IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 November 2023, accepted 25 November 2023, date of publication 30 November 2023,
date of current version 14 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3338168

RESEARCH ARTICLE

Performance of Cipher Image Transmission in Free Space Optics Under Foggy Weather

SOMIA A. ABD EL-MOTTALEB[1], AMIRA G. MOHAMED[2], (Student Member, IEEE), ABDELLAH CHEHRI[3], (Senior Member, IEEE), MEHTAB SINGH[4], AHMAD ATIEH[5], HASSAN YOUSIF AHMED[6], AND MEDIEN ZEGHID[6,7]

[1]Department of Mechatronics Engineering, Alexandria Higher Institute of Engineering and Technology, Alexandria 21311, Egypt
[2]Department of Electronics and Communications Engineering, Alexandria Higher Institute of Engineering and Technology, Alexandria 21311, Egypt
[3]Department of Mathematics and Computer Science, Royal Military College of Canada, Kingston, ON K7K 7B4, Canada
[4]Department of Electronics and Communication Engineering, University Institute of Engineering, Chandigarh University, Mohali, Punjab 140413, India
[5]Optiwave Systems Inc., Ottawa, ON K2E 8A7, Canada
[6]Department of Electrical Engineering, College of Engineering in Wadi Alddawasir, Prince Sattam bin Abdulaziz University, Al-Kharj 16273, Saudi Arabia
[7]Electronics and Micro-Electronics Laboratory (E. μ. E. L), Faculty of Sciences, University of Monastir, Monastir 5000, Tunisia

Corresponding author: Abdellah Chehri (chehri@gel.ulaval.ca)

ABSTRACT This paper proposes a new cipher image transmission system in free space optics system (FSO). A secure and effective image cryptosystem algorithm based on the Choquet fuzzy integral (CFI) technique and the integer wavelet transform is utilized. Numerical simulations are conducted to examine the efficacy of encrypted images against different attacks. The pixel correlation coefficient is found to be quite small for horizontally, vertically, and diagonally in the ranges 2.0557×10^{-4} to 0.00057, 9.0256×10^{-4} to 0.0045, and 0.00035 to 0.00342, respectively. Additionally, the information entropy of the encrypted image is found to be within the range of 7.9991:7.9972, which is very close to the ideal value of 8. As for the unified average changing intensity (UACI) and the number of pixel change rate (NPCR) metrics, they are in the ranges 33.46 to 33.42 and 99.58 to 99.63, respectively, which are also very close to the optimum values. Median and high pass filters are employed for further enhancing the received decrypted image. Different fog conditions are considered during the transmission of the encrypted image over FSO channel. The signal to noise ratio (SNR), FSO propagation range, and structured similarity index method (SSIM) are metrics used for performance evaluation. The results indicate that images transmitted with ciphering exhibit better performance than plain images. The maximum FSO spans over which the image can propagate in the channel while maintaining good quality are 1790 m, 1198 m, and 947 m under light fog (LF), medium fog (MF), and heavy fog (HF), respectively. In contrast, these ranges extend to 1798 m (LF), 1206 m (MF), and 953 m (HF) with good visual quality when ciphered images are transmitted. Furthermore, the employed enhancement technique demonstrates improvements in SNR and SSIM values for the received images. For instance, when the original image is transmitted in an FSO channel affected by MF, the SNR is -21 dB. This value significantly improves to 12.6 dB when median and high pass filters are applied for enhancement. In addition, the SSIM value goes from 0.18 for the original image to 0.29 when enhancement techniques like median and high pass filters are used at a 1206 m FSO range in MF weather. Consequently, the proposed encrypted image transfer improves image quality. This advancement can be attributed to the CFI encryption algorithm's rigorous security mechanisms, which assure data safety as it travels through the atmosphere.

INDEX TERMS Choquet fuzzy integral (CFI), image encryption, free space optics (FSO), signal to noise ratio (SNR), structured similarity index method (SSIM).

I. INTRODUCTION

The previous decade witnessed a significant growth in the accessibility and capabilities of telecommunications, broadband, and broadcasting services [1]. It is anticipated that the number of internet-connected devices will reach 29.3 billion, with machine-to-machine (M2M) communication accounting for the largest portion of this growth, followed by smartphones and televisions. Within this evolving landscape, it is expected that multimedia devices will

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

assert their prominence in terms of precipitating traffic load, accounting for a substantial portion, exceeding 90% of the aggregate share. It is noteworthy that multimedia applications, characterized by their content-rich nature, impose heightened bandwidth demands, with UHD security cameras necessitating a minimum of 16 Mbps. UHD virtual reality applications demanding a significantly higher bandwidth of 500 Mbps [2], [3]. Additionally, the utilization of multimedia services at accelerated rates necessitates a substantial allocation of bandwidth spanning from core networks to end users [4].

The utilization of radio frequency (RF) in diverse wireless applications is ever increasing. Nevertheless, the current allocation of RF spectrum proves inadequate in satisfying the escalating requirement for 5G wireless bandwidth. This insufficiency arises due to several factors. Firstly, the spectrum band below 10 GHz, which RF heavily relies upon, exhibits limitations in terms of its width. Additionally, this band is subject to regulatory constraints regarding spectrum usage. Lastly, the presence of substantial interference among neighboring RF access points further exacerbates the issue [5], [6], [7].

The photonics discipline is profoundly engrossed in the pursuit of attaining a considerable capacity increase for data processing, with a concurrent emphasis on addressing the formidable challenge of unmet bandwidth requirements [8]. Free Space Optical (FSO) refers to a wireless communication technology that operates within the optical spectrum [9], [10]. Compared to RF technology, optical communication offers numerous advantages. Firstly, it enables high transmission speeds for communication links. Additionally, it is immune to electromagnetic interference (EMI), ensuring reliable and uninterrupted data transfer. Furthermore, optical communication utilizes a free usage spectrum, eliminating the need for costly frequency licenses. Lastly, it provides secure transmission, safeguarding sensitive information from unauthorized access [11], [12], [13]. FSO communication can be used in military services, areas where installation of fiber cables are costly and difficult, and inter-satellite communication. Nonetheless, the susceptibility of Free-Space Optical (FSO) transmission to atmospheric attenuation, despite its advantages, results in signal deterioration, an elevated Bit Error Rate (BER), and information loss. An array of atmospheric circumstances, encompassing haze, dust storms, fog, and snowfall, collectively contribute to the attenuation of the transmitted signal. This attenuation is primarily induced by the phenomena of scattering and absorption affecting the transmitted optical signals [14], [15].

