IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Chaos Fractal Digital Image Encryption Transmission in Underwater Optical Wireless Communication System

Amira G. Mohamed[1], Somia A. Abd El-Mottaleb[2], Mehtab Singh[3], Hassan Yousif Ahmed*[4], Medien Zeghid[4,6], Wazie M. Abdulkawi[4], Belgacem Bouallegue[5,6], Osman Ahmed Abdalla[7]

[1]Department of Electronics and Communications Engineering, Alexandria Higher Institute of Engineering, Alexandria 21311, Egypt
[2]Department of Mechatronics Engineering, Alexandria Higher Institute of Engineering, Alexandria 21311, Egypt
[3]Department of Electronics and Communication Engineering, University Institute of Engineering, Chandigarh University, Mohali 140413, Punjab, India
[4]Electrical Engineering Department, College of Engineering at Wadi Aldwaseer, Prince Sattam Bin Abdulaziz University, KSA.
[5]College of Computer Science, King Khalid University, Abha, Saudi Arabia
[6]Electronics and Micro-Electronics Laboratory (E. µ. E. L), Faculty of Sciences, University of Monastir, Tunisia
[7] Department of Computer Science, University College of Tayma, University of Tabuk, Tabuk 71491, Saudi Arabia

Corresponding author: Hassan Yousif Ahmed

ABSTRACT This study introduces a novel image cryptosystem designed to improve security and reliability within underwater optical wireless communication (UOWC) systems particularly for water bodies that exhibits higher absorption and scattering coefficients. An image encryption scheme, characterized by high security, and consists of a chaotic iteration of dragon fractal shapes (ChDrFr). The system performance is assessed across five distinct water types, each exhibiting unique optical properties. For enhancing the quality of encrypted images received, median and high-pass filters are utilized. To test the ability of this new algorithm to ward off different types of attacks, numerical simulation is applied. Specifically, a correlation coefficient of approximately zero is witnessed between the original images and those generated by encryption. The optimum values for information entropy and unified average changed intensity (UACI) are almost reached for the encrypted images. A comparison is undertaken between different encryption methods and the one proposed in this paper, depending on ChDrFr. Results show that the proposed encryption scheme yields better results and achieves much securer encrypted images, when compared to the images encrypted by other encryption algorithms. Additionally, the encrypted images show enhancement in the underwater transmission distance with 6% for Pure Sea (PS) and Clear Ocean (CL), 4% for Coastal Sea (CS), 0.9% for Harbor I (HI), and 0.8% for Harbor II (HII). Moreover, the utilization of filters results in improvement in the Structured Similarity Index (SSIM), Peak-Signal-to-Noise-Ratio (PSNR), and Signal-to-Noise-Ratio (SNR).

INDEX TERMS Underwater optical wireless communication (UOWC), Chaotic iteration of dragon fractal (ChDrFr), Water attenuation, Signal to noise ratio (SNR), Information entropy, Structured similarity index method (SSIM)

I. INTRODUCTION

A significant portion of the earth's surface consists of oceans and seas. The depths of these waters remain largely unexplored. Oceanographers and research scientists are increasingly interested in investigating these vast, uncharted areas [1]. Additionally, increased underwater activities, such as deep-sea mining, monitoring of oceanic ecosystems, and underwater rescue operations, require the development of effective communication methods to transmit large amounts of undersea data to aerial vehicles and, subsequently, to terrestrial stations. Accordingly, the demand for adaptable and dependable communication links to handle high data throughput is increasing7ymly critical. Conventional communication systems like acoustic waves and radio frequency (RF) signals are inadequate in this scenario.

Acoustic waves face challenges due to their restricted bandwidth, notable reflection problems at the water surface, and long latency. In addition, acoustic waves have a negative impact on marine fish and mammals. These factors make them unsuitable for high-speed applications [1].

Radio frequency (RF) signals, commonly used in wireless communication, experience significant attenuation in water. Conversely, cable-based communication, though stable, limits the mobility of remotely operated vehicles

(ROVs) due to their tethered connections, which restrict range, maneuverability, and independence. This issue is particularly problematic for multiple ROVs, as it significantly increases the risk of cable entanglement [2]. These limitations highlight the need for alternative communication solutions that can overcome the challenges posed by traditional methods.

Alternatively, optical wireless communication (OWC) offers a promising solution for short- to medium-range communication scenarios. This is due to its several advantages, including high bandwidth, relative flexibility, secure communication, low latency, and moderate attenuation in water [3]. Consequently, underwater wireless optical communication (UWOC) has emerged as a promising technology, attracting significant interest from commercial, military, and scientific sectors. This growing interest is further fueled by advancements in optical sources, such as laser diodes (LDs) and LEDs, optical receivers, such as Si PIN photodiodes (PDs) and avalanche photodiodes (APDs), and enhanced digital signal processing, which are driving the increasing demand for UWOC links [4, 5].

Many digital applications and smart devices are used in the transmission of multimedia files, including video, audio, and photo files with sensitive information, as multimedia development and telecommunication technologies develop at a high rate. Images are characterized by strong visual characteristics and are files that can hold large amounts of information. As such, they are an integral part of the communication that takes place over the internet. When transmitting images over unprotected channels of communication, intruders can access confidential information and may easily alter and abuse it, leading to threats in terms of security. As such, it is important to close this breach of security by employing methods that prevent access to images and the confidential information they hold [6-8]. The methods currently employed to secure text do not seem to fit, when it comes to image data. Images, specifically when shared in real time, represent unsuitable targets for these methods of encryption, since they are slow to execute and can be more easily attacked. To secure digital images, the standard encryption approaches, including Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA), Data Encryption Standard (DES), as well as the family of elliptic curve-based encryption (ECC) have set added specific requirements. To be able to encrypt image files, these methods need more time, must make extra computations, and require higher performing equipment. As such, special encryption methods, which consider the specific nature of image files, need to be developed. These schemes should have higher security and should be able to withstand the different types of attacks. Also, they need to have the ability to get executed in real time [9, 10]. As such, scientists are putting much effort into the development of newer encryption schemes, specific to images. One of these methods, which has received a lot of attention and testing is to generate dragon fractal shapes with an added parameter of chaotic iteration (ChDrFr), for use in image encryption. These fractal images are characterized by randomness, as such they are recommended for use in developing encryption schemes that are highly secure and reliable. Another important characteristic of fractals is their sensitivity to their initial values. This is a highly desirable characteristic in encryption systems, making them more robust and resistant to attacks [11].

A. RELATED WORKS

There were several studies done in UOWC systems which used light sources operating in blue-green visible light spectrum as they provide the least attenuation in underwater [1]. Nakamura et al. in [12] used a blue LD in UOWC system and a successful transmission in underwater of 4.8 m was achieved with data rate of 1.45 Gbps. Abd El-Mottaleb et al. in [13] utilized green LDs sources in UOWC system and the study was carried out considering three types of waters: pure seawater (PS), clear ocean (CL), and coastal sea (CS). The findings reported an overall capacity of 4.5 Gbps. Shao et al. in [14] a real-time OWC system with a data rate of 2.2 Gbps was implemented for transmitting 4K video over a 3.6 m underwater channel and an 8 m air optical wireless channel using time-division multiplexing. Gai et al. in [15] proposed an UOWC system that is used to transmit images. The system utilized circular polarization multiplexing technology for single-photon detection. Moreover, an underwater attenuation coefficient of 0.24 m^{-1} was considered, and the results demonstrated successful image transmission over a range of 13.42 m.

Additionally, there were previous research in the field of image encryption. Researchers in [16] explored using particle swarm optimization (PSO) for key optimization, as well as a novel modular integrated logistic exponential (MILE) map, for image encryption. In [17], a variable S-box was used in a scheme employed for encryption based on AES. Blocks of 128 bits were created through the division of the plain image. Each of these blocks was encrypted with a different S-box, generated from a hyperchaotic system. In [18], an algorithm using both a 2D coupled chaotic system and diagonal scrambling was proposed to encrypt images. The first step involved the decomposition of the plain color image into three grayscale plain images. This was followed by the use of an operation of discrete cosine transform (DCT) to convert the grayscale images into the frequency domain coefficient matrices (FDCM). Two groups of matrices were then generated through the 2D coupled chaotic system (2DCS), namely embedded and encryption matrices, consecutively. To fulfill the frequency domain encryption, the first type of matrices was integrated within the FDCM, followed by the recovery of the spatial domain signal, a process performed through inverse DCT processing. To reach the final color ciphertext, both the function of encryption matrices and the proposed diagonal scrambling algorithm were employed. Another research proposed the use of dynamic DNA encoding, along with DNA operations related to simple structure chaotic maps (Logistic, Henon, and Lorenz), in the development of a highly secure image

encryption scheme. To make this algorithm more robust, other techniques were added to it, including the zigzag traversal techniques and the SHA-256 hash. The novelty in this study was in using improved DNA coding techniques, for the encoding of four instead of two bits at the same time. For each session of either encryption or decryption, a unique and random set of keys was employed [19]. A 6D hyperchaotic system, along with random signal insertion were the two techniques used in the development of a new encryption technique in [20]. During iteration, random signals were inserted into the system's variables for the enhancement of the hyperchaotic system's performance. The initial values of the system were obtained through the summation of the plaintext's pixel values. As such, the plain image and the proposed encryption system were closely related. This means that a larger matrix was formed by splitting pixels into two equal parts. This new matrix was subject to scrambling, cycle shift, and diffusion to reach the encrypted image.

B. CONTRIBUTION

In previous studies, images were transmitted without any encryption process, and the attenuation caused by water bodies impacted the transmitted data. Since encryption protects data from external effects, in this study, we propose a digital image transmission system in UOWC communication based on the ChDrFr encryption algorithm. The main contributions of this work are:

- Introducing a new encryption scheme based on fractal shapes, with iterations from a chaotic map. This scheme is highly efficient, more complex in structure, has added security features, and can better resist attacks, making it more effective than other encryption algorithms.
- Proposing an underwater digital encrypted image transmission system in UOWC using the ChDrFr algorithm.
- Studying the impact of attenuation caused by five different water bodies with varying optical properties.
- Investigating the system performance in terms of SNR, PSNR, and SSIM.
- Considering several attacks (visual, statistical, and differential) to test the proposed ChDrFr scheme to ensure its efficiency, robustness, and its ability to resist cryptanalysis.

C. PAPER ORGANIZATION

The rest of the paper is organized as follows. Section 1 explains the proposed image encryption algorithm based on dragon fractal images. Section 2 discusses the absorption and scattering attenuations that occur in UOWC systems. Section 3 presents the layout of the digital ciphered image transmission using the ChDrFr algorithm in UOWC systems. Section 4 provides the results and discussion, followed by the main conclusions.

II. PROPOSED ENCRYPTING IMAGE ALGORITHM UTILIZING CHAOTIC DRAGON FRACTAL IMAGES

In the world of telecommunication, there is constant need for more improved, higher security cryptosystems. For this reason, fractal shapes and chaotic maps are employed as the basis for the image encryption structure proposed in this work. An improvement is also added to the fractal shapes employed in the encryption process. This improvement consists of using a chaotic map as the initiator pattern for the chaotic dragon fractals produced (this map replaces the lines used to generate standard dragon fractals). Applying the above measures ensures that the new cryptosystem is of higher security and avoids all the drawbacks of other image encryption algorithms. This new system starts with the creation of new chaos dragon fractals (ChDrFr), as seen in [21].

The hyper chaotic map is subsequently utilized to extract a set of random values, which are then employed to occupy the vacant spaces within the sparse fractal shapes. The second step involves using integer wavelet transform (IWT) on the input image to extract three detail and one approximation sub-bands. The third step consists of the normalization of the detail sub-bands to maintain them within the range of 0 and 255 (range of the ChDrFr images). As such, the intensity of pixels is changed. The following step involves the use of three different ChFrDr images to diffuse the shuffled detail sub-images. As for the approximation image, to ensure its complexity, a logistic chaotic map helps in the shuffling of its pixels. With the help of another image obtained through the ChDrFr technique, the shuffled sub-image is diffused. The resultant cipher image is produced, once the four sub-bands are arranged. The proposed algorithm, with its different steps can be seen in Figure 1. It is based on these steps.

