RESEARCH ARTICLE

Performance Enhancement of FSO Communication System Under Rainy Weather Environment Using a Novel Encryption Technique

SOMIA A. ABD EL-MOTTALEB[1], **AMIRA G. MOHAMED**[2], **(Student Member, IEEE),**
HASSAN YOUSIF AHMED[3], **AND MEDIEN ZEGHID**[3,4]

[1]Department of Mechatronics Engineering, Alexandria Higher Institute of Engineering and Technology, Alexandria 21311, Egypt
[2]Department of Electronics and Communications, Alexandria Higher Institute of Engineering and Technology, Alexandria 21311, Egypt
[3]Department of Electrical Engineering, College of Engineering in Wadi Alddawasir, Prince Sattam bin Abdulaziz University, Wadi Alddawasir 11991, Saudi Arabia
[4]Electronics and Micro-Electronics Laboratory (E. μ. E. L), Faculty of Sciences, University of Monastir, Monastir 5000, Tunisia

Corresponding author: Hassan Yousif Ahmed (h.ahmed@psau.edu.sa)

ABSTRACT Free Space Optics (FSO) has emerged as a viable solution to meet the growing demand for high bandwidth, secure data transmission, and high speed. However, the FSO system is highly susceptible to environmental factors, with precipitation in particular having a significant impact on FSO links. Optical loss, phase fluctuation, and multipath fading of the received optical power are all caused by these external factors. From this perspective, to improve the system's performance in such conditions, a novel image encryption technique based on the Choquet Fuzzy Integral (CFI) in conjunction with the integer wavelet transform is proposed. The security of the proposed method is demonstrated via analysis security on the one, and its efficacy in terms of transmission performance of an encrypted image over an FSO channel exposed to rainy weather conditions is analyzed on the other. Authentic meteorological data from two distinct cities are considered to demonstrate the model's real-world applicability: Alexandria, Egypt, in Africa, and Jeddah, Kingdom of Saudi Arabia (KSA), in Asia. To evaluate the system's performance, a variety of metrics such as FSO range, Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio (PSNR), and the Structural Similarity Index Method (SSIM) are used. Furthermore, the findings from studying the impact of weather conditions reveal that, as the intensity of rainfall increases, the encrypted image experiences a reduction in its propagation range within the FSO channel. For example, under heavy rain (HR) conditions, the maximum FSO range for high-quality received encrypted images is 1055 m, which extends to 2290 m as rain intensity decreases (for light rain). In terms of the two cities, Jeddah, with its lower average rainfall intensity compared to Alexandria, allows the encrypted image to travel an additional 2400 m.

INDEX TERMS FSO, rainy weather environment, image encryption, security analysis, CFI, PSNR, SSIM.

I. INTRODUCTION

The global development of wireless communication technologies has grown in importance to meet the growing demand for high-speed communication and broadband internet services [1]. Consequently, there is a burgeoning need for expanded bandwidth, leading to congestion within the radio frequency (RF) spectrum. This congestion arises as an ever-growing number of devices and services compete for access to the limited RF spectrum available, underscoring the urgent necessity for effective spectrum management and allocation [2]. Considering these challenges, the imperative to develop new communication systems capable of accommodating these requirements becomes increasingly vital.

Optical Wireless Communication (OWC) system has emerged as a promising alternative to traditional RF systems. It serves as a supplementary communication link that complements existing wireless technologies. OWC offers

The associate editor coordinating the review of this manuscript and approving it for publication was Tariq Umer.

several operational advantages, most notably the ability to overcome bandwidth limitations associated with RF systems. This advantage makes OWC a dependable and adaptable solution, particularly for applications involving Internet of Things (IoT) devices and various other communication needs [3], [4], [5].

In the realm of long distance outdoor wireless optical communications, the utilization of light as a medium for data transmission between two locations via lasers has been seen. This technology is commonly referred to as free space optics (FSO) [6]. FSO systems share similarities with OFC systems. In both cases, signals carrying information can be transmitted at high data rates. The primary distinction lies in the transmission channel: OFC systems use fiber cables as the medium, while FSO systems utilize the atmosphere as the propagation medium. Furthermore, FSO systems offer a practical solution to last-mile connectivity challenges, especially in scenarios where deploying fiber cables proves difficult and costly due to geographical constraints [7], [8]. It offers several advantages, including high-speed data transmission in communication links, immunity to electromagnetic interference (EMI) for reliable and uninterrupted data transfer, the use of a spectrum that doesn't necessitate costly licenses, and secure data transfer, protecting sensitive information from unauthorized access [2], [7]. However, despite its benefits, FSO transmission is vulnerable to atmospheric attenuation, leading to signal degradation, a higher Bit Error Rate (BER), and loss of information. Various atmospheric conditions, including haze, dust storms, fog, and rain, all contribute to the weakening of the transmitted signal [9], [10], [11], [12]. Different techniques have therefore been proposed to improve FSO performance in adverse weather conditions such as: Adaptive Modulation, Wavelength Diversity, Error Correction Coding, etc. . .

Furthermore, the extensive use of wireless communication technologies has spurred the rapid expansion of image transmission as a prominent application. Additionally, higher network bandwidths and advanced technologies have contributed to the currently exploding trends of information sharing, whether on public or private networks. Shared items include text, image, and multimedia files. This enormous amount of information sharing is coupled with a large number of security breaches, which cause many problems at different levels, including the societal level. As such, it is important to ensure that the transmitted information can be stored and shared at high security, especially in applications including confidential video conferencing, medical images, military images, and diplomatic information storage, along with satellite information systems. To ensure the security and privacy of this data, encryption has been applied [13], [14]. The security of different encryption systems has been ensured by the algorithm they use, as they treat plaintext as a type of binary stream. These systems include the data encryption standard (DES) and the advanced encryption standard (AES). However, one of the disadvantages of these systems

is that they result in huge amounts of image data stored as two-dimensional arrays. To encrypt an image using data encryption methods, the first step consists of rearranging the data of the image, followed by rearranging the ciphertext into the image storage format. This leads to slower operation speed, which is unable to reach real time requirements [15], [16]. As such, it is noted that this is where the use of the fuzzy integral will make a difference. With its benefits, the Choquet fuzzy integral (CFI) has many advantages, which have a positive influence on effective image encryption. These benefits include its ease of implementation, simplicity of computing, effectiveness in reaching higher levels of security, as well as high speed and sensitivity [17], [18].

A. CONTRIBUTION

In light to the aforementioned challenges, we propose in this paper an efficient encryption technique for improving the operational efficiency of an FSO communication system under various precipitation conditions, including light rain (LR), moderate rain (MR), and heavy rain (HR). To accomplish the proposed work, we have proposed several layers of coherent and interdependent efforts, specifically:

- Introducing a CFI-based cryptographic method for image data encryption and decryption for reliable performance.
- Security analysis including the visual, statistical, and differential attacks to ensure that the proposed technique is efficient, robust, and can resist such attacks.
- Discussing the image transmission in FSO channel under rainy weather.
- Actual meteorological data for average rainfall intensities over a four-year period in Alexandria, Egypt and Jeddah, Saudi Arabia were used to assess FSO performance under these conditions as a proof of concept in two cases: with and without encryption.
- Evaluating the Peak -signal to noise ratio (PSNR), signal to noise ratio (SNR), and structure similarity index method (SSIM) as to show the quality of the received image after propagating in FSO channel.

This article is structured as follows. Section II shows related works about different encryption algorithms and studies of using image transmission over FSO channel under different climate changes. Section III describes the encrypted image transmission system using CFI algorithm over FSO channel. Results and discussion are given in Sec. IV, followed by conclusion in Sec. V.

II. RELATED WORKS

There are previous research studies that carried out on transmitting image in FSO systems. In [19], authors evaluated the performance of color image transmission in FSO channel. Double generalized Gamma turbulence effect was considered in that study. Another image transmission system was proposed over an FSO communication link for optical

applications in [20]. The suggested model was simulated under the effect of turbulence effects and at a FSO range of 1 km. The simulation model comprised the process of encoding and decoding image pixels. Gill and Singh et al. [21], evaluated the performance in terms of PSNR, SNR, and SSIM for a colored image transmission in FSO systems under the impact of MR and HR. In [22], a transmission for AVB-T image over an FSO channel under different turbulence was proposed for Single Input Single Output (SISO) and Multi Input Multi Output (MIMO) systems. The performance was carried out in terms of SSIM. The study in [23] evaluated the FSO system performance under foggy conditions when modulating images using Quadrature Phase Shift Keying (QPSK) and On-Off Keying (OOK) Non-Return-to-Zero (NRZ) modulators, reporting results for Q-factor, PSNR, and SSIM. The study in [24] was conducted to ascertain the Quality of Experience (QoE) for the transmission of images over a FSO link affected by turbulent conditions.

Moreover, there are several encrypted algorithms that proposed by researchers.

DNA computing and a finite state machine (FSM) were the basis for the new algorithm presented in [25]. This algorithm has the following advantages: statistical randomness and increased flexibility in its designed key schedule. The purpose of this algorithm was to reach confusion and diffusion simultaneously. Diffusion could be achieved with the help of the bases of DNA, which were in turn employed to extract random integers that accomplished confusion. In [26], a hyper-chaotic system and bit-level permutation were used to develop a novel encryption algorithm. In this new technique, the first step involves the diffusion of the image with the help of a two-dimensional (2D) XOR operation, in a method involving forward diffusion. The second step is the rearrangement and scrambling of images in different directions. In the last step, the ciphertext image is produced through a 2D XOR backward diffusion. An encryption algorithm was proposed in [27] for color images, by using a hyper-chaotic system, developed with the help of a tri-valued memristor. To achieve encryption, the permutation-diffusion process was used. Hyper-chaotic synchronization technology was used for the transmission of important image information. In this technique, the initial key was generated using the hash value of the plaintext image. Operations pertaining to permutation at the pixel and bit levels were accomplished through the permutation sequence, having the Hash-table structure based on the hyper-chaotic sequence. To finalize diffusion, an application of Hilbert curves, along with ciphertext feedback mechanism is performed. Another study proposed the improved sinusoidal dynamic non-adjacent coupled mapping lattice (ISDNCML), which is an infinite parameter-range, spatiotemporal chaotic system [28]. It was the characteristics of this ISDNCML that contributed to the globally coupled private image encryption scheme. For the purpose of encryption, this algorithm works by first identifying private areas within an image and then couples both private and non-

private areas. In this coupled encryption, the private areas witnessed ill-conditioned dynamic diffusion. This process helps to ensure the security of private information, by avoiding the re-encryption of private areas. In order to improve the security and efficiency of the encryption process, a study proposed an integration of chaotic image encryption and convolutional neural networks (CNN) [29]. The properties of chaotic sequences and CNN modeling, i.e., randomness and nonlinear mapping along with extraction capabilities, respectively, were used to strengthen image encryption. Another study explored the use of DNA coding and RNA computing, to develop a chaotic image encryption scheme [30]. This research started by developing a 4D hyperchaotic system with more complex dynamics. To dynamically encrypt the plaintext image with DNA, the hyperchaotic system was induced to generate a plaintext-related keystream. This was followed by conversion using RNA coding and the generation of amino-acid substitution boxes (S-box). To reach the final ciphertext image, a replacement operation was conducted using pseudo-random sequences, which were generated by an improved replacement-sequence generator.

III. PROPOSED IMAGE ENCRYPTION TECHNIQUE

In this section, the encryption CFI algorithm and the description for image transmission system over FSO channel are given.

A. CFI ALGORITHM

CFI is chosen in this research, as a basis for the developed algorithm, as it is highly sensitive, complex, and nonlinear. These characteristics yield a highly secure algorithm. The resulting scheme provides higher security than other available image cryptosystems. Firstly, the encryption processes involves the use of CFI to generate pseudo-random sequences [17], [18]. The input image is then subjected to integer wavelet transform (IWT) to obtain one approximate and three detail sub-bands from the previously stated image. Then, the normalization of the three detail sub-bands takes place, so that they are maintained within the range of 0 to 255, i.e., the sequences generated by CFI. As such, a modification of the intensity of pixels takes place. Then, a control map is applied, so that CFI can produce three sequences used to diffuse the three detail sub-bands. For a more complex approximation, these sub-bands' pixels are shuffled using a logistic chaotic map. The shuffled sub-image is diffused using another sequence produced through CFI. When the approximation and the three details sub-bands are rearranged, the final encrypted image can be obtained.