Moreover, the utilization of wireless communication technology has led to the emergence of image transmission as a rapidly expanding application. As science and technology continue to progress, various facets of people's lives have transitioned towards greater informatization. As a medium in the information age, images can directly convey the message that people want to express. Digital images can include medical, political, military, and business information. Once the important information in the image is intercepted and tampered by the attackers, the damage caused cannot be undone. Additionally, owing to the voluminous data size and pronounced redundancy inherent in raw images, conventional encryption algorithms face limitations. Therefore, it is very important to protect the information in transmitted images. To ensure the security of digital images [16], [17], there are different types of algorithms used in cryptographic systems. Among them are Advanced Encryption Standard (AES) and Data Encryption Standard (DES). However, encrypting images have been difficult using most methods because images contain large amounts of information. This has been the reason behind developing other systems of encryption designed for specific applications. These systems include methods that apply fuzzy integral. Choquet fuzzy integral (CFI) has many benefits and add great value to the area of image encryption. These benefits include easy to implement, simple to compute, effective in reaching high-level security, and high speed and sensitivity [18], [19].

The reminder of the paper is organized as follows. Section II shows the main contribution of this study. Section III discusses the related works. Section IV provides the description of the proposed image encryption algorithm based on CFI. Section V shows the design of the proposed cipher image transmission in FSO system under foggy weather conditions, followed by the results and discussion in Section VI. Conclusion and future work are devoted in Sec. VII.

II. CONTRIBUTION

In this paper, images that encrypted using CFI algorithm are transmitted over an FSO communication system under different fog conditions; low fog (LF), medium fog (MF), and heavy fog (HF). Accordingly, the main contributions of this paper are:

- Introducing an image encryption/decryption cryptosystem based on CFI for robust performance.
- Evaluating the structure similarity index method (SSIM) and signal to noise ratio (SNR) for encrypted images that are transmitted over FSO channel under the impact of foggy weather conditions.
- Implementing enhancements technique on the decrypted received images.
- Subjecting the proposed algorithm to a series of visual, statistical, and differential attacks, thereby facilitating a comprehensive evaluation of the algorithm efficiency, robustness, and resilience against cryptanalysis.

III. RELATED WORKS

In this section, some related works about image encryption algorithms and image transmission in FSO systems are reviewed.

Several encryption algorithms were studied by researchers. The authors in [20] proposed an encryption algorithm that utilizes two keys and a combination of one- and multi-

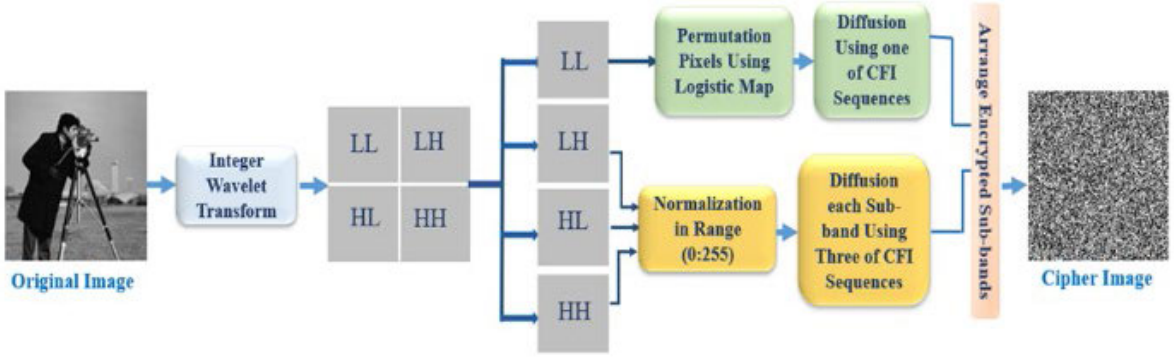


FIGURE 1. Block diagram of the proposed image encryption algorithm.

dimensional (1D and MD) chaotic functions in addition to the KAA map. Du et al. presented a novel image encryption scheme employing integer wavelet transformation (IWT) in conjunction with the Rivest-Shamir-Adleman (RSA) algorithm [21]. Another encryption algorithm that is based on both DNA computing and a finite state machine (FSM) was proposed by the authors in [22]. In this algorithm, a key schedule with statistical randomness and high flexibility was designed based on combining DNA and FSM. In [23], the authors introduced an image encryption algorithm that employs a composite of three enhanced and adapted chaotic 1D mappings. This approach was devised to mitigate the limitations inherent in both 1D and MD mappings. Moreover, an encryption based on adaptive 2D compressive sensing, and a chaotic system was proposed by the authors in [24].

Further, several studies were done on image transmission in FSO systems. In [4], image transmission over the FSO channel was discussed under the influence of atmospheric turbulence, where performance analysis like peak-SNR (PSNR), SSIM, and Pearson correlation coefficient were discussed. Also, the PSNR for the image transmission in the presence of the turbulence effect was discussed in [25]. The effect of rain on the image transmission in the FSO channel was studied by the authors in [26] and the evaluation metrics like received SNR and SSIM were discussed. In [27], authors evaluated the Q-factor, PSNR, and SNR for images propagated in FSO channel affected by fog conditions. In [28], the performance of images modulated using quadrature phase shift keying (QPSK) and on-off keying (OOK) using non-return-to-zero (NRZ) pulse format was investigated under the impact of fog conditions in a FSO channel, where Q-factor, PSNR, and SSIM are used as performance metrics.

Although the above-mentioned studies discussed image transmission in the FSO system, neither of them encrypted the image before transmitting it. In this paper, CFI algorithm is used to encrypt the images before transmission over FSO system. The purpose of employing new cipher image transmission is to ensure data protection as it traverses through the atmosphere. As utilizing CFI encryption technique will provide an additional layer of security and robustness to the transmitted data. The effect of fog conditions in the FSO channel on the encrypted images is discussed, where the system performance is investigated in terms of SNR, various FSO ranges, and SSIM. Further, spatial filters such as median filters and sharped filters are used after decrypting the received image to enhance the visual quality, as these filters remove the unwanted noise that was added during propagation in the channel. Moreover, security analysis is conducted to demonstrate the resilience to various potential attacks.

IV. PROPOSED IMAGE ENCRYPTION ALGORITHM BASED ON CFI

This study proposes an encryption algorithm based on the Choquet fuzzy integral (CFI), which was chosen for its high sensitivity, complexity, and nonlinearity. These properties provide higher security. A new highly secure image encryption system is developed, which avoids the disadvantages of other image cryptosystems. The first step in the proposed encryption system involves the generation of pseudo-random sequences based on CFI [18], [19]. The second step consists of reaching an approximation and creating three detail sub-bands from the plain image, upon the application of the integer wavelet transform (IWT) on the input image. In the third step, detail sub-bands are normalized to ensure that they are kept within the range of sequences generated by CFI (0–255). Thus, pixel intensity is modified. With the application of a control map, CFI generates three sequences used in the diffusion of the three detail sub-bands. To ensure that the approximation is more complex, a logistic chaotic map is used to help shuffle its pixels. Another sequence generated through CFI is used to diffuse the shuffled sub-image. The arrangement of the generated four sub-bands leads to the final encrypted image. Figure 1 shows the block diagram of the proposed algorithm based on the following steps:

A. GENERATION OF PSEUDO RANDOM SEQUENCES BASED ON CFI ALGORITHM

Four highly secure random sequences are generated using CFI algorithm. An external key and a secret image are

employed in the calculation of the initial input of CFI, i.e., h_1, h_2, h_3, h_4. The secret image is chosen through the application of a key to a series of images. Thus, this image is variable. These steps and parameters increase the security of the whole process. The random sequences of CFI along with a brief illustration showing how they were generated are presented in Algorithm 1 below.