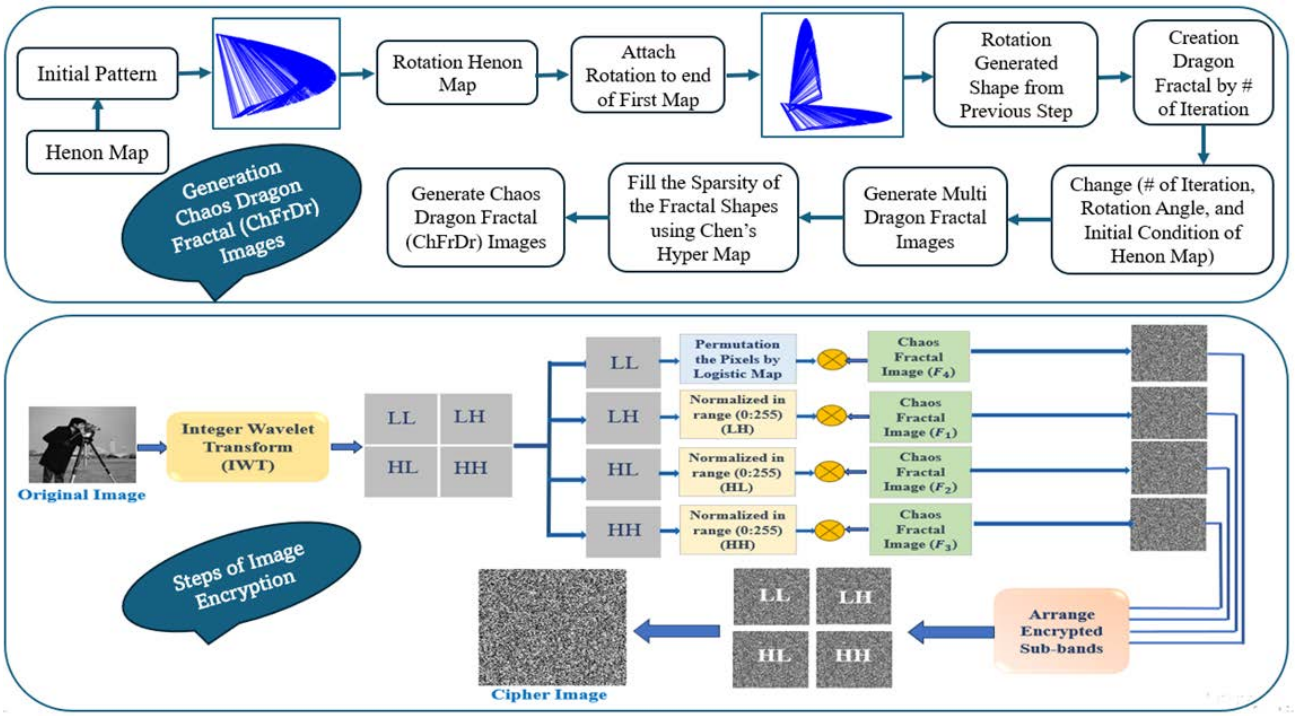


FIGURE 1.Block diagram of the proposed image encryption algorithm.

A. GENERATION OF CRYPTOGRAPHIC KEYS USING THE ChDrFr

In fractal science, iterative or recursive algorithms are employed to create novel shapes that are characterized by self-similarity. This study employs complicated generators to develop new fractal shapes. The initiator and the generator are the two parameters necessary to produce a fractal. In this paper, the Henon map is used as the fractal initiator. On the other hand, the generator involves a number of iterations (n), initial condition map and the rotation angle (R). Applying these parameters ameliorates the security of fractal generation. To generate dragon fractals, Algorithm (1) below is employed:

Step 1: The Henon map is used as the starting pattern to produce the fractal structure. It has good chaotic behavior and discrete time dynamics. Its initial conditions are $\{x_n, y_n\}$ and its parameters, $\{a, b\}$, are given the values 1.4 and 0.3, respectively, for the purpose of this study. With these conditions, the output behavior of the produced fractal is determined. The Henon map can be expressed as [22]

$$x_{n+1} = 1 - ax^2 + y_n \quad (1)$$

$$y_{n+1} = 1 - bx_n \quad (2)$$

Step 2: To produce the fractal shape the map described above undergoes counterclockwise rotation by an angle of (R) degrees, and the resulting shape is subsequently appended to the previous one. The resulting shape is then attached to the end of the previous one.

Step 3: The process outlined in Step 2 is then repeated and starts at the endpoint attained in the prior step. During each iteration, twice the number of copies is generated of the starting generator. Depending on the use of this fractal, the number of iterations is set. The different stages of the production of a ChFrDr can be seen in Fig. 2, while Fig. 3 depicts the variety of shapes of the same fractal, with different parameters.

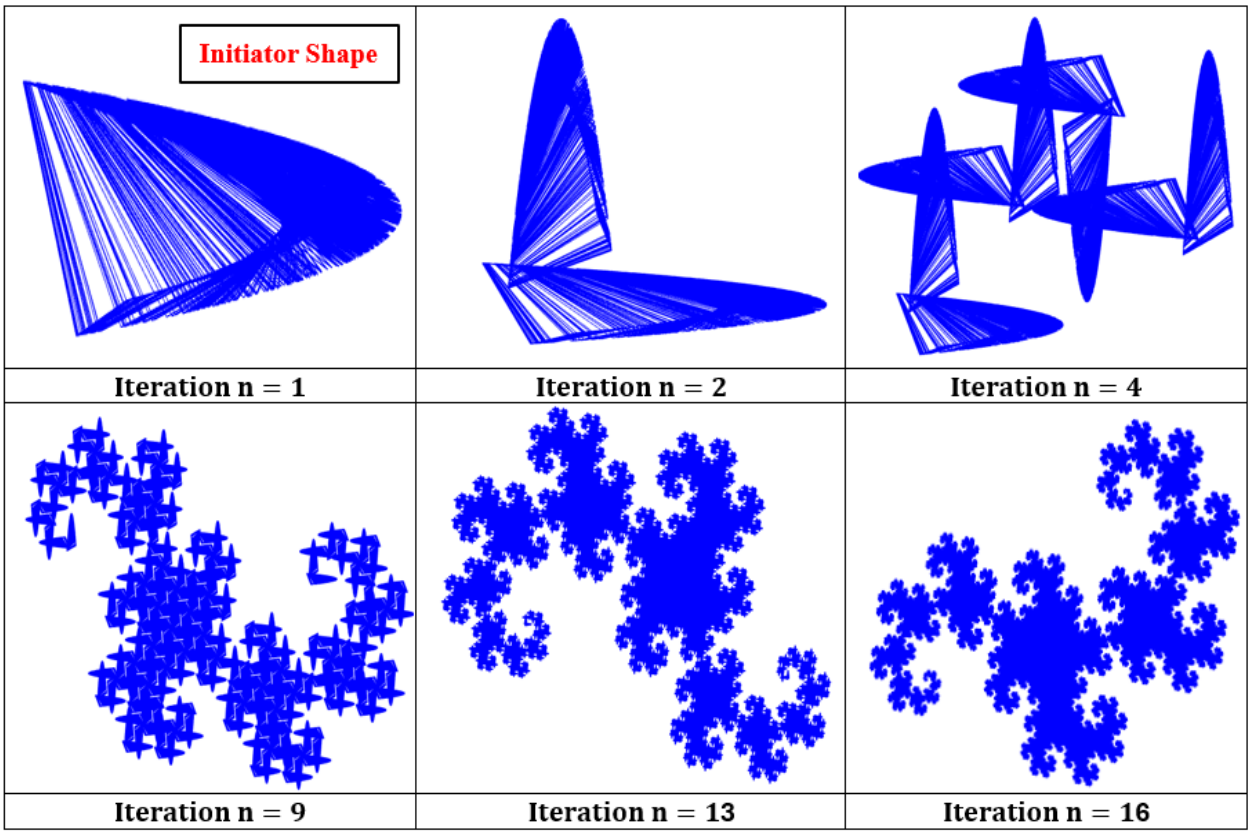


FIGURE 2. **ChFrDr shapes in various iterations.**

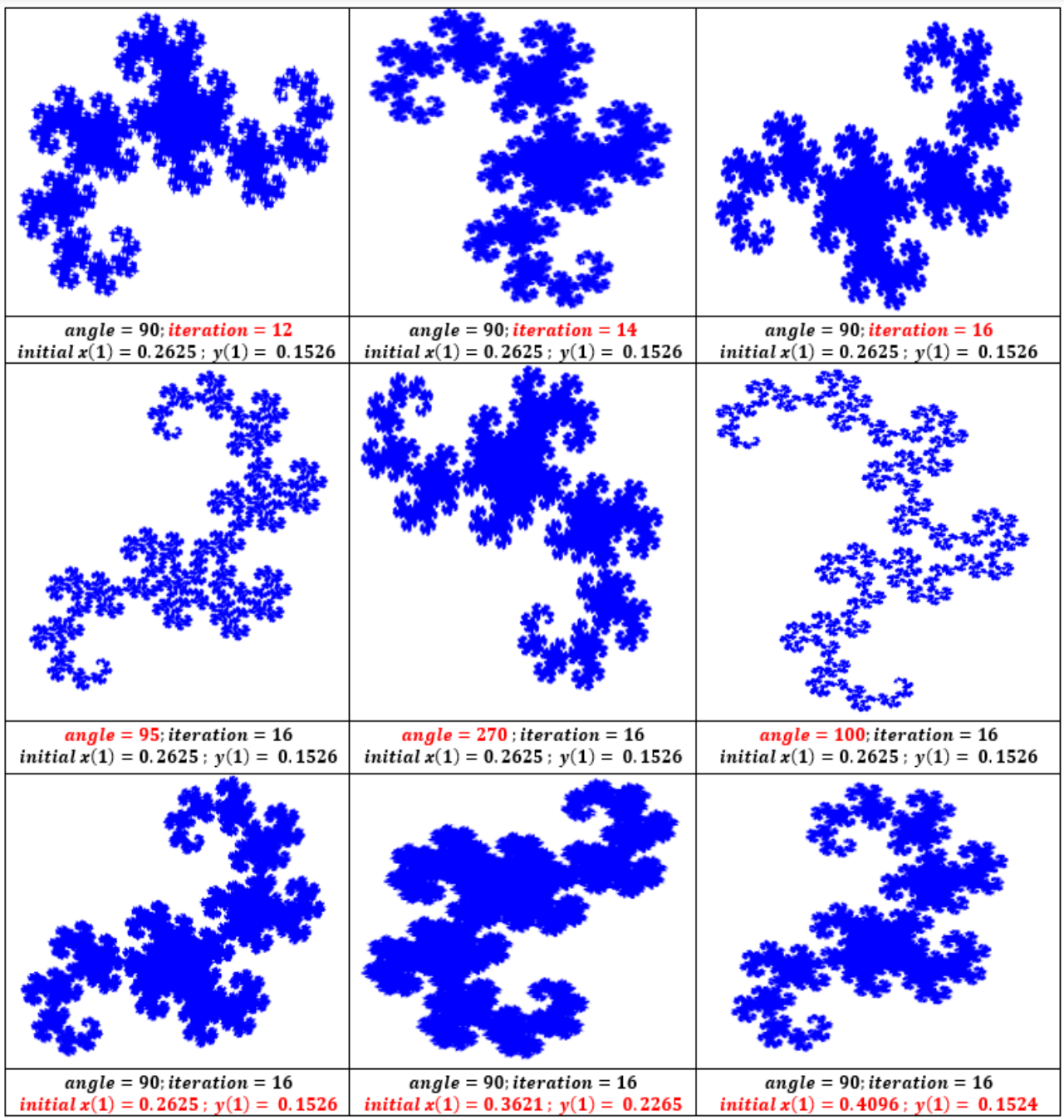


FIGURE 3. Generation various forms of ChFrDr using different control parameters.

Algorithm 1: Generation of cryptographic keys using the ChFrDr

Input: Initial pattern (Henon map with control parameters $\{a, b\}$ initial conditions $\{x_n, y_n\}$, number of iterations (n), and rotation angle (R)).

Output: ChFrDr images.

1: Insert initial inputs.
2: $\{x_o, y_o\}$: Initial conditions.
3: $(a = 1.4, b = 0.3)$: Control parameters.
4: # Eq. (1, 2)
5: Draw Henon map $\{x_n, y_n\}$.
6: Number of iterations (n), and Rotation Angle (R).
7: From the end point of the attractor, rotate the shape at (R) angle in the anti-clockwise direction.
8: Repeat the process, starting from the new endpoint, while rotating in the anti-clockwise direction.
9: With successive iterations, patterns begin to show.
10: The process is repeated as many times as necessary.
11: Return: ChFrDr images.

B. MODIFICATION OF ChFrDr IMAGES

In the suggested algorithm, a control map facilitates the selection of the four ChDrFr images. These fractals are sparse in nature. As such, a Chen hyper-chaotic system supplies random values to fill this sparsity. A Chen map can be expressed as [23]

$$\dot{x_1} = a(x_2 - x_1) \tag{3}$$

$$\dot{x_2} = -x_1 x_3 + d x_1 + c x_2 - q \tag{4}$$

$$\dot{x_3} = x_1 x_2 - b x_3 \tag{5}$$

$$\dot{x_4} = x_1 + k \tag{6}$$

Algorithm 2: Modification of ChFrDr Images

Input: Hyper map with control parameters $a, b, c, d,$ $and\ k$, and initial conditions x_1, x_2, x_3 selected (ChFrDr) images.

Output: Modification of ChFrDr images.

