

A Hybrid Security Framework for Medical Image Communication

Walid El-Shafai^{1,2}, Hayam A. Abd El-Hameed³, Ashraf A. M. Khalaf³, Naglaa F. Soliman⁴,
Amel A. Alhussan^{5,*} and Fathi E. Abd El-Samie¹

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

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

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

⁴Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, 11671, Saudi Arabia

⁵Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia

*Corresponding Author: Amel A. Alhussan. Email: aaalhussan@pnu.edu.sa

Received: 16 February 2022; Accepted: 24 March 2022

Abstract: Authentication of the digital image has much attention for the digital revolution. Digital image authentication can be verified with image watermarking and image encryption schemes. These schemes are widely used to protect images against forgery attacks, and they are useful for protecting copyright and rightful ownership. Depending on the desirable applications, several image encryption and watermarking schemes have been proposed to moderate this attention. This framework presents a new scheme that combines a Walsh Hadamard Transform (WHT)-based image watermarking scheme with an image encryption scheme based on Double Random Phase Encoding (DRPE). First, on the sender side, the secret medical image is encrypted using DRPE. Then the encrypted image is watermarking based on WHT. The combination between watermarking and encryption increases the security and robustness of transmitting an image. The performance evaluation of the proposed scheme is obtained by testing Structural Similarity Index (SSIM), Peak Signal-to-Noise Ratio (PSNR), Normalized cross-correlation (NC), and Feature Similarity Index (FSIM).

Keywords: Walsh hadamard transform; watermarking; encryption; double random phase encoding; structural similarity index

1 Introduction

The rapid growth of the computerized world and its widespread pose many challenges to secure transmitted information. Therefore, we have to get solutions to transfer data securely. We are using two possible solutions for secure image transfer in this paper: watermarking and encryption of images. Network and Internet technology have advanced rapidly, threatening data security and privacy. So,



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

to preserve digital information, content documentation and copyright protection from duplication effectively meeting the actual challenges and recipient threats. Digital image watermarking provides an alternative solution to ensure image tampering, guarantee intellectual property rights and improve the security of transmitted media. Watermarking schemes can hide secret data in any digital medium. Therefore, it is possible to easily possess digital content illegally and multiply its distribution through communication, image processing, and data storage through a physical medium. Therefore, digital watermarking has become a primary need for the multimedia industry.

These methods ensure tamper-proof, documentation, and verification of the content of digital images [1]. The watermark was achieved by including the watermark in the spatial domain [1] or frequency domains [2]. Frequency domain methods such as methods based on discrete Fourier transform (DFT) [3] discrete wavelet transform (DWT), discrete cosine transform (DCT) [2], ridgelet transform [4], and hybrid method using DWT-DCT [5]. It may be most used in modern business.

The watermark detection methods can be divided into two broad classes: non-blind, where the cover image is needed in the detector during the watermark extraction process [6–11], and blind detection, where the cover image is not available. To realize a watermark blind scheme, the statistical properties of the wavelet coefficients can be taken into consideration. Encryption schemes are providing better mechanisms for information security in open networks. These techniques need to provide the general and private keys for recovering the original information. One of the encryption techniques is DRPE. Encryption by DRPE is very successful and used widely in image security [12–15] will be used in this framework before watermarking the medical image.

The contributions of this work are structured as follows. Section 2 summarises the main works in the related studies. Section 3 explains the main requirements of image watermarking schemes. Section 4 discusses background information of the first part of the proposed scheme, DRPE, and the second part of the proposed scheme, WHT. Section 5 explains the proposed scheme of the encryption and decryption process of the secret image based on DRPE, and the embedding and extraction process is explained by a blind watermark of a suggested color image based on WHT. Section 6 introduces the simulation outcomes and analysis. Finally, Section 7 gives the concluding remarks.

2 Related Work

Digital image authentication is a very big challenge in our computerized world, as it is not difficult to manipulate with an image. Depending on the required applications, many steganography schemes have been developed to confirm the authenticity of a digital image. In [16], the authors verified the content from the encrypted image transmitted over Additive White Gaussian Noise (AWGN) wireless channels. In this paper, the author does not test the encrypted image with various types of noise such as Gaussian noise, rotation noise, and speckle noise. As a result, the simulation results of our scheme using DRPE are more robust than the scheme using a 2-D chaotic baker map that verifies image content integrity and protects from attack.

In [17], the Least Significant Bit (LSB) steganography and chaotic baker ciphering is employed to increase the security of wireless image communication. Hiding information means hiding the presence of the data within a medium cover, while encryption means hiding the cover medium with the secret data inside it using specific algorithms. The proposed algorithm could provide better protection for the image transmission through AWGN wireless channel, but these algorithms did not present a content-based image verification for the original image. Also, it did not consider another type of noise and attack to measure the robustness and quality of the proposed schemes. Such as our schemes which present content-based image verification for images and consider many types of noise and attacks to

test the performance of proposed schemes. In [18], a watermarking scheme based on the integer DCT domain is presented. A watermarking scheme had been presented using DCT and chaotic map. This paper considered a watermarking scheme that directly embeds the watermark in the singular sets of a circulate matrix obtained from the coefficients of integer DCT using a non-linear chaotic map. In [19], a digital image watermarking scheme to protect copyright and tampering detection is proposed. The goal of the proposed scheme in this paper is to embed a robust and fragile watermark into the host image at the same time so that the proposed scheme can possess dual functions: one is copyright protection, and the other is tampering detection.

Authors in [20] produced a security enhancement based on DRPE. Security enhancements are produced for dual random phase coding using rear-mounted phase masking. Based on an extensive study of the cryptanalysis achievements of DRPE and its derivatives, revoking the second lens, which plays an important role in cryptanalysis operations, is concluded. In [21], a scheme based on WHT was proposed for blind color image watermarking. In this method, the image is converted using WHT. Then, the watermark is inserted into the final two rows of WHT parameters of the color image using the suggested scheme.

3 Main Requirements of Image Watermarking Schemes

- ***Imperceptibility***

Imperceptibility is the main condition for calculating the efficiency of a watermarking technique. Imperceptibility means that the watermarked image is the same as the original image. It should be sensually ambiguous to the human eye, regardless of slight deterioration in brightness or image contrast. Hence, the quality of the image should not be affected. To evaluate the imperceptibility of a watermarking technique, there are various methods, such as Peak Signal-to-Noise Ratio (PSNR), which imply good imperceptibility if PSNR is high. The best watermarking techniques ensure better imperceptibility [22]. This method measures watermark imperceptibility by Structural Similarity Index Measure (SSIM) metric. However, it is often unnoticed by the human eyes in an invisible watermark. In [23], the authors selected the preferred area in the cover image to include the watermark for better imperceptibility. Sometimes, it is best to put a watermark visible in the image [24]. Therefore, in all image security systems, invisible watermarking techniques are used. Imperceptibility is sometimes used in digital imaging, E-mails, medical image, digital commerce, and so on.