Algorithm 1 Generation of Pseudo Random Sequences

Input: External Key with size 128-bit $(\boldsymbol{K})$, Secret Image $\boldsymbol{I}(\boldsymbol{M} \times \boldsymbol{N})$
Output: Random Sequences $\boldsymbol{C_j}$
1: Divide $\boldsymbol{K}$ into four blocks $(\boldsymbol{k_1}, \boldsymbol{k_2}, \ldots\ldots\ldots \boldsymbol{k_{16}})$
2: Calculate key parameters $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D})$
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 $(\boldsymbol{h_1}, \boldsymbol{h_2}, \boldsymbol{h_3}, \boldsymbol{h_4})$
7: # Eq. (6, 7, 8, 9)
8: Calculate Membership Grades $(\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3}, \boldsymbol{g_4})$
9: # Eq. (10)
10: Calculate $\boldsymbol{\lambda_s}$ based on Eq. (11)
11: Calculate fuzzy measures $\boldsymbol{F}(\boldsymbol{A_i})$
12: # Eq. (12)
13: Use Eq. (13) to calculate CFI
14: Generate random sequences $\boldsymbol{C_j}$ based on Eq. (14)
15: return $\boldsymbol{C_j}$

Step 1: The 128-bit secret key is comprised of 16 blocks of 8 bits each $(k_1, k_2, \ldots\ldots\ldots k_{16})$. To calculate the key parameters, the equations below are used.

$$A = (K_1 \oplus K_2 \oplus K_3 \oplus K_4) \tag{1}$$
$$B = (K_5 \oplus K_6 \oplus K_7 \oplus K_8) \tag{2}$$
$$C = (K_9 \oplus K_{10} \oplus K_{11} \oplus K_{12}) \tag{3}$$
$$D = (K_{13} \oplus K_{14} \oplus K_{15} \oplus K_{16}) \tag{4}$$
$$K = \sum_{i=1}^{i=16} (K_i) \tag{5}$$

Step 2: The insertion of the 256 × 256 gray-level matrix of the input image takes place here. Four values of $I(s)$ are obtained upon dividing the image into 2 × 2 blocks. Then, XOR operation is applied for the gray level of each block. h_1, h_2, h_3, h_4, i.e., initial inputs, are obtained through the described equations.

$$h_1 = ((A + K)\, mod 256) \oplus I(1) \tag{6}$$
$$h_2 = ((B + K)\, mod 256) \oplus I(2) \tag{7}$$
$$h_3 = ((C + K)\, mod 256) \oplus I(3) \tag{8}$$
$$h_4 = ((D + K)\, mod 256) \oplus I(4) \tag{9}$$

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.

Step 3: In this step, the initial inputs (hi), as well as the key are calculated for the image. Equation 10 is then used for the calculation of the membership grade using (hi). Equations 11 and 12 are consecutively employed to calculate λ_s and the fuzzy measure, respectively.

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

Sugeno* $\boldsymbol{\lambda_s}$ *Measure:

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

Fuzzy Measure:

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

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

*Step 4:*In this step, the initial inputs (h_1, h_2, h_3, h_4) and the fuzzy measure $F(A_i)$ are used in Equation 13 to calculate the CFI. In Equation 14, CFI is used to create the PN sequence.

$$CFI = \int hdg = \sum_{i=1}^{n} [h(x_i) - h(x_{i-1})\, F(A_i) \tag{13}$$
$$C_j = \left(ARS\left(int\,(CFImod\ 1) \times 10^{14}, S\right)\right) mod 256$$
$$j = 1, 2, 3, 4 \tag{14}$$

where, ARS is the arithmetic right shift of the binary sequence, CFI mod 1 is the normalized fraction value, S assuming values from 0 to 7, and C_1, C_2, C_3, $C_4$are the four random sequences created.

Step 5: created C_1, C_2, C_3, C_4 from CFI are resized to yield four 64 × 64 FZ matrices. Numbers ranging from 0 to 255 make up the 256 integers of 8 bits of each matrix.

B. IMAGE ENCRYPTION BASED ON CFI

The following steps describe the encryption process of the sequences.

Step 1: The 128 × 128 original image gets inserted. This image is then subjected to IWT to yield one approximation (LL) and three detail sub-bands (HL, LH, and HH) of this initial image.

Step 2: The normalization of the intensity of pixels in the three detail sub-bands (HL, LH, and HH) to keep them in the range from 0 to 255 and achieve encryption. CFI sequences are used to XOR the normalized sub-bands. A control code is employed for the selection of four random sequences. Each is used for the encryption of one sub-band, whereas (C_1), (C_2), and (C_3) are used to encrypt the (LH), (HH), and (HL) sub-bands, respectively.

Step 3: As for the approximation sub-band (LL), its pixels are shuffled by using a logistic map. This process is a type of chaotic system, characterized by (r), (X_o), and (X),

the control parameters, the initial condition, and an output, respectively. Inputs are represented by the Equation below:

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

where, r and n are the chaotic parameter and the number of iterations, respectively. $r \in [0, 4]$ and $x \in [0, 1]$. When $r \in [3.57, 4]$, the chaotic attitude is realized. At the end of this step, XOR is performed on the shuffled sub-band image, by using C_4, one of the sequences of CFI. After encryption, the resulting image appears after the arrangement of the approximation and the three detail sub-images (for a total of four sub-bands) takes place.

A brief description of image encryption based on CFI algorithm is given in algorithm 2.

Algorithm 2 Image Encryption Based on CFI

Input: Four Fuzzy Random Sequences ($\boldsymbol{C_1}, \boldsymbol{C_2}, \boldsymbol{C_3}, \boldsymbol{C_4}$), Initial Condition of Logistic Map ($\boldsymbol{X_o}$, $\boldsymbol{r}$), Original Image $\boldsymbol{I}(\boldsymbol{M} \times \boldsymbol{N})$.
Output: Final Cipher Image
1: IWT for original image.
2: Yield one approximation (LL) and three detail sub-bands (HL, LH, and HH).
3: Normalize of the intensity of pixels in the three detail sub-bands (HL, LH, and HH).
4: Use random sequences ($\boldsymbol{C_1}$), ($\boldsymbol{C_2}$), and ($\boldsymbol{C_3}$) to apply XOR for each three detail sub-bands.
5: Generate Random Sequence based on logistic map.
6: Shuffle the approximation sub-band (LL) by using a logistic map.
7: Perform XOR on the shuffled sub-band image, by using $\boldsymbol{C_4}$.
8: Arrange of the encrypted approximation and the three detail sub-images.
9: return **Final Cipher Image**

V. MODEL DESIGN

Figure 2 shows a schematic diagram for images transmission over the FSO channel. At the transmitter, a grey image (128×128) is first encrypted using the CFI algorithm, and its size is converted from matrix form to binary vector representation to be loaded in the user defined bit sequence generator (UDBSG) component. The binary signal is modulated using NRZ pulses at a data rate of 10 Gbps, and is expressed as [27]

$$S_{NRZ}(t) = \sum_{m=-\infty}^{+\infty} a_m p(t - mT_b) \tag{16}$$

where a_m is the m^{th} amplitude symbol, $p(t)$ represents the rectangular shape pulse, and T_b indicates the bit duration which is equal to $(1/R_b)$ where R_b is the bit rate.