1: Insert initial inputs
2: Insert dragon fractal images $F_n \quad (n = 1, 2, 3, 4)$
3: $x_o = 0.2243, y_o = 0.5876, z_o = 0.9855$
4: $a = 36, b = 3, c = 28, d = -16, \quad and\ k = 0.2$
5: $\#\ Eq.\ (3, 4, 5, 6)$
6: $\dot{x_1} = mod((\dot{x_1} \times 10^{14}), 256))$
7: $\dot{x_2} = mod((\dot{y} \times 10^{14}), 256))$
8: $\dot{x_3} = mod((\dot{z} \times 10^{14}), 256))$
9: $\dot{x_4} = mod((\dot{u} \times 10^{14}), 256))$
10. $for\ i = 1{:}m$
11. $\quad for\ j = 1{:}n$
12. $\quad\quad if\ F_n\ (i, j) == 255$
13. $\quad\quad F_n\ (i, j) = x_n\ (i, j)$
14. $\quad\quad end$
15. $\quad end$
16. end
17: The process is repeated as many times as necessary.
18**: Return:** ChFrDr images.

C. ENCRYPTING IMAGE ALGORITHM UTILIZING ChFrDr IMAGES

Step 1: The process begins with the insertion of a 128 × 128 image, followed by applying an IWT (Inverse Wavelet Transform) operation to the image, leading to three detail sub-bands (LH, HL, and HH) and an approximation (LL) sub-band. Normalization of pixel intensity follows, for detail sub-bands. This ensures that pixel intensity falls within the range from 0 to 255.

Step 2: ChFrDr images are applied to XOR each normalized detail sub-bands. The (F1, F2, and F3) ChFrDr images are used to encrypt HL, LH, and HH, respectively, following normalization.

Step 3: A logistic map is used to shuffle the pixels of the approximation band (LL). This map is part of the chaotic system with (r) the control parameters, (X_o) the initial condition, and (X) the output. Equation (7) represents the inputs:

$$X_{n+1} = rX_n(1 - X_n), \tag{7}$$

where, r is the chaotic parameter, while n is the number of iterations. $r \in [0,4]$ and $x \in [0,1]$. The chaotic attitude is achieved when $r \in [3.57,4]$. Following this step, the ChFrDr image, F_4, is utilizied to XOR the shuffled approximation sub-band. The final image appears, when the approximation and four sub-bands are arranged, following encryption.

III. UOWC CHANNEL ATTENUATION

In UOWC system, absorption and scattering are the two main factors that cause attenuation which results in changing the optical signal direction during propagation and degrading the signal intensity.

The combined of both the absorption and scattering coefficients that are denoted respectively, by $\propto_{abs} (\lambda)$ and $\propto_{scat} (\lambda)$, where λ is the wavelength, are known as beam extinction coefficient and represented as $\propto_c (\lambda)$ [24, 25].

The $\propto_{abs} (\lambda)$ depends on the absorption coefficients due to pure water, $\alpha_{abs}^{PW}(\lambda)$ =0.0445 m^{-1} at 532 nm , chlorophyll concentration, α_{abs}^{CH}, color dissolved organic matter which is the sum of both humic and fulvic acids. The α_{abs}^{CH} can be estimated as [26, 27]

$$\alpha_{abs}^{CH}(\lambda) = \propto_{CH}^{o} (\lambda) \left(\frac{C_{CH}}{C_{CH}^{o}}\right)^{0.62}, \tag{8}$$

where $\propto_{CH}^{o}(\lambda)$ is the spectral coefficient and has a value of 0.0127 m^{-1} at 532 nm, C_{CH} is the total concentration of the chlorophyll in the water with respect to C_{CH}^{o} = 1 mg/m^3, and its value depends on the type of water body. In this study, we consider PS, CL, CS, harbor I (HI), and harbor II (II), which have the values of 0.005 mg/m^3, 0.31 mg/m^3, 0.83 mg/m^3, 2.99 mg/m^3, and 5.9 mg/m^3, respectively, for C_{CH} [25, 26]. The absorption coefficients due to humic acid, α_{abs}^{Hu}, and fulvic acid, α_{abs}^{Fu}, can be expressed as [26, 27]

$$\alpha_{abs}^{Hu}(\lambda) = \propto_{Hu}^{a}(\lambda)\left(0.19334 C_{CH}\exp\left(\frac{C_{CH}}{C_{CH}^{o}}\right)\right)\exp(-k_{Hu}\lambda). \quad (9)$$

$$\alpha_{abs}^{Hu}(\lambda) = \propto_{Fu}^{a}(\lambda)\left(1.74098 C_{CH}\exp\left(\frac{C_{CH}}{C_{CH}^{o}}\right)\right)\exp(-k_{Fu}\lambda), \quad (10)$$

where $\alpha_{abs}^{Hu}(\lambda)$ is the humic acid reference absorption coefficient and has a value of 18.828 m^2/mg at 532 nm, k_{Hu} is the constant and has value of 0.01105 nm^{-1}, $\alpha_{abs}^{Fu}(\lambda)$ is the fulvic acid reference absorption coefficient and has a value of 35.959 m^2/mg at 532 nm, k_{Fu} is the constant and has value of 0.0189 nm^{-1}[25, 26].
Finally, the $\propto_{abs}(\lambda)$ can be expressed as [26, 27]

$$\propto_{abs}(\lambda) = \alpha_{abs}^{PW}(\lambda) + \alpha_{abs}^{CH}(\lambda) + \alpha_{abs}^{Hu}(\lambda) + \alpha_{abs}^{Hu}(\lambda), \quad (11)$$

The $\propto_{scat}(\lambda)$ is expressed as [26, 27]

$$\propto_{scat}(\lambda) = \propto_{scat}^{PW}(\lambda) + \propto_{scat}^{S}(\lambda) + \propto_{Scat}^{L}(\lambda). \quad (12)$$

where $\propto_{scat}^{PW}(\lambda)$ is the scattering coefficient of pure water and is expressed as [26, 27]

$$\propto_{scat}^{PW}(\lambda) = 0.005826\left(\frac{400}{\lambda}\right)^{4.322}, \quad (13)$$

The parameters $\propto_{scat}^{S}(\lambda)$ and $\propto_{Scat}^{L}(\lambda)$ represent the scattering coefficients due to small and large particles, respectively, and can be expressed as [26, 27]

$$\propto_{scat}^{S}(\lambda) = 1.151302\left(\frac{400}{\lambda}\right)^{1.7}\left(0.01739 C_{CH}\exp\left[0.11631\left(\frac{C_{CH}}{C_{CH}^{o}}\right)\right]\right), \quad (14)$$

$$\propto_{Scat}^{L}(\lambda) = 0.341100\left(\frac{400}{\lambda}\right)^{0.3}\left(0.76284 C_{CH}\exp\left[0.03092\left(\frac{C_{CH}}{C_{CH}^{o}}\right)\right]\right), \quad (15)$$

The propagation loss factor is given as [28]

$$P_L(\lambda, L) = exp^{-\propto(\lambda)L}, \quad (16)$$

where L is the underwater distance.

The relation between power transmitted (P_T) and power received (P_R) in case of line of sight (LOS) link is given as [28]

$$P_R = P_T\,\eta_T\,\eta_R\,\frac{A_R\,cos\theta}{2\pi L^2[1-cos\,(\theta_b)]}P_L\left(\lambda, \frac{L}{cos\theta}\right), \quad (17)$$

where η_T is the transmitter optical efficiency and has a value of 0.9, η_R is the receiver optical efficiency and has a value of 0.9, and A_R is the receiver aperture area and has a value of 1 mm^2[24, 27]. θ is the misalignment angle and we assumed it zero degree in this study and θ_b is the beam divergence angle and has a value of 75 mrad [24, 27].

This study considers digital image transmission in five types of water, each with distinct properties. For PS, absorption is calculated as the sum of absorption in pure water (lacking suspended particulate matter) and absorption by salts in the water. In CL, the concentration of dissolved particles, including colored dissolved organic matter, mineral components, and dissolved salts, is greater than in PS. CS contains an even higher concentration of dissolved particles, resulting in elevated absorption and scattering coefficients. HI and HII have the highest absorption and scattering coefficients due to the highest concentration of suspended and dissolved particles, significantly limiting the optical signal during propagation [28].

IV. DESIGN OF DIGITAL IMAGE TRANSMISSION SYSTEM BASED UOWC SYSTEM

Figure 3 shows the layout of the proposed digital encrypted image with ChDrFr fractal transmission system based UOWC system. In the proposed model, an intensity modulation direct detection (IM/DD) on-off keying (OOK) non-return-to-zero (NRZ) modulation scheme is utilized to transmit the gray image at a data rate of 10 Gbps. The system is composed of the transmitter, responsible for data generation and modulation; the channel, which acts as the medium for signal transmission; and the receiver, where the data is demodulated and recovered.

At the transmitter side, the gray image of size 128×128 is first encrypted with ChDrFr algorithm and then converted to binary bits of length 2^{17}. The binary bits are then uploaded to a user defined bit sequence generator (UDBSG) at a data rate of 10 Gbps. Then the bits are line encoded by OOK-NRZ modulation scheme. A LD source operating at 532 nm is utilized for generating the optical carrier that carries the digital image information. Additionally, a Mach-Zehnder-modulator (MZM) is used to modulate the signal resultant from NRZ modulator onto the optical signal generated from the LD. Thus, the total transmitted signal, $S_T(t)$, is expressed as [29]

$$S_T(t) = \sum_{i=1}^{131072} h_i P(t - jT_b), \quad (18)$$

where $h_i \in \{0, 1\}$ is the bit values in the i^{th} time slot, $P(t)$ is the rectangular pulse shape, and T_b is the bit duration that has a value equal to (1/bit rate). The intensity-modulated signal is directed to the transmitter aperture, which focuses the

transmitted beam before it propagates through the underwater channel.

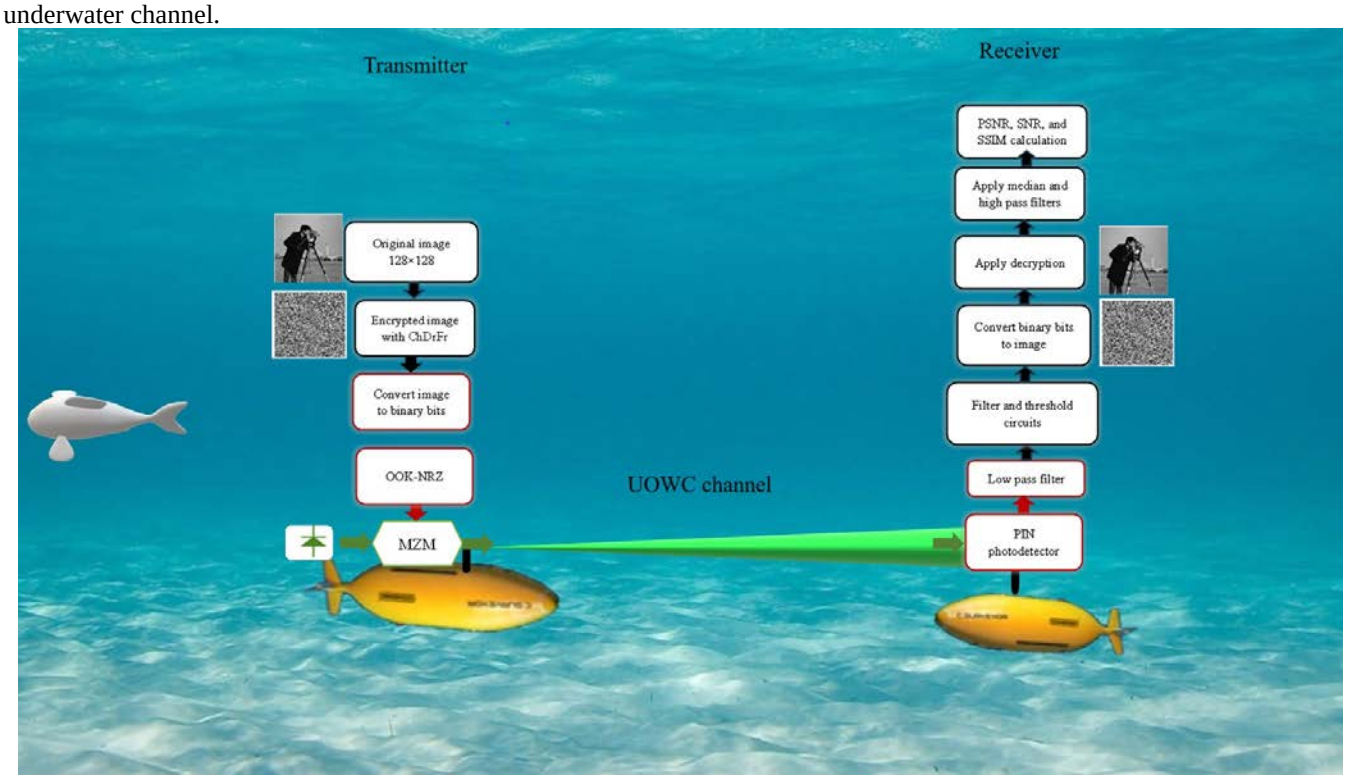


FIGURE 3. Layout of the proposed digital encrypted image with ChDrFr fractal transmission system based UOWC system.

The optical signal during propagating in the channel is affected by attenuation that caused by the water medium. In this work, we consider attenuation caused by five types of waters which are PS, CL, CS, HI, and HII.

