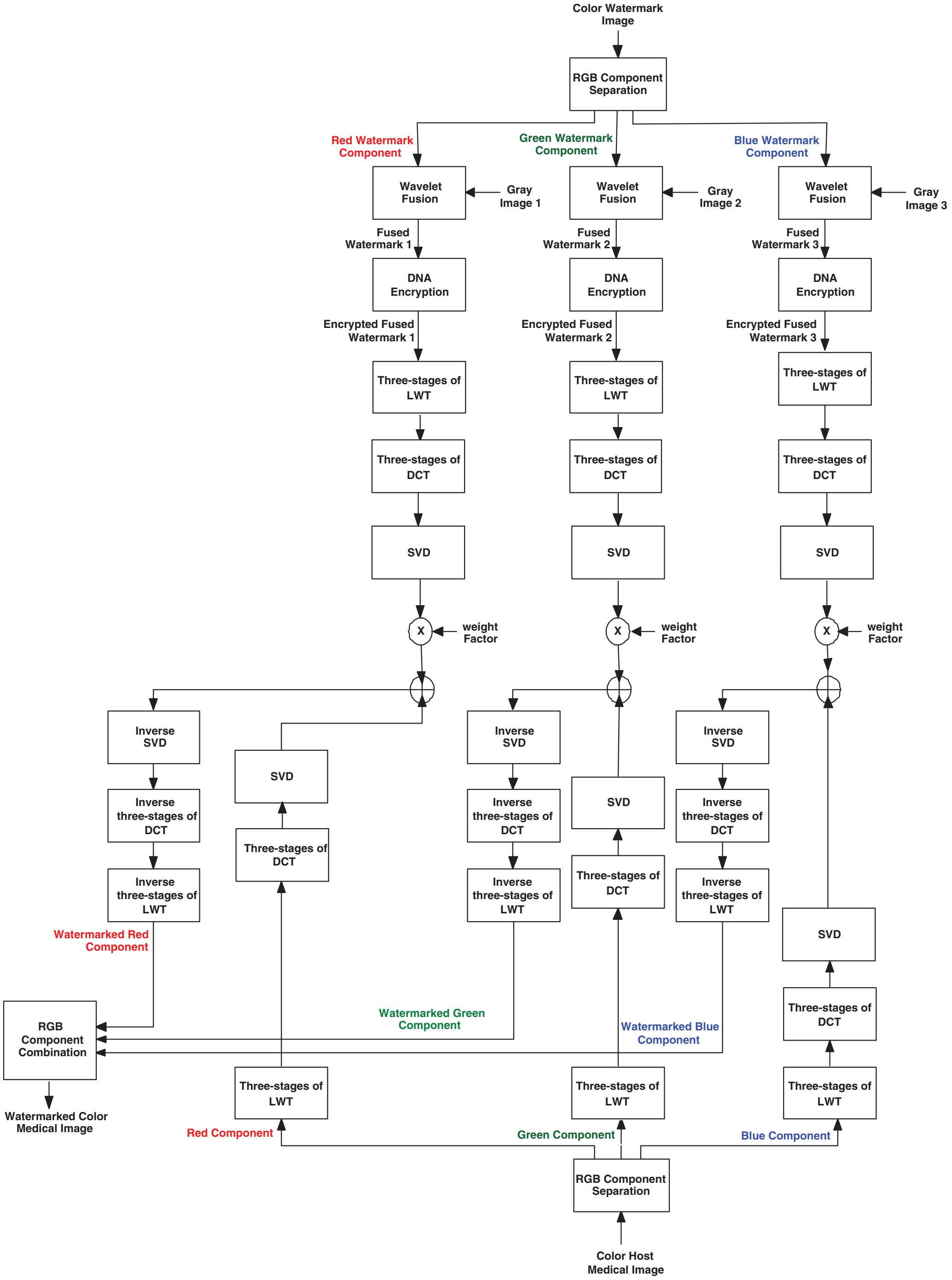


Figure 5: Embedding process of the proposed multi-level security algorithm

9. Three levels of DCT are applied on the analyzed LL_3 sub-band of the host color medical image to obtain the coefficient matrices.
10. The SVD transform is performed on the resulting DCT matrices of the host color image.

$$\mathbf{B}_i = \mathbf{U}_i \mathbf{S}_i \mathbf{V}_i^T \tag{2}$$

where i is equal to 3, and it refers to the DCT frequency components of the $\{HH_3, LL_3, LH_3, HL_3\}$.