- ***Robustness***

Robustness measures the immunity and strength of secret data from digital signal processing attacks against a trial to remove or discover it. So, a good image watermarking technique must be having a good strong against various types of attacks. Some watermarking techniques are strong against various image processing attacks, while others are weak against other attacks [25]. Therefore, we can classify robustness as robust, fragile, and semi-fragile.

Robust watermark: from its name, it prevents many types of attacks. After some attacks, the watermark did not change and remained the same [26]. The robust watermark protects copyright authentication, monitoring the broadcast, banking, and fingerprinting [26]. Fragile watermark: this watermark verifies if it has been altered with or not. A fragile watermark is the easiest technique to execute [27]. watermark: semi-fragile watermark may hold some attacks but is not successful with other malicious attacks. Semi-fragile watermarks are used for image authentication [28].

- **Security**

Security is the main concern in watermarking schemes. If watermarking schemes are fragile techniques, they cannot be applied in applications that need high security, such as copyright protection, fingerprinting, and data authentication. Therefore, to obtain a high level of security, we can perform various types of encryptions, where the encrypted image can not be detected easily [29]. Security requests can be applied in medical imaging, digital image transmission, telecommunications, etc.

- **Capacity**

Watermarking payload capacity evaluates the amount of information included in the cover image, based on the amount of watermark. However, the payload capacity marked the limitations of the watermarking schemes. If the number of embedded bits in the cover image is less than channel capacity, the watermark extraction is successful [30].

- **Watermark Keys**

The key used for the watermarking process defines many constraints of the watermarking process, such as (the image coefficients subset, the direction of embedding, and the domain that the embedding is used). In addition, the strength of the watermarking scheme is determined by the watermark key [31]. Therefore, to ensure the security of any system, a private key is needed for the embedding and extraction processes [32].

- **Reversibility**

The reversibility characteristic ensures watermark extraction and accurate cover image reconstruction [33].

4 Background Information

4.1 Walsh-Hadamard Transform

WHT is an orthogonal function that has low computational complexity [34]. WHT is represented for an input $f(x)$ that has ‘ N ’ number of samples as,

$$F(U) = \frac{1}{N} \times [H_N] \times f(x) \quad (1)$$

where $[H_N]$ is the Hadamard matrix with $N \times N$ dimension. The matrix with a size 2×2 is written as,

$$[H_2] = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (2)$$

The 4×4 Hadamard matrix is expressed as,

$$[H_4] = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix} \quad (3)$$

Therefore, Walsh Hadamard transform general form is;

$$[H_{2i}] = \begin{bmatrix} H_{2i-1} & H_{2i-1} \\ H_{2i-1} & -H_{2i-1} \end{bmatrix} \quad \text{for } i = 1, 2, 3, 4, \dots \quad (4)$$

where i is based on N , i.e., $N = 2^i$, the inverse WHT is given by (5),

$$f(x) = [H_N] \times F(U) \quad (5)$$

Similarly, the WHT of a 2-D image is given by (6),

$$F(U, V) = \frac{1}{N} \times [H_N] \times f(x, y) \quad (6)$$

The inverse 2-D WHT is given as,

$$f(x, y) = \frac{1}{N} \times [H_N] \times F(U, V) \quad (7)$$

Finally, WHT general form for the 4×4 image block is given by (8),

$$F(U, V) = \begin{bmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{bmatrix} \quad (8)$$

The data are embedded in the coefficient sets (c_{31}, c_{41}) , (c_{32}, c_{42}) , (c_{33}, c_{43}) , and (c_{34}, c_{44}) . The data embedding is chosen to be in the final two-row elements.

4.2 Double Random Phase Encoding

DRPE is explained by Refregier and Javid [12] depending on changing the spectral distributions of an image. At the receiver, it is necessary to have information about the spectral distributions to decode the image. The block diagram of DRPE is explained in Fig. 1.

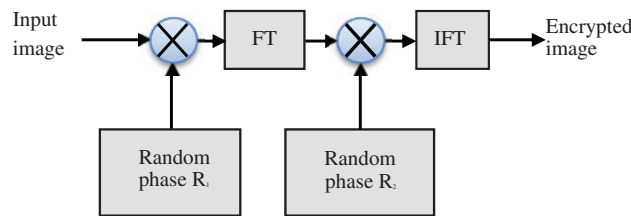


Figure 1: DRPE steps

The input image $f(x, y, z)$ is the secret medical image, where x, y , and z are in space coordinates multiplied by the first mask $R_1(x, y, z)$ and is subsequently Fourier transformed. Then, the second phase mask $R_2(u, v, w)$ is multiplied with the Fourier transformed image, where u, v , and w are Fourier domain coordinates [35]. Finally, inverse Fourier transformed is applied to the obtained image to obtain the encrypted medical image.

In the decryption process of DRPE, Fourier transform is applied on encrypted medical images and then multiplied with the complex conjugate of $R_2(u, v, w)$. Finally, the obtained image is Inverse Fourier transformed to obtain the decrypted medical image, as shown in Fig. 2.

To explain DRPE mathematically, let $\psi(x, y, z)$ is the encrypted image and $n(x, y, z)$ and $m(x, y, z)$ are independent white sequences, two Random Phase Masks (RPMs) are $R_1(x, y, z) = \exp(2i\pi n(x, y, z))$ and $R_2(x, y, z) = \exp(2i\pi m(x, y, z))$. The encrypted image is complex, with amplitude and phase [36], and it is given by Eq. (9)

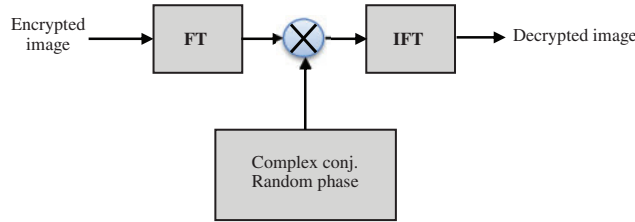


Figure 2: Double random phase decoding

$$\psi(x, y, z) = \{f(x, y, z) R_1(x, y, z)\} * FT^{-1}\{R_2(u, v, w)\} \quad (9)$$

where the symbol (*) denotes convolution and the second random phase mask $R_2(u, v, w)$ is a Fourier transform of function $h(x, y, z)$ where $h(x, y, z) = m(x, y, z)$ which is a phase function. Thus, $R_2(u, v, w)$ is given by Eq. (10)

$$R_2(u, v, w) = FT\{h(x, y, z)\} = \hat{h}(u, v, w) = \exp[2i\pi m(u, v, w)] \quad (10)$$

The inverse Fourier transform is described as in Eq. (11).

$$\begin{aligned} FT^{-1}\{FT[\psi(x, y, z)] R_2^*(u, v, w)\} &= FT^{-1}\{FT[f(x, y, z) R_1(x, y, z)] R_2(u, v, w) R_2^*(u, v, w)\} \\ &= f(x, y, z) R_1(x, y, z) \end{aligned} \quad (11)$$

Then, the absolute value is taken to the output to turn out the decrypted image $f(x, y, z)$.