To generate the optical signal, a continuous wave (CW) laser source operating at 1550 nm is used to modulate the NRZ pulses of the $S_{NRZ}(t)$ using a Mach-Zehnder modulator (MZM). The optical signal that carries the image is propagated in the FSO channel. The attenuations caused by various fog conditions are considered in this work. The presence of fog can exert a substantial influence on the operational efficiency of FSO communication channels.

The presence of fog poses difficulties in the transmission of light signals because of the scattering and absorption characteristics exhibited by fog particles resulting in attenuation and degradation of the signal. Consequently, these attenuation factors result in diminished signal strength, heightened bit error rates, and diminished link ranges. The extent of the fog impact hinges on the density and thickness of the fog [15]. The attenuation, $\propto$, in dB/km caused by fog is expressed as

$$\propto = \frac{3.912}{B} \left(\frac{\lambda}{550nm} \right)^{-z} \tag{17}$$

where B and λ are visibility range in km and wavelength in nm, respectively, while f is the size distribution of the scattering particles and its value depend on B, and according to Kim model, it can be expressed as [15]

$$f = \begin{cases} 1.6 & B > 50 \\ 1.3 & 6 < B < 50 \\ 0.16\,B + 0.34 & 1 < B < 6 \\ B - 0.5 & 0.5 < B < 1 \\ 0 & B < 0.5 \end{cases} \tag{18}$$

The attenuation values for different levels of haze and fog are presented in Fig. 3 [15], [29].

The power level of the received optical signal that carries the image is affected by the attenuation caused by the fog conditions. The received power, P_{Rec} (dBm), is expressed as [30], and [31]

$$P_{Rec} = P_{Tra} \left(\frac{D_{Rec}}{D_{Tra} + \theta L_{ch}} \right)^2 10^{\frac{-\alpha L_{ch}}{10}} \tag{19}$$

where P_{Tra} (dBm) is the transmitted power, D_{Tra} (cm) and D_{Rec} (cm) are the aperture diameters of the transmitter and receiver telescopes, respectively, L_{ch} (km) is the propagation range of FSO channel, and θ is the beam divergence angle.

Further, to convert the received optical signal back to the electrical domain, a positive over intrinsic negative (PIN) photodetector (PD) is used. Additionally, a low pass filter (LPF) is used to filter the signal. Finally, data recovery is used to convert an electrical signal into binary bits, which are converted into an image. Moreover, decryption is done to recover the original image. Median and high pass filters are used to enhance the view of the decrypted image.

The output electrical signal from the PD, E_{PD}, is expressed as [32]

$$E_{PD} = P_{Rec}\Re + n(t) \tag{20}$$

where $\Re$ is the responsivity of the PIN and $n(t)$ represents the total noise received with variation given as [33]

$$\sigma_v^2 = \frac{1}{2} N_o \tag{21}$$

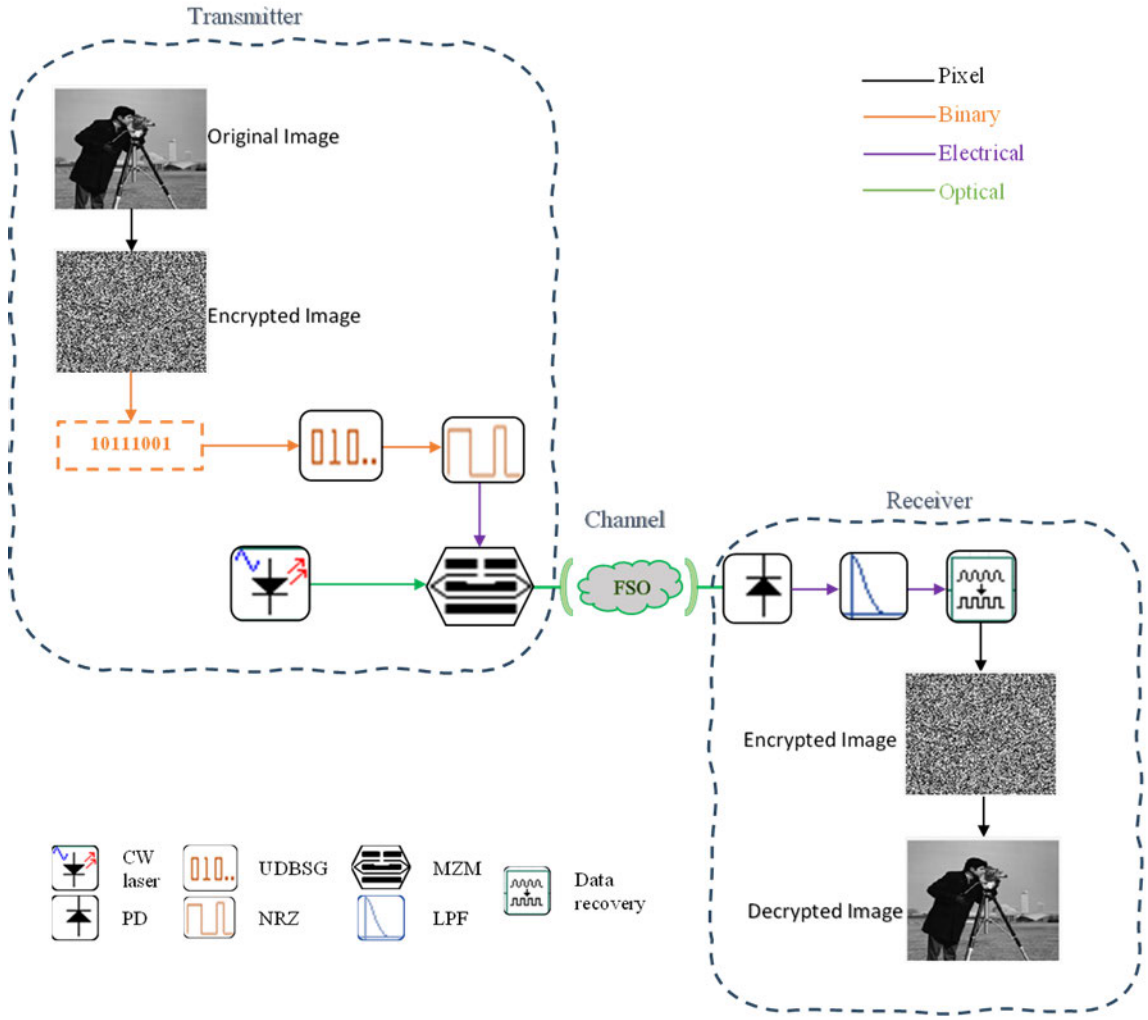


FIGURE 2. Schematic diagram for proposed image transmission over FSO channel.