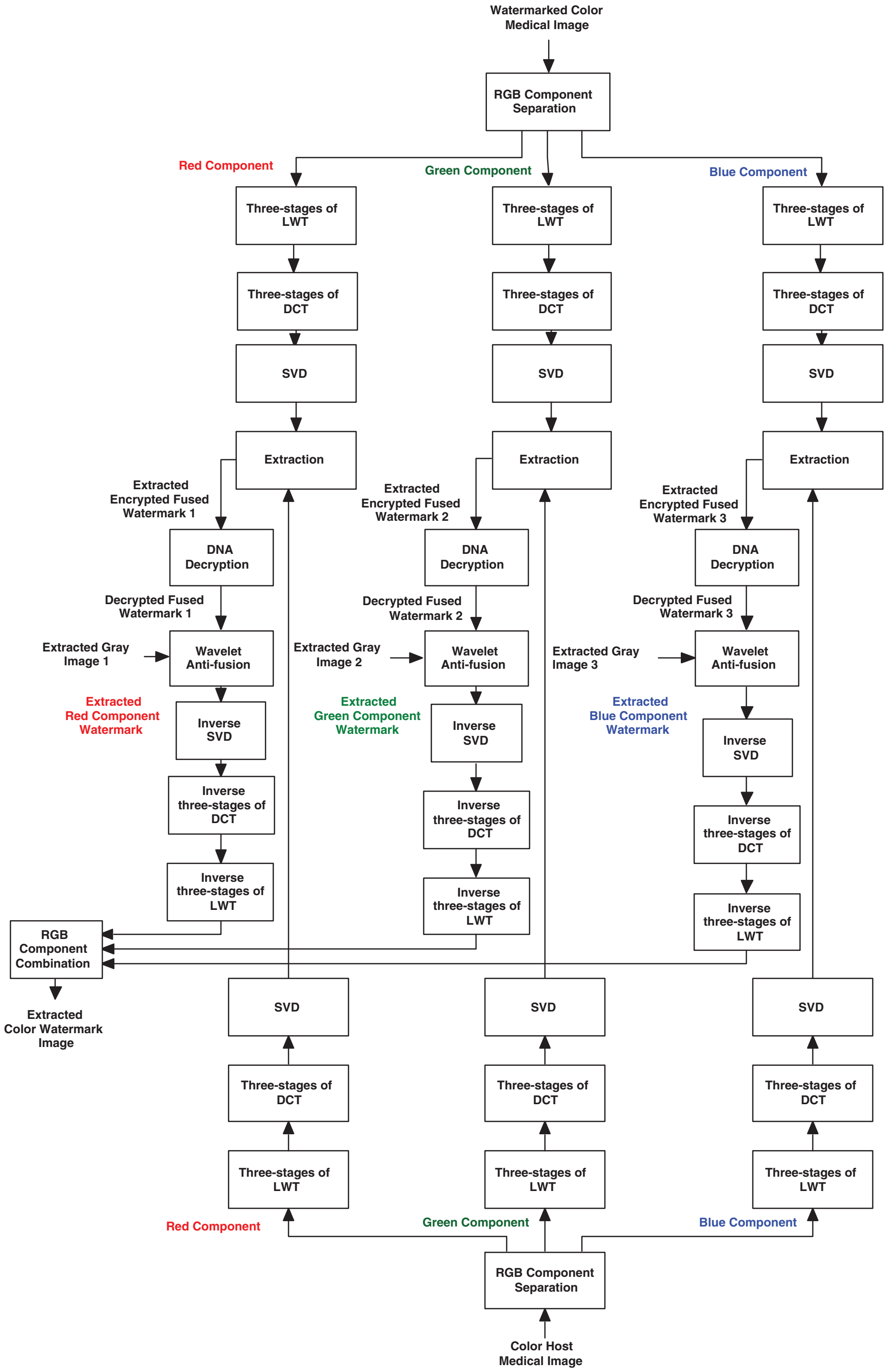

Watermarked Color Medical Image
RGB Component Separation
Red Component
Green Component
Blue Component
Three-stages of LWT
Three-stages of DCT
SVD
Extraction
Extracted Encrypted Fused Watermark 1
Extracted Encrypted Fused Watermark 2
Extracted Encrypted Fused Watermark 3
DNA Decryption
Decrypted Fused Watermark 1
Decrypted Fused Watermark 2
Decrypted Fused Watermark 3
Extracted Gray Image 1
Extracted Gray Image 2
Extracted Gray Image 3
Wavelet Anti-fusion
Extracted Red Component Watermark
Extracted Green Component Watermark
Extracted Blue Component Watermark
Inverse SVD
Inverse three-stages of DCT
Inverse three-stages of LWT
RGB Component Combination
Extracted Color Watermark Image
SVD
Three-stages of DCT
Three-stages of LWT
Red Component
Green Component
Blue Component
RGB Component Separation
Color Host Medical Image

Figure 6: Extraction process of the proposed multi-level security algorithm

11. The singular values (SVs) of the host color image are embedded in the SVs components of the ciphered watermark images.

$$\mathbf{S}_w = \mathbf{S}_i + \alpha \mathbf{S}_j \tag{3}$$

where α is the watermarking factor.

12. The SVD is performed on the new modified ($\mathbf{S}_\mathrm{w}$ matrix) of each one of the three watermarked ciphered fused images: encrypted fused image1, encrypted fused image2, and encrypted fused image3, repeatedly.

$$\mathbf{S}_w = \mathbf{U}_w \mathbf{S} \mathbf{V}_w^T \tag{4}$$

13. The $\mathbf{A}_\mathrm{w}$ matrices of the color watermarked image components are acquired using the matrices $\mathbf{V}^\mathrm{T}$, $\mathbf{S}_\mathrm{w}$, and $\mathbf{U}$.

$$\mathbf{A}_w = \mathbf{U} \mathbf{S}_w \mathbf{V}^T \tag{5}$$

14. Three levels of the inverse DCT are implemented to generate the watermarked image.
15. Three levels of the inverse LWT are implemented to generate the watermarked image.

2.3.2 Extraction Steps

The steps of the watermark extraction process from the host color medical image are shown in Fig. 6, and they can be summarized as follows:

1. The colored watermarked medical image is divided into three RGB components (Blue, Green, and Red).
2. Three levels of the LWT are repeatedly separated for the color watermarked medical image.
3. Three levels of the DCT are performed on the obtained LWT sub-bands to get their corresponding frequency coefficient matrices.
4. The SVD transform is applied to the DCT coefficients of the color watermarked image.

$$\mathbf{A}_{wi}^* = \mathbf{U}_i^* \mathbf{S}_{wi}^* \mathbf{V}_i^{*T} \tag{6}$$

where i is equal to 3, and it refers to the DCT frequency components of the {LL_3, LH_3, HL_3, HH_3}.

5. Matrices of the color watermarked image are calculated.

$$\mathbf{D}^* = \mathbf{U}_w \mathbf{S}_{wi}^* \mathbf{V}_w^T \tag{7}$$

where $*$ refers to the conjugate transpose.

6. The three extracted ciphered fused images: ciphered fused image1, ciphered fused image2, and ciphered fused image3 are obtained, repeatedly.

$$\mathbf{W}^* = \left(\mathbf{D}^* - \mathbf{S}_{wj}\right)/\alpha \tag{8}$$

7. Three levels of the inverse LWT and DCT are implemented to construct the extracted three ciphered fused images: ciphered fused image1, ciphered fused image2, and ciphered fused image3.
8. The DNA decryption process is applied on the extracted ciphered fused image1, ciphered fused image2, and ciphered fused image3.
9. The wavelet anti-fusion process is employed on the resulting decrypted fused images to obtain the gray-scale watermark images, respectively.
10. The correlation value between the separated fused and original images is determined.
11. The correlation value between the separated gray-scale watermarks and original images is determined.

3 Results and Discussions

This section presents the simulation environment and experiment results to evaluate the performance of the proposed multi-level security solution that utilizes fusion, encryption, and watermarking techniques. Three different color medical images were examined in our assessment experiments. The simulation experiments were conducted using MATLAB 2018a on Windows 10 with an Intel® Core™i7-7890HD CPU @2.80 GHz with 16 GB memory capacity. The correlation coefficient (CC) and the $PSNR$ were used as quality metrics to evaluate the suggested security solution. The mathematical formulas of these evaluation metrics are presented in Eqs. (9)–(11) [21–25].

$$MSE = \sum_{i=1}^{m}\sum_{j=1}^{n}\frac{(ORG\,(i,j) - WM\,(i,j))^{2}}{m \times n} \tag{9}$$

$$PSNR = 10\log_{10}\left(\frac{\max^{2}}{MSE}\right)\text{dB} \tag{10}$$

where the original image size is given by m and n. For a gray image, where max = 255. It is the maximum possible pixel value, e.g., 255 for an 8-bit gray-level image. As the host image has 8-level grayscale bits, so, max $= 2^8 - 1 = 255$, WM = watermarked image, and ORG = original image.

$$CC = \frac{\sum_{m}\sum_{n}(X_{mn} - X')\,(Y_{mn} - Y')}{\sqrt{\left(\sum_{m}\sum_{n}(X_{mn} - X')^{2}\right)\left(\sum_{m}\sum_{n}(Y_{mn} - Y')^{2}\right)}} \tag{11}$$

where X' is the estimated average value of the original image X. Y' is the estimated average value of the modified image Y. In the embedding algorithm, the original image is the host image, while the modified image is the watermarked image. In the extraction algorithm, the original image is the original watermark image, while the modified image is the extracted watermark image. For further details and explanations of the CC parameter, it can be investigated and found in [26–29].