5 Proposed Security Framework

The proposed framework is considered a multi-level security system for medical image communications. The first level of security is encrypting secret medical color images before watermarking by using DRPE. The second level of security is the watermarking based on WHT of the encrypted medical image on the color cover image, which has an important feature that it may not affect the visibility of the cover image. In this section, the encryption and watermark embedding scheme is explained then the watermark extraction and decryption scheme is explained.

5.1 Encryption and Watermark Embedding Scheme

Let the input secret medical image $M(x, y, z)$ be encrypted is multiplied by a first phase mask $R_1(x, y, z)$, then it is Fourier transformed. Then, the resulting image is multiplied with the second phase mask $R_2(u, v, w)$. After that, the encrypted medical image in space domain $D(x, y, z)$ is obtained by applying the inverse Fourier transform of the final image. For example, assume the original image is $I(x, y, z)$, and the watermark encrypted medical image is $D(x, y, z)$. The watermarked image $W(x, y, z)$ is obtained from embedding the encrypted image into the cover image. The encryption and embedding process is explained as steps as follows:

Step (1): Multiply secret medical image by first key $R_1(x, y, z)$, as indicated in Fig. 1.

Step (2): Apply Fourier transform on the resulting image.

Step (3): Multiply the resulting image with the $R_2(u, v, w)$.

Step (4): The image is inverse Fourier transform to acquire the encrypted medical image $D(x, y, z)$.

Step (5): Calculate the difference d_i and average avg_i from the coefficients c_{3i} and c_{4i} , as:

$$d_i = |[c_{3i}] - [c_{4i}]| \tag{12}$$

$$avg_i = |[c_{3i}] + [c_{4i}]| / 2 \tag{13}$$

Step (6): Calculate coefficients l_i and m_i of data embedded from Eqs. (14) and (15) as:

If $rem(|d_i|, 2) = 0$

$$l_i = \begin{cases} avg_i - \left(\frac{d_i}{2}\right) & if b_i = 0 \\ avg_i - \left(\frac{d_i}{2} - 0.5\right) & if b_i = 1 \end{cases} \tag{14}$$

$$m_i = \begin{cases} avg_i + \left(\frac{d_i}{2}\right) & if b_i = 0 \\ avg_i + \left(\frac{d_i}{2} - 0.5\right) & if b_i = 1 \end{cases} \tag{15}$$

If $rem(|d_i|, 2) = 1$

$$l_i = \begin{cases} avg_i - \left(\frac{d_i}{2}\right) & if b_i = 1 \\ avg_i - \left(\frac{d_i}{2} - 0.5\right) & if b_i = 0 \end{cases} \tag{16}$$

$$m_i = \begin{cases} avg_i + \left(\frac{d_i}{2}\right) & if b_i = 1 \\ avg_i + \left(\frac{d_i}{2} - 0.5\right) & if b_i = 0 \end{cases} \tag{17}$$

Step (7): Values of l_i and m_i are replaced by c_{3i} and c_{4i} based on the min. and max. values of e_{3i} and e_{4i} .

$$e_{3i} = \begin{cases} \max(l_i, m_i) & if c_{3i} \geq c_{4i} \\ \min(l_i, m_i) & if c_{3i} < c_{4i} \end{cases} \tag{18}$$

$$e_{4i} = \begin{cases} \max(l_i, m_i) & if c_{4i} > c_{3i} \\ \min(l_i, m_i) & if c_{4i} \leq c_{3i} \end{cases} \tag{19}$$

The embedded coefficients for Walsh Hadamard after embedding the data are represented as,

$$F(U, V) = \begin{bmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ e_{31} & e_{32} & e_{33} & e_{34} \\ e_{41} & e_{42} & e_{43} & e_{44} \end{bmatrix} \tag{20}$$

After that, estimate the inverse WHT of each 4×4 sub-block. Then, to obtain the image with watermark $W(x, y, z)$, merge all the 4×4 sub-blocks.

Algorithm 1: Medical image encryption using DRPE and data embedding using WHT

Step (1): Multiply secret medical image by the $R_1(x, y, z)$ as in Fig. 1.

Step (2): Apply Fourier transform on the resulting image.

Step (3): Multiply the resulting image with another phase mask $R_2(u, v, w)$.

Step (4): The image is inverse Fourier transformed to acquire the encrypted image $D(x, y, z)$.

Step (5): Converting the image $D(x, y, z)$ to binary information.

Step (6): Dividing encrypted image $I(x, y, z)$ to 4×4 various blocks.

Step (7): WHT is applied to the image.

Step (8): Estimate d_i and avg_i as explained in Eqs. (12) and (13).

Step (9): Using Eqs. (14)–(17), l_i and m_i are obtained.

Step (10): Calculate values of e_{3i} , e_{4i} , l_i , and m_i using Eqs. (16) to (19).

Step (11): Obtain the inverse WHT floor value.

Step (12): Mix all 4×4 sub-blocks obtained from step 11 to obtain the watermarked digital image $W(x, y, z)$.

The encryption scheme of the medical image using DRPE and data embedding using WHT data is explained in Fig. 3.