The block diagram of the process described above is shown in Fig. 1. There are two stages applied in the proposed algorithm.

In first stage, the generation of Pseudo random sequences based on CFI is done in. CFI produced four random sequences of high security. h_1, h_2, h_3, h_4, constituting the initial input of CFI, are calculated using an external key and a secret image. By applying a key to a series of images, the secret image is
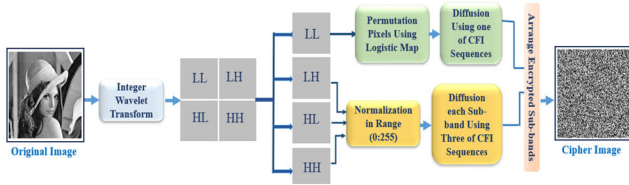
FIGURE 1. Schematic layout for the image encryption algorithm.

chosen. As such, this image can be changed. By applying these parameters and implementing these steps, the process' security is increased. Algorithm 1 depicts the random sequences of CFI, as well as a brief illustration of how they are generated. They are generated in five steps.

Algorithm 1 Generation of Pseudo Random Sequences

Input: External Key with size 128-bit (K), Secret Image $I(M \times N)$
Output: Random Sequences C_j
1: Divide K into four blocks $(k_1, k_2, \ldots \ldots .. k_{16})$
2: Calculate key parameters (A, B, C, D)
3: # Eq. (1, 2, 3, 4, 5)
4: Divide secret image into 2×2 blocks
5: XOR Operation for each of the gray levels within each block
6: Calculate initial inputs (h_1, h_2, h_3, h_4)
7: # Eq. (6, 7, 8, 9)
8: Calculate Membership Grades (g_1, g_2, g_3, g_4)
9: # Eq. (10)
10: Calculate λ_s based on Eq. (11)
11: Calculate fuzzy measures $F(A_i)$
12: # Eq. (12)
13: Use Eq. (13) to calculate CFI
14: Generate random sequences C_i based on Eq. (14)

In the **first step**, blocks of eight bits $(k_1, k_2, \ldots \ldots \ldots .. k_{16})$ make up the 128-bit secret key. The following equations are employed to calculate the key parameters.

$$A = (K_1 \oplus K_2 \oplus K_3 \oplus K_4) \tag{1}$$

$$B = (K_5 \oplus K_6 \oplus K_7 \oplus K_8) \tag{2}$$

$$C = (K_9 \oplus K_{10} \oplus K_{11} \oplus K_{12}) \tag{3}$$

$$D = (K_{13} \oplus K_{14} \oplus K_{15} \oplus K_{16}) \tag{4}$$

$$K = \sum_{i=1}^{i=16} (K_i) \tag{5}$$

While in the **second step**, image is inserted, a process performed using the 256×256 gray-level matrix of the image. The image is divided into 2×2 blocks to obtain four values for $I(s)$. Each block's grey-level is subjected to XOR. Thus, the initial inputs, marked by h_1, h_2, h_3, h_4, are obtained by applying the equations to follow.

$$h_1 = ((A + K) \, mod \, 256) \oplus I(1) \tag{6}$$

$$h_2 = ((B + K) \, mod \, 256) \oplus I(2) \tag{7}$$

$$h_3 = ((C + K) \, mod \, 256) \oplus I(3) \tag{8}$$

$$h_4 = ((D + K) \, mod \, 256) \oplus I(4) \tag{9}$$

where, $I(1), I(2), I(3),$ *and* $I(4)$ represent the diffused values of each block, upon application of XOR. K represents the sum of blocks for the secret key.

The same image is then used in the **third step**, to calculate both the initial input (h) and the key. Then, (h) is inserted in Equation 10 to calculate the membership grade, while Equation 11 is used to calculate λ_{sg} and this last variable is inserted in Equation 12 for the calculation of the fuzzy measure.

$$g_i = \frac{1}{1 + h_i} \quad i = 1, 2, 3, 4 \tag{10}$$

Sugeno λ_{sg} Measure:

$$1 + \lambda_s = \prod_{i=1}^{n} (1 + \lambda_{sg} g_i) \tag{11}$$

Fuzzy Measure:

$$F(A_1) = g_1$$
$$F(A_i) = g_i + F(A_{i-1}) + \lambda_{sg} g_i . F(A_{i-1}), \ 1 \le i < n \tag{12}$$

where, g_i and $F(A_i)$ are the membership grade and the fuzzy measure over the corresponding membership grades, respectively.

Further, in **step 4**, to calculate CFI, Eq. (13) is used with an insertion of the initial inputs (h_1, h_2, h_3, h_4) and the fuzzy measure $F(A_i)$. As for the Pseudo random sequence, it is reached, when CFI is inserted in Eq. (14).

$$CFI = \int h dg = \sum_{i=1}^{n} [h(x_i) - h(x_{i-1}) F(A_i) \tag{13}$$

$$C_j = \left(ARS \left(int \, (CFI mod \, 1) \times 10^{14}, S \right) \right) \, mod \, 256$$
$$j = 1, 2, 3, 4 \tag{14}$$

where, ARS and CFI mod 1 are the arithmetic right shift of the binary sequence and the normalized fraction value, both seen in Eq. (14), respectively. The values for C_1, C_2, C_3, C_4 can be obtained when S takes values between 0 and 7. Finally, in the **last step**, four 64×64 FZ matrices can be obtained with the resize of C_1, C_2, C_3, C_4, resulting from CFI. Each matrix has 8 bits in the range of 0 to 255, which constitute its 256 integers.

Next stage includes the image encryption based on CFI. This is performed in three steps. **Firstly**, the original image (128×128 in size) is inserted. IWT is performed on the original image to reach one approximation (LL) and three detail sub-bands (HL, LH, and HH). To perform encryption, the intensity of pixels of HL, LH, and HH is maintained in the 0-255 range, through normalization and that is performed in **second step**. These normalized sub-bands are then XORed using three random CFI sequences, selected through a control code. In that case, (C_1) is used to encrypt LH, while (C_2), and (C_3) encrypt (HH) and (HL), respectively.
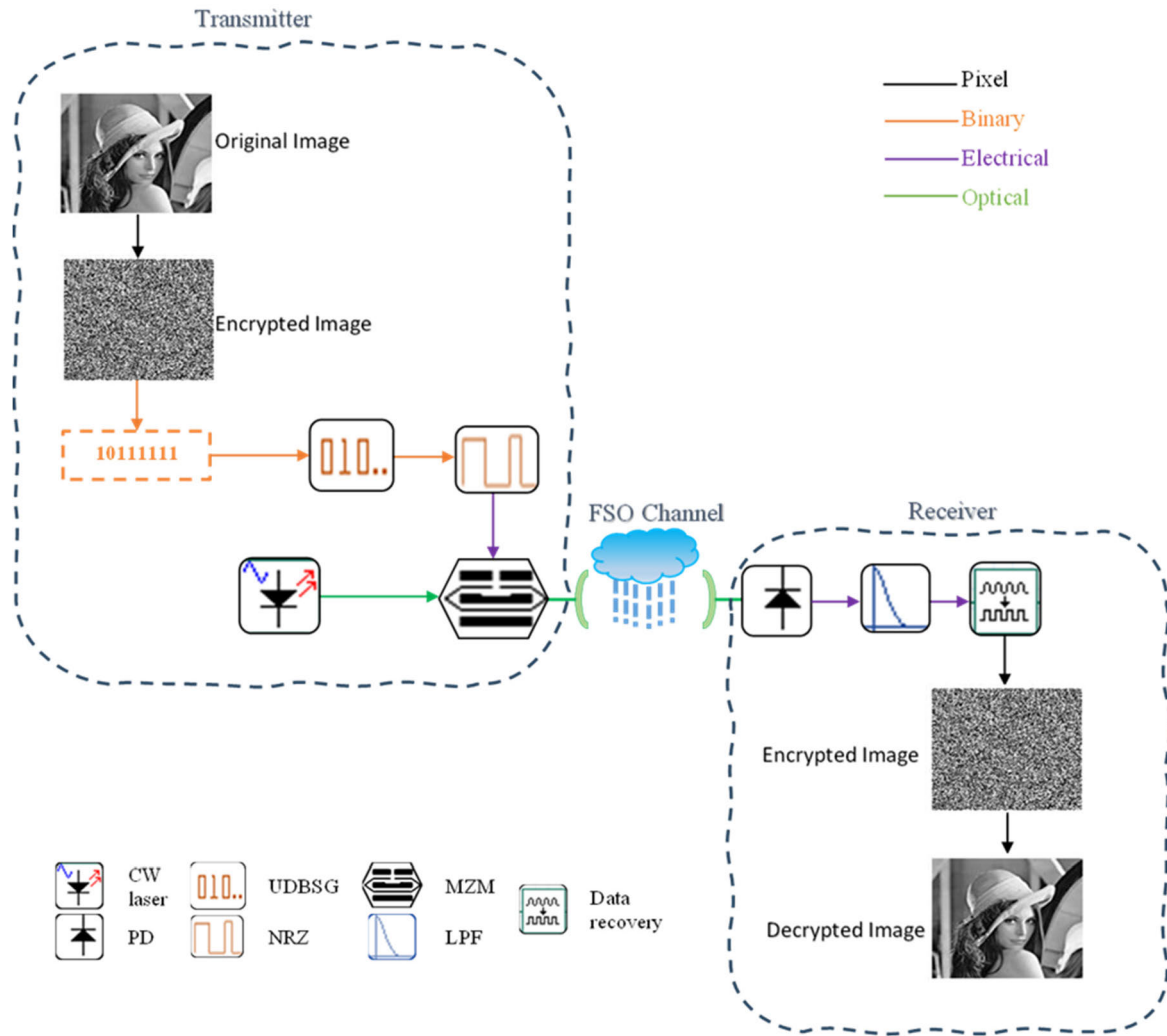
FIGURE 2. Layout diagram for proposed image transmission over FSO rainy channel.

Lastly, to shuffle the pixels of the approximation sub-band (LL), a logistic map (a chaotic system) is used. In this system, (r) is the control parameter, while (X_o) marks the initial conditions, and (X) is the output. The following Equation shows the inputs of this system:

$$X_{n+1} = rX_n (1 - X_n), \tag{15}$$

where, r is the chaotic parameter, while n is the number of iterations, $r \in [0, 4]$, and $x \in [0, 1]$. To reach the chaotic attitude, r needs to $\in [3.57, 4]$. Following this step, this approximation sub-band is XORed with C_4, a CFI generated sequence. Afterwards, the approximation and detail sub-bands are arranged to obtain the encrypted image.

B. MODEL DESIGN

The layout for the proposed image transmission system over FSO channel is shown in Fig. 2. It consists of three parts including transmitter side, FSO channel, and receiver side.

1) TRANSMITTER

An encrypted gray image of size 128×128 is converted to bits and then loaded to User Defined Bit Sequence Generator (UDBSG) at data rate of 20 Gbps. Then transformed to a NRZ modulator and the output signal from it is expressed as [31]

$$S_{NRZ}(t) = \sum_{i=-\infty}^{+\infty} h_i p(t - iT_b) \tag{16}$$

where $S_{NRZ}(t)$ is the output signal from NRZ modulator, h_i represents the amplitude of the ith symbol, and $p(t)$ and T_b are rectangular pulse shape and bit duration has value equal to 1/bit rate, respectively.

As for optical signal, a single continuous wave (CW) laser source is utilized and operating at wavelength of 1550 nm. Additionally, to modulate the $S_{NRZ}(t)$ electrical signal on to the optical signal resulted from a CW source, a Mach-Zehnder modulator (MZM) is utilized. The resultant signal is then travelled in the FSO channel.

2) FSO CHANNEL

In this study, the impact of attenuations caused by various levels of rain on the optical signal that carries the image is studied. Additionally, the attenuation caused by Alexandria, Egypt is considered on evaluating the image transmission performance. The average rainfall intensities for Alexandria and Jeddah cities (obtained for years from 2014 to 2018 from www.worldweatheronline.com, accessed on 20-1-2023) is 1.14 mm/hr and 0.28 mm/hr, respectively.

The atmospheric attenuation caused by rain, $\propto$, is expressed in terms of rainfall intensity, R_r, as [32] and [33]

$$\propto = 1.07 \, (R_r)^{0.67} \tag{17}$$

Figure 2 shows the attenuations of LR, MR, HR [32], [33], and Alexandria which are obtained from substituting the value of R_r for Alexandria city in Eq. (17).