The performance efficiency of an image watermarking algorithm can be evaluated by calculating the CC value. Therefore, the range of the CC value is [0–1]. Therefore, to achieve a high image embedding/extraction performance, it is better to get a high CC value between the original and extracted watermark images. Also, it is better to have a high CC value between the host and watermarked images [30,31].

The two main benefits of the suggested watermarking process are preserving the quality of the watermarked image and concealing encrypted watermarks in the host medical image. The PSNR and MSE (Mean Square Error) calculate the watermarked medical image quality. In the standard case, lower MSE and higher PSNR values are appropriate. In addition, in the best situation, the CC has the value of one. However, this is not probable; therefore, a near value to one is desired.

3.1 Experiments

Simulation tests on three medical images have been carried out to evaluate the presented multi-stage security solution. The subjective results guarantee watermark indiscernibility and no retrogression in the watermarked color medical image quality in contrast to the host images. The CC values of the extracted distorted watermarks and the PSNR values of the watermarked images were calculated. Various multimedia attacks were implemented and tested in the simulation experiments on the watermarked medical images. Then, the watermarks were extracted to assess the strength of the proposed security algorithm. Different simulation experiments were conducted on three host medical images. Fig. 7 shows the three host medical images and their RGB elements. All these plaintext medical images are collected from (https://openmd.com/) and (https://medpix.nlm.nih.gov). Fig. 8 presents the color watermarks and their RGB elements, whereas Fig. 9 shows the gray watermarks.

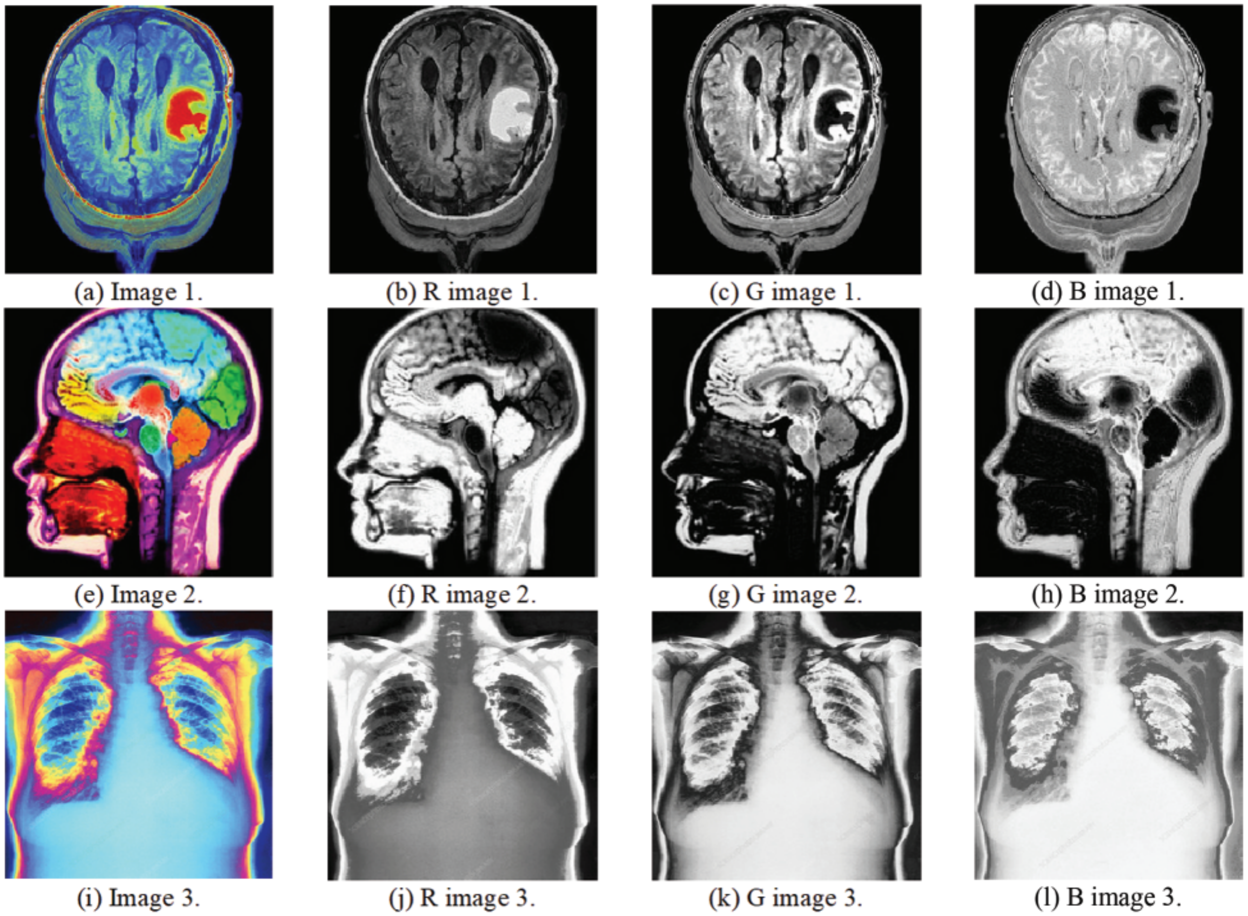

(a) Image 1.
(b) R image 1.
(c) G image 1.
(d) B image 1.
(e) Image 2.
(f) R image 2.
(g) G image 2.
(h) B image 2.
(i) Image 3.
(j) R image 3.
(k) G image 3.
(l) B image 3.

Figure 7: Medical images and their RGB elements

(a) Color watermark image 1. (b) R image 1. (c) G image 1. (d) B image 1.
(e) Color watermark image 2. (f) R image 2. (g) G image 2. (h) B image 2.
(i) Color watermark image 3. (j) R image 3. (k) G image 3. (l) B image 3.