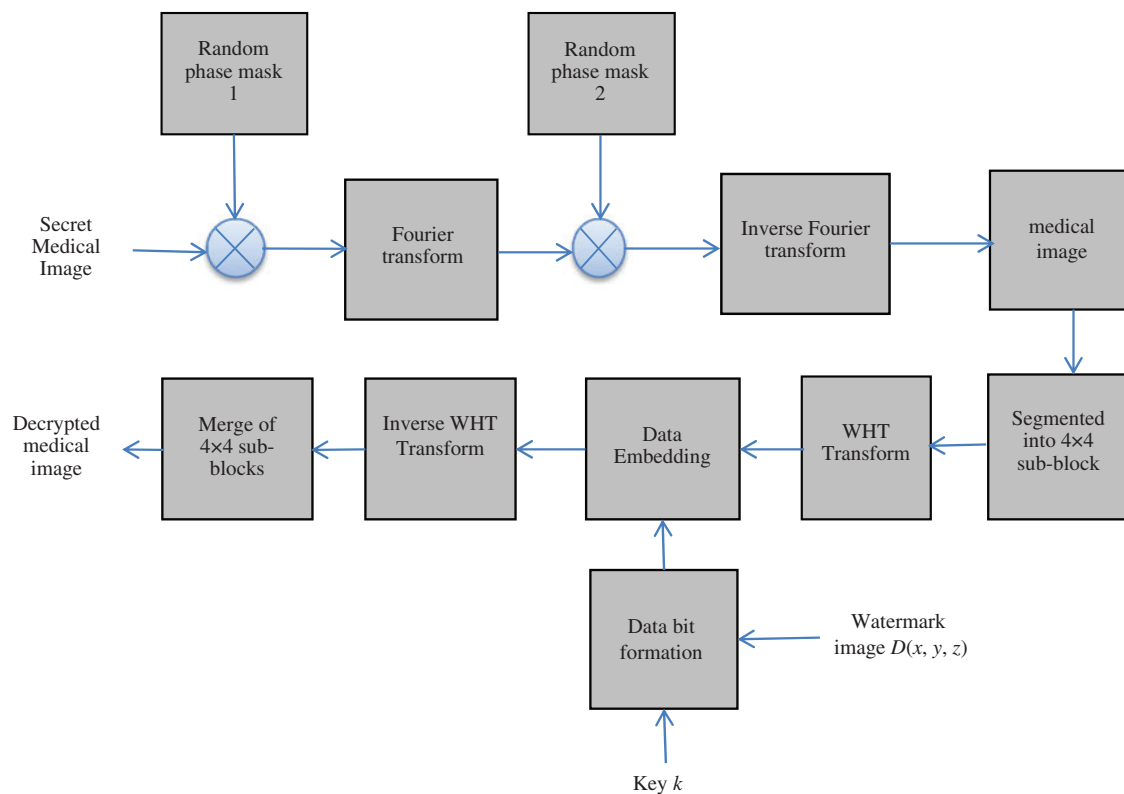


Figure 3: Proposed scheme (encryption of medical image using DRPE and data embedding using WHT)

5.2 Watermark Extraction and Decryption Scheme

In Fig. 4, the watermark extraction and decryption scheme are explained. The $W(x, y, z)$ is divided into 4×4 different blocks. After that, these blocks are converted to WHT factors as defined in Eq. (6). WHT coefficients for data embedding are written by,

$$W(U, V) = \begin{bmatrix} \hat{c}_{11} & \hat{c}_{12} & \hat{c}_{13} & \hat{c}_{14} \\ \hat{c}_{21} & \hat{c}_{22} & \hat{c}_{23} & \hat{c}_{24} \\ \hat{e}_{31} & \hat{e}_{32} & \hat{e}_{33} & \hat{e}_{34} \\ \hat{e}_{41} & \hat{e}_{42} & \hat{e}_{43} & \hat{e}_{44} \end{bmatrix} \quad (21)$$

The difference \hat{d}_i between the values \hat{e}_{3i} and \hat{e}_{4i} is calculated using,

$$\hat{d}_i = |\hat{e}_{3i} - \hat{e}_{4i}| \quad (22)$$

where \hat{e}_{3i} and \hat{e}_{4i} are third and fourth rows data embedded WHT coefficient. \hat{b}_i is extracted from the value \hat{d}_i to obtain the hidden data as

$$\hat{b}_i = \text{rem}(|\hat{d}_i|, 2) \quad (23)$$

The resulting image is encrypted medical image $\psi(x, y, z)$ which after that is Fourier transformed and multiplied by $R_2(u, v, w)$ which is the complex conjugate of the second RPM then resulting image is inverse Fourier transformed to obtain decrypted secret medical color image.

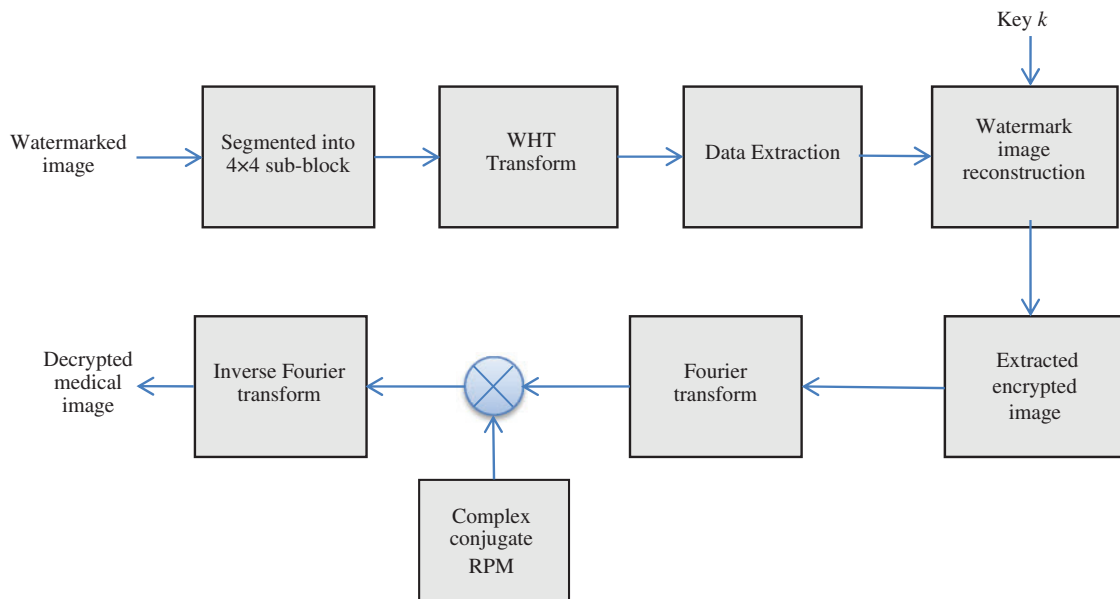


Figure 4: Steps of watermark extraction and decryption

Algorithm 2: Data extraction and image decryption process

Step 1: The $W(x, y, z)$ image is divided into 4×4 sub-blocks.

Step 2: WHT is applied on sub-blocks.

Step 3: Calculate the difference \hat{d}_i using Eq. (22).

Step 4: Extract the hidden data \hat{b}_i using Eq. (23).

Step 5: Watermark image is reconstructed from the extracted data \hat{b}_i using the key 'K'.

Step 6: Employ the Fourier transform to the reconstructed watermark encrypted image.