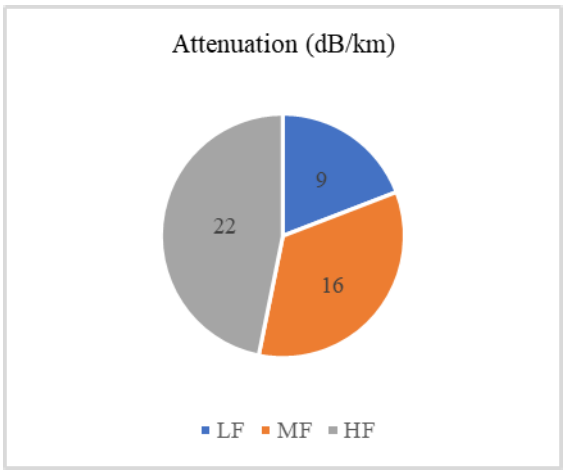


FIGURE 3. Attenuation for various levels of fog.

where N_o is the power spectral density of all noise sources including shot noise, σ_{sh}^2, relative intensity noise, σ_{RIN}^2, and thermal noise, σ_{th}^2 given by [34]

$$N_o = \sigma_{sh}^2 + \sigma_{RIN}^2 + \sigma_{th}^2 \tag{22}$$

where σ_{sh}^2, σ_{RIN}^2, and σ_{th}^2 are expressed as [31], and [34]

$$\sigma_{sh}^2 = 2e(I_{PD} + I_D)\nu \tag{23}$$

$$\sigma_{RIN}^2 = N_{RIN}\,(I_{PD})^2 \tag{24}$$

$$\sigma_{th}^2 = \frac{4k_B T_a \nu}{R_l} \tag{25}$$

where e, I_D, ν, N_{RIN}, k_B, R_l, and T_a are electron charge (C), dark current (nA), noise bandwidth (Hz), relatively intensity noise (dB/Hz), Boltzmann constant (J/K), receiver load resistance (Ω), and temperature (K), respectively. I_{PD} denotes the output current of the PD and it is expressed as

$$I_{PD} = P_{Rec}\Re \tag{26}$$

Hence, the SNR can be expressed as [34]

$$SNR = \frac{(I_{PD})^2}{N_o} \tag{27}$$

VI. RESULTS AND DISCUSSION

The proposed model is simulated using both Matlab and OptiSystem software using the parameter described in Table 1.

TABLE 1. Systems Parameters values.

Parameter	Value (unit)
Image dimension	128×128
Sequence length	2^{17} bits
P_{Tra}	15 dBm
R_b	10 Gbps
a_m	1 V
λ	1550 nm
D_{Tra}	5 cm
θ	2 mrad
D_{Rec}	20 cm
$\Re$	0.8 A/W
I_D	10 nA
ν	0.7×R_b HZ
N_{RIN}	-130 DB/HZ
T_a	300 K
R_l	50 Ω

The results in this section is divided into two parts. The first part shows the effect of various ranges in foggy weather on the system's performance. The security analysis is discussed in the second part.

A. IMPACT OF VARIOUS FSO RANGES ON THE RECEIVED IMAGE IN THE PRESENCE OF FOGGY WEATHER

The propagation range in the free space channel affect the performance and the quality of the received images due to the impact of LF, MF, and HF. Figure 4 show the original image and the cipher image that are transmitted over the FSO channel.

(a) (b)

FIGURE 4. Transmitted images (a) Original image and (b) Cipher image.

1) LOW FOG

As LF has the lowest attenuation value, the image can propagate over a longer range in the FSO channel. Figure 5 displays the received images when they are transmitted in their original form and the cipher form at various FSO spans under LF condition. It can be observed that as the traveling distance increases, the quality of the image becomes poorer. The view of the received image is very clear at 1776 m FSO range, but it starts degrading until it become black when the FSO link reaches 1798 m.

Figure 6 depicts the images under low levels of fog at various FSO ranges after decrypting, while Fig. 7 shows them after applying enhancement technique to them. It is noticed when comparing the received images when plain image is transmitted in Fig. 5 with Fig. 6, the quality of decrypted images is much better. This is because the employed CFI encryption algorithm offers a high level of security, safeguarding the data as it traverses the FSO channel. This security measure facilitates the subsequent retrieval of the original data at the receiver's end. Moreover, the utilization of median and high pass filters in combination is effectively enhancing the image clarity, mitigate noise, and augment visual attributes, thereby leading to a comprehensive enhancement of image quality. The enhancement process is used after decrypting the images, and the resulting visual images are shown in Fig. 7. The quality of images is enhanced at 1798 m.

Figure 8 shows the calculated SNR for the received images versus FSO ranges under the effect of LF. For shorter ranges (from 1776 nm to 1782 nm), it is seen that the three received images nearly have the same SNR values. Also, as the FSO ranges increase, the SNR decreases, and the use of median and high pass filters leads to enhanced images with higher SNR at longer FSO ranges. At SNR $\sim$ 12 dB, the FSO range of 1784 m is achieved when the original image is transmitted. This range is increased to 1789 m when a cipher image is sent, and a range of 1796 m is obtained when median and high pass filters are used for enhancing the images.

To evaluate the visual quality of restored images, the SSIM is employed. It is considered as a metric for assessing the quality of experience (QoE) and is expressed as [35], and [36]

$$\mathrm{SSIM}(O,R)=\frac{(2\mu_O\mu_R+C_1)\,(2\sigma_{OR}+C_2)}{\left(\mu_O^2+\mu_R^2+C_1\right)\left(\sigma_O^2+\sigma_R^2+C_2\right)} \tag{28}$$

where O and R denote the original image that is transmitted and received image, respectively, $\mu_O$and μ_R are the means, σ_O^2 and σ_R^2 represent the standard deviations, σ_{OR} is the cross covariance for the O and R images, and C_1 and C_2 are constants.

Figure 9 illustrates the impact of FSO ranges on SSIM values under LF condition. It is clear from Fig. 9 that as the optical signal that carries the image travelling long ranges, the SSIM values degrades and the enhanced received images have the higher SSIM values. At 1776 m, all received images have SSIM = 1, while this value decreases to 0.06, 0.18, and 0.2951 for received image when original image is transmitted without encryption, when original image is encrypted, and when enhancing technique is used for the encrypted image, respectively.