Figure 8: Color watermarks and their RGB elements

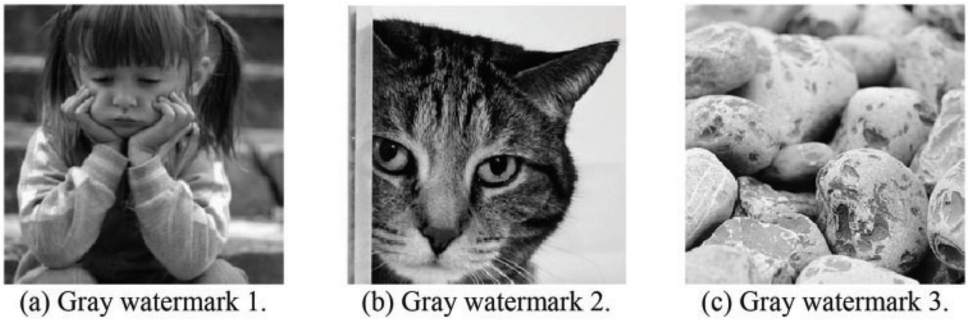

(a) Gray watermark 1. (b) Gray watermark 2. (c) Gray watermark 3.

Figure 9: Gray watermarks

3.2 Non-Attack Scenario

This section examines the proposed security algorithm in case of no attacks. The experiments and evaluations are based on both subjective and objective outcomes, including the CC of the extracted watermarks and the PSNR values of the watermarked medical color images. Figs. 10, 12, and 14 present the subjective outcomes with the obtained CC and PSNR values of the examined watermark and watermarked images. Figs. 11, 13, and 15 illustrate the subjective findings with the obtained

CC outcomes of the examined enciphered images. It is clear from all presented results that a higher similarity amongst the watermarked and original images is found in addition to achieving higher PSNR and CC values and good imperceptibility and robustness.

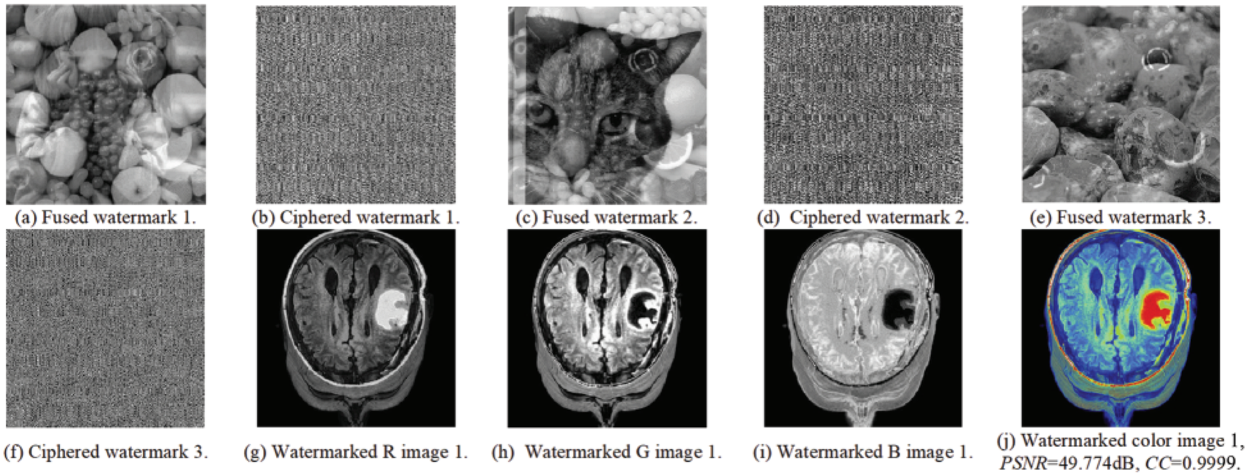

(a) Fused watermark 1. (b) Ciphered watermark 1. (c) Fused watermark 2. (d) Ciphered watermark 2. (e) Fused watermark 3. (f) Ciphered watermark 3. (g) Watermarked R image 1. (h) Watermarked G image 1. (i) Watermarked B image 1. (j) Watermarked color image 1, *PSNR*=49.774dB, *CC*=0.9999.

Figure 10: The embedding results of examined medical image 1

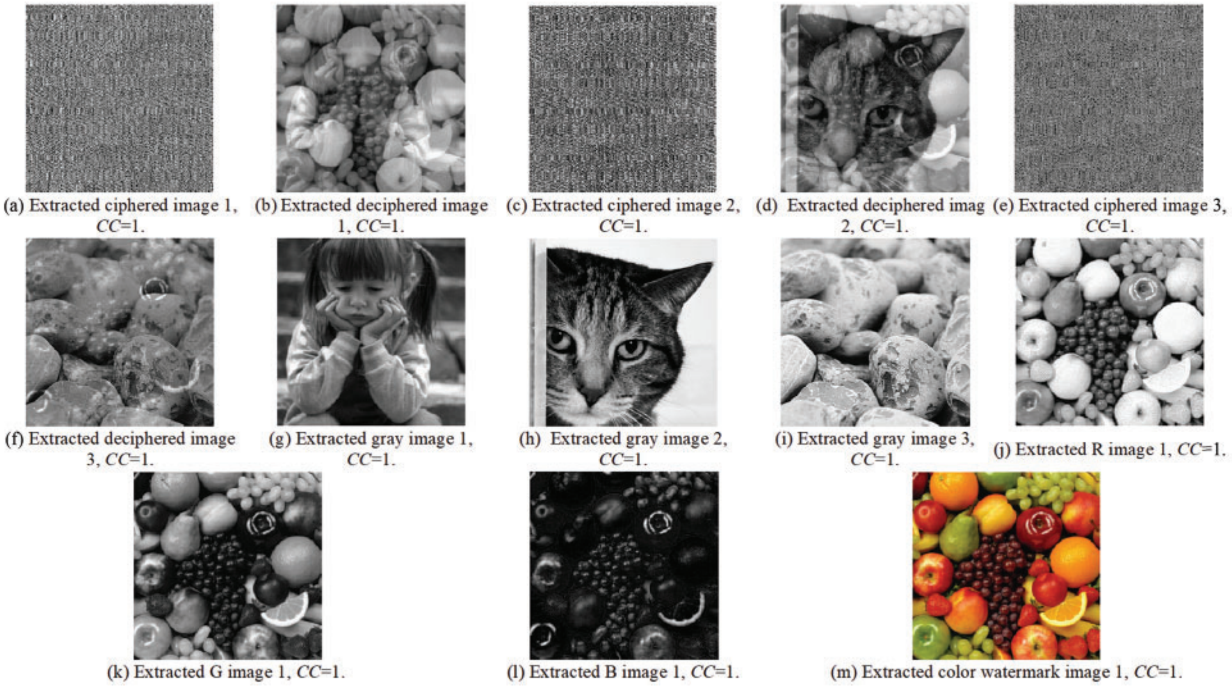
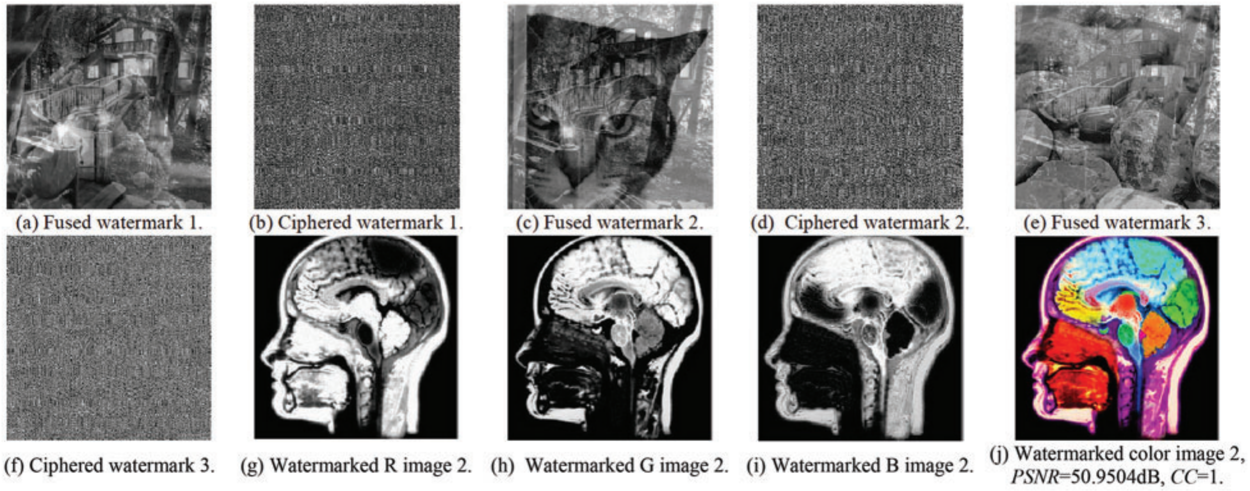