Step 7: The image obtained from step 6 and the complex conjugate of $R2(u, v, w)$ are multiplied together.

Step 8: Finally, to get the decrypted secret medical image, apply Inverse Fourier transform on the image obtained from step 7.

6 Simulation Results and Discussions

6.1 Evaluation Metrics

1. Peak Signal-to-Noise Ratio

The PSNR metric is based on the Root Mean Square Error (RMSE) and maximum pixel gray level value. It is calculated as in (24) [37–39]:

$$PSNR = 10 \log\left(\frac{(I_m(x, y, z))^2}{RMSE^2}\right) \quad (24)$$

where I_m is the maximum pixel gray level value in the reconstructed image. The RMSE is formulated as,

$$RMSE = \frac{1}{3 \times M \times N} \sum_{z=1}^3 \sum_{x=1}^M \sum_{y=1}^N [W(x, y, z) - I(x, y, z)]^2 \quad (25)$$

2. Structure Similarity Index

The structural similarity index method (SSIM) tests the quality of the digital image as it measures the similarity between two images. The SSIM index is estimated on different blocks of an image [37]. The measure between the two blocks $\{x\}$ $\{y\}$ is:

$$SSIM = L(W, I) C(W, I) S(W, I) \quad (26)$$

where $L(W, I)$ is the luminance component, $C(W, I)$ is the contrast component and $S(W, I)$ is the saturation component.

3. Normalized Cross-correlation

It measures the correlation between two images $D(x, y, z)$, the watermark image and $\hat{D}(x, y, z)$ the extracted image from Eq. (27) [37–39]:

$$NC = \frac{\sum_{z=1}^3 \sum_{x=1}^M \sum_{y=1}^N D(x, y, z) \times \hat{D}(x, y, z)}{\sqrt{\sum_{z=1}^3 \sum_{x=1}^M \sum_{y=1}^N D(x, y, z)^2} \sqrt{\sum_{z=1}^3 \sum_{x=1}^M \sum_{y=1}^N \hat{D}(x, y, z)^2}} \quad (27)$$

where M and N indicate watermark image dimensions.

4. Feature Similarity Index

A Feature Similarity Index Matrix (FSIM) is used for image quality assessment. If the first image is f_1 (recovered secret image) and the second image f_2 (secret image). The Magnitude Gradient maps G_1 and G_2 are taken away from images f_1 and f_2 . FSIM can be estimated depending on $PC_1, PC_2, G_1,$ and $G_2,$ as shown from Eqs. (28) to (30) [37,38].

We can estimate the similarity of two images using phase congruency as:

$$S_{PC} = \frac{(2PC_1PC_2 + T_1)}{(PC_1^2 + PC_2^2 + T_1)} \tag{28}$$

where T_1 is a constant. Similarly, the similarity from Magnitude Gradient maps G_1 and G_2 is as follow [37]:

$$S_G = \frac{(2G_1G_2 + T_2)}{(G_1^2 + G_2^2 + T_2)} \tag{29}$$

where T_2 is a constant. From Eqs. (28) and (29), the FSIM can be calculated as in (30):

$$S_l(x) = [S_{PC}(x)]^\alpha \cdot [S_G(x)]^\beta \tag{30}$$

5. Histogram Evaluation

The histogram is a diagrammatic performance of the brightness distribution in an image [39]. The histogram plots the total pixel number in the image (vertical axis) with a specific brightness (horizontal axis). In this paper, the histogram is used to normalize two images (watermark and extracted watermark) and (cover image and cover image with watermark) and take the difference between them.

6.2 Simulation Results and Discussion

On the sending side, the first step of the scheme is the encryption process of the medical image to be watermarked in the cover color image to be transmitted securely. The DRPE algorithm does the encryption and decryption processes. Fig. 5 shows an encrypted secret medical image using DRPE. The resulting image shows that the encryption process has a high-quality encrypted image. Furthermore, the resulting images from the system show the efficiency of the DRPE system, as the encrypted image does not have any features or limits to know the shape of the encrypted image.

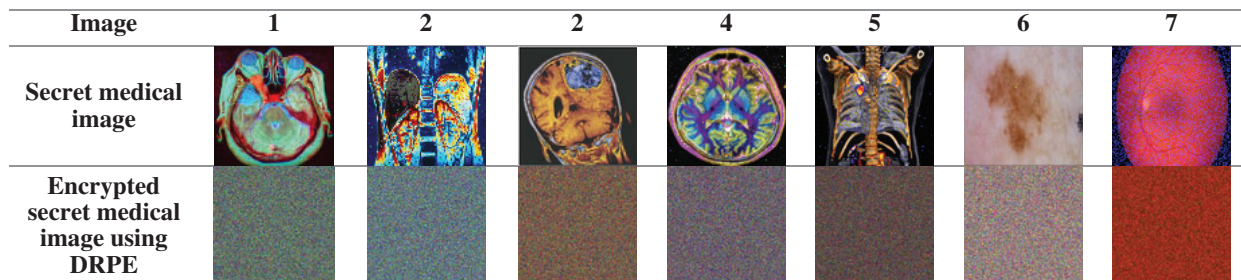


Figure 5: Encrypted secret medical image using DRPE

After encrypting the secret medical image, the least significant WHT hides the watermark medical image in the color cover image. First, we must choose the size of the watermarked image so that there

is enough embedded space to fit the original image. So, the cover image is chosen to be $512 \times 512 \times 3$ and the watermark medical image $90 \times 90 \times 3$ (Because with that size, the original image will divide 163844×4 blocks per color channel watermarked image will have 162001×4 blocks to embed, almost enough). Then, the encrypted image is concealed inside the cover image using WHT. The resulting image shown in Fig. 6 clarifies that the digital cover image after the encrypted image is quite close to the original cover image in human perception vision.