After propagating in the atmosphere, the signal is then received with received optical power, P_{rx}^O, in dBm that is expressed as [12] and [34]

$$P_{rx}^O = P_{tx}^O \left(\frac{D_{rx}}{D_{tx} + \emptyset L_F} \right)^2 10^{\frac{-\alpha L_F}{10}} \tag{18}$$

where P_{tx}^O and D_{rx} denote the transmitted power in dBm and the diameter of the receiver aperture in cm, respectively, D_{tx} (cm) and $\emptyset$ (mrad) are the receiver aperture diameter and beam divergence angle, and finally, L_F is the FSO transmission link.

3) RECEIVER

The received optical signal undergoes conversion to an electrical signal by passing through a positive-over-intrinsic (PIN) photodetector (PD). The electrical output signal from PD is expressed as [35]

$$I_P = \Re P_{rx}^O + n(t) \tag{19}$$

where I_P, $\Re$, and $n(t)$, are PD output current, PD responsivity, and total received noise, respectively.

The variance of the $n(t)$ is expressed as [36]

$$\sigma_{var}^2 = o.5 N_o \tag{20}$$

where σ_{var}^2 denotes the noise variance and N_o is the power spectral density and is expressed as [36]

$$N_o = \sigma_s^2 + \sigma_{RIN}^2 + \sigma_T^2 \tag{21}$$

where σ_s^2 is the shot noise, σ_{RIN}^2 represents the relative intensity noise (RIN) and σ_{th}^2 is the thermal noise. As for σ_s^2, it is expressed as [11] and [36]

$$\sigma_{sh}^2 = 2q_e(I_{PD} + I_d)B_e \tag{22}$$

The σ_{RIN}^2 is expressed as [36]

$$\sigma_{RIN}^2 = N_{RIN} \, (I_{PD})^2 \tag{23}$$

The σ_{th}^2 is expressed as [19]

$$\sigma_{th}^2 = \frac{4k_B T_a B_e}{R_l} \tag{24}$$

The SNR is then expressed as [19]

$$SNR = \frac{(I_{PD})^2}{\sigma_{sh}^2 + \sigma_{RIN}^2 + \sigma_{th}^2} \tag{25}$$

Table 1 shows the symbols notifications with values that used in Matlab and Optisystem [12], [34], [37].

TABLE 1. Symbols notifications and values used in simulation.

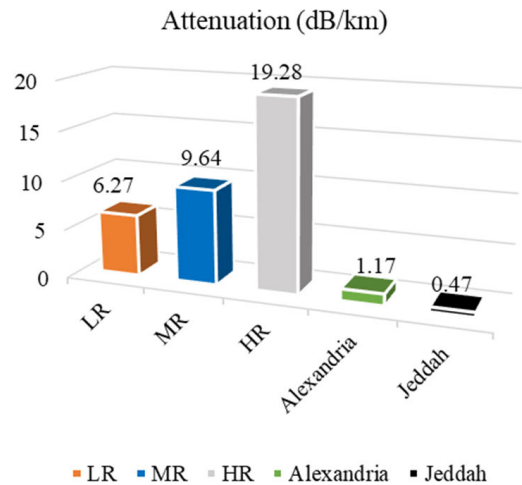| Symbol	Name	Value
q_e	Electron charge	$1.60217663 \times 10^{-19}$ C
I_d	Dark current	10 nA
B_e	Electrical bandwidth	$0.7 \times R_b$ Hz
N_{RIN}	Relatively intensity noise	-130 dB/Hz
T_{rl}	Temperature	300 K
k_B	Boltzmann constant	1.380649×10^{-23} J/K
R_l	Receiver load resistance	50 Ω

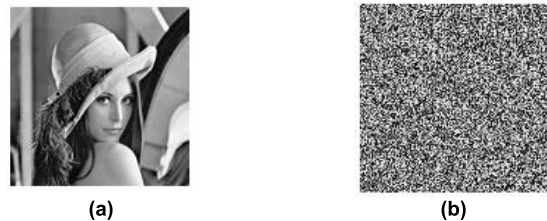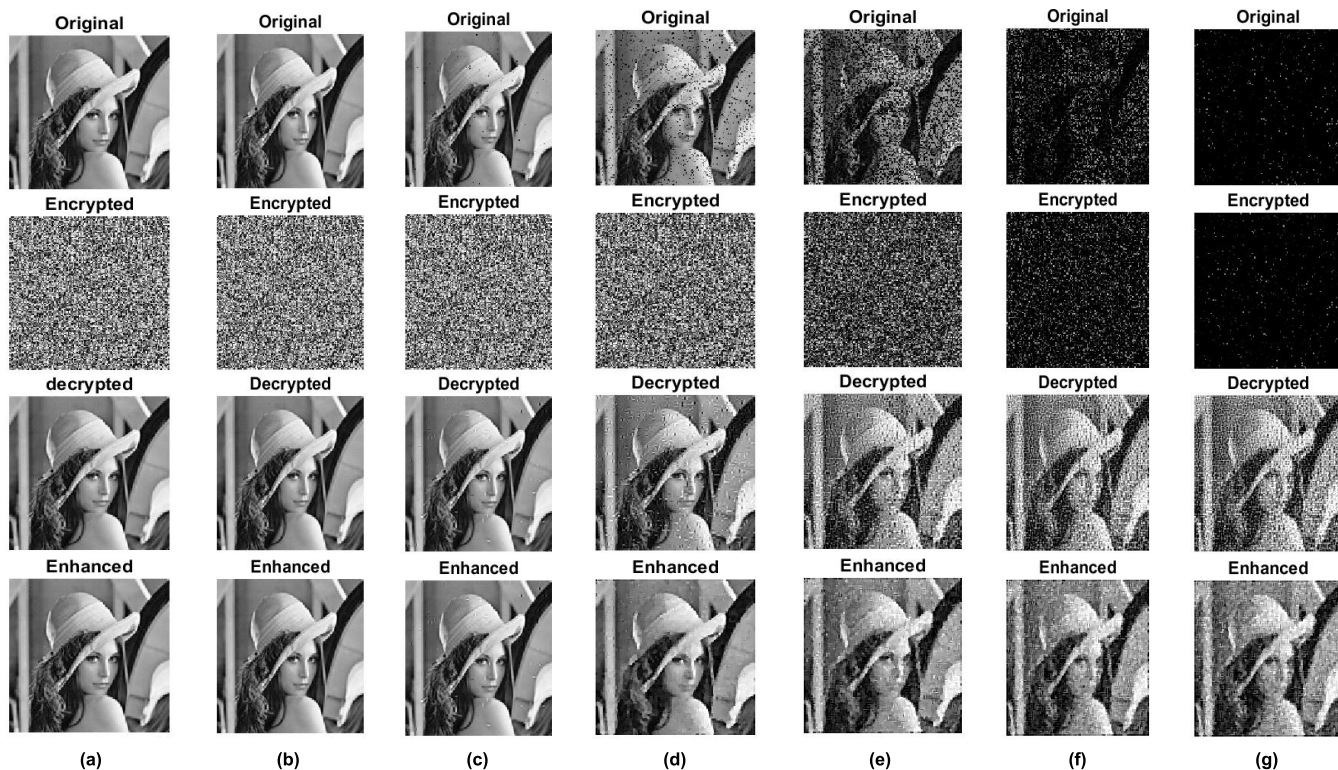**FIGURE 3.** Attenuation for different rain conditions.

FIGURE 4. Transmitted images (a) Lena image and (b) Cipher Lena image with CFI algorithm.
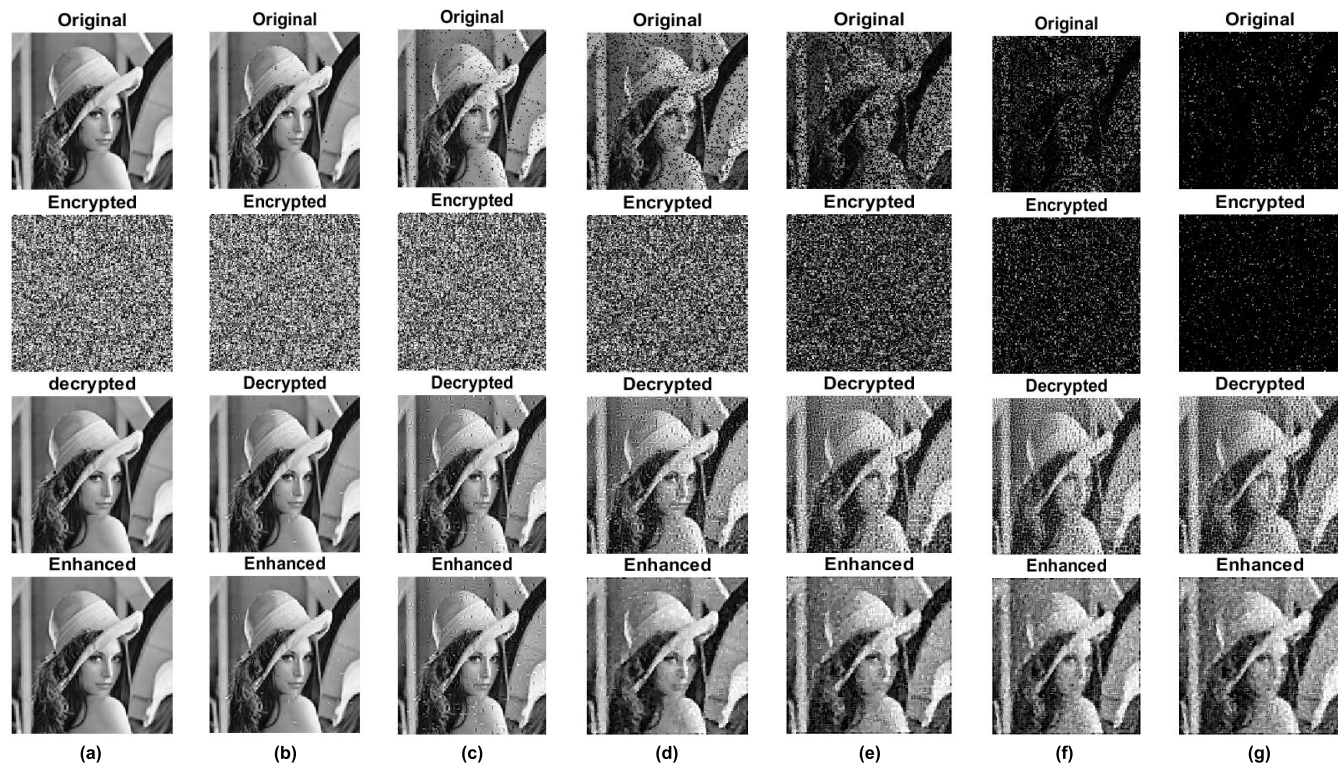
IV. RESULTS AND DISCUSSION

The proposed image transmission model is simulated via both Optisystem and Matlab software using the parameter values given in Tables 1 and 2 [12], [38], and [39].

FIGURE 5. View of received images under LR weather condition at (a)2230 m, (b) 2240 m, (c) 2250 m, (d) 2260 m, (e) 2270 m, (f) 2280 m, and (g) 2290 m.

FIGURE 6. View of received images under MR weather condition at (a)1690 m, (b) 1695 m, (c) 1700 m, (d) 1705 m, (e) 1710 m, (f) 1715 m, and (g) 1720 m.