After travelling through the underwater channel, the signal reached the receiver side. On the receiver end, the distorted received beam is directed to the receiver aperture, where it is collimated and directed onto the photodetector. The output electrical signal from the photodetector is expressed as [30, 31]

$$I_{photodetector} = \Re P_R + n(t), \tag{19}$$

where $\Re$ represents the responsivity of the PIN photodetector and has a value of 0.8 A/W and $n(t)$ denotes the cumulative noises with a variance of 0.5 N_o, where N_o is the noise power spectral density [31]. Various noises as shot noise, relative intensity noise (RIN), and thermal noises are added to the received signal. The variance of shot noise is expressed as [30, 31]

$$\sigma_{Shot}^2 = 2eB_e\left(I_{photodetector} + I_d\right), \tag{20}$$

where e is the electron charge (1.60217663× 10^{-19} C), B_e is the electrical bandwidth (0.7×Data rate Hz), and I_d is the dark current (6 nA) [32].
The variance of the RIN noise is expressed as [30, 31]

$$\sigma_{RIN}^2 = N_R\left(I_{photodetector}\right)^2, \tag{21}$$

where N_R is the relatively intensity noise.
The variance of thermal noise is expressed as [30, 31]

$$\sigma_{Thermal}^2 = \frac{4K_BTB_e}{R_L}, \tag{22}$$

where K_B is the Boltzmann constant (1.380649× 10^{-23}J/K), T is the absolute temperature (288K), and R_L is the load resistance (50 Ω) [32].
The *SNR* is expressed as[30, 31]

$$SNR = \frac{\left(I_{photodetector}\right)^2}{\sigma_{Shot}^2+\sigma_{RIN}^2+\sigma_{Thermal}^2}, \tag{23}$$

The received signal is then directed towards the low pass filter (LPF) to recover the original signal. Additionally, the signal is converted to binary bits and then to image. Furthermore, the transmission of an image through the underwater channel results in distortion of the received reconstructed image, leading to a degradation in PSNR, SNR, and SSIM. This distortion introduces random fluctuations in the received pixel values, causing them to deviate significantly from the true pixel values of the transmitted image and resulting in substantial errors. To address this issue and restore image quality, this work proposes the use of median and high-pass filters. The median filter, being a nonlinear approach, corrects pixel errors by computing the median of neighbouring pixel values.

In image the SNR is defined as the ratio between the signal power (original image) to the noise power (distorted

image which is the received image at various underwater ranges in this work) and is calculated as [33]

$$SNR = 10log_{10}\left(\frac{\sum_{a=1}^{M}\sum_{b=1}^{N}I(a,b)^2}{\sum_{a=1}^{M}\sum_{b=1}^{N}[I(a,b)-K(a,b)]^2}\right), \quad (24)$$

where $I(a,b)$ and $K(a,b)$ are the pixel value at position (a,b) in the original image and the received image, respectively. M and N are the dimensions of the original and received images, respectively, and in this work are equal to 128.

Another metric used to measure the peak error which quantifies how close the received image to the original image. It can be calculated as [31-33]

$$PSNR = 10log_{10}\left(\frac{W^2}{MSE}\right), \quad (25)$$

where W represents the highest possible pixel value in the image, which is 255 for an 8-bit image. MSE is the mean square error that measure the original image and the received image and can be calculated as [31-33]

$$MSE = \frac{1}{MN}\sum_{a=0}^{M-1}\sum_{b=0}^{N-1}(I(a,b) - K(a,b))^2, \quad (26)$$

where μ_I and σ_I^2 are the mean and variance of the original image, respectively. μ_K and σ_K^2 are the mean and variance of the received image, respectively. σ_{IK} is the covariance of original and received images, and C_1 and C_2 are constants.

Additionally, the SSIM evaluates the similarity between two images by analyzing variations in structural information, luminance, and contrast. It produces a score ranging from -1 to 1, with a value of 1 indicating identical similarity and can be calculated as [31-33]

$$SSIM(I,K) = \frac{(2\mu_I\mu_K+C_1)(2\sigma_{IK}+C_2)}{(\mu_I^2+\mu_K^2+C_1)(\sigma_I^2+\sigma_K^2+C_2)}, \quad (27)$$

V. RESULTS AND DISCUSSION

The proposed digital image transmission in the UOWC system is simulated using Optisystem ver. 21 and MATLAB software. The analysis is divided into two parts. The first part examines the encryption analysis, while the second part focuses on the performance of digital image transmission in the UOWC system.

A. SECURITY ANALYSIS OF IMAGE ENCRYPTION

1) CORRELATION COEFFICIENT

Correlation analysis is performed to examine if the encoded image resembles the original image. In general, there is high correlation between any two adjacent pixels on an image. The encryption algorithm is deemed successful, if it succeeds in breaking this link and disrupting this resemblance. When this occurs, the correlation coefficient between the two adjacent pixels becomes proximal to zero. In this case, the encryption is considered effective [34, 35]. For the purpose of testing, the correlation coefficient can be calculated for two horizontally, vertically, and diagonally adjacent pixels, as

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\times\sqrt{D(y)}}, \quad (28)$$

where, (x) is the grayscale value of a pixel on the plaintext image, while (y) is the grayscale value of a pixel on the encrypted image. r_{xy} is the correlation coefficient, cov represents the covariance between the two pixels, $D(x)$ denotes the variance, and $E(x)$ is the mean. The correlation between two adjacent pixels on the original image, as well as on the encrypted image in the horizontal, vertical, and diagonal directions can be seen on Figure 4. The decrease in pixel correlation on the encrypted image is easily detected, compared to the original image. The proposed algorithm was used to encrypt the images listed in Table 1, where the correlation coefficient of adjacent pixels was calculated and marked. Before encryption, the correlation coefficient of these images was close to one. It can be concluded that the proposed algorithm is successful, as it was able to lower the correlation between two neighboring pixels on the encrypted image and to bring it close to zero.

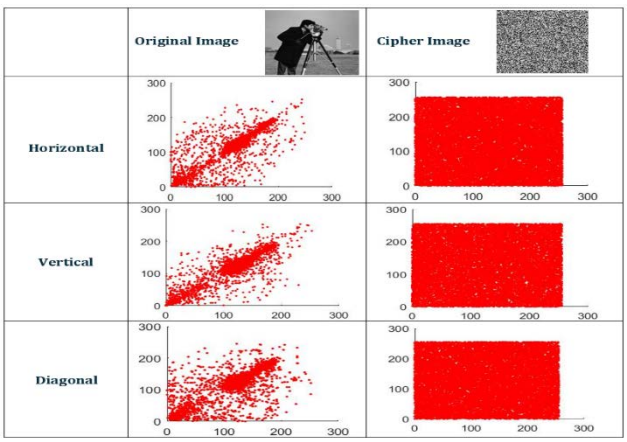


Figure 4. Correlation of two adjacent pixels of the original and its ciphered image.

TABLE I
CORRELATION COEFFICIENTS BETWEEN TWO ADJACENT PIXELS ON THE ORIGINAL AND CIPHERED IMAGES.

Algorithm	Image Name	Plain Image			Encrypted Image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Proposed Algorithm	Cameraman	0.9207	0.9538	0.8894	0.00021	0.00032	0.0010
	Peppers	0.9213	0.9419	0.8695	8.0356e-04	0.00016	0.00132
	Lena	0.8968	0.9525	0.8572	0.00038	6.5689e-04	0.00035
	Baboon	0.8701	0.8700	0.8086	7.2465e-04	0.0003	0.0015
	Airplane	0.8406	0.8784	0.7047	0.00014	0.00039	0.0013
	Boat	0.9117	0.9034	0.8329	0.0012	0.00069	0.0030

2) INFORMATION ENTROPY ANALYSIS

Information entropy is conducted to check the uncertainty of the image's information, as well as to evaluate the gray value

distribution of the image. This variable's value lies in the range from zero to eight, which represents the optimum value. As such, an encrypted image with information entropy close to eight is an indication of a successful encryption algorithm [34, 35]. Equation 29 is used to calculate the information entropy of a specific image:

$$E = \sum_{i=1}^{N-1} P(X_i)\, log_2\, P(X_i), \quad (29)$$

where, N and $P(X_i)$ are is the total number of (X) and the possibility of its occurrence, respectively. Information entropy of the images encrypted with the proposed algorithm can be seen in Table 2. As can be seen, all values of information entropy are close to eight.

TABLE II
INFORMATION ENTROPY ANALYSIS.

Algorithm	Image Name	Information Entropy Analysis
Proposed Algorithm	Cameraman	7.9993
	Peppers	7.9978
	Lena	7.9991
	Baboon	7.9992
	Airplane	7.9985
	Boat	7.9989

2) DIFFERENTIAL ATTACK

NPCR and UACI are used to measure the change in a single bit on the original, as well as the cipher image. This change has a certain effect [34-37]. The following Equations are used to calculate these two variables:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \quad (30)$$

$$UACI = \frac{\sum_{i,j} C_1(i,j) - C_2(i,j)}{255 \times W \times H} \times 100\%, \quad (31)$$

where, W is the width of the cipher image, while H is its height. $C_1(i,j)$ marks the representation of the cipher image before this single bit of change, while $C_2(i,j)$ is the representation after the change. Values for NPCR and UACI can be seen in Table 3. It can be concluded from this Table that these values are close to the ideal values for these variables, where NPCR is equal to 99.6094%, and UACI is equal to 33.4635%. This result demonstrates that the new algorithm is sensitive to minute changes in the original image.

TABLE III
NPCR AND UACI OF DIFFERENT CIPHER IMAGES

Algorithm	Image Name	UACI	NPCR
Proposed Algorithm	Cameraman	33.44	99.59
	Peppers	33.46	99.61
	Lena	33.46	99.61
	Baboon	33.45	99.60
	Airplane	33.43	99.58
	Boat	33.42	99.62

2) HISTOGRAM ANALYSIS

The histogram analysis and its results for both original and encrypted images are shown in this section. From a statistical standpoint, the two images are structurally different. As such, the histogram of the original images shows tilts and spikes, while that of the cipher images is flat and uniform. The conclusion drawn is that there is no statistical resemblance between the two images. The proposed algorithm was used to encrypt several images and Fig. 5 lists the histograms of the original and encrypted versions of these images. To perform quantity analysis and check the uniformity of the images, variance x is calculated for the cipher image, using the Equation below, where $x_i$is the number of pixels whose gray value is equal to i and x_j is the number of the pixels whose gray value is equal to j [38, 39].

$$Var(x) = \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{1}{2} (x_i - x_j)^2, \quad (32)$$

When the calculated variance is found to be small, then the cipher image is deemed uniform. For the encrypted images in this study, Table 4 holds a list of their variance. It can be concluded from this Table, that all histograms analyzed have a uniform distribution. Results of the simulation prove that images encrypted with the proposed algorithm have a uniform histogram. In the comparison conducted between images encrypted with the proposed algorithm and images encrypted with other algorithms, the histograms of the first had smaller variance values than those of the second. This is an indication of the robustness of the proposed algorithm and its ability to fend off statistical attacks.

TABLE IV
VARIANCE VALUES FOR THE HISTOGRAM ANALYSIS OF DIFFERENT CIPHER IMAGES.

Algorithm	Image Name	Histogram Variance
Proposed Algorithm	Cameraman	223.4256
	Peppers	239.5298
	Lena	218.6635
	Baboon	245.4362
	Airplane	241.6385
	Boat	234.9235

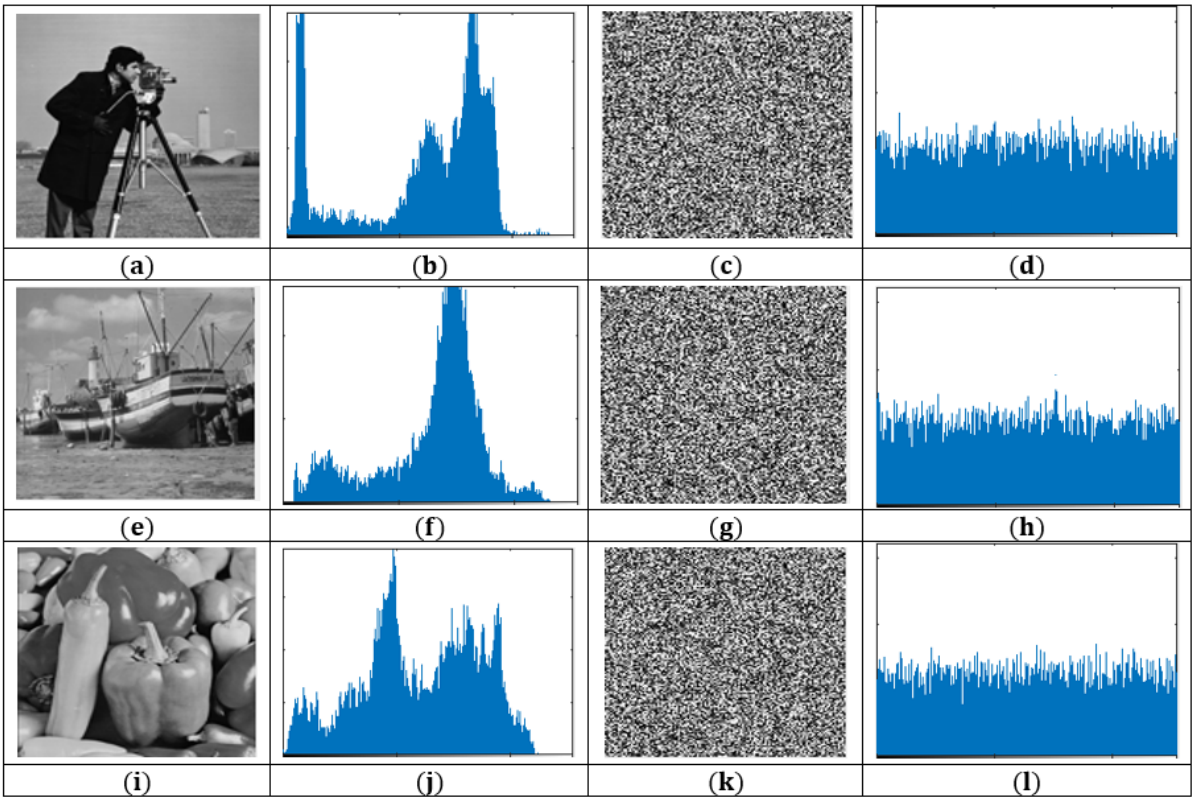


Figure 5. Histogram of test images and corresponding ciphered images.