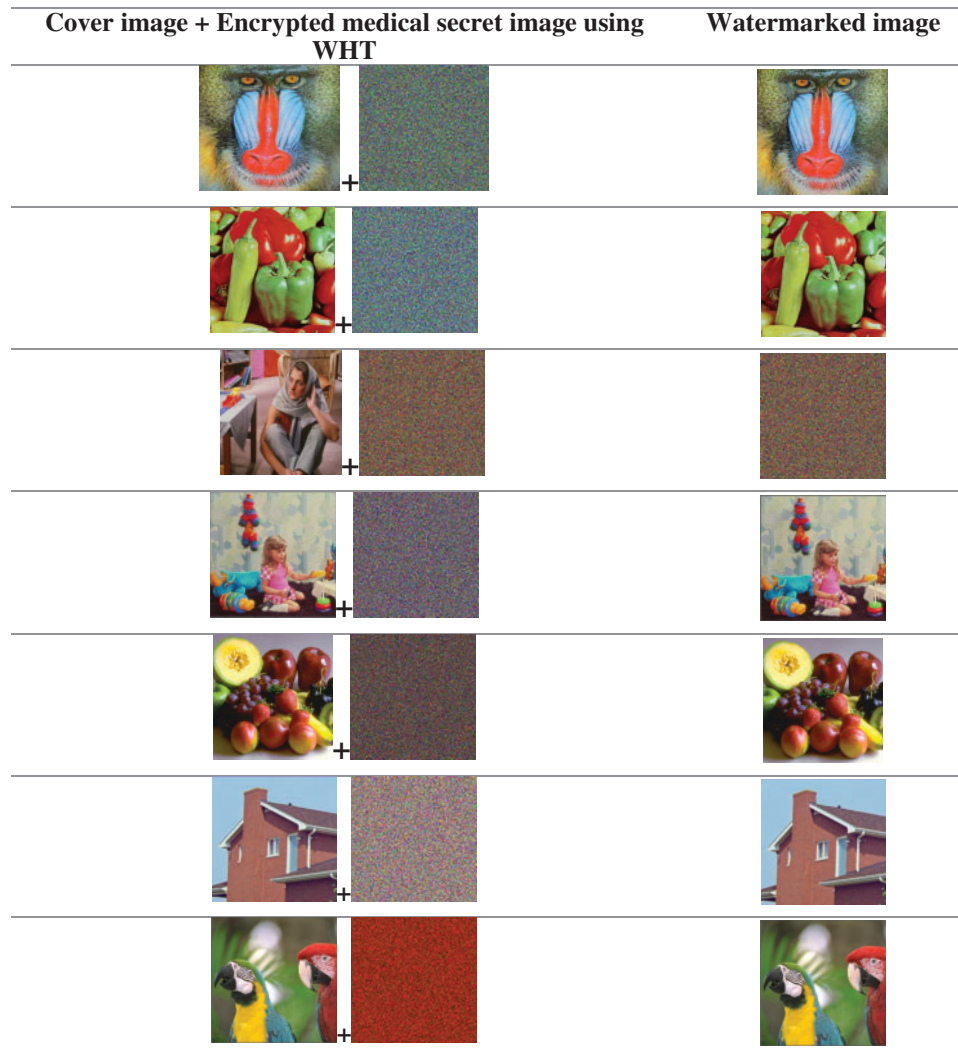


Figure 6: Watermarked image using WHT

On the receiver side, the received watermarked image is the image that contains the encrypted image inside it, so the first step in the receiver is the inverse process of WHT to extract a secret medical encrypted image. After the extraction process, the encrypted medical image is decrypted using the inverse of the DRPE process. The resulting image from the inverse of the DRPE algorithm is the secret image. The obtained images after the inverse process of WHT and inverse process of DRPE are shown in Fig. 7.




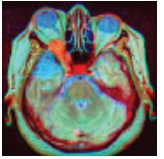


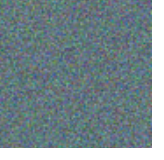
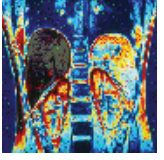



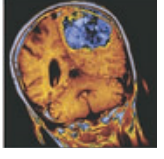
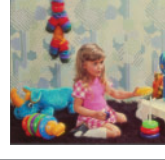
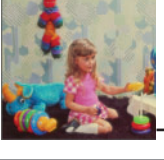
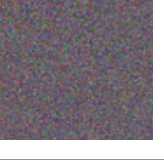
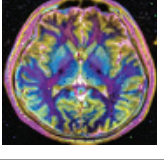


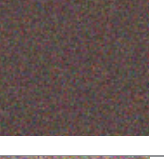


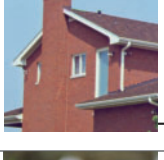

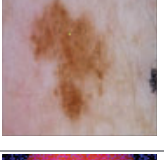
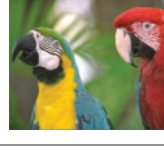
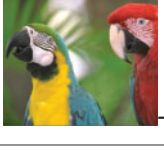

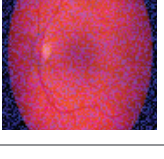
Received image	Cover image + Encrypted watermark image using inverse WHT		Extracted watermark after Inverse DRPE
			
			
			
			
			
			
			

Figure 7: Extracted watermark image using IWHT and decrypted secret medical image using inverse DRPE

Tab. 1 tabulates the PSNR, NC, SSIM, and FSIM outcomes for the received watermarked images with respect to the original cover image. They are checked for seven types of images. As shown from the results, the quality of the watermarked image is very good for all images as PSNR values are large and reasonable to a large extent. The high correlation values reflect the compatibility between the watermarked image and the cover image. The maximum value of NC is 1; as shown from the table, all

NC values are near to 1, which means the proposed algorithm has a high correlation value. Also, it is clear from [Tab. 1](#) that SSIM and FSIM are approximately 1, meaning the similarity of cover image with secret medical image and without it are very close to each other. The visual percipient between two images is not observed to human eyes.

Table 1: PSNR, NC, SSIM, and FSIM for the watermarked image at the receiver

Parameter	Watermarked image 1	Watermarked image 2	Watermarked image 3	Watermarked image 4	Watermarked image 5	Watermarked image 6	Watermarked image 7
PSNR	51.6573	49.7680	49.6650	49.6887	49.9349	49.9201	50.1490
NC	0.9999	0.9999	0.9998	0.9999	0.9999	0.9998	0.9999
SSIM	0.9996	0.9983	0.9988	0.9987	0.9982	0.9970	0.9977
FSIM	0.9998	0.9998	0.9998	0.9998	0.9998	0.9997	0.9997

This paper uses the histogram to normalize two images and differentiate them. As shown in [Fig. 8](#), the graphical representation of the brightness distribution in two images (the cover color image and watermarked image within secret medical image) is almost the same to a very large degree to the degree that the difference between them is approximately zero.

[Tab. 2](#) tabulates the values of PSNR, NC, SSIM, and FSIM for the extracted watermark image with respect to the secret watermark image. They are checked for seven types of medical images. The results show that the quality of extracted watermark images is very good for all images as PSNR values are large and reasonable to a large extent. The high correlation values reflect the compatibility between the extracted and the secret images. The maximum value of NC is 1; as shown from the table, all NC values are near to 1, which means the proposed algorithm has a high correlation value. Also, it is clear from [Tab. 2](#) that SSIM and FSIM are approximately 1, which means the similarity of extracted watermark cover image and watermark medical image are very close to each other. The visual percipient between two images is not observed to human eyes.