(a) Extracted ciphered image 1, *CC*=1. (b) Extracted deciphered image 1, *CC*=1. (c) Extracted ciphered image 2, *CC*=1. (d) Extracted deciphered imag 2, *CC*=1. (e) Extracted ciphered image 3, *CC*=1. (f) Extracted deciphered image 3, *CC*=1. (g) Extracted gray image 1, *CC*=1. (h) Extracted gray image 2, *CC*=1. (i) Extracted gray image 3, *CC*=1. (j) Extracted R image 1, *CC*=1. (k) Extracted G image 1, *CC*=1. (l) Extracted B image 1, *CC*=1. (m) Extracted color watermark image 1, *CC*=1.

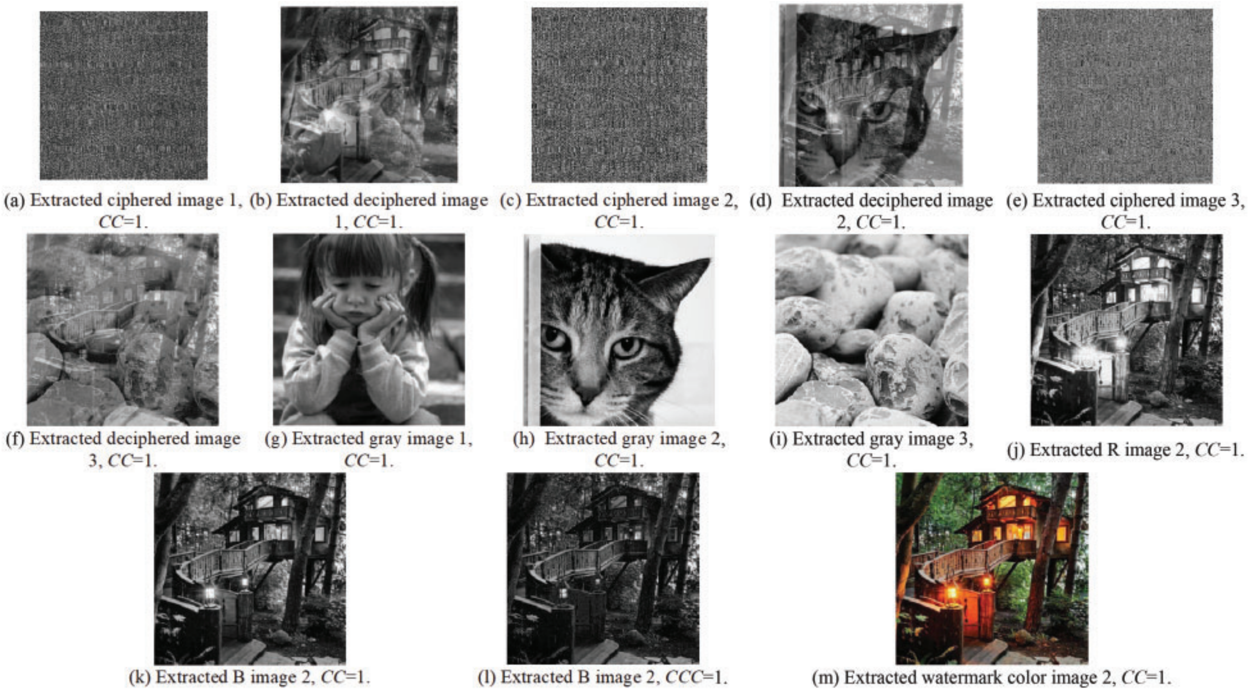
Figure 11: The extraction results of the examined medical image 1



(a) Fused watermark 1. (b) Ciphered watermark 1. (c) Fused watermark 2. (d) Ciphered watermark 2. (e) Fused watermark 3.

(f) Ciphered watermark 3. (g) Watermarked R image 2. (h) Watermarked G image 2. (i) Watermarked B image 2. (j) Watermarked color image 2, *PSNR*=50.9504dB, *CC*=1.