5) CONTRAST

Contrast is defined as the variation in intensity between adjacent pixels. An encrypted image with a high contrast value is an indication that it was encrypted with an effective algorithm. To calculate contrast, Equation 33 is used [40]

$$Contrast = \sum |i-j|^2 P(i,j), \tag{33}$$

where, $p(i,j)$ marks the location of a specific pixel in the gray-level co-occurrence matrix (GLCM). Contrast values for images encrypted with the algorithm under study are shown in Table 5.

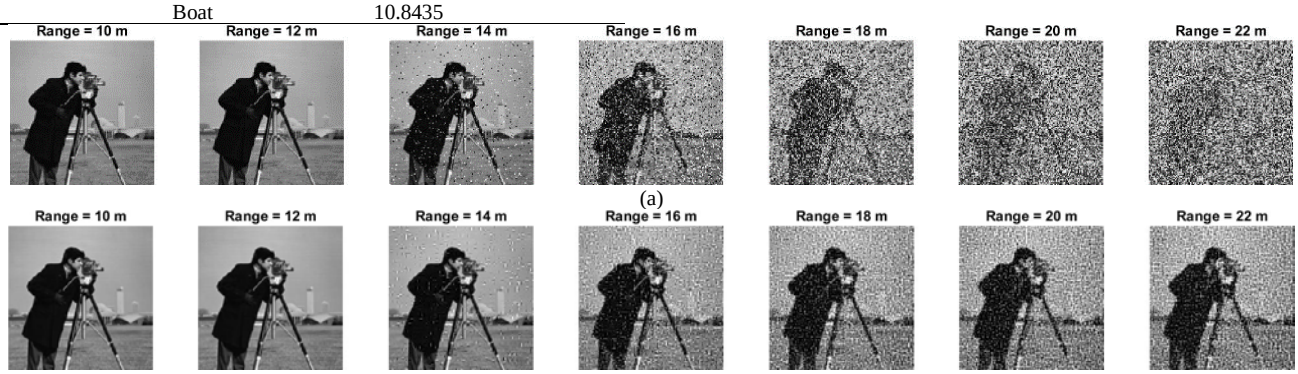
TABLE V
CONTRAST OF VARIOUS CIPHER IMAGES.

Algorithm	Image Name	Contrast
Proposed Algorithm	Cameraman	10.8052
	Peppers	10.8162
	Lena	10.8738
	Baboon	10.8237
	Airplane	10.8448
	Boat	10.8435

B. PERFORMANCE OF DIGITAL IMAGE TRANSMISSION IN THE UOWC SYSTEM

1) PURE SEA

Figure 6 illustrates the quality of received digital images at various underwater distances in PS. Given that PS has the lowest $e(\lambda)$ which is 0.043 m^{-1} at 532 nm, it supports the longest transmission distances for digital images [28]. The ChDrFr encryption algorithm effectively protects the image from external attenuation caused by the PS water. As shown in Fig. 6(b), the encrypted digital image maintains good visual quality up to 22 m underwater. In contrast, the original digital image retains good visual quality only up to 16 m, as seen in Fig. 6(a), which is 6 m shorter than the encrypted image's range. Additionally, the application of filters further enhances the visual quality of the received encrypted images which is cleared from Fig. 6(c).



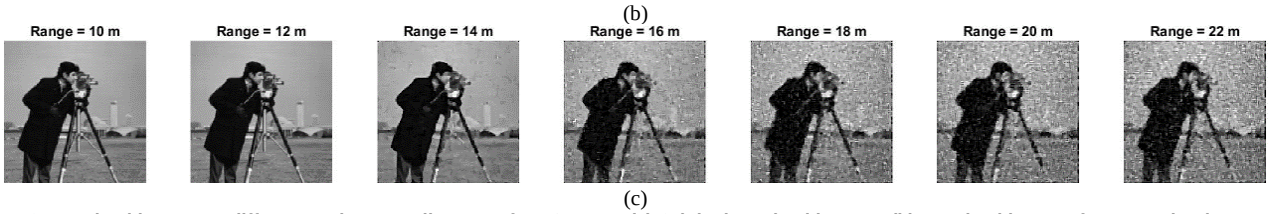


Figure 6. Received images at different underwater distances for PS water: (a) Original received images, (b) Received images for transmitted encrypted images without filters, and (c) Received images for transmitted encrypted images with filters.

In an image, the SSIM evaluates the visual attributes of structure, contrast, and luminance. It is used to make a comparison between two images. Accordingly, in this study, we consider it when evaluating the performance of the received image at various underwater spans with respect to the plain image. Figure 7 illustrates the impact of underwater transmission distances on the SSIM for PS water. The SSIM values exhibit a declining trend as the underwater propagation distance increases. Notably, encrypted received images with enhancement filters consistently display higher SSIM values compared to the other ones. At the initial transmission point, all received images achieve a perfect SSIM value of 1. However, this value declines to 0.0384, 0.1899, and 0.3027 for the original image transmitted without encryption, the encrypted image, and the encrypted image with filters, respectively. This observation underscores the improved clarity of the image after adding filters, particularly at an underwater link of 22 m, where it surpasses the visual quality of the other received images.

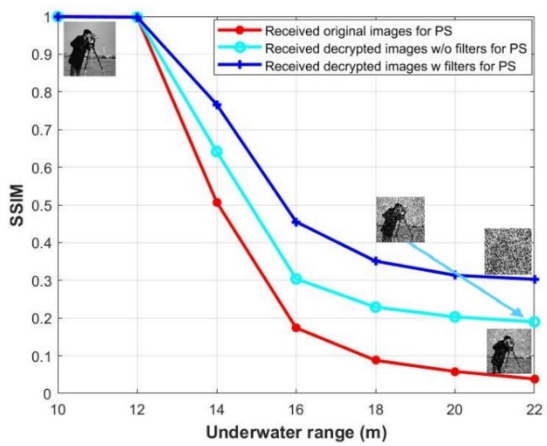


Figure 7. SSIM for proposed digital image transmission versus underwater range for PS water.

Additionally, PSNR and SNR are critical metrics for evaluating image quality as they provide detailed insights into the fidelity and clarity of images. Table 6 presents a comparison of PSNR values for three scenarios involving received digital images at various underwater transmission distances: (1) transmission of plain images, (2) transmission of encrypted images, and (3) transmission of encrypted images followed by filtering at the receiver. The results indicate that PSNR decreases as the optical signal travels longer distances. Notably, the received encrypted images with filters exhibit the highest PSNR value, reaching 18.5609 dB.

TABLE VI
COMPARISON BETWEEN PSNR OF DIFFERENT RECEIVED IMAGES FOR PS WATER.

Underwater distance (m)	PSNR (dB)		
	When plain image transmitted	When encrypted image transmitted	When filters added to received encrypted images
10	Infinity	47.1450	47.1450
12	53.1150	46.4794	46.4794
14	21.5800	25.2494	25.2494
16	13.6751	18.0233	21.4784
18	10.8787	15.8435	19.6602
20	9.7942	15.0203	18.8132
22	9.3222	14.8111	18.5609

Table 7 presents a comparison of SNR values for three scenarios of received digital images transmitted over varying underwater distances: (1) plain image transmission, (2) encrypted image transmission, and (3) encrypted image transmission with subsequent filtering at the receiver. The results indicate that SNR degrades as the optical signal propagates over longer distances in PS water. Notably, the highest SNR of 12.9207 dB is achieved when filters are applied to the received encrypted images. Conversely, the lowest SNR of 4.5592 dB is observed for plain image transmission. This finding underscores the significant enhancement in image quality and SNR provided by the filtering process.

TABLE VII
COMPARISON BETWEEN SNR OF DIFFERENT RECEIVED IMAGES FOR PS WATER.

Underwater distance (m)	SNR (dB)		
	When plain image transmitted	When encrypted image transmitted	When filters added to received encrypted images
10	Infinity	41.5155	41.5155
12	47.4844	40.8500	40.8500
14	16.0763	19.7480	19.7480
16	8.5910	12.5856	15.7424
18	5.9701	10.5407	13.9416
20	4.9610	9.7849	13.1317
22	4.5592	9.5879	12.9207

2) CLEAR OCEAN

CL water exhibits relatively low attenuation of $0.151\ m^{-1}$, but slightly higher than that of PS. Figure 8 displays the received digital images at various underwater distances ranges from 9 m to 15 m for CL water body. Without using any encryption algorithm, the digital image can travel 11 m with good quality as cleared from Fig. 8(a). On the other hand,

using ChDrFr encryption algorithm allows the digital image to be transmitted 4 m longer with good visuality. Moreover, it is evident from Fig. 8 (c) that the application of filters enhances the visual quality of the received encrypted images especially at longer underwater distance.

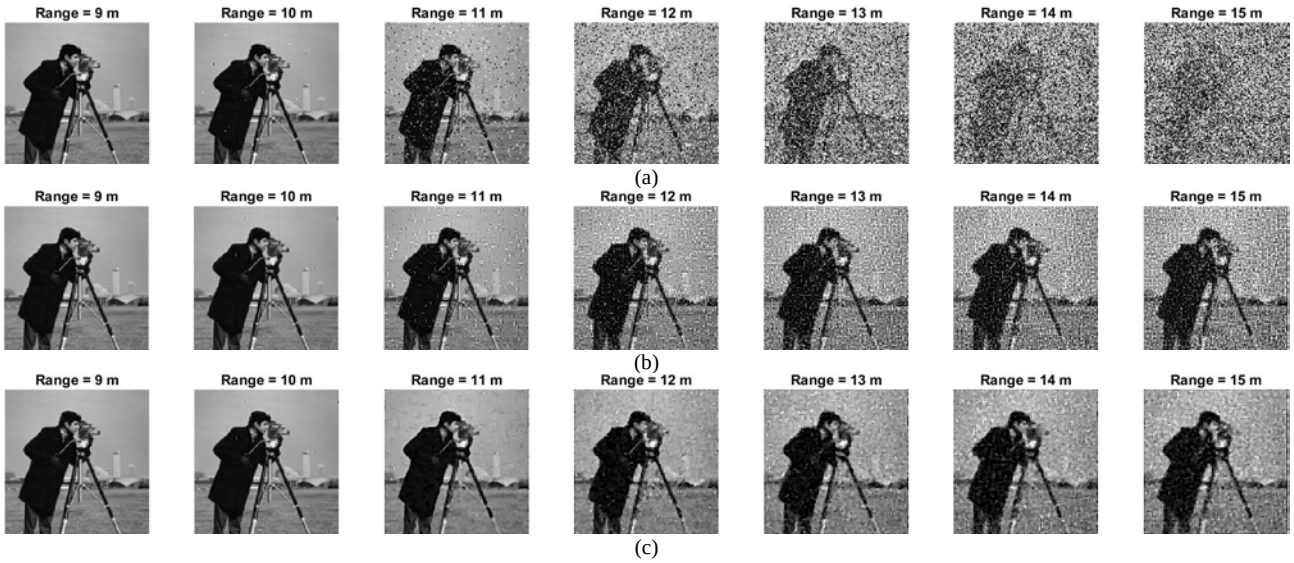


Figure 8. Received images at different underwater distances for CL water: (a) Original received images, (b) Received images for transmitted encrypted images without filters, and (c) Received images for transmitted encrypted images with filters.

Figure 9 demonstrates the effect of underwater transmission distances on the SSIM for CL water. The SSIM values exhibit a decreasing trend as the underwater transmission distance increases from 9 m to 15 m. When the original digital image is transmitted, its quality declines significantly with distance, as indicated by the SSIM value dropping from 1 at 9 m to 0.040788 at 15 m. In contrast, transmitting an encrypted digital image in the UOWC channel results in better quality and higher SSIM values compared to the unencrypted image. Furthermore, the application of filters enhances the SSIM value even more; without filters, the SSIM value is 0.194718, which improves to 0.306453 with the addition of filters.