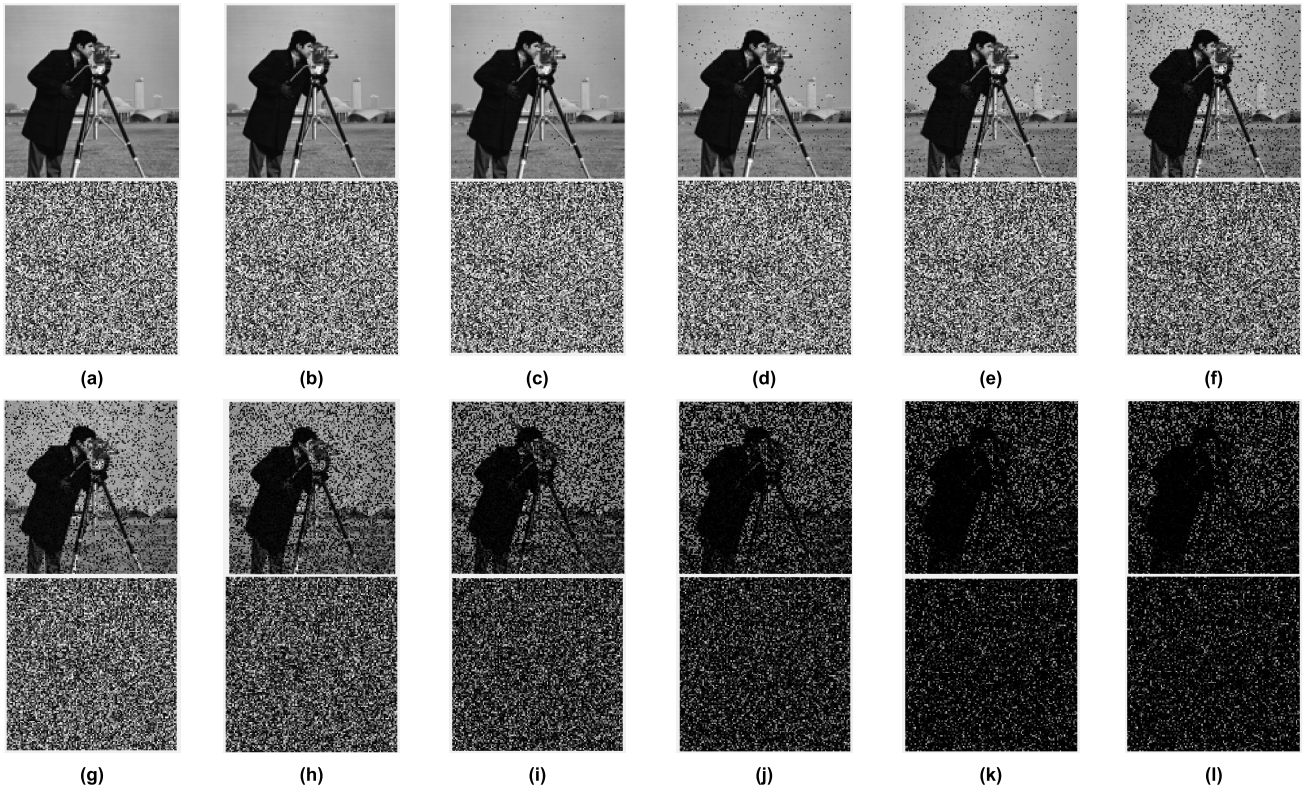


FIGURE 5. View of received images when transmitted in its original and cipher forms under LF condition at (a)1776 m, (b) 1778 m, (c) 1780 m, (d) 1782 m, (e) 1784 m, (f) 1786 m, (g) 1788 m, (h) 1790 m, (i) 1792 m, (j) 1794 m, (k) 1796 m, and (l) 1798 m.

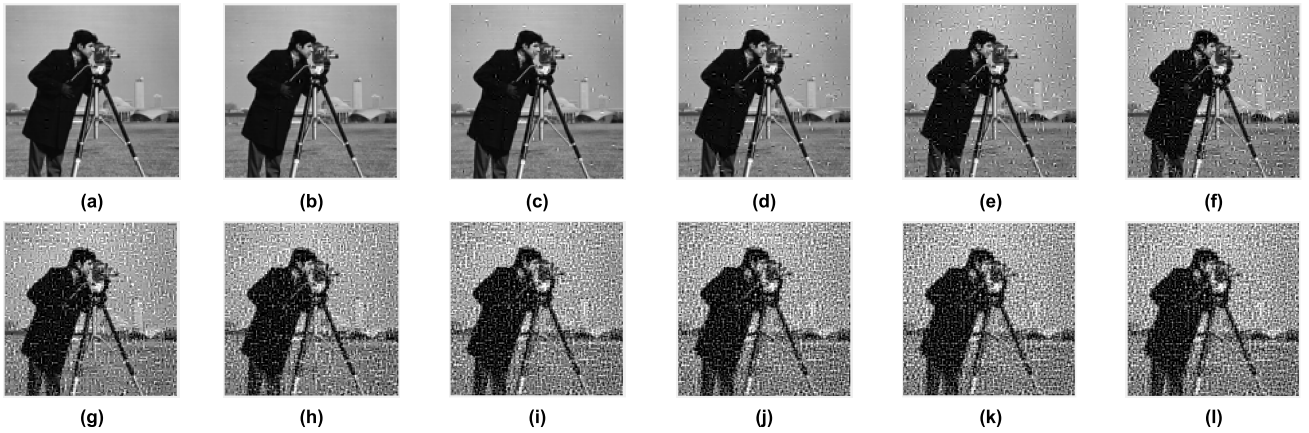


FIGURE 6. View of decrypted images under LF condition at (a)1776 m, (b) 1778 m, (c) 1780 m, (d) 1782 m, (e) 1784 m, (f) 1786 m, (g) 1788 m, (h) 1790 m, (i) 1792 m, (j) 1794 m, (k) 1796 m, and (l) 1798 m.

2) MEDIUM FOG

The MF weather condition causes higher attenuation than LF, leading to a shorter FSO link. Figures 10-12 show the quality of images received at different FSO spans under moderate levels of fog. It is observed that decrypted images and enhanced images show better qualities for images at all ranges than the original images received as in the LF. However, the FSO range is shorter.

Figure 13 illustrates the calculated SNR in relation to FSO ranges for the received images under the influence of MF condition. In the case of distances in the range from 1190 nm to 1194 nm, the SNR values for the three received images are approximately identical. Moreover, with the expansion of FSO ranges, there is a discernible reduction in SNR, while the application of median and high-pass filters results in improved images displaying higher SNR levels over extended FSO ranges. It can be noticed that at 1206 m, the SNR improved from -21.8 dB to 12.6 dB when median and high-pass filters applied to the decrypted image.