Figure 12: The embedding results of the examined medical image 2

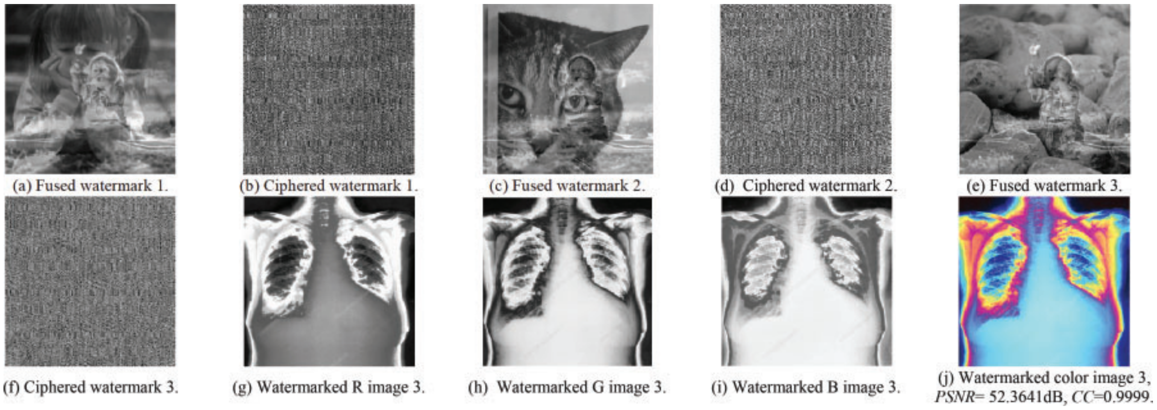


(a) Extracted ciphered image 1, *CC*=1. (b) Extracted deciphered image 1, *CC*=1. (c) Extracted ciphered image 2, *CC*=1. (d) Extracted deciphered image 2, *CC*=1. (e) Extracted ciphered image 3, *CC*=1.

(f) Extracted deciphered image 3, *CC*=1. (g) Extracted gray image 1, *CC*=1. (h) Extracted gray image 2, *CC*=1. (i) Extracted gray image 3, *CC*=1. (j) Extracted R image 2, *CC*=1.

(k) Extracted B image 2, *CC*=1. (l) Extracted B image 2, *CCC*=1. (m) Extracted watermark color image 2, *CC*=1.

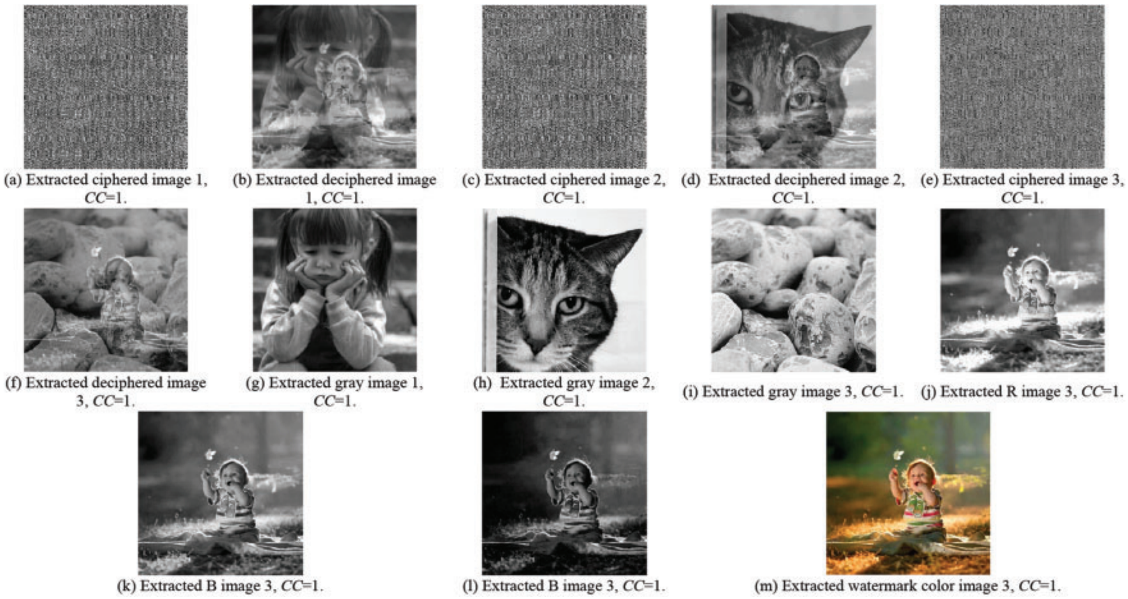
Figure 13: The extraction results of the examined medical image 2



(a) Fused watermark 1. (b) Ciphered watermark 1. (c) Fused watermark 2. (d) Ciphered watermark 2. (e) Fused watermark 3.

(f) Ciphered watermark 3. (g) Watermarked R image 3. (h) Watermarked G image 3. (i) Watermarked B image 3. (j) Watermarked color image 3, *PSNR*= 52.3641dB, *CC*=0.9999.

Figure 14: The embedding results of the examined medical image 3



(a) Extracted ciphered image 1, *CC*=1. (b) Extracted deciphered image 1, *CC*=1. (c) Extracted ciphered image 2, *CC*=1. (d) Extracted deciphered image 2, *CC*=1. (e) Extracted ciphered image 3, *CC*=1.

(f) Extracted deciphered image 3, *CC*=1. (g) Extracted gray image 1, *CC*=1. (h) Extracted gray image 2, *CC*=1. (i) Extracted gray image 3, *CC*=1. (j) Extracted R image 3, *CC*=1.

(k) Extracted B image 3, *CC*=1. (l) Extracted B image 3, *CC*=1. (m) Extracted watermark color image 3, *CC*=1.

Figure 15: The extraction results of the examined medical image 3

Table 1 introduces the average outcomes of the CPU time in the absence of attacks. The results reveal that the proposed security algorithm introduces suitable CPU time for the embedding process, which makes it recommended for real-time and online telemedicine applications.

Table 1: Estimated CPU times of the embedding process

Image	CPU time of embedding technique (s)
# 1	1.6437
# 2	1.5582
# 3	1.4968

3.3 Attacks Scenarios

Tables 2–5 present the obtained *PSNR*s of the watermarked images and the obtained *CC* values of the obtained images in the presence of different attacks, where CC_1 to CC_3 are the correlation coefficient in the case of the examined attacks. The obtained results prove that the proposed security algorithm accomplishes recommended security performance. Moreover, it is noticed that the security algorithm has in average a significant gain in the *PSNR* and *CC* values for the tested medical images in the presence of various categories of multimedia attacks.

Table 2 presents the simulation findings in the presence of resizing, crop, and blurring (Motion, Disk, and Average) attacks. Table 3 introduces the results in the presence of rotation attacks. Table 4 includes the results in the presence of Gaussian attacks. Table 5 gives the simulation results in the presence of JPEG compression attacks. It is perceived that the proposed security algorithm provides the highest PSNRs in the presence of blurring, crop, resizing rotation, Gaussian noise, and JPEG compression attacks.