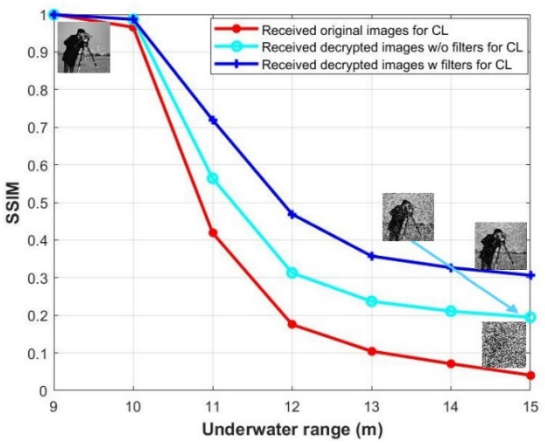


Figure 9. SSIM for proposed digital image transmission versus underwater range for CL water.

Tables 8 and 9 provide a comparison of PSNR and SNR values, respectively, for received digital images in three scenarios: unencrypted, encrypted, and encrypted with filters applied at the receiver. It is observed that shorter underwater transmission distances yield higher PSNR and SNR values compared to longer distances. Notably, digital encrypted images with filters demonstrate superior performance at extended underwater ranges. For instance, at an underwater distance of 15 m, the PSNR and SNR values are 11.2540 dB and 4.6482 dB, respectively, for the unencrypted image. When encryption is applied, these values increase to 18.3588 dB and 9.6594 dB, respectively. Further enhancement is achieved with the application of filters, resulting in PSNR and SNR values of 18.6051 dB and 12.9226 dB, respectively.

TABLE VIII
COMPARISON BETWEEN PSNR OF DIFFERENT RECEIVED IMAGES FOR CL WATER.

Underwater distance (m)	PSNR (dB)		
	When plain image transmitted	When encrypted image transmitted	When filters added to received encrypted images
9	Infinity	47.1450	47.1450
10	36.7198	40.0852	40.0852
11	19.8210	23.7107	24.9113
12	13.7378	18.3588	21.7697
13	11.2540	16.1837	19.8597
14	10.0323	15.2864	19.2250
15	9.4163	14.8955	18.6051

TABLE IX

COMPARISON BETWEEN SNR OF DIFFERENT RECEIVED IMAGES FOR CL WATER.

Underwater distance (m)	SNR (dB) When plain image transmitted	When encrypted image transmitted	When filters added to received encrypted images
9	Infinity	41.5155	41.5155
10	31.0956	34.4563	34.4563
11	14.3703	18.1341	19.2564
12	8.6009	12.9165	16.0400
13	6.2791	10.8537	14.1230
14	5.1506	10.0288	13.5145
15	4.6482	9.6594	12.9226

3) COASTAL SEA

Coastal regions typically exhibit a higher concentration of particulates that differentially scatter light wavelengths. As a result, CS water exhibits an attenuation of 0.398 m^{-1},which surpasses the attenuation observed in PS and CL water bodies. Figure 10 presents the digital images received at varying underwater distances, ranging from 6.5 m to 10.5 m, for the CS water body. Without the application of any encryption algorithm, the digital image retains its quality up to an underwater transmission distance of 7.83 m, as illustrated in Fig. 10(a). In contrast, the employment of the ChDrFr encryption technique allows the encrypted digital image to traverse an underwater span of 10.5 m while maintaining its visual integrity, a distance greater than that achievable by the unencrypted image. Moreover, as depicted in Fig. 10(C), the incorporation of filters markedly enhances the visual quality of the received encrypted images, especially at longer underwater distances.

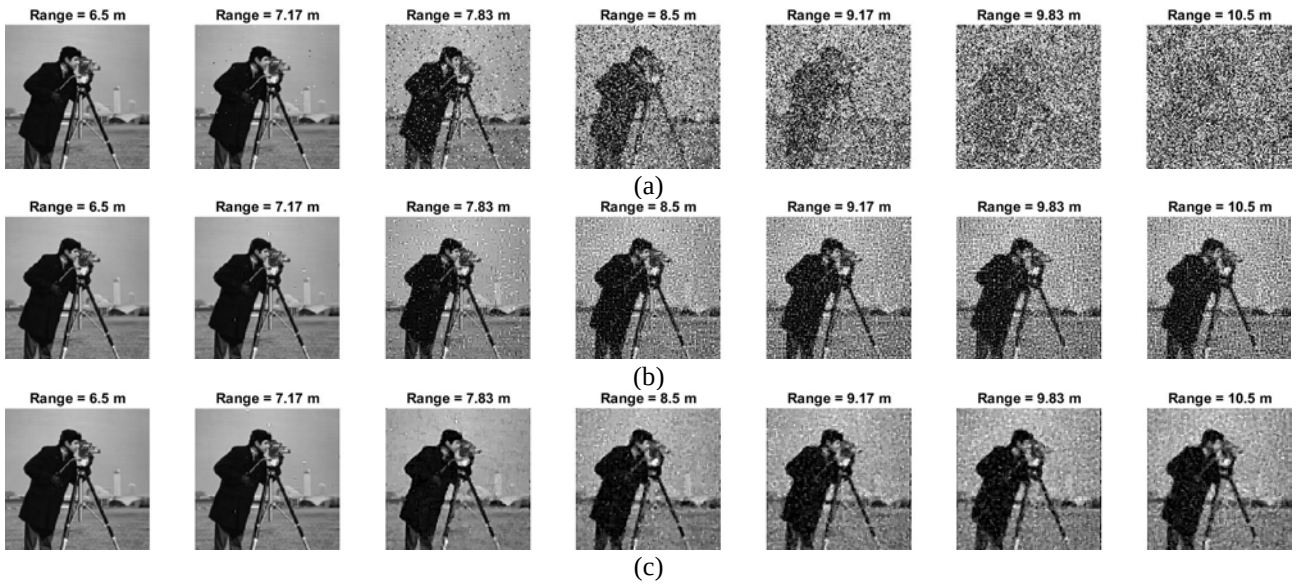


Figure 10. Received images at different underwater distances for CS water: (a) Original received images, (b) Received images for transmitted encrypted images without filters, and (c) Received images for transmitted encrypted images with filters.

Figure 11 illustrates the impact of varying underwater transmission distances on the SSIM for CL water. SSIM values are higher at shorter underwater ranges. Transmission of the original digital image results in a significant decrease in image quality as the distance increases, with the SSIM value dropping sharply from 1 at 6.5 m to 0.037933 at 10.5 m. In contrast, the encrypted digital image transmitted through the UOWC channel maintains higher quality and SSIM values compared to the unencrypted image. The SSIM value improves from 0.037933 for the unencrypted image to 0.182011 for the encrypted image. Furthermore, the application of filters further enhances the SSIM value, underscoring the effectiveness of encryption and filtering techniques in preserving image quality over longer underwater transmission distances.

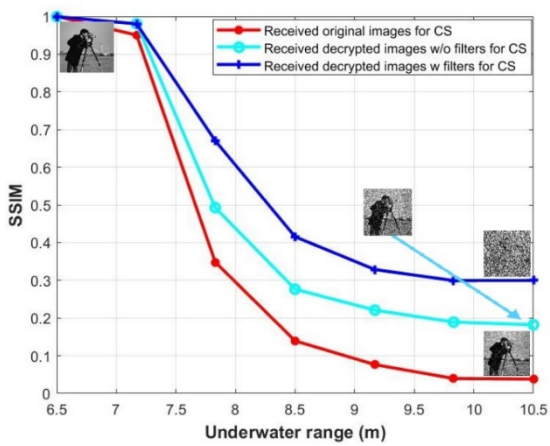


Figure 11. SSIM for proposed digital image transmission versus underwater range for CS water.

Tables 10 and 11 provide a comparative analysis of PSNR values for received digital images across three scenarios: unencrypted, encrypted, and encrypted with

receiver-applied filters. It is clear that shorter underwater transmission distances yield higher PSNR and SNR values than longer distances for CS water body. Encrypted digital images with filters show notably better performance over extended underwater ranges. For instance, at an underwater distance of 10.5 meters, the PSNR and SNR values for the unencrypted image are 9.0809 dB and 4.2787 dB, respectively. When encryption is applied, these values increase to 14.7353 dB and 9.5073 dB, respectively. Further enhancements are observed with the use of filters, achieving PSNR and SNR values of 18.5037 dB and 12.8614 dB, respectively.

TABLE X
COMPARISON BETWEEN PSNR OF DIFFERENT RECEIVED IMAGES FOR CS WATER.

Underwater distance (m)	PSNR (dB)		
	When plain image transmitted	When encrypted image transmitted	When filters added to received encrypted images
6.5	Infinity	47.1450	47.1450
7.17	34.5741	39.3190	39.3190
7.83	18.4293	22.2553	24.2274
8.5	12.4293	17.1582	20.9561
9.17	10.4392	15.4995	19.2019
9.83	9.4681	14.8687	18.5487
10.5	9.0809	14.7353	18.5037

TABLE XI
COMPARISON BETWEEN SNR OF DIFFERENT RECEIVED IMAGES FOR CS WATER.

Underwater distance (m)	SNR (dB)		
	When plain image transmitted	When encrypted image transmitted	When filters added to received encrypted images
6.5	Infinity	41.5155	41.5155
7.17	28.9537	33.6905	33.6905
7.83	12.8546	16.7054	18.5570
8.5	7.3551	11.7778	15.2216
9.17	5.5967	10.2214	13.4839
9.83	4.7032	9.6297	12.8955
10.5	4.2787	9.5073	12.8614

4) HARBORS I AND II

HI and HII waters exhibit higher extinction coefficients, primarily due to the dense concentrations of suspended and dissolved particles, compared to PS, CL, and CS. The extinction coefficients $e(\lambda)$ of HI and HII at 532 nm are 1.1 m^{-1} and 2.19 m^{-1}, respectively. These high attenuation levels significantly restrict the effective range of UOWC in these environments. Figures 12 and 13 display the quality of received digital images at various underwater distances in HI and HII, respectively. As expected, the original digital cameraman image achieves longer underwater transmission distances in HI due to its lower extinction coefficient compared to HII. In HII, the plain digital image can transmit up to 3.2 m with good visual quality, which is 1.4 m shorter than in HI. Additionally, the encrypted image can propagate distances of 5.8 m in HI and 4 m in HII, outperforming the unencrypted image. Furthermore, the application of filters enhances the quality of received images at 5.8 meters in HI and 4 m in HII, as evidenced by Fig. 12(c) for HI and Fig. 13(c) for HII.

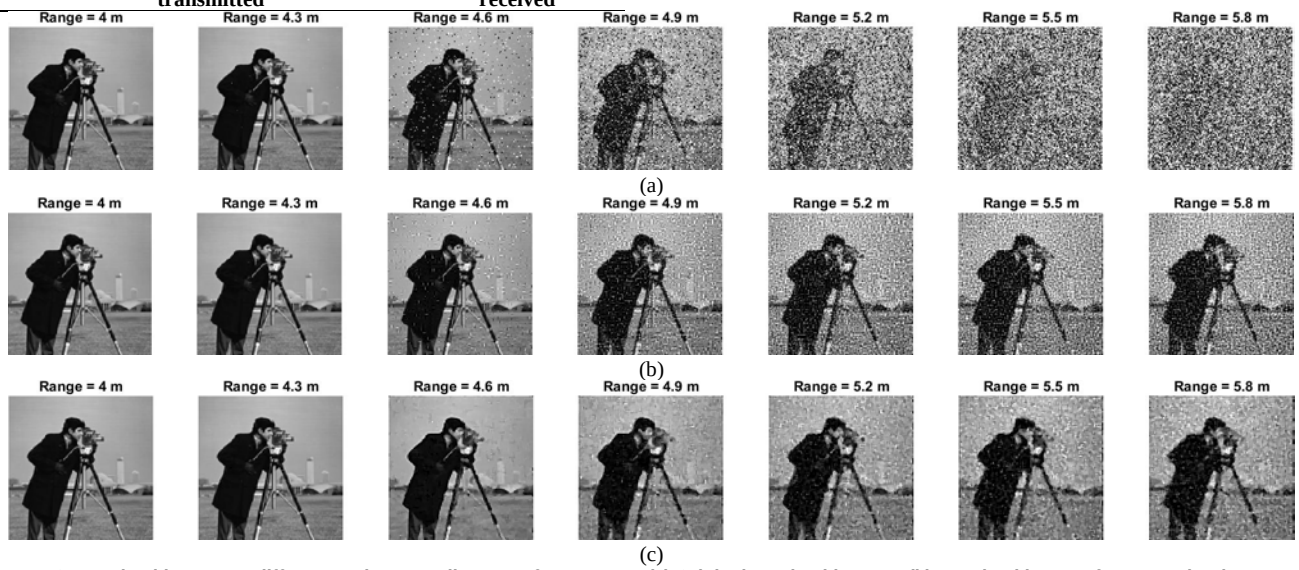
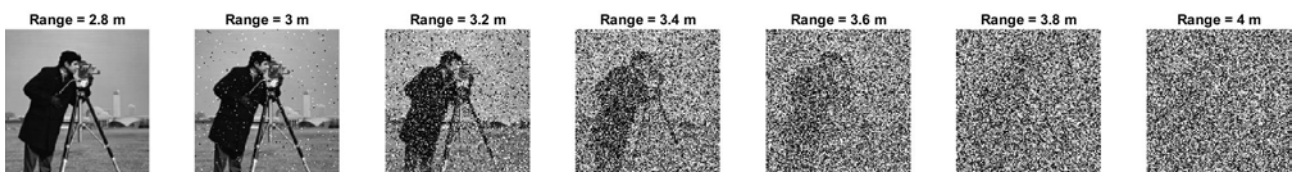


Figure 12. Received images at different underwater distances for HI water: (a) Original received images, (b) Received images for transmitted encrypted images without filters, and (c) Received images for transmitted encrypted images with filters.