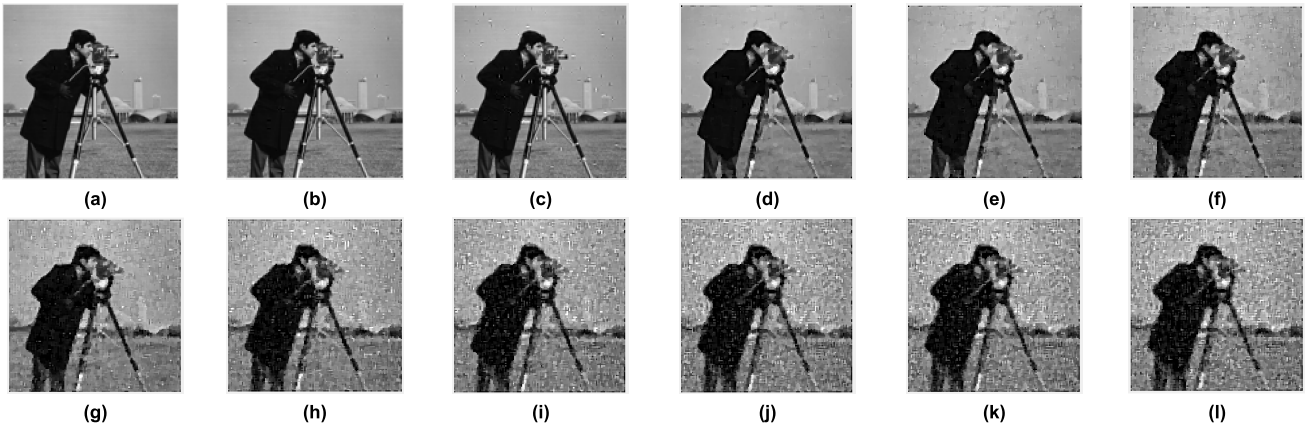


FIGURE 7. Enhanced images under LF condition at (a)1776 m, (b) 1778 m, (c) 1780 m, (d) 1782 m, (e) 1784 m, (f) 1786 m, (g) 1788 m, (h) 1790 m, (i) 1792 m, (j) 1794 m, (k) 1796 m, and (l) 1798 m.

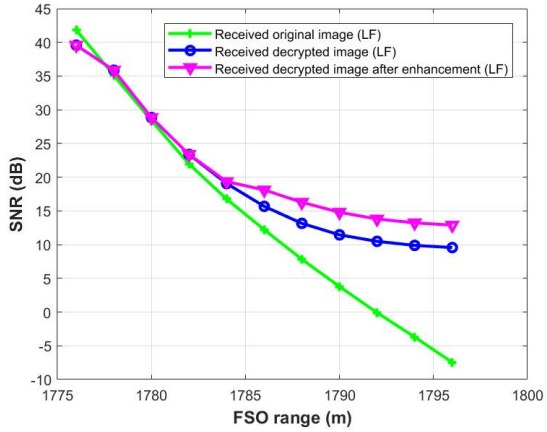


FIGURE 8. SNR versus various FSO ranges under LF condition.

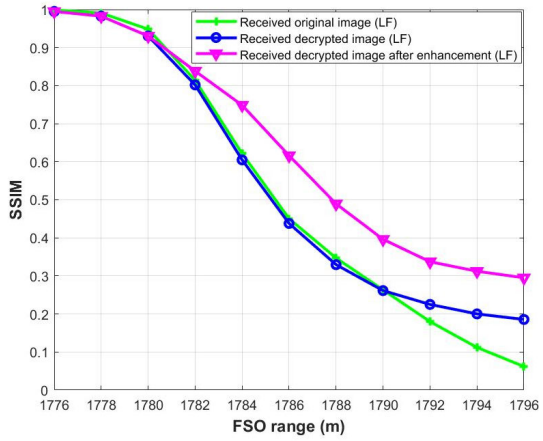


FIGURE 9. SSIM versus various FSO ranges under LF condition.

Further, the influence of FSO ranges on the SSIM values in the presence of MF condition is depicted in Fig. 14. When the image is transmitted without encryption, the received image is distorted at higher ranges, and the SSIM at 1206 m for this case is zero. Using the CFI algorithm for encrypting the original image leads to an increase in the SSIM value compared to the original transmitted image without encryption. At the same range, applying filters after the decryption process leads to more improvement in the value of SSIM (0.29).

3) HEAVY FOG

Larger attenuation is caused when the level of fog become heavier. Consequently, shortest transmission ranges occurred. The results presented in Table 2 illustrate the image quality within the range of 941 m to 953 m for different image transmission conditions. It is evident that the image quality remains satisfactory until a range of 947 m when transmitting an unencrypted image. Conversely, when the received image is encrypted and subjected to the decryption process, visual clarity persists up to an FSO range of 957 m. Furthermore, image enhancement achieves an improved viewing experience.

The performance in terms of SNR and SSIM are presented for HF condition in Figs. 15 and 16, respectively. As ranges between transmitter and receiver increase, the SNR and the SSIM decrease, while using filters enables the enhanced image to achieve higher SNR and SSIM values. At 953 m, a SNR improvement of 25.4 dB (from −12.7 dB to 12.7 dB) and a SSIM enhancement of 0.26 (from 0.02 to 0.28) are achieved.

Table 3 shows a comparison between previous works on image transmission in FSO channel and proposed model.

B. SECURITY ANALYSIS OF IMAGE ENCRYPTION

1) HISTOGRAM ANALYSIS

The histogram analysis for both original and encrypted images are investigated in this study. From a statistical viewpoint, the two images are structurally different. The histogram of the original image has tilts and spikes, which is different from the flat and uniform histogram of the cipher image. As such, the two images are statistically different. For the different sub-bands, the histogram of the images encrypted