Table 2: Obtained objective findings in the presence of resizing, crop, and blurring attacks

Images	$PSNR$ (dB)/CC/CC_1/CC_2/CC_3				
	Resize	Crop	Motion	Disk	Average
Medical image 1	37.8277/0.992/0.9927/0.9852/0.9831	37.8267/0.9834/0.9824/0.9676/0.9656	37.8277/0.9724/0.9724/0.9417/0.9390	37.8277/0.9614/0.9614/0.9196/0.9196	37.8277/0.9680/0.9680/0.9328/0.9318
Medical image 2	39.0199/0.994/0.9945/0.9926/0.9903	39.0198/0.9840/0.9830/0.9722/0.9745	39.0199/0.9670/0.9670/0.9557/0.9485	39.0199/0.9620/0.9620/0.9492/0.9415	39.0199/0.9707/0.9707/0.9607/0.9537
Medical image 3	40.3251/0.993/0.9933/0.9911/0.9855	40.3451/0.9799/0.9887/0.9895/0.97652	40.3251/0.9697/0.9697/0.9589/0.9379	40.3251/0.9649/0.9649/0.9523/0.9290	40.3251/0.9698/0.9698/0.9587/0.9378

Table 3: Obtained objective findings in the presence of rotation attacks

Images	$PSNR$ (dB)/CC/CC_1/CC_2/CC_3		
	Rotation 30°	Rotation 45°	Rotation 60°
Medical image 1	37.8277/0.9884/0.9884/0.9811/ 0.9743	37.8277/0.9909/0.9909/0.9869/ 0.9809	37.8277/0.9883/0.9883/0.9809/ 0.9734
Medical image 2	39.0199/0.9911/0.9911/0.9863/ 0.9833	39.0199/0.9968/0.9968/0.9948/ 0.9930	39.0199/0.9932/0.9932/0.9894/ 0.9834
Medical image 3	40.3251/0.9913/0.9913/0.9850/0.9741	40.3251/0.9908/0.9908/0.9857/0.9763	40.3251/0.9910/0.9910/0.9845/0.9742

Table 4: Obtained objective findings in the presence of Gaussian noise attacks

Images	$PSNR$ (dB)/CC/CC_1/CC_2/CC_3		
	0.01	0.05	0.1
Medical image 1	37.8277/0.9995/ 0.9995/0.9990/0.9983	37.8277/0.9859/ 0.9859/0.9736/0.9666	37.8277/0.9734/ 0.9734/0.9510/0.9383
Medical image 2	39.0199/0.9989/ 0.9989/0.9985/0.9970	39.0199/0.9786/ 0.9786/0.9711/0.9596	39.0199/0.9469/ 0.9469/0.9292/0.9147
Medical image 3	40.3251/0.9966/ 0.9966/0.9939/ 0.9909	40.3251/0.9632/ 0.9632/0.9523/0.9272	40.3251/0.9347/ 0.9347/0.9162/0.8825

Table 5: Obtained objective findings in the presence of JPEG compression attacks

Images	$PSNR$ (dB)/CC/CC_1/CC_2/CC_3		
	20%	40%	60%
Medical image 1	37.8277/0.9943/ 0.9776/0.9661/ 0.9357	37.8277/0.9811/ 0.9780/0.9683/ 0. 9482	37.8277/0.9942/ 0.9872/0.9710/ 0.9470
Medical image 2	39.0199/0.9939/ 0.9871/0.9859/ 0.9936	39.0199/0.9944/ 0.9869/0.9857/ 0.9935	39.0199/0.9936/ 0.9867/0.9855/ 0.9933
Medical image 3	40.3251/0.9981/ 0.9982/0.9993/ 0.9988	40.3251//0.9979/ 0.9981/0.9991/ 0.9985	40.3251//0.9977/ 0.9979/0.9988/ 0.9984

3.4 Comparisons with Related Works

Furthermore, more simulation tests were carried out to compare the proposed security algorithm with the state-of-the-art techniques [7,8,10,14,22,23,24,25] to validate the security and robustness efficiency of the multi-level security algorithm. Table 6 presents the $PSNR$ findings of the watermarked images, the CC values of the extracted watermarks, and the calculated CPU times for the proposed algorithm in comparison with the related work without the existence of attacks. The comparison results show that the presented security work accomplishes higher $PSNR$ and CC values than the conventional techniques.

Table 6: Comparison PSNR, CPU time, and CC findings.

Watermarking technique	Image 1			Image 2			Image 3		
	$PSNR$ (dB)	CC	CPU time (s)	$PSNR$ (dB)	CC	CPU time (s)	$PSNR$ (dB)	CC	CPU time (s)
Proposed work	**49.7740**	**0.9999**	**1.6437**	**50.9504**	**1**	**1.5582**	**52.3641**	**0.9999**	**1.4968**
LWT [7]	45.6900	0.9634	1.2537	45.2869	0.9999	1.2435	47.4862	0.9887	1.3001
DCT-LWT [8]	45.2547	0.9468	1.4425	46.2674	0.9564	1.5371	48.5241	0.9607	1.4489

(Continued)

Table 6: Continued

Watermarking technique	Image 1			Image 2			Image 3		
	PSNR (dB)	*CC*	CPU time (s)	*PSNR* (dB)	*CC*	CPU time (s)	*PSNR* (dB)	*CC*	CPU time (s)
DCT-SVD [10]	44.8234	0.9827	4.6684	45.3324	0.9934	3.9897	47.6847	0.9962	3.7628
DWT-SVD [10]	44.8052	0.9895	1.5273	44.8957	0.9864	1.4368	47.2308	0.9889	1.5314
LWT- DCT- Arnold [14]	46.9297	0.9873	1.5604	47.8547	0.9992	1.6342	49.7652	0.9994	1.5642
DWT [22]	32.4339	0.9562	1.7094	39.5347	0.9674	1.6480	42.2009	0.9721	1.5573
DWT+DCT [22]	45.4098	0.9643	1.9357	45.2249	0.9687	1.8673	47.3440	0.9773	1.7867
DWT+DCT+BFO [22]	49.1608	0.9464	2.3924	49.8627	0.9554	2.2358	51.2437	0.9604	2.1286
DWT+DCT+PBFO [22]	45.3439	0.9658	2.5348	44.9864	0.9678	2.4284	46.8209	0.9705	2.4627
DWT-DCT-SVD [23]	49.4387	0.9879	1.7241	48.7586	0.9967	1.6634	50.2761	0.9984	1.5986
NSCT-DCT-Chaotic [24]	44.4165	0.9743	8.8698	45.2576	0.9807	9.2053	46.3359	0.9842	7.3567
LWT-SVD [25]	46.6196	0.9824	1.4531	48.9927	0.9989	1.5526	49.8937	0.9976	1.4865

4 Conclusion and Future Work

This paper proposed an efficient security solution for medical images communications. This security solution uses multi-level LWT, DCT, SVD watermarking, wavelet-based fusion process, and DNA-based encryption algorithms. The combination of LWT, DCT, and SVD results in better performance than applying state-of-the-art methods. Furthermore, the watermark is encrypted using DNA encryption technique before being embedded in the cover color medical image to provide additional security and confidentiality. Moreover, to improve the capacity of the embedded information, the proposed wavelet-based fusion technique is employed to increase the robustness of the proposed security algorithm without affecting the perceptual quality of the original color medical images. The security algorithm is validated by using different medical images under the presence of different attacks on the transmitted images. Additionally, this paper provided a comparison study between the proposed security algorithm and the existing ones. In addition, the proposed multi-level security algorithm is tolerant to versatile attacks. This signifies the supremacy of the suggested security algorithm in maintaining superior reliability and strength in the occurrence of multimedia attacks.