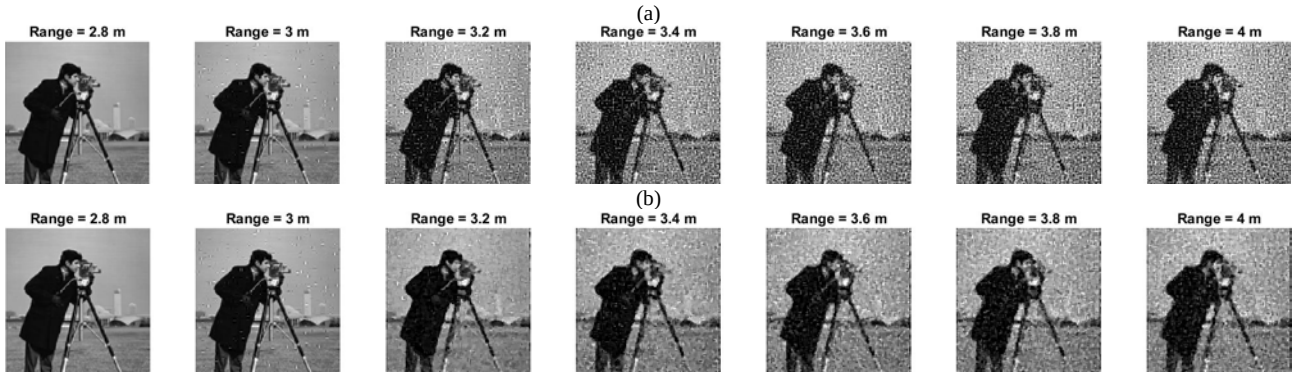
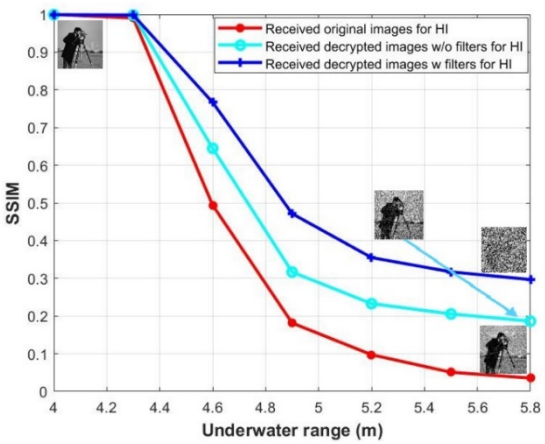
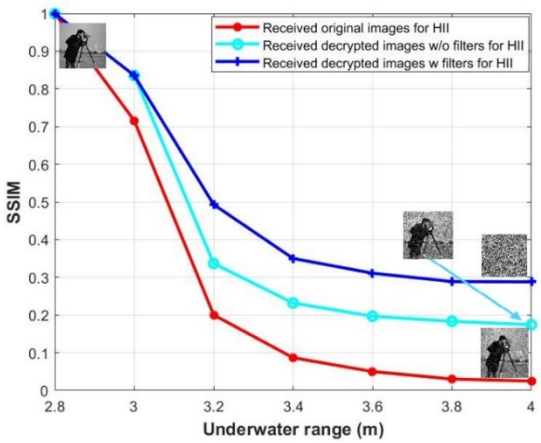


Figure 13. Received images at different underwater distances for HII water: (a) Original received images, (b) Received images for transmitted encrypted images without filters, and (c) Received images for transmitted encrypted images with filters.

Figure 14 illustrates the impact of varying underwater transmission distances on the SSIM for HI and HII water bodies, respectively. SSIM values are higher at shorter underwater ranges. Transmission of the original digital image results in a significant decline in image quality as the distance increases. Specifically, at an SSIM value of approximately 0.03, the plain cameraman image can reach distances of 5.8 m for HI and 3.8 m for HII. In contrast, the encrypted digital image maintains better SSIM values at these distances, achieving 0.186253 for HI and 0.183249 for HII. Additionally, the application of filters further enhances these SSIM values to 0.296733 for HI and 0.28876 for HII, respectively. These results underscore the effectiveness of encryption and filtering techniques in preserving image quality over extended underwater transmission distances.



(a)



(b)

Fig. 14 SSIM for proposed digital image transmission versus underwater range for (a) HI water and (b) HII.

Figure 14. SSIM for proposed digital image transmission versus underwater range for (a) HI water and (b) HII.

Tables 12 and 13 provide a comparative analysis of PSNR values for received digital images of digital image transmission system that utilized in HI and HII, respectively, across three scenarios: unencrypted, encrypted, and encrypted with receiver-applied filters. Shorter underwater transmission distances yield higher PSNR values than longer distances. Encrypted digital images with filters show notably better performance over extended underwater ranges. Furthermore, enhancements are observed with the use of filters.

TABLE XII
COMPARISON BETWEEN PSNR OF DIFFERENT RECEIVED IMAGES FOR HI WATER.

Underwater distance (m)	PSNR (dB)		
	When plain image transmitted	When encrypted image transmitted	When filters added to received encrypted images
4	Infinity	47.1450	47.1450
4.3	41.9872	43.3307	43.3307
4.6	21.2953	25.5557	25.2185
4.9	13.8151	18.2772	21.8793
5.2	11.0046	15.9134	19.7252
5.5	9.6057	15.1720	18.8631
5.8	9.1354	14.7649	18.4567

TABLE XIII
COMPARISON BETWEEN PSNR OF DIFFERENT RECEIVED IMAGES FOR HII WATER.

Underwater distance (m)	PSNR (dB) When plain image transmitted	When encrypted image transmitted	When filters added to received encrypted images
2.8	Infinity	47.1450	47.1450
3	25.4398	30.0766	30.0766
3.2	14.4402	18.8670	22.1351
3.4	10.7476	15.8529	19.5964
3.6	9.5552	14.9882	18.7240
3.8	8.9738	14.6628	18.3124
4	8.7469	14.5388	18.3409

Tables 14 and 15 compare the SNR values for received digital images of digital image transmission system that utilized in HI and HII, respectively, under three different scenarios: unencrypted, encrypted, and encrypted with filters applied at the receiver. The data clearly show that longer underwater links result in lower SNR values. Digital images that are encrypted and have filters applied demonstrate significantly better performance at longer underwater distances compared to original digital transmission images.

TABLE XIV
COMPARISON BETWEEN SNR OF DIFFERENT RECEIVED IMAGES FOR HI WATER.

Underwater distance (m)	**SNR (dB) When plain image transmitted**	**When encrypted image transmitted**	**When filters added to received encrypted images**
4	Infinity	41.5155	41.5155
4.3	36.3584	37.7014	37.7014
4.6	15.7906	19.9620	19.5874
4.9	8.6712	12.8392	16.1319
5.2	6.0520	10.6037	14.0021
5.5	4.7524	9.9212	13.1855
5.8	4.3633	9.5417	12.8232

TABLE XV
COMPARISON BETWEEN SNR OF DIFFERENT RECEIVED IMAGES FOR HII WATER.

Underwater distance (m)	SNR (dB) When plain image transmitted	When encrypted image transmitted	When filters added to received encrypted images
2.8	Infinity	41.5155	41.5155
3	19.8714	24.4594	24.4594
3.2	9.2436	13.3997	16.4000
3.4	5.8226	10.5518	13.8677
3.6	4.7430	9.7470	13.0353
3.8	4.1882	9.4490	12.7084
4	4.0139	9.3296	12.7044

VI. Conclusion

This study introduces a novel approach for ciphered digital image transmission in UOWC systems using the ChDrFr encryption algorithm. The ChDrFr algorithm is distinguished by its complex structure, enhanced security features, and robustness against various attacks. By incorporating this encryption scheme into UOWC systems, we address the significant challenge of data security in underwater communications, thereby enabling more reliable and secure transmission of digital images. The performance of the ciphered digital image transmission is evaluated across five different water bodies, each exhibiting unique extinction attenuation values. To enhance the visual quality of the received digital images, median and high-pass filters are employed. The proposed ChDrFr algorithm is also subjected to external effects to examine its security, demonstrating superior resilience. The transmission of ciphered images in UOWC systems using the ChDrFr algorithm allowed the optical carrier to propagate longer underwater distances compared to those carrying unencrypted images, resulting in better SSIM, PSNR, and SNR values. Furthermore, the application of median and high-pass filters significantly improved the quality of the received encrypted images. Consequently, we recommend the implementation of our proposed model in marine applications that require high security, such as military services.

ACKNOWLEDGMENT

The authors acknowledge the Deanship of Scientific Research for providing administrative and financial support. Funding for this work has been provided by the Deanship of Scientific Research, King Khalid University, Ministry of Education, Kingdom of Saudi Arabia, under research Group Project grant award number RGP.1/157/42.

REFERENCES

[1] Z. Zeng, S. Fu, H. Zhang, Y. Dong, and J. Cheng, "A survey of underwater optical wireless communications," *IEEE communications surveys & tutorials*, vol. 19, no. 1, pp. 204–238, 2016, doi: 10.1109/COMST.2016.261884.1

[2] P. P. Ganesh and H. Venkataraman, "RF-based wireless communication for shallow water networks: Survey and analysis," *Wireless Personal Communications*, vol. 120, no. 4, pp. 3415–3441, 2021, doi: 10.1007/s11277-021-09068-w.

[3] L.-K. Chen, Y. Shao, and Y. Di, "Underwater and water-air optical wireless communication," *Journal of Lightwave Technology*, vol. 40, no. 5, pp. 1440–1452, 2022, doi: 10.1109/jlt.2021.3125140.

[4] Y.-C. Chi, D.-H. Hsieh, C.-T. Tsai, H.-Y. Chen, H.-C. Kuo, and G.-R. Lin, "450-nm GaN laser diode enables high-speed visible light communication with 9-Gbps QAM-OFDM," *Optics express*, vol. 23, no. 10, pp. 13 051–13 059, 2015, doi: 10.1364/oe.23.013051.

[5] R. X. Ferreira, E. Xie, J. J. McKendry, S. Rajbhandari, H. Chun, G. Faulkner, S. Watson, A. E. Kelly, E. Gu, R. V. Penty et al., "High band- width GaN-based micro-LEDs for multi-Gb/s visible light communications," *IEEE Photonics Technology Letters*, vol. 28, no. 19, pp. 2023–2026, 2016, doi: 10.1109/lpt.2016.2581318.

[6] N. A. Azam, G. Murtaza, and U. Hayat, "A novel image encryption scheme based on elliptic curves and coupled map lattices," *Optik*, vol. 274, p. 170517, 2023, doi: 10.1016/j.ijleo.2023.170517.

[7] N.-R. Zhou, L.-J. Tong, and W.-P. Zou, "Multi-image encryption scheme with quaternion discrete fractional Tchebyshev moment transform and cross- coupling operation," *Signal Processing*, vol. 211, p. 109107, 2023, doi: 10.1016/j.sigpro.2023.109107.

[8] C. Wang and L. Song, "An image encryption scheme based on chaotic system and compressed sensing for multiple application scenarios," *Information Sciences*, vol. 642, p. 119166, 2023, doi: 10.1016/j.ins.2023.119166.