The findings are presented in two subsections. The first subsection demonstrates the impact of various rainy weather conditions on the system's performance, while the second subsection focuses on the security analysis.
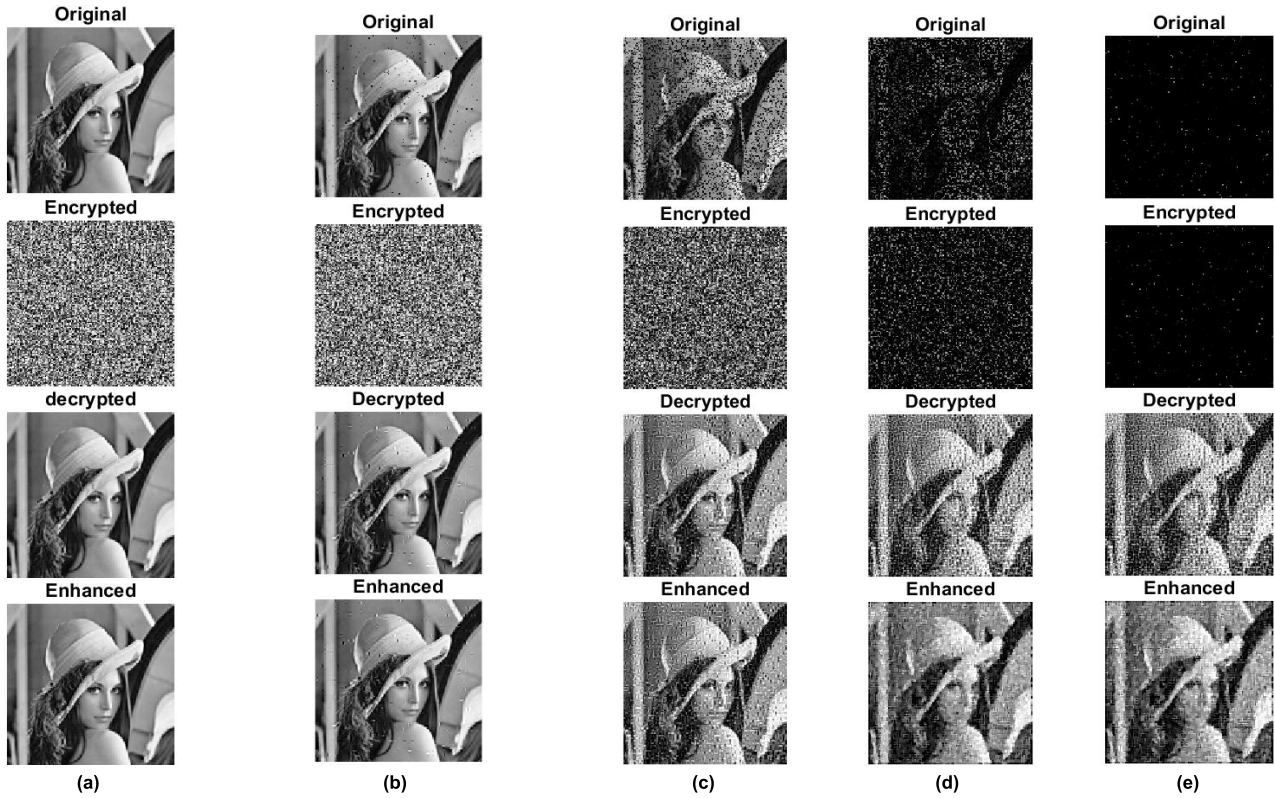
FIGURE 7. View of received images under HR weather condition at (a) 1035 m, (b) 1040 m, (c) 1045 m, (d) 1050 m, and (e) 1055 m.

TABLE 2. Model parameters values.

Parameter	Value (unit)
Image dimension	128×128
Sequence length	2^{17} bits
R_b	20 Gbps
h_i	1 V
Wavelength	1550 nm
P_{tx}^O	15 dBm
D_{tx} and D_{rx}	5 cm and 20 cm, respectively
$\emptyset$	2 mrad

A. EFFECT OF DIFFERENT FSO SPANS UNDER EFFECT OF RAINY WEATHER ON IMAGE TRANSMISSION

Rainy weather-induced attenuation significantly affects system performance, and propagation range plays a crucial role as well. Therefore, this subsection discusses the impact of different levels of rainfall, ranging from light to heavy, as well as the specific atmospheric conditions in Alexandria City, on the transmission of both original and ciphered images.

Figure 4 displays both the original image of Lena and its corresponding encrypted image using the CFI algorithm.

1) EFFECT OF VARIOUS RANGES ON IMAGE TRANSMISSION UNDER RAINY WEATHER

Figure 5 demonstrates the impact of various FSO spans on the transmission of both original and ciphered images in the presence of LR. It is evident that shorter ranges provide a clear view of images for both the original and encrypted versions, while visual distortion becomes apparent at longer ranges. Notably, ciphered images can propagate over longer distances while maintaining good quality. Figure 5(g) particularly highlights that the original image is entirely damaged (appearing black) when transmitted through the FSO channel at 2290 m, whereas the view of the decrypted image at this range remains quite satisfactory. Furthermore, the application of filters (median and HPF) results in improved visual quality of decrypted images, this effect becomes more noticeable at longer transmission ranges.

Figure 6 illustrates the influence of different FSO distances on image transmission in the presence of MR. Since, MR exhibits attenuation slightly higher than LR, so the signal that carries image travel a distance shorter than that achieved under LR. Additionally, the quality of decrypted images significantly surpasses that of the received plain images across all distances ranging from 1690 m to 1720 m. This notable improvement in image quality can be attributed to the robust security measures provided by the CFI encryption algorithm, which guarantee data protection as it traverses through the atmosphere. Furthermore, since the combined use of median

and high-pass filters can effectively improve image clarity, reduce noise, and enhance visual characteristics, resulting in an overall enhancement in image quality, these filters are applied after the image decryption process. As depicted in Fig. 6(g), it is noticeable that the original image appears black, with a slight improvement observed in the decrypted image and further enhancement achieved in the enhanced image.

Figure 7 displays the received images under HR. Notably, the quality of the received images deteriorates as the FSO ranges increase. Furthermore, when comparing Fig. 7 with Figs. 5 and 6, it becomes evident that in the case of the original image, the maximum FSO range that the system can achieve while maintaining a good image view is 2260 m under LR conditions. This range decreases to 1705 m under MR conditions and further diminishes to the shortest FSO span of 1045 m when the level rainfall intensity become highest. Similarly, the decrypted images exhibit better image clarity than the original image. Moreover, image can visualize with good quality at 1055 m propagation range when enhancement is done after decryption process.

Figure 8 presents the SNR for received images under varying rain conditions and at different FSO ranges. It is notable that SNR remains relatively high at shorter ranges for all images (original, decrypted, and enhanced), while enhanced images exhibit good SNR at longer FSO ranges. Additionally, an increase in FSO span results in a decrease in SNR. Due to the minimal signal attenuation in LR conditions, the longest achievable FSO range is 2290 m, accompanied by SNR values of -19.41 dB for the received original image, 8.89 dB for decrypting the ciphered image, and 12.38 dB for the enhanced image. In contrast, the highest attenuation caused by HR lead to a shorter FSO range of 1055 meters, resulting in SNRs of -23.01 dB, 8.88 dB, and 12.34 dB for the original, decrypted, and enhanced images, respectively.

The PSNR is widely recognized as a prominent method for assessing the difference in quality between two images (transmitted and received). It can be expressed as [40]

$$\text{PSNR} = 10 log_{10}\left[\frac{(2^b-1)^2}{MSE}\right] \quad (26)$$

where b and MSE are total number of bits and mean square error, respectively. The MSE is expressed as [40]

$$MSE = \frac{1}{S}\sum_{x,y}[R(x,y)-T(x,y)]^2 \quad (27)$$

where S, $R(x,y)$, and $T(x,y)$ are size of image (128×128), received image, and original transmitted image, respectively. It is observed that a higher PSNR signifies an improved quality of the transmitted image.

The PSNR is discussed under LR, MR, and HR at various FSO links in Fig. 9. It is clear that PSNR decreases as L_F increases while received images with enhancement show higher PSNR in all rain conditions. The PSNRs for received original images are 5.50 dB, 5.69 dB, and 5.49 dB at 2290 m
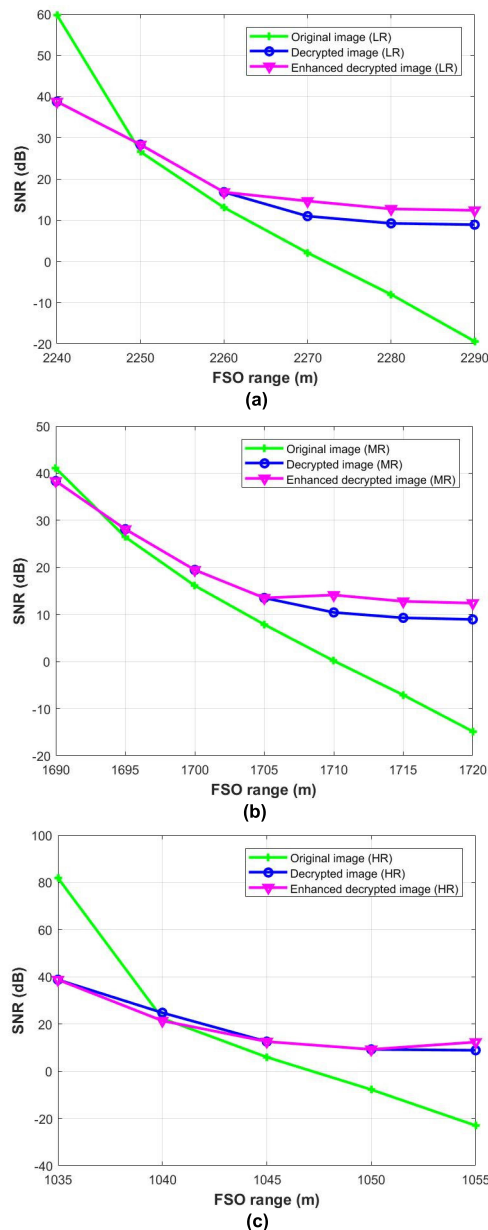

FIGURE 8. SNR versus various FSO propagation ranges under (a) LR, (b) MR, and (c) HR conditions.

(LR), 1720 m (MR), and 1055 m (HR), respectively. These values are improved to 13.9 dB for LR at 2290 m, 13.95 dB for MR at 1720 m, and 13.88 dB for HR at 1055 m when decrypting the received ciphered images. The PSNRs are further enhanced at the same ranges when median filter and HPF are utilized and reach 17.7 dB, 17.66 dB, and 17.62 dB for light, moderate, and heavy rain, respectively.

Additionally, SSIM is discussed as it shows the quality of received image with respect to original transmitted image. It is expressed as [42] and [43]

$$\text{SSIM}(T,R) = \frac{(2\mu_T\mu_R+C_1)(2\sigma_{TR}+C_2)}{(\mu_T^2+\mu_R^2+C_1)(\sigma_T^2+\sigma_R^2+C_2)} \quad (28)$$
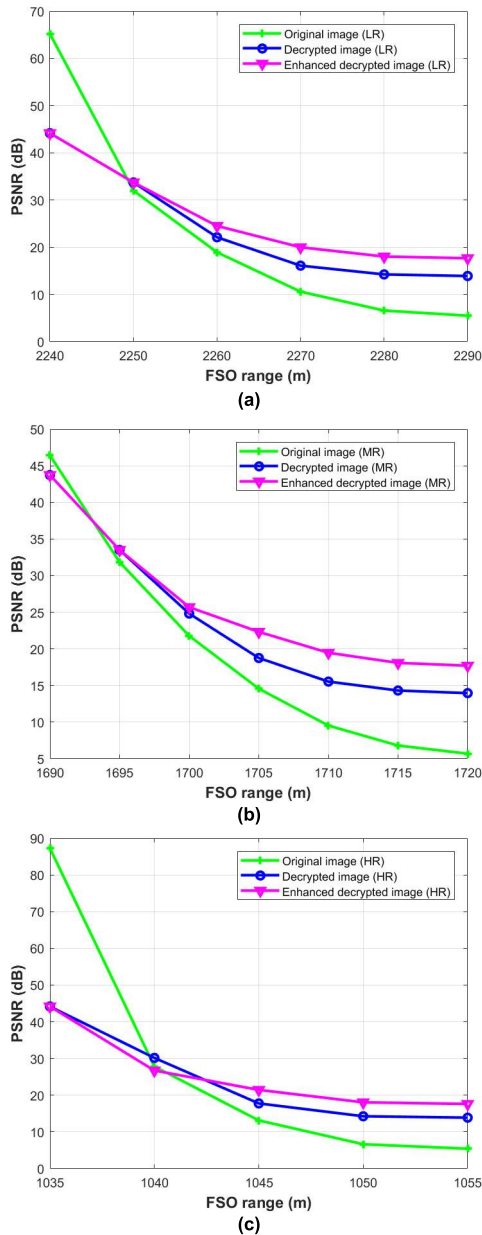
FIGURE 9. PSNR versus various FSO propagation ranges under (a) LR, (b) MR, and (c) HR conditions.
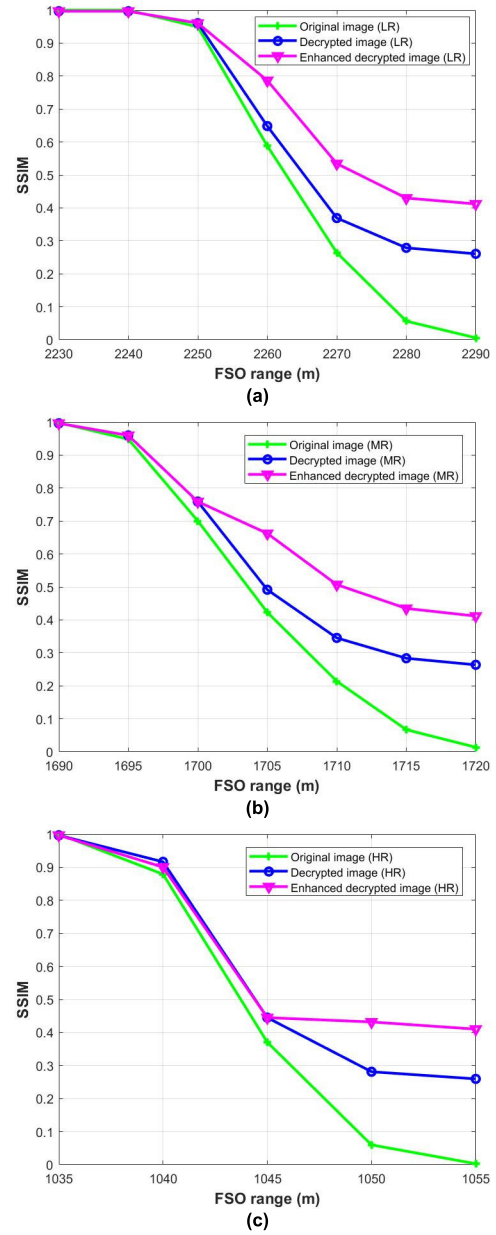