As part of future plans, the security performance of the suggested security algorithm can be improved by building a multi-level security framework that combines efficient encryption, steganography, and watermarking algorithms to achieve higher fidelity, robust storage, and transmission of color medical images. Additionally, simultaneous implementation of compression encryption on medical images to be compatible with big data analysis applications could be considered.

Acknowledgement: The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

Funding Statement: The authors received no specific funding for this study.

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

References

[1] X. Zhou, Z. Ma, Q. Zhang, M. Mohammed and R. Damaševičius, “A reversible watermarking system for medical color images: Balancing capacity, imperceptibility, and robustness,” *Electronics*, vol. 10, no. 9, pp. 10–24, 2021.

[2] N. Kumar, C. Shahnaz, K. Kumar, M. Mohammed and R. Raw, “Advance concepts of image processing and pattern recognition,” *Pattern Recognition*, vol. 4, no. 2, pp. 1–10, 2020.

[3] A. Al-Haj, N. Hussein and G. Abandah, “Combining cryptography and digital watermarking for secured transmission of medical images,” in *Proc. IEEE Int. Conf. on Green Computing Communication and Electrical Engineering (ICGCCEE)*, Coimbatore, India, pp. 1–5, 2014.

[4] S. Ghosh, S. De, S. Maity and H. Rahaman, “A novel dual purpose spatial domain algorithm for digital image watermarking and cryptography using extended hamming code,” in *Proc. IEEE Annual Int. Conf. of the Engineering in Medicine and Biology Society (ICEMBS)*, Minneapolis, MN, USA, pp. 3707–3710, 2009.

[5] S. Kumar and A. Dutta, “A novel spatial domain technique for digital image watermarking using block entropy,” in *Proc. IEEE 14th IEEE India Council Int. Conf. (INDICON)*, Roorkee, India, pp. 1–5, 2017.

[6] M. Malonia and S. Agarwal, “Digital image watermarking using discrete wavelet transform and arithmetic progression technique,” in *Proc. IEEE Int. Conf. on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, Chennai, India, pp. 748–753, 2017.

[7] H. Chen and W. Xu, “Secure and robust color image watermarking for copyright protection based on lifting wavelet transform,” in *Proc. IEEE Int. Conf. on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, pp. 144–148, 2018.

[8] V. Tomar, A. Kumar and A. Choudhary, “Conception & implementation of a novel digital image watermarking algorithm using cascading of DCT and LWT,” in *Proc. IEEE Visual Communications and Image Processing (VCIP)*, Singapore, pp. 1–4, 2015.

[9] A. Mishra, C. Agarwal and G. Chetty, “Lifting wavelet transform based fast watermarking of video summaries using extreme learning machine,” in *Proc. Int. Conf. on Signal Processing, Communication, Power and Embedded System (SCOPES)*, Paralakhemundi, India, pp. 1202–1207, 2016.

[10] N. Lalitha, P. Prasad and S. Rao, “Performance analysis of DCT and DWT audio watermarking based on SVD,” in *Proc. IEEE Visual Communications and Image Processing (VCIP)*, Chengdu, China, pp. 1–4, 2016.

[11] M. El-Khalil 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, no. 9, pp. 1–29, 2021.

[12] 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.

[13] X. Wang and C. Liu, “A novel and effective image encryption algorithm based on chaos and DNA encoding,” *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 62–99, 2021.

[14] C. Preet and R. Aggarwal, “Multiple image watermarking using LWT, DCT and arnold transformation,” in *Proc. IEEE Visual Communications and Image Processing (VCIP)*, Chengdu, China, pp. 16–20, 2019.

[15] O. Faragallah, H. El-sayed and A. Afifi, “Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform,” *Optics and Lasers in Engineering*, vol. 137, no. 6, pp. 1–15, 2021.

[16] H. Huang, T. Gong, N. Ye and Y. Dou, “Private and secured medical data transmission and analysis for wireless sensing healthcare system,” *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1227–1237, 2019.

[17] E. Baran, A. Kuzu, S. Bogosyan and A. Sabanovic, "Comparative analysis of a selected DCT-based compression scheme for haptic data transmission," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 3, pp. 1146–1155, 2019.

[18] A. Kamili, N. Hurrah, S. Parah and K. Muhammad, "DWFCAT: Dual watermarking framework for industrial image authentication and tamper localization," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 5108–5117, 2020.

[19] D. Wang, J. Huang, Y. Tang and F. Li, "A watermarking strategy against linear deception attacks on remote state estimation under K–L divergence," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3273–3281, 2020.

[20] C. Guo, S. Su, K. Choo and X. Tang, "A fast nearest neighbor search scheme over outsourced encrypted medical images," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 514–523, 2018.

[21] A. Alarifi, M. Amoon and M. Aly, "Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system," *IEEE Access*, vol. 8, pp. 221246–221268, 2020.

[22] W. El-Shafai and E. Hemdan, "Robust and efficient multi-level security framework for color medical images in telehealthcare services," *Journal of Ambient Intelligence and Humanized Computing*, vol. 5, no. 8, pp. 1–16, 2021.

[23] O. Faragallah, M. Alzain, H. El-Sayed and J. Al-Amri, "Block-based optical color image encryption based on double random phase encoding," *IEEE Access*, vol. 7, pp. 4184–4194, 2018.

[24] K. Al-Afandy, F. Abd El-Samie, E. El-Rabaie, F. Abd El-Samie and O. Faragallah, "Robust hybrid watermarking techniques for different color imaging systems," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25709–25759, 2018.

[25] W. El-Shafai, S. El-Rabaie 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.

[26] 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.

[27] S. Ibrahim, M. Egila, H. Shawky and M. Elsaid, "Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption," *Multimedia Tools and Applications*, vol. 79, pp. 1–26, 2020.

[28] O. Faragallah, M. AlZain, H. El-Sayed and J. Al-Amri, "Secure color image cryptosystem based on chaotic logistic in the FrFT domain," *Multimedia Tools and Applications*, vol. 79, no. 3, pp. 2495–2519, 2020.

[29] O. Faragallah, A. Afifi and H. El-Sayed, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," *IEEE Access*, vol. 8, pp. 42491–42503, 2020.

[30] M. El-Halawany, "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.

[31] 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.