[9] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik*, vol. 272, p. 170316, 2023, doi: 10.1016/j.ijleo.2022.170316.
[10] N. A. E.-S. Mohamed, H. El-Sayed, and A. Youssif, "Mixed multi-chaos quantum image encryption scheme based on quantum cellular automata (QCA)," *Fractal and Fractional*, vol. 7, no. 10, p. 734, 2023, doi: 10.3390/fractalfract7100734.
[11] S. Agarwal, "Secure image transmission using fractal and 2D-chaotic map," *Journal of Imaging*, vol. 4, no. 1, p. 17, 2018, doi: 10.3390/jimaging4010017.
[12] K. Nakamura, I. Mizukoshi, and M. Hanawa, "Optical wireless transmission of 405 nm, 1.45 Gbit/s optical IM/DD-OFDM signals through a 4.8 m underwater channel," *Optics express*, vol. 23, no. 2, pp. 1558–1566, 2015, doi: 10.1364/oe.23.001558.
[13] S. A. A. El-Mottaleb, M. Singh, A. Atieh, and M. H. Aly, "OCDMA transmission-based underwater wireless optical communication system: performance analysis," *Optical and Quantum Electronics*, vol. 55, no. 5, p. 465, 2023, doi: 10.1007/s11082-023-04742-8.
[14] Y. Shao, R. Deng, J. He, K. Wu, and L.-K. Chen, "Real-time 2.2-Gb/s water- air OFDM-OWC system with low-complexity transmitter-side DSP," *Journal of Lightwave Technology*, vol. 38, no. 20, pp. 5668–5675, 2020, doi: 10.1109/jlt.2020.3001864.
[15] L. Gai, W. Li, Q. Zhu, X. Hei and G. Wang, "Underwater transmission of digital image in wireless optical communication based on single photon detection technology," *2022 International Conference on Computers, Information Processing and Advanced Education (CIPAE)*, Ottawa, ON, Canada, 2022, pp. 406-410, doi: 10.1109/CIPAE55637.2022.00091.
[16] O. Kocak, U. Erkan, A. Toktas, and S. Gao, "PSO-based image encryption scheme using modular integrated logistic exponential map," *Expert Systems with Applications*, vol. 237, p. 121452, 2024, doi: 10.1016/j.eswa.2023.121452.
[17] A. Hadj Brahim, A. Ali Pacha, and N. Hadj Said, "An image encryption scheme based on a modified AES algorithm by using a variable S-box," *Journal of Optics*, vol. 53, no. 2, pp. 1170–1185, 2023, doi: 10.1007/s12596-023-01232-8.
[18] J. Su, Y. Hong, S. Fang, and Y. Wen, "A color image encryption scheme based on 2D coupled chaotic system and diagonal scrambling algorithm," *Chinese Physics B*, vol. 33, no. 7, p. 070502, 2024, doi: 10.1088/1674-1056/ad3efa.
[19] B. Rahul, K. Kuppusamy, and A. Senthilrajan, "Dynamic DNA cryptography- based image encryption scheme using multiple chaotic maps and SHA-256 hash function," *Optik*, vol. 289, p. 171253, 2023, doi: 10.1016/j.ijleo.2023.171253.
[20] S. Sun, "A New Image Encryption Scheme Based on 6D Hyperchaotic System and Random Signal Insertion," *IEEE Access*, vol. 11, pp. 66009–66016, 2023, doi: 10.1109/access.2023.3290915.
[21] A. G. Mohammed and S. E. El-Khamy, "Innovative chaotic dragon fractal (ChDrFr) shapes for efficient encryption applications: a new highly secure image encryption algorithm," *Multimedia Tools and Applications*, vol. 83, no. 17, pp. 50449–50475, 2024, doi: 10.1007/s11042-023-17183-y.
[22] P. Parida, C. Pradhan, J. A. Alzubi, A. Javadpour, M. Gheisari, Y. Liu, and C.-C. Lee, "Elliptic curve cryptographic image encryption using Henon map and Hopfield chaotic neural network," *Multimedia Tools and Applications*, vol. 82, no. 22, pp. 33 637–33 662, 2023, doi: 10.1007/s11042-023-14607-7
[23] D. Singh and S. Kumar, "A multiphase encryption scheme using RSA, modified RMAC and Chen's hyperchaotic map," *Multimedia Tools and Applications*, pp. 1–30, 2023, doi: 10.1007/s11042-023-17727-2.
[24] S. M. Hameed, A. A. Sabri, and S. M. Abdulsatar, "Filtered OFDM for underwater wireless optical communication," *Optical and Quantum Electronics*, vol. 55, no. 1, p. 77, 2023, doi: 10.1007/s11082-022-04359-3.
[25] C. Kandouci, "Investigation of Jervol water types properties effects on underwater optical wireless OCDMA system performances for different modulation techniques," *Optical and Quantum Electronics*, vol. 54, no. 1, p. 3, 2022, doi: 10.1007/s11082-021-03390-0.
[26] C. Gabriel, M.-A. Khalighi, S. Bourennane, P. Léon, and V. Rigaud, "Monte-Carlo-based channel characterization for underwater optical communication systems," *Journal of Optical Communications and Networking*, vol. 5, no. 1, pp. 1–12, 2013, doi: 10.1364/jocn.5.000001.
[27] S. A. Abd El-Mottaleb, M. Singh, A. Atieh, and M. H. Aly, "Performance evaluation of a UOWC system based on the FRS/OCDMA code for different types of Jerlov waters," *Applied Optics*, vol. 63, no. 3, pp. 762–771, 2024, doi: 10.1364/ao.507674.
[28] H. Kaushal and G. Kaddoum, "Underwater optical wireless communication," IEEE access, vol. 4, pp. 1518–1547, 2016, doi: 10.1109/ACCESS.2016.2552538.
[29] S. A. Abd El-Mottaleb, A. G. Mohamed, A. Chehri, M. Singh, A. Atieh, H. Y. Ahmed, and M. Zeghid, "Performance of cipher image transmission in free space optics under foggy weather," *IEEE Access*, vol. 11, pp. 139478-139497, 2023, doi: 10.1109/ACCESS.2023.3338168.
[30] X. Huang, Y. Bai, and X. Fu, "Image transmission with binary coding for free space optical communications in the presence of atmospheric turbulence," *Applied optics*, vol. 59, no. 33, pp. 10 283–10 288, 2020, doi: 10.1364/ao.405152.
[31] S. A. Abd El-Mottaleb, A. G. Mohamed, H. Y. Ahmed, and M. Zeghid, "Performance enhancement of FSO communication system under rainy weather environment using a novel encryption technique," *IEEE Access*, vol. 12, pp. 13729-13746, 2024, doi: 10.1109/ACCESS.2024.3357396.
[32] M. Singh, M. L. Singh, G. Singh, H. Kaur, Priyanka, and S. Kaur, "Real-time image transmission through underwater wireless optical communication link for internet of underwater things," *International Journal of Communication Systems*, vol. 34, no. 16, p. e4951, 2021, doi: 10.1002/dac.4951.
[33] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," *Journal of Computer and Communications*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.
[34] H. Zhao, S. Wang, and Z. Fu, "A new image encryption algorithm based on cubic fractal matrix and L-LCCML system," *Chaos, Solitons & Fractals*, vol. 185, p. 115076, 2024, doi: 10.1016/j.chaos.2024.115076.
[35] Y. Wang, L. Teng, and X. Wang, "An image encryption algorithm based on circular rotation and generalized Feistel structure," *Soft Computing*, vol. 28, no. 5, pp. 4335–4358, 2024, doi: 10.1007/s00500-023-08747-z.
[36] M. Alawida, "A novel DNA tree-based chaotic image encryption algorithm," *Journal of Information Security and Applications*, vol. 83, p. 103791, 2024, doi: 10.1016/j.jisa.2024.103791.
[37] Q. Lai and H. Zhang, "A new image encryption method based on memristive hyperchaos," *Optics & Laser Technology*, vol. 166, p. 109626, 2023, doi: 10.1016/j.optlastec.2023.109626.
[38] N. Rani, V. Mishra, and S. R. Sharma, "Image encryption model based on novel magic square with differential encoding and chaotic map," *Nonlinear Dynamics*, vol. 111, no. 3, pp. 2869–2893, 2023, doi: 10.1007/s11071-022-07958-7.
[39] J. I. M. Bezerra, G. Machado, A. Molter, R. I. Soares, and V. Camargo, "A novel simultaneous permutation–diffusion image encryption scheme based on a discrete space map," *Chaos, Solitons & Fractals*, vol. 168, p. 113160, 2023, doi: 10.1016/j.chaos.2023.113160.
[40] A. G. Mohamed, N. O. Korany, and S. E. El-Khamy, "New DNA coded fuzzy based (DNAFZ) S-boxes: Application to robust image encryption using hyper chaotic maps," *IEEE ACCESS*, vol. 9, pp. 14 284–14 305, 2021, doi: 10.1109/access.2021.3052161.

Amira G. Mohamed (S'13) received the B.S. degree in Electronics and Communication engineering from Alexandria Higher Institute of Engineering and Technology (AIET), Alexandria, Egypt, in 2013, the M.S. degree in Electrical engineering from Faculty of Engineering, Alexandria University, Alexandria, Egypt, in 2017, and the Ph.D. degree in Electrical engineering from Faculty of Engineering, Alexandria University, Alexandria, Egypt, in 2021. degree in Electrical engineering at the Faculty of

Engineering, Alexandria University, Alexandria, Egypt. She is currently a lecturer with the Electronics and Communication Department at Alexandria Higher Institute of Engineering and Technology (AIET), Alexandria, Egypt. Her research interests include image processing, steganography, cryptography, and information security.

Somia A. Abd El-Mottaleb received her B.Sc. degree in Electrical (Electronics and Communications) Engineering in 2010 from faculty of Engineering, Alexandria University, followed by M.Sc. degree in Electronics and Communications Engineering in 2014 from faculty of Engineering, Arab Academy for Science, Technology and Maritime Transport and Ph.D. degree in Electrical (Electronics and Communications) Engineering in 2020 with main focus on optical communication from faculty of Engineering, Alexandria University. She is currently a lecturer at Alexandria Higher Institute of Engineering and Technology, Alexandria, Egypt. She has published papers in Q1 and Q2 Scopus journals. Her research interests are free space optics, optical amplifiers, detection techniques, multiplexing techniques, optical fiber communications, underwater optical wireless communication system, image transmission, and internet of things.

Mehtab Singh received the Bachelor of Engineering degree in electronics and communication engineering from the Thapar Institute of Engineering and Technology, Patiala, India, and the Master of Technology degree in electronics and communication engineering with specialization in communication systems and the Doctor of Philosophy degree in electronics technology from Guru Nanak Dev University, Amritsar, India. He has published over 80 research papers in SCI/SCIE and SCOPUS-indexed journals and conferences. His research interests include optical communication systems (wired and wireless), photonic radars, and opto-electronic devices. He is featured in the World's Top 2% Scientist List released by Stanford University and Elsevier B. V., in October 2021 and 2022, respectively. He serves as an Academic Editor for International Journal of Optics (Hindawi) and Frontiers in Signal Processing.

Hassan Yousif Ahmed received the B.Eng. in Computer Engineering (Network systems) and M.Sc in Computer Science and Information from Gezira University, Sudan in 2002 and 2007 and Ph.D. degree in Electrical and Electronic Engineering, University Tecknolgi PETRONAS, Malaysia, 2010. Currently he is a full Professor in Electrical Engineering Department, College of Engineering, Prince Sattam Bin AbdulAziz University.. His research interests are on computer network, wireless communications networks, optical communications and cryptography systems.

Medien Zeghid received the Ph.D. degree in Information and Communication, Sciences and Technologies from University of South Brittany, Lorient-France, in 2011. He was an Assistant Professor with Department of Electronic Engineering, Higher Institute of Applied Sciences and Technology, Sousse University, Tunisia from 2012-2014. Currently, he is an Assistant Professor with Department of Computer Engineering and Networks, Prince Sattam Bin Abdulaziz University. His research interests include information security, Architectural Synthesis for the Crypto-systems, Image & Video Coding, and Optical communication.

WAZIE M. ABDULKAWI did his B.Sc. degree in electronics engineering from Ibb University, Ibb, Yemen, in 2007. His M.S. and Ph.D. in Electrical Engineering are from King Saud University Riyadh KSA, completed in 2013 and 2020, respectively. He worked as a researcher in the electrical engineering department at King Saud University, Riyadh, Saudi Arabia from 2008 to 2022. He is currently an assistant professor with the electrical engineering department, college of engineering in Wadi Addawasir, Prince Sattam bin Abdulaziz University, Saudi Arabia. He has published more than 30 international publications and holds a patent for chipless RFID tags. His research interests include reconfigurable antennas, chipless RFID tags, biomedical engineering systems, and RFID sensors.

Belgacem Bouallegue earned his B.Sc. and M.Sc. degrees from the University of Monastir in Tunisia, and his Ph.D. from the Graduate School of Engineering Science and Technology, University of Southern Brittany in Lorient, France, with the University of Monastir in Tunisia's cooperation. He is currently an Assistant Professor at the College of Computer Science at King Khalid University in Saudi Arabia, where he works in the Department of Computer Engineering. Integrated System Design, Fault Tolerance, HW/SW Co-design, Parallel Computers, Embedded Systems and IoT, Network on Chip NoC, AI, IPs and MPSoCs, Machine Learning, Deep Learning, Homogeneous/Heterogeneous Systems, Wireless Sensor Networks Security, and Cryptography are just a few of his research interests. He is collaborating with Lorient, France's Lab-STICC Laboratory and LIP6, Computer Science.

Osman Ahmed Abdalla is an Assistant Professor at the University College of Tayma, University of Tabuk, Tabuk, Kingdom of Saudi Arabia. He earned a PhD in Information Technology with a focus on Artificial Intelligence. The research of Dr. Abdalla focuses on machine learning, data mining, the analytical hierarchy process, and classification models