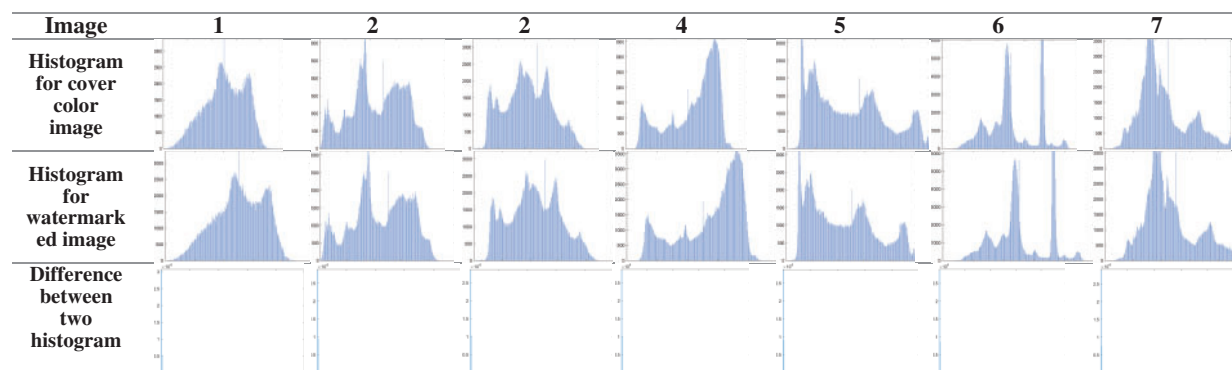


Figure 8: Difference between histograms for cover color image and watermarked image

The histogram is utilized to normalize extracted watermark image, and the watermark secret medical image then takes the difference between them. As shown in [Fig. 9](#), the graphical representation of the brightness distribution in the two images is almost the same to a very large degree to the degree that the difference between them is approximately zero.

Table 2: PSNR, NC, SSIM, and FSIM for extracted watermark image at receiver

Parameter	Extract watermark 1	Extract watermark 2	Extract watermark 3	Extract watermark 4	Extract watermark 5	Extract watermark 6	Extract watermark 7
PSNR	53.5210	24.3880	99	35.5510	37.9910	49.7140	26.7448
NC	0.9998	0.9698	1	0.9958	0.9630	0.9994	0.7162
SSIM	0.9996	0.9334	1	0.9866	0.9899	0.9965	0.6295
FSIM	0.9994	0.9521	1	0.9954	0.9935	0.9997	0.8072

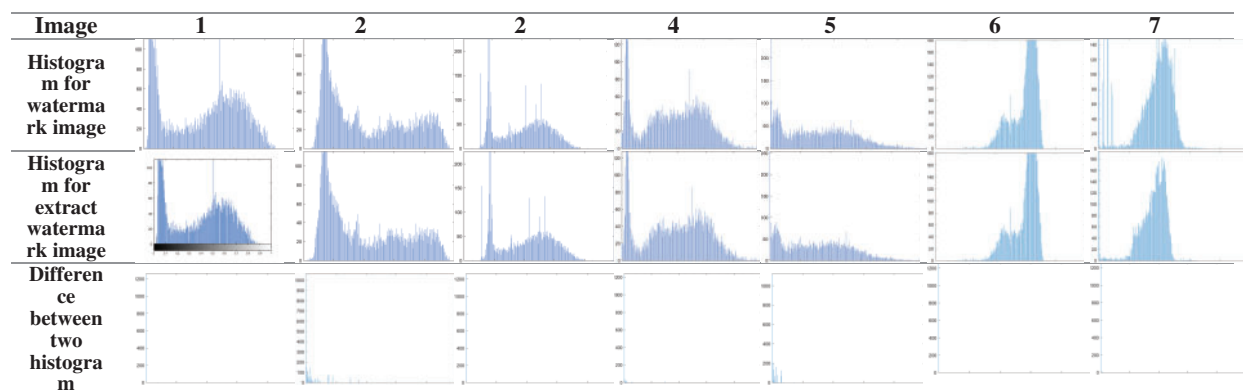


Figure 9: Difference between histograms for watermark image and extract watermark image

7 Conclusions and Future Work

This paper produced a new algorithm in security systems where DRPE encryption is combined with the WHT algorithm to provide a highly secure method of medical image and its transmission between the sender and the receiver. DRPE algorithm is used as an encryption scheme to encrypt the secret medical image, and WHT is used to hide it into a color cover image. The secret image is hidden inside the cover color image, making it difficult for the intruder to access the secret medical image. The obtained outcomes confirm the extent of its success in our electronic world. Various applications of this proposed approach include financial services (banking), agencies, medical images, hiding passwords, encryption keys, and transporting highly private documents. They also need a small processing time. Therefore, the proposed schemes are suited for image transmission in wireless authentication systems and other real-time applications. In future work, the utilization of artificial neural networks for image segmentation can be introduced. Moreover, in the future, more suggestions can be employed to enhance the proposed work performance, such as utilizing deep learning techniques for segmentation and classification purposes.