FIGURE 10. SSIM versus various FSO propagation ranges under (a) LR, (b) MR, and (c) HR conditions.

where μ_T and μ_R indicate the means, C_1 and C_2 are constants. σ_T^2 and σ_R^2 are the standard deviations and σ_{TR} represent the cross covariance for the original transmitted image and the received image.

Figure 10 demonstrates the impact of various FSO distances on SSIM values under various rain conditions. It is noticed that SSIM has value of 1 in shortest FSO ranges which are 2230 m for LR, 1690 m for MR, and 1035 m for HR. Conversely, minimum values of SSIM occurred at higher FSO spans. Additionally, received image from plain transmitted image observed the lowest SSIM. For LR (2290 m), MR (1720 m), and HR (1055m), the SSIM values in case of received original images are 0.058, 0.013, and 0.002. These

values at same ranges are improved to 0.261 and 0.412 (LR), 0.263 and 0.411 (MR), 0.259 and 0.410 (HF) for decrypted and enhanced decrypted images, respectively.

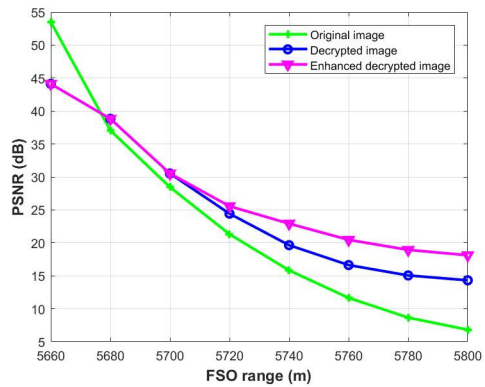### 2) EFFECT OF VARIOUS RANGES ON IMAGE TRANSMISSION FOR ALEXANDRIA AND JEDDAH CITIES

As a demonstration of its feasibility, we have evaluated the performance of image transmission using actual meteorological data from Alexandria City, serving as evidence of its applicability in real-world scenarios. Given that Alexandria City experiences the lowest $\propto$ when compared to LR, MR, and HR conditions, it allows the optical signal carrying either the original image or ciphered image to achieve the longest
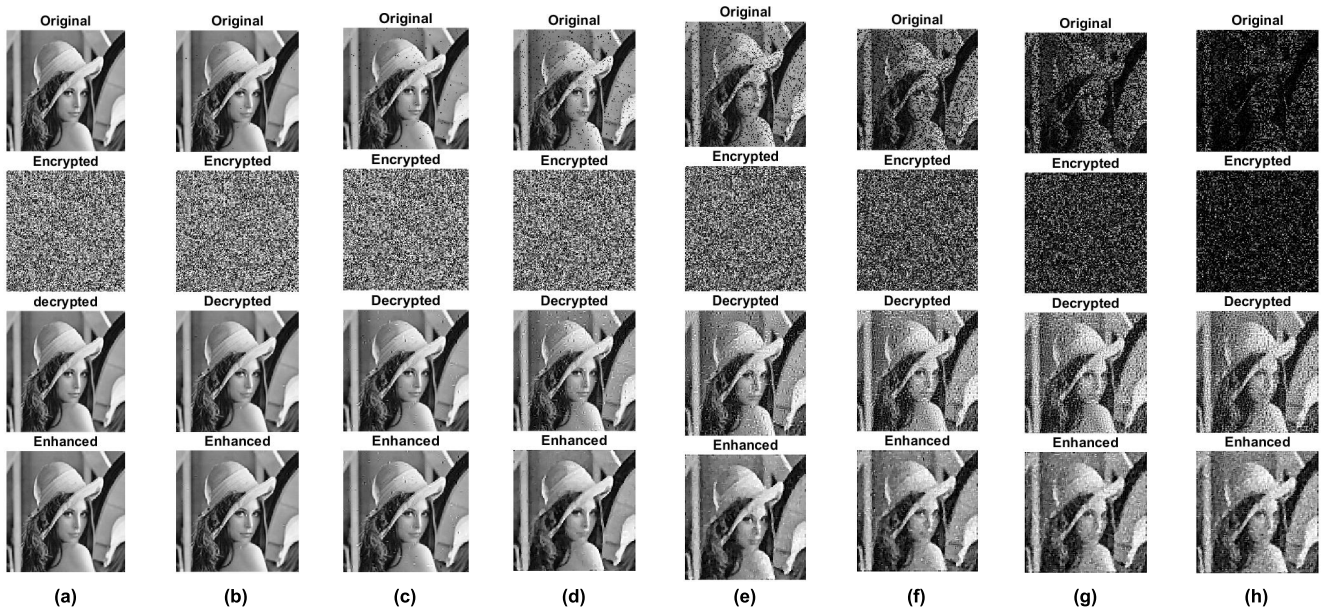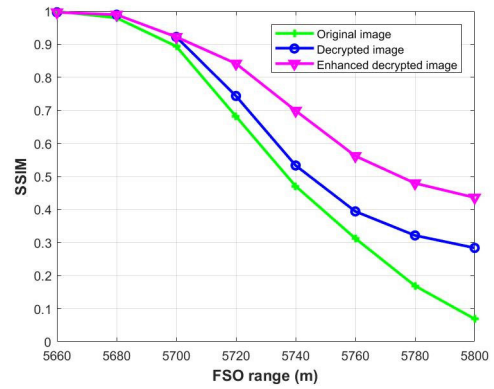
FIGURE 11. View of received images under Alexandria weather at (a) 5660 m, (b) 5680 m, (c) 5700 m, (d) 5720 m, (e) 5740 m, (f) 5760 m, (g) 5780 m, and (h) 5800 m.
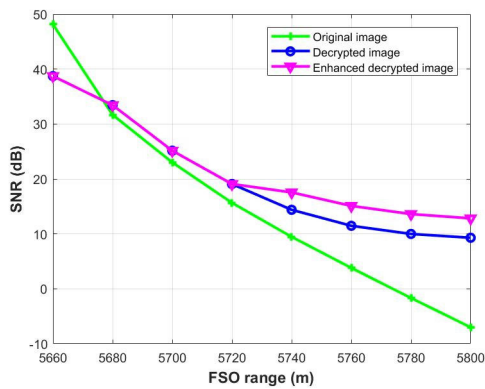
FIGURE 12. SNR versus various FSO propagation ranges for Alexandria City.

FIGURE 14. SSIM versus various FSO propagation ranges for Alexandria City.

FIGURE 13. PSNR versus various FSO propagation ranges for Alexandria City.

FSO propagation range when operating under its atmospheric conditions and that is clear from Fig. 11 that shows view of different images versus FSO ranges. Image when encrypted and transmitted, can be received with better quality than when sent as a plain image. Plain image can be received with slightly good view till distance of 5740 m, which is extended to 5800 m when received as encrypted image and then perform decrypting process. Further view enhancement for decrypted at the same range is observed after using median filter and HPF.

Figures 12-14 show SNR, PSNR, and SSIM, respectively for the proposed image transmission based FSO system for Alexandria city. Similarly, as the distance between the transmitter and receiver increases, these three-quality metrics decreases. At 5800 m, the values for SNR, PSNR, and SSIM are 12.82 dB, 18.12 dB, and 0.43 when enhancement is done for the received decrypted images. On the other hand, at the same range but original image is received, these values are −7 dB, 6.8 dB, and 0.06, respectively.
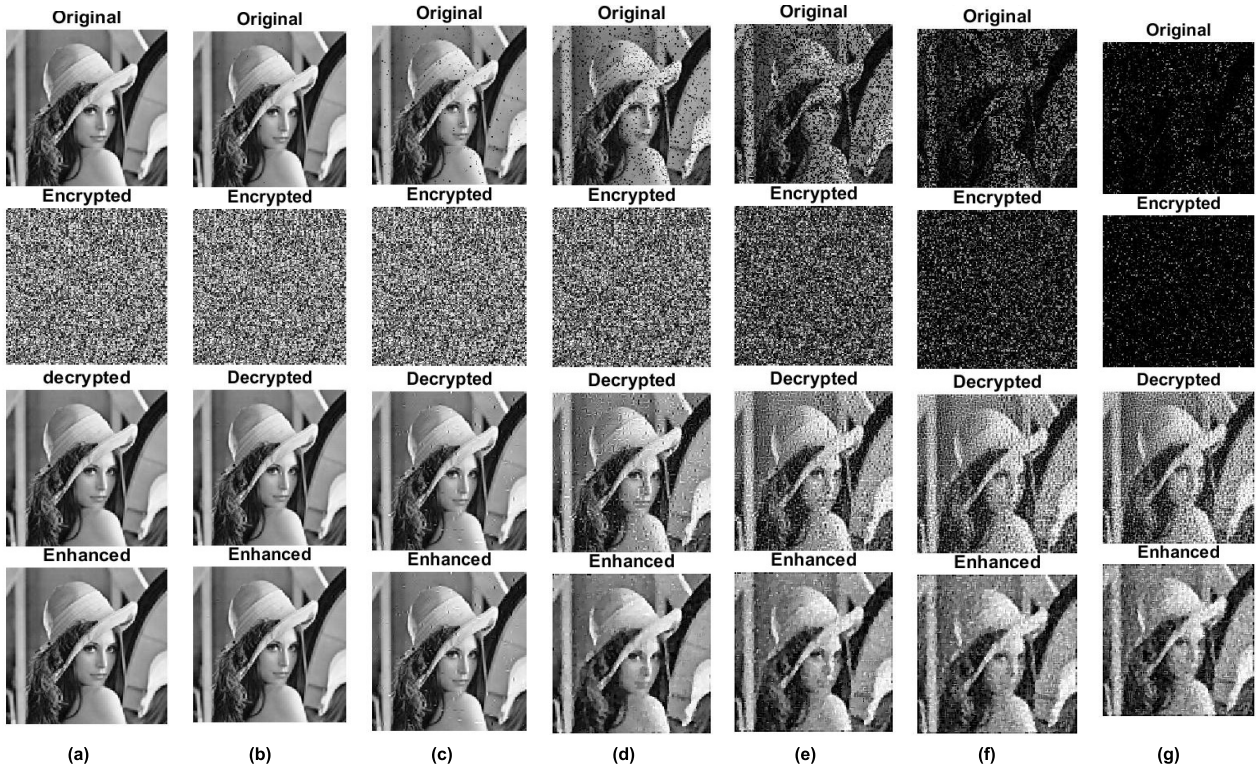
FIGURE 15. View of received image for Jeddah City at (a) 7900 m, (b) 7950 m, (c) 8000 m, (d) 8050 m, (e) 8100 m, (f) 8150 m, and (g) 8200 m.
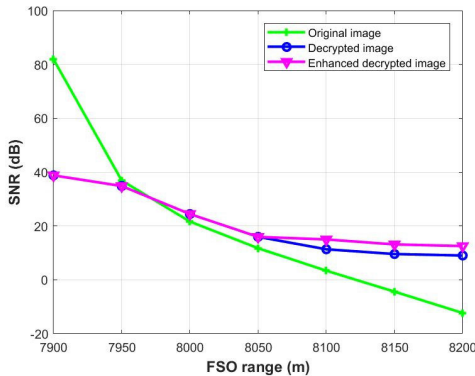

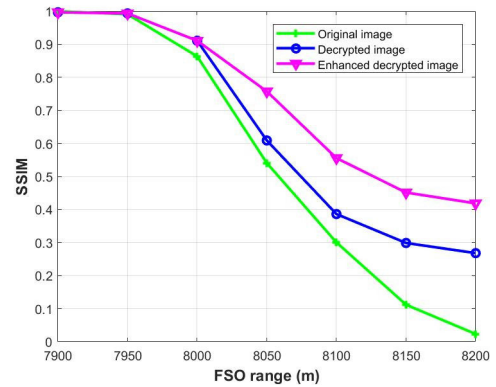**FIGURE 16.** SNR versus various FSO propagation ranges for Jeddah City.