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

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

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

References

- [1] A. Alarifi, S. Sankar, T. Altameem, K. Jithin, M. Amoon *et al.*, “A novel hybrid cryptosystem for secure streaming of high efficiency H. 265 compressed videos in IoT multimedia applications,” *IEEE Access*, vol. 8, pp. 128548–128573, 2020.
- [2] O. Faragallah, H. El-sayed, A. Afifi and W. El-Shafai, “Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional fourier transform,” *Optics and Lasers in Engineering*, vol. 137, no. 6, pp. 1–15, 2021.
- [3] A. Alarifi, M. Amoon, M. Aly and W. El-Shafai, “Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system,” *IEEE Access*, vol. 8, pp. 221246–221268, 2020.
- [4] O. Faragallah, M. Alzain, H. El-Sayed, J. Al-Amri, W. El-Shafai *et al.*, “Block-based optical color image encryption based on double random phase encoding,” *IEEE Access*, vol. 7, pp. 4184–4194, 2018.
- [5] K. Al-Afandy, W. El-Shafai, E. El-Rabaie, F. Abd El-Samie, O. Faragallah *et al.*, “Robust hybrid watermarking techniques for different color imaging systems,” *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25709–25759, 2018.
- [6] W. El-Shafai, S. El-Rabaie, M. El-Halawany and F. Abd El-Samie, “Security of 3D-HEVC transmission based on fusion and watermarking techniques,” *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 27211–27244, 2019.
- [7] W. El-Shafai, S. El-Rabaie, M. El-Halawany and F. Abd El-Samie, “Efficient hybrid watermarking schemes for robust and secure 3D-MVC communication,” *International Journal of Communication Systems*, vol. 31, no. 4, pp. 1–23, 2018.
- [8] O. Faragallah, M. AlZain, H. El-Sayed, J. Al-Amri, W. El-Shafai *et al.*, “Secure color image cryptosystem based on chaotic logistic in the FrFT domain,” *Multimedia Tools and Applications*, vol. 79, no. 3, pp. 2495–2519, 2020.
- [9] O. Faragallah, A. Afifi, W. El-Shafai, H. El-Sayed, E. Naeem *et al.*, “Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications,” *IEEE Access*, vol. 8, pp. 42491–42503, 2020.
- [10] A. Mahmoud, W. El-Shafai, T. Taha, S. El-Rabaie, O. Zahran *et al.*, “A statistical framework for breast tumor classification from ultrasonic images,” *Multimedia Tools and Applications*, vol. 80, no. 4, pp. 5977–5996, 2021.
- [11] 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.
- [12] 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.
- [13] A. Algarni, G. El Banby, S. Ismail, W. El-Shafai, F. El-Samie *et al.*, “Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security application,” *Entropy*, vol. 22, no. 12, pp. 1–32, 2020.
- [14] S. Ibrahim, M. Egila, H. Shawky, M. Elsaid, W. El-Shafa *et al.*, “Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption,” *Multimedia Tools and Applications*, vol. 13, pp. 1–26, 2020.
- [15] N. Soliman, M. Khalil, A. Algarni, S. Ismail, R. Marzouk *et al.*, “Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication,” *Multimedia Tools and Applications*, vol. 9, pp. 1–35, 2020.
- [16] S. Nassar, N. Ayad, H. Kelash, H. El-sayed and F. Abd El-Samie, “Content verification of encrypted images transmitted over wireless awgn channels,” *Wireless Personal Communication*, vol. 88, no. 9, pp. 479–491, 2016.

- [17] S. Nassar, N. Ayad, H. Kelash, H. El-sayed and F. E. Abd El-Samie, "Secure wireless image communication using lsb steganography and chaotic baker ciphering," *Wireless Personal Communication*, vol. 91, no. 8, pp. 1023–1049, 2016.
- [18] S. Singh and G. Bhatnagar, "A new robust watermarking system in integer DCT domain," *Journal of Visual Communication: Image Representation*, vol. 53, no. 5, pp. 86–101, 2018.
- [19] C. Hsu and S. Tu, "Digital watermarking scheme for copyright protection and tampering detection," *International Journal of Information Technology and Security*, vol. 11, no. 4, pp. 107–119, 2019.
- [20] J. Chena, Y. Zhanga, L. Jinchang and L. Zhang, "Security enhancement of double random phase encoding using rear-mounted phase masking," *Optics and Lasers in Engineering*, vol. 101, no. 2, pp. 51–59, 2018.
- [21] K. Prabha and I. Sam, "A novel blind color image watermarking based on walsh hadamard transform," *Multimedia Tools and Applications*, vol. 79, no. 5, pp. 6845–6869, 2020.
- [22] H. Zhang, C. Wang and X. Zhou, "A robust image watermarking scheme based on svd in the spatial domain," *Future Internet*, vol. 9, no. 45, pp. 201–211, 2017.
- [23] T. Takore, P. Kumar and G. Devi, "A new robust and imperceptible image watermarking scheme based on hybrid transform and PSO," *International Journal of Security Systems and Applications*, vol. 11, no. 4, pp. 50–63, 2018.
- [24] J. Liu and X. He, "A review study on digital watermarking," in *Proc. of the 1st Int. Conf. on Information and Communication Technologies, ICICT*, Karachi, Pakistan, pp. 337–341, 2005.
- [25] R. Olanrewaju, "Development of intelligent digital watermarking via safe region," Ph.D. Thesis, Kulliyah of Engineering, International Islamic University Malaysia, Selangor, Malaysia, 2011.
- [26] U. Yadav, J. Sharma, D. Sharma and P. Sharma, "Different watermarking techniques & its applications: A review," *International Journal of Science Engineering and Research*, vol. 5, no. 4, pp. 1288–1294, 2014.
- [27] N. Cvejic, "Algorithms for audio watermarking and steganography," Master's Thesis, Department of Electrical and Information Engineering, University of Oulu, Oulu, Finland, 2004.
- [28] J. Sang and M. Alam, "Fragility and robustness of binary-phase-only-filter-based fragile/semi fragile digital image watermarking," *IEEE Transaction Instrumentation and Measurements*, vol. 57, no. 3, pp. 595–606, 2008.
- [29] N. Loani, N. Hurrabi, S. Parah and G. MohiuddinBhat, "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption," *IEEE Access*, vol. 6, pp. 19876–19897, 2018.
- [30] S. Katti, V. Namuduri and K. Namuduri, "A practical approach for evaluating the capacity of watermarking channel," in *Proc. of the Int. Conf. on Intelligent Sensing and Information Processing*, Chennai, India, pp. 193–198, 2005.
- [31] L. P'erez-Freire, P. Na and J. Ramon, "Watermarking security: A survey," in *Transactions on Data Hiding and Multimedia Security; Lecture Notes in Computer Science*. Berlin/Heidelberg, Germany, 41–72, 2006.
- [32] W. El-Shafai, F. Mohamed, H. Elkamchouchi, M. Abd-Elnaby and A. ElShafee, "Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm," *IEEE Access*, vol. 9, pp. 1–25, 2021.
- [33] A. Qasim, F. Meziane and R. Aspin, "Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review," *Computer Science Review*, vol. 27, pp. 45–60, 2018.
- [34] K. Meenakshi, C. Rao and K. Prasad, "A robust watermarking scheme based walsh-hadamard transform and SVD using ZIG ZAG scanning," in *Proc. of 13th Int. Conf. on Information Technology (ICIT)*, Cairo, Egypt, pp. 167–172, 2014.
- [35] W. El-Shafai, I. Almomani and A. Alkhayer, "Optical bit-plane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication," *IEEE Access*, vol. 9, pp. 35004–35026, 2021.
- [36] W. El-Shafai, E. El-Rabaie, M. El-Halawany and F. Abd El-Samie, "Efficient multi-level security for robust 3D color-plus-depth HEVC," *Multimedia Tools and Applications*, vol. 77, no. 23, pp. 30911–30937, 2018.
- [37] U. Sara, M. Akter and M. Uddin, "Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study," *Journal of Computer and Communications*, vol. 7, no. 4, pp. 1–13, 2019.

- [38] X. Zhang, W. Zhang, W. Sun, X. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.
- [39] X. Zhang, X. Sun, X. Sun, W. Sun and S. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.