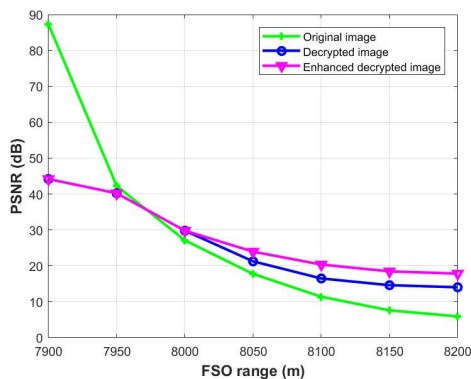**FIGURE 18.** SSIM versus various FSO propagation ranges for Jeddah City.

TABLE 3. Variance values for different Ciphered Images by CFI Algorithm.

Images	Histogram Variance
Lena	223.5392
Tree	250.0712
Boat	233.5642
Peppers	245.5698
Cameraman	241.9827
Airplane	244.6245
Baboon	235.3325
Truck	238.3369

FIGURE 17. PSNR versus various FSO propagation ranges for Jeddah City.

Furthermore, the performance of image transmission is discussed for Jeddah City. Figure 15 displays the received

images when plain and encrypted images are transmitted in the challenging rainy weather conditions of Jeddah City. The unencrypted, plain image achieved a maximum FSO range of 8050 m while maintaining good image visibility. Remarkably, this FSO range is extended to 8200 m after enhancing the received decrypted images. This demonstrates the advantage
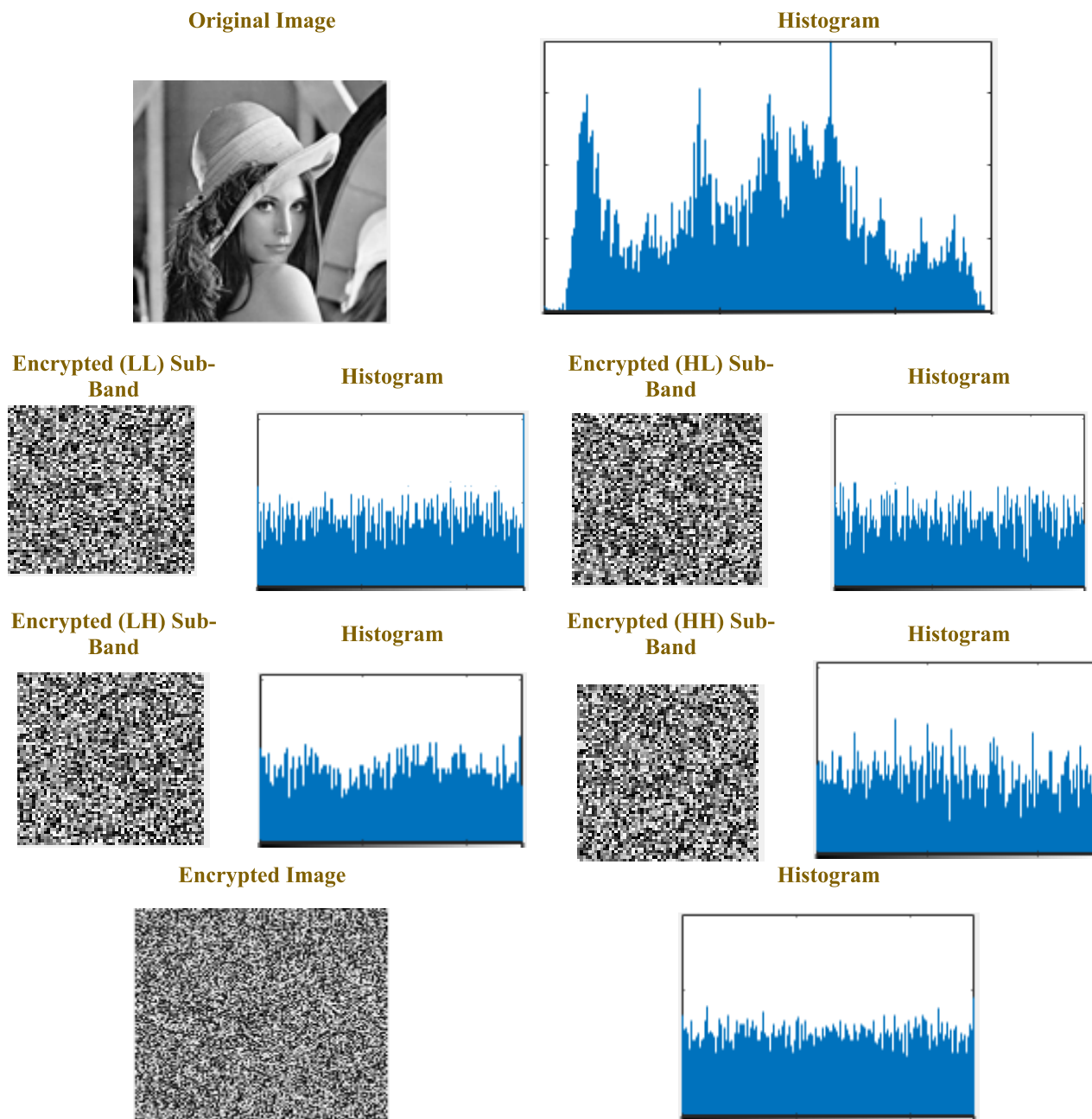
Original Image

Histogram

Encrypted (LL) Sub-Band

Histogram

Encrypted (HL) Sub-Band

Histogram

Encrypted (LH) Sub-Band

Histogram

Encrypted (HH) Sub-Band

Histogram

Encrypted Image

Histogram

**FIGURE 19.** Histogram analysis for images produced by each encryption sub-band.

TABLE 4. Various images UACI and NPCR.

Images	UACI	NPCR
Lena	33.44	99.61
Tree	33.44	99.62
Boat	33.43	99.59
Peppers	33.42	99.57
Cameraman	33.46	99.61
Airplane	33.42	99.63
Baboon	33.45	99.58
Truck	33.45	99.62

of encrypting images for extended FSO communication in adverse weather conditions. The encryption not only secures the data but also enhances the range of successful image transmission.

Figures 16-18 illustrate the SNR, PSNR, and SSIM for the proposed FSO-based image transmission system in Jeddah city. Correspondingly, with an increase in the distance between the transmitter and receiver, there is a noticeable decline in these three-quality metrics. For instance, when the distance reaches 8200 m, the values for SNR, PSNR, and SSIM stand at 12.52 dB, 17.82 dB, and 0.41, respectively, for the enhancement images. In contrast, at the same distance when the original image is received, these values are significantly lower, measuring at -12.34 dB, 5.9 dB, and 0.0231, respectively.
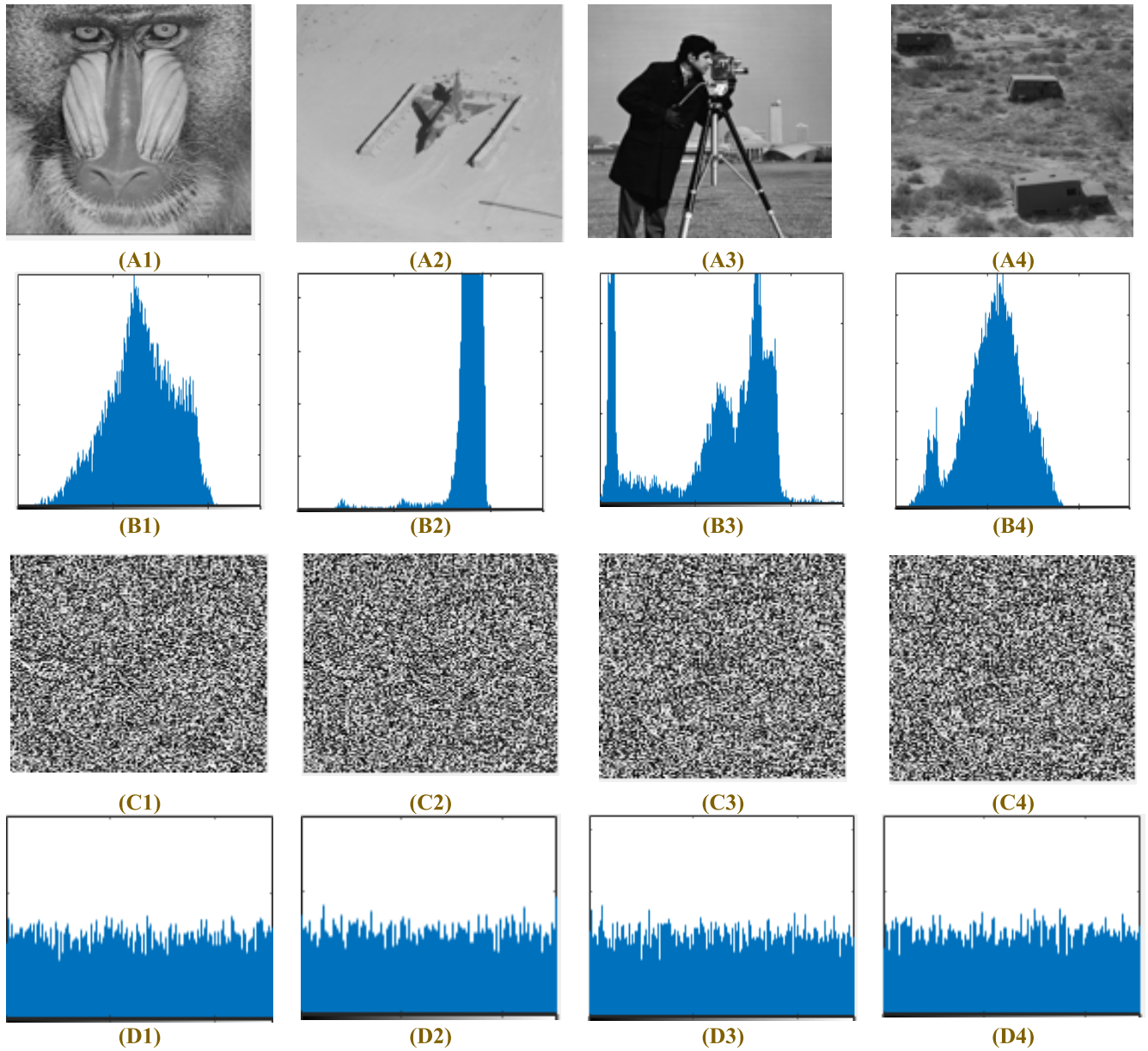
FIGURE 20. Original and cipher images histograms: (A1) - (A4) Original images; (B1) - (B4) Original images histograms; (C1) - (C4) Ciphered images; (D1) - (D4) Ciphered images histograms.

B. SECURITY ANALYSIS

1) HISTOGRAM ANALYSIS

The study in this part shows the results of the histogram analysis for the original image and its encrypted version. The two images were structurally different, when inspected from a statistical standpoint. The original image has tilts and spikes in its histogram. As for the cipher image, its histogram is marked by flatness and uniformity. This proves the difference between the two images, on the statistical plane. Figure 19 shows the histogram of the sub-bands of the images encoded with the proposed scheme. As for Fig. 20, the histograms displayed correspond to original images, as well as encrypted ones, encoded with the scheme described in this study. These

histograms show that images encrypted with the algorithm proposed in this paper are random. To calculate variance (x) of a histogram, as well as determine its uniformity, quantity analysis is conducted. x_i and x_j are the number of pixels with gray value equals to i and j, respectively. Equation 16 is used to calculate variance (x) [17], [18]

$$Var(x) = \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{1}{2}(x_i - x_j)^2 \qquad (29)$$

A small value for variance (x) is an indication that the image is uniform. Values of this variance for encrypted images can be seen in Table 3. Results marked in this Table are an indication
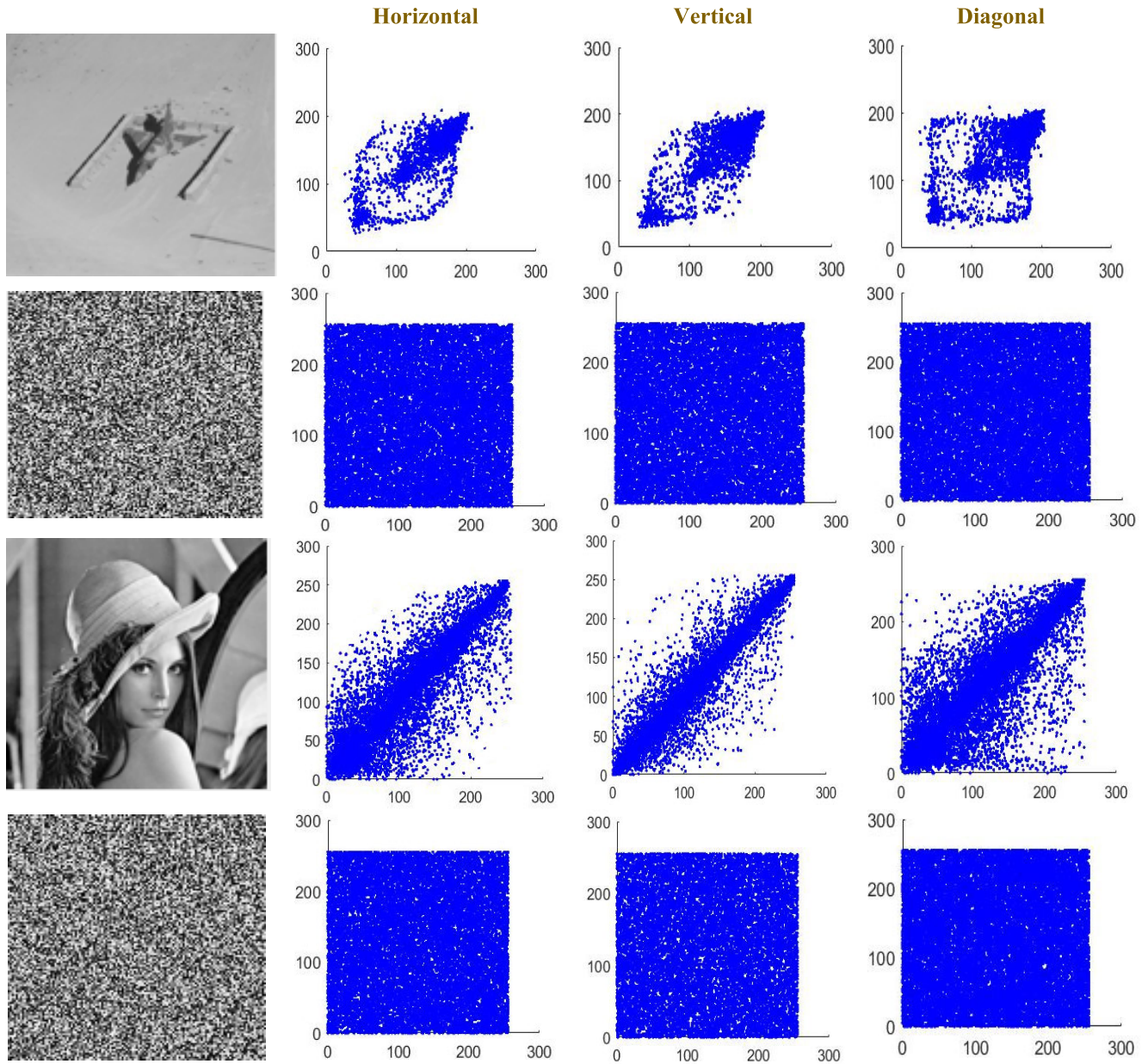
FIGURE 21. Correlation between two adjacent pixels on the original image and its encrypted version.

of the uniformity of the histogram of the encrypted image, after running encryption simulation.

2) DIFFERENTIAL ATTACK

To check the difference between a single bit on the original image and its encrypted version, two measures are used, i.e., the number of pixel change rate (NPCR) and the unified average changing intensity (UACI). Equations 30 and 31 are used to calculate the former and latter, respectively [43], [44]

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

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

TABLE 5. Different images information entropy.

Algorithm	Images	Information Entropy
	Lena	7.9985
	Tree	7.9952
	Boat	7.9988
Proposed work	Peppers	7.9987
	Cameraman	7.9984
	Airplane	7.9991
	Baboon	7.9986
	Truck	7.9972
Ref. [38]	Lena	7.9973
Ref. [44]	Lena	7.9975
Ref.[45]	Boat	7.9918

where, W and H are the width and height of the encoded image, respectively. As for $C_1(i,j)$, it represents the cipher

TABLE 6. Correlation coefficients between two adjacent pixels on the original and encrypted images.

Algorithm	Images	Correlation Coefficients					
		Horizontal		Vertical		Diagonal	
		Plain	Encrypted	Plain	Encrypted	Plain	Encrypted
CFI algorithm	Lena	0.9729	2.0557e-04	0.9463	0.00045	0.9402	0.00063
	Tree	0.9682	7.6542e-04	0.9451	0.00028	0.9312	0.00284
	Boat	0.9268	0.00057	0.9452	0.0045	0.9152	0.00342
	Peppers	0.9634	7.0325e-04	0.9704	9.0256e-04	0.9014	0.00035
	Cameraman	0.9592	0.00043	0.9335	0.00035	0.9452	0.00172
	Airplane	0.9166	0.000345	0.9318	6.7686e-04	0.9621	0.00253
	Baboon	0.8736	0.00024	0.8261	0.00013	0.8132	0.00076
	Truck	0.9477	0.00012	0.8955	0.00092	0.8745	0.00136
Ref. [15]	Peppers	NA	0.0006	NA	0.00208	NA	0.00204
Ref. [39]	Lena	NA	0.0044	NA	0.0033	NA	0.0701
Ref.[45]	Lena	NA	0.0008	NA	0.0041	NA	0.0011

image before one bit of change. On the other hand, $C_2(i, j)$ is the same image, but after this change. Table 4 shows values of NPCR and UACI of images encrypted with the algorithm proposed in this paper. They all appear to be in the vicinity of the optimum values for these variables. On average, these values were 99.6094% for NPCR and 33.4635% for UACI. As such, it can be concluded that this algorithm is highly sensitive to even small changes in the original image.

3) INFORMATION ENTROPY ANALYSIS

Entropy analysis is performed to measure the amount of uncertainty in image information, as well as to check the distribution of the gray value of the image. Information entropy has a value between zero and eight (the optimum value for entropy). Thus, an information entropy close to eight is possessed by an image, encrypted with an effective algorithm. Equation 32 is used to calculate information entropy [46-47]

$$E_n = \sum_{i=1}^{N-1} P(X_i) log_2 P(X_i) \qquad (32)$$

where, N is the total number of (X), while $P(X_i)$ is the possibility of its occurrence. In Table 4, the information entropy values for different images encrypted with the proposed encryption scheme can be seen. It could be concluded by checking this results in Table 5 that the proposed algorithm leads to values for information entropy of encrypted images close to the optimum value.

4) CORRELATION COEFFICIENT

To check the similarity between the encrypted image and its original, correlation analysis is performed. There are usually a lot of similarities between adjacent pixels, leading to a high correlation coefficient, when calculated for these specific pixels. When encryption employs an efficient algorithm, the correlation between such pixels is broken. When the value of the correlation coefficient between two adjacent pixels is zero or a figure close to it, then there is low correlation between the

two, and the algorithm is deemed effective. To calculate the correlation coefficient in the horizontal, vertical, and diagonal directions, Eq. (33) 18 is used [44, 48].

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \qquad (33)$$

where, r_{xy} is the correlation coefficient, cov is the covariance between pixels (x) and (y), while $D(x)$ is the variance and $D(y)$ is the mean. (x) represents a certain pixel on the plaintext image, in its grayscale value, while (y) is the same pixel but on the encrypted image. The correlation between two adjacent pixels, in all three directions (horizontal, vertical, and diagonal) for original images and their encrypted versions can be seen in Fig. 21. Cipher images are found to have smaller pixel correlation than original images. Table 6 holds a recording of the correlation coefficients of images encoded with the algorithm proposed in this study. When compared with the original images, it could be noted that originals had correlation coefficients of one. It can be concluded that the proposed scheme has the ability to decrease the correlation coefficient between adjacent pixels on the images resulting from encryption, bringing it down to a value close to zero.

V. CONCLUSION

This paper introduces a secure image transmission approach utilizing the CFI algorithm over an FSO channel. The performance of both original and encrypted image transmissions is assessed under varying rain conditions, including LR, MR, and HR levels. Moreover, real meteorological data for average rainfall intensities spanning four years (2014 to 2018) in two cities with distinct geographical locations are incorporated to evaluate system performance.

SNR, PSNR, and SSIM serve as key metrics for assessing the visual quality of received images. To further enhance image quality, two filters, namely the median filter and HPF, are applied.

In addition to the visual quality assessment, a comprehensive security analysis is conducted, encompassing factors

such as histograms, differential attacks, entropy, and correlation coefficients, applied to various images.

The results highlight that as rainfall intensities increase, the maximum propagation range for image transmission through the atmosphere decreases, leading to reductions in SNR, PSNR, and SSIM. Notably, the encrypted images exhibit an extended FSO range compared to plain images.

For instance, as the city of Jeddah is characterized by low rainfall intensity, the maximum FSO range for achieving high-quality received encrypted images extends to 8200 m, with SNR, PSNR, and SSIM values of 12.52 dB, 17.82 dB, and 0.41 dB, respectively. Conversely, the highest attenuation during HR results in the lowest FSO span of 1055 m.

Regarding the security analysis, the CFI algorithm demonstrates positive results in terms of information entropy values and correlation coefficients.

REFERENCES

[1] Z. Ghassemlooy, S. Zvanovec, M.-A. Khalighi, W. O. Popoola, and J. Perez, *Optical Wireless Communication Systems*. Cham, Switzerland: Springer, 2017, pp. 1–6, doi: 10.1007/978-3-319-30201-0.

[2] H. Kaushal and G. Kaddoum, "Optical communication in space: Challenges and mitigation techniques," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 57–96, 1st Quart., 2017, doi: 10.1109/COMST.2016.2603518.

[3] N. A. Mohd Nor, Z. Ghassemlooy, S. Zvanovec, M.-A. Khalighi, M. R. Bhatnagar, J. Bohata, and M. Komanec, "Experimental analysis of a triple-hop relay-assisted FSO system with turbulence," *Opt. Switching Netw.*, vol. 33, pp. 194–198, Jul. 2019, doi: 10.1016/j.osn.2017.11.002.

[4] A. K. Majumdar, *Optical Wireless Communications for Broadband Global Internet Connectivity: Fundamentals and Potential Applications*. Amsterdam, The Netherlands: Elsevier, 2018, doi: 10.1016/b978-0-12-813365-1.00008-4.

[5] H. Hong, Y. Xu, D. He, N. Gao, Y. Wu, and W. Zhang, "Evaluation of non-uniform constellations for the converged network of broadcast and broadband," in *Proc. IEEE Int. Symp. Broadband Multimedia Syst. Broadcast. (BMSB)*, Jeju, South Korea, Jun. 2019, pp. 1–5, doi: 10.1109/BMSB47279.2019.8971876.

[6] H. S. Gill, M. L. Singh, M. Singh, Priyanka, S. Kaur, and H. Kaur, "Analysis of full reference quality metrics for image transmission over a MIMO OWC channel under varying turbulent conditions," *Int. J. Commun. Syst.*, vol. 36, no. 5, p. e5426, Jan. 2023, doi: 10.1002/dac.5426.

[7] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2231–2258, 4th Quart., 2014, doi: 10.1109/COMST.2014.2329501.

[8] S. Chaudhary and A. Amphawan, "The role and challenges of free-space optical systems," *J. Opt. Commun.*, vol. 35, no. 4, pp. 327–334, 2014, doi: 10.1515/JOC-2014-0004.

[9] S. A. A. El-Mottaleb, M. Singh, H. Y. Ahmed, M. Zeghid, K. S. Nisar, M. F. Alotaibi, M. Mahmoud, and W. Weera, "Performance evaluation of a 160-Gbit/s OCDMA-FSO system via Laguerre–Gaussian beams under weather conditions," *Alexandria Eng. J.*, vol. 63, pp. 661–674, Oct. 2023.

[10] I. I. Kim, B. McArthur, and E. J. Korevaar, "Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications," *Opt. Wireless Commun. III*, vol. 4214, pp. 26–37, Feb. 2001, doi: 10.1117/12.417512.

[11] S. El-Mottaleb, M. Singh, A. Chehri, H. Ahmed, M. Zeghid, and A. Khan, "Capacity enhancement for free space optics transmission system using orbital angular momentum optical code division multiple access in 5G and beyond networks," *Energies*, vol. 15, no. 19, p. 7100, Sep. 2022, doi: 10.3390/EN15197100.

[12] M. Singh, J. Kříž, M. M. Kamruzzaman, V. Dhasarathan, A. Sharma, and S. A. Abd El-Mottaleb, "Design of a high-speed OFDM-SAC-OCDMA-based FSO system using EDW codes for supporting 5G data services and smart city applications," *Frontiers Phys.*, vol. 10, Jul. 2022, Art. no. 934848.

[13] P. Murali, G. Niranjana, A. J. Paul, and J. S. Muthu, "Domain-flexible selective image encryption based on genetic operations and chaotic maps," *Vis. Comput.*, vol. 39, no. 3, pp. 1057–1079, Mar. 2023.

[14] S. Sabir and V. Guleria, "Multi-layer security based multiple image encryption technique," *Comput. Electr. Eng.*, vol. 106, Mar. 2023, Art. no. 108609.

[15] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik*, vol. 272, Feb. 2023, Art. no. 170316, doi: 10.1016/J.IJLEO.2022.170316.

[16] S. E. El-Khamy, N. O. Korany, and A. G. Mohamed, "A new fuzzy-DNA image encryption and steganography technique," *IEEE Access*, vol. 8, pp. 148935–148951, 2020, doi: 10.1109/ACCESS.2020.3015687.

[17] 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. 14284–14305, 2021, doi: 10.1109/ACCESS.2021.3052161.

[18] M. N. Ilic, B. P. Prlincevic, P. C. Spalevic, S. R. Panic, and D. D. Drajic, "On the transmission of colour image over double generalized gamma FSO channel," *Elektronika ir Elektrotechnika*, vol. 23, no. 2, pp. 79–83, Apr. 2017, doi: 10.5755/J01.EIE.23.2.18004.

[19] X. Huang, Y. Bai, and X. Fu, "Image transmission with binary coding for free space optical communications in the presence of atmospheric turbulence," *Appl. Opt.*, vol. 59, no. 33, p. 10283, Nov. 2020, doi: 10.1364/ao.405152.

[20] A. Djir, F. Meskine, and M. L. Tayebi, "Rain effects analysis on image transmission through free space optical communication system," *J. Opt. Commun.*, Jul. 2023, doi: 10.1515/joc-2023-0165.

[21] H. S. Gill and M. L. Singh, "Performance evaluation of DVB-t image transmission over a MIMO OWC channel at 650 nm under varying turbulence regimes," *Wireless Netw.*, vol. 27, no. 3, pp. 1965–1979, Apr. 2021, doi: 10.1007/s11276-021-02559-5.

[22] A. Djir, F. Meskine, and M. L. Tayebi, "Image transmission performance analysis through free space optical communication link using coherent QPSK modulation under various environmental conditions," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 9, p. e4821, Jun. 2023, doi: 10.1002/ett.4821.

[23] H. S. Gill and M. L. Singh, "Estimation of visual performance enhancement with spatial filters for an image transmission over a turbulent OWC link," *Wireless Pers. Commun.*, vol. 122, no. 1, pp. 523–541, Jan. 2022, doi: 10.1007/s11277-021-08911-4.

[24] M. Alawida, J. S. Teh, and W. H. Alshoura, "A new image encryption algorithm based on DNA state machine for UAV data encryption," *Drones*, vol. 7, no. 1, p. 38, Jan. 2023, doi: 10.3390/drones7010038.

[25] D. Wei, M. Jiang, and Y. Deng, "A secure image encryption algorithm based on hyper-chaotic and bit-level permutation," *Exp. Syst. Appl.*, vol. 213, Oct. 2023, Art. no. 119074.

[26] X. Wang, X. Zhang, M. Gao, Y. Tian, C. Wang, and H. H.-C. Iu, "A color image encryption algorithm based on hash table, Hilbert curve and hyper-chaotic synchronization," *Mathematics*, vol. 11, no. 3, p. 567, Jan. 2023.

[27] P. Liu, X. Wang, Y. Su, H. Liu, and S. Unar, "Globally coupled private image encryption algorithm based on infinite interval spatiotemporal chaotic system," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 6, pp. 2511–2522, Jun. 2023, doi: 10.1109/tcsi.2023.3250713.

[28] L. Feng, J. Du, C. Fu, and W. Song, "Image encryption algorithm combining chaotic image encryption and convolutional neural network," *Electronics*, vol. 12, no. 16, p. 3455, Aug. 2023.

[29] Q. Cun, X. Tong, Z. Wang, and M. Zhang, "A new chaotic image encryption algorithm based on dynamic DNA coding and RNA computing," *Vis. Comput.*, vol. 39, no. 12, pp. 6589–6608, Jan. 2023, doi: 10.1007/s00371-022-02750-5.

[30] A. Djir, F. Meskine, and M. L. Tayebi, "Free space optical communication study for image transmission under foggy conditions," in *Proc. 2nd Int. Conf. Adv. Electr. Eng. (ICAEE)*, Constantine, Algeria, Oct. 2022, pp. 1–6, doi: 10.1109/ICAEE53772.2022.9962014.

[31] S. S. Muhammad, P. Kohldorfer, and E. Leitgeb, "Channel modeling for terrestrial free space optical links," in *Proc. 7th Int. Conf. Transparent Opt. Netw.*, 2005, pp. 407–410.

[32] A. N. Z. Rashed and M. M. E. El-Halawany, "Transmission characteristics evaluation under bad weather conditions in optical wireless links with different optical transmission windows," *Wireless Pers. Commun.*, vol. 71, no. 2, pp. 1577–1595, Jul. 2013.

[33] H. Y. Ahmed and K. S. Nisar, "Diagonal eigenvalue unity (DEU) code for spectral amplitude coding-optical code division multiple access," *Opt. Fiber Technol.*, vol. 19, no. 4, pp. 335–347, Aug. 2013.

[34] B. T. Vu, N. T. Dang, T. C. Thang, and A. T. Pham, "Bit error rate analysis of rectangular QAM/FSO systems using an APD receiver over atmospheric turbulence channels," *J. Opt. Commun. Netw.*, vol. 5, no. 5, pp. 437–446, May 2013, doi: 10.1364/JOCN.5.000437.

[35] M. Singh, S. A. Abd El-Mottaleb, S. A. Aljunid, H. Y. Ahmed, M. Zeghid, and K. S. Nisar, "Performance investigations on integrated MMF/FSO transmission enabled by OAM beams," *Results Phys.*, vol. 51, Aug. 2023, Art. no. 106656, doi: 10.1016/j.rinp.2023.106656.

[36] T. V. Nguyen, T. V. Pham, N. T. Dang, and A. T. Pham, "Performance of generalized QAM/FSO systems with pointing misalignment and phase error over atmospheric turbulence channels," *IEEE Access*, vol. 8, pp. 203631–203644, 2020, doi: 10.1109/ACCESS.2020.3036643.

[37] A. Kumar, P. Singh, K. A. K. Patro, and B. Acharya, "High-throughput and area-efficient architectures for image encryption using PRINCE cipher," *Integration*, vol. 90, pp. 224–235, May 2023, doi: 10.1016/j.vlsi.2023.01.011.

[38] M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, "An efficient image encryption technique based on two-level security for Internet of Things," *Multimedia Tools Appl.*, vol. 82, no. 4, pp. 5091–5111, Feb. 2022, doi: 10.1007/s11042-022-12169-8.

[39] P. Xie, X. Shi, X. Huang, Y. Bai, and X. Fu, "Binary detection in ghost imaging with preserved grayscale," *Eur. Phys. J. D*, vol. 73, no. 5, pp. 1–5, May 2019.

[40] U. Sara, M. Akter, and M. S. Uddin, "Image quality assessment through FSIM, SSIM, MSE and PSNR—A comparative study," *J. Comput. Commun.*, vol. 7, no. 3, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[41] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004, doi: 10.1109/tip.2003.819861.

[42] Y. Alghamdi, A. Munir, and J. Ahmad, "A lightweight image encryption algorithm based on chaotic map and random substitution," *Entropy*, vol. 24, no. 10, p. 1344, Sep. 2022.

[43] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color image encryption through chaos and KAA map," *IEEE Access*, vol. 11, pp. 11541–11554, 2023, doi: 10.1109/ACCESS.2023.3242311.

[44] Y. Chen, S. Xie, and J. Zhang, "A hybrid domain image encryption algorithm based on improved Henon map," *Entropy*, vol. 24, no. 2, p. 287, Feb. 2022.

[45] L. Teng, X. Wang, and Y. Xian, "Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion," *Inf. Sci.*, vol. 605, pp. 71–85, Aug. 2022.

AMIRA G. MOHAMED (Student Member, IEEE) received the B.S. degree in electronics and communication engineering from the Alexandria Higher Institute of Engineering and Technology (AIET), Alexandria, Egypt, in 2013, and the M.S. and Ph.D. degrees in electrical engineering from the Faculty of Engineering, Alexandria University, Alexandria, in 2017 and 2021, respectively. She is currently a Lecturer with the Department of Electronics and Communications, AIET. Her research interests include image processing, steganography, cryptography, and information security.

HASSAN YOUSIF AHMED received the B.Eng. degree in computer engineering (network systems) and the M.Sc. degree in computer science and information from Gezira University, Sudan, in 2002 and 2007, respectively, and the Ph.D. degree in electrical and electronic engineering from University Tecknolgi PETRONAS, Malaysia, in 2010. He is currently a Full Professor with the Department of Electrical Engineering, College of Engineering, Prince Sattam bin Abdulaziz University. His research interests include computer networks, wireless communications networks, optical communications, and cryptography systems.

SOMIA A. ABD EL-MOTTALEB received the B.Sc. degree in electrical (electronics and communications) engineering from the Faculty of Engineering, Alexandria University, in 2010, the M.Sc. degree in electronics and communications engineering from the Faculty of Engineering, Arab Academy for Science, Technology and Maritime Transport, in 2014, and the Ph.D. degree in electrical (electronics and communications) engineering from the Faculty of Engineering, Alexandria University, in 2020, with a focus on optical communication. She is currently a Lecturer with the Alexandria Higher Institute of Engineering and Technology, Alexandria, Egypt. She has published papers in Q1 and Q2 Scopus journals. Her research interests include free space optics, optical amplifiers, detection techniques, multiplexing techniques, optical fiber communications, and the Internet of Things.

MEDIEN ZEGHID received the Ph.D. degree in information and communication, sciences and technologies from the University of South Brittany, Lorient, France, in 2011. From 2012 to 2014, he was an Assistant Professor with the Department of Electronic Engineering, Higher Institute of Applied Sciences and Technology of Sousse, Sousse University, Tunisia. He is currently an Assistant Professor with the Department of Computer Engineering and Networks, Prince Sattam bin Abdulaziz University. His research interests include information security, architectural synthesis for crypto-systems, image and video coding, and optical communication.

• • •