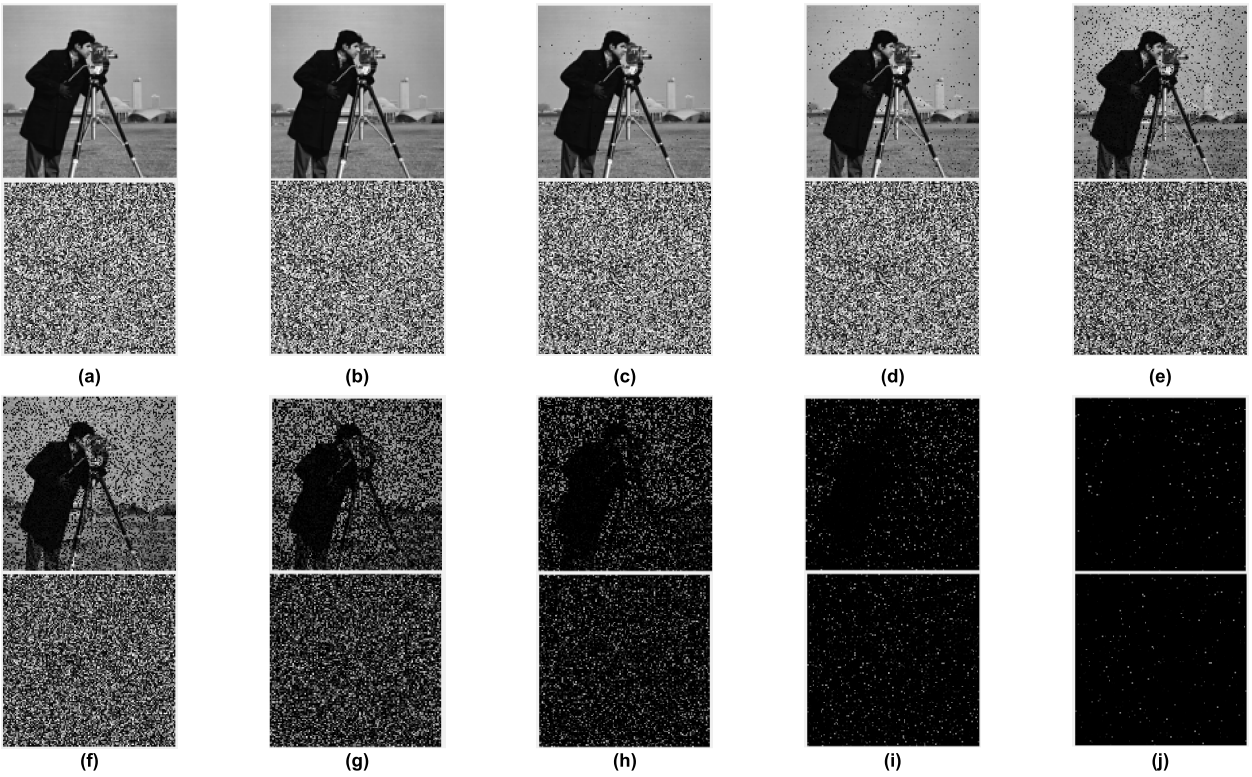


FIGURE 10. View of received images when transmitted in its original and cipher under MF condition at (a) 1188 m, (b) 1190 m, (c) 1192 m, (d) 1194 m, (e) 1196 m, (f) 1198 m, (g) 1200 m, (h) 1202 m, (i) 1204 m, and (j) 1206 m.

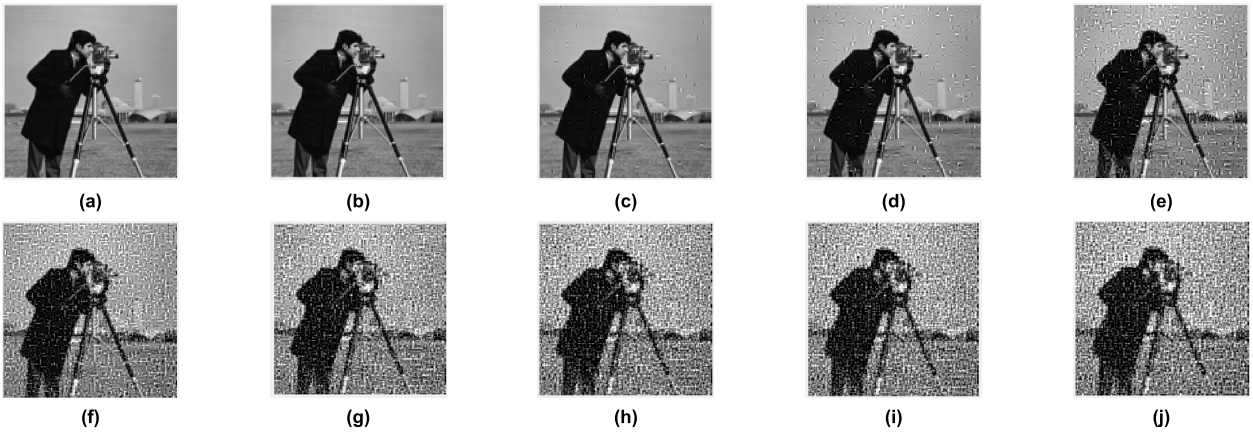


FIGURE 11. View of decrypted images when transmitted in its original under MF condition at (a)1188 m, (b) 1190 m, (c) 1192 m, (d) 1194 m, (e) 1196 m, (f) 1198 m, (g) 1200 m, (h) 1202 m, (i) 1204 m, and (j) 1206 m.

with the proposed algorithm can be seen in Fig. 17. Figure 18 shows the histograms of different original images and their encrypted versions, coded with the help of the algorithm described in this work. The results demonstrated the randomness of the images encrypted using the proposed algorithm. Quantity analysis of the images checks the uniformity of the image, while calculating the variance (x) of its histogram. The number of pixels whose gray value is equal to i is represented by x_i, as for x_j, it is the number of pixels whose gray value is equal to j. As for variance (x), it can be calculated using equation 16 as follows [37], and [38]:

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

Uniformity of the image is demonstrated when the calculated variance (x) of the cipher image is of a small value. Table 4 shows the value of the calculated variance (x) for the encrypted images. Results seen in Table 4 indicate that the histogram of the encrypted image is uniform, as the simulation of encryption was done on the original images.

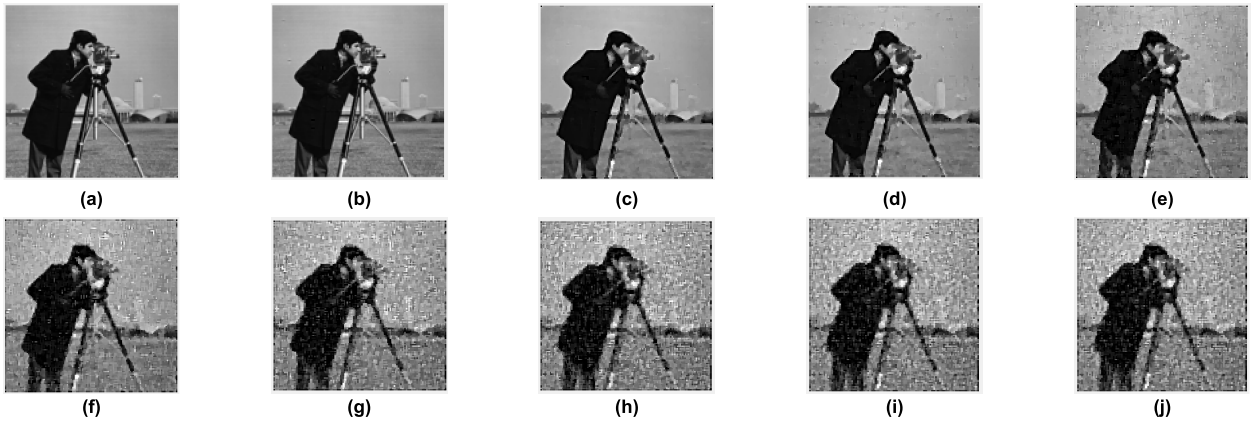


FIGURE 12. View of enhanced images when transmitted in its original under MF condition at (a) 1188 m, (b) 1190 m, (c) 1192 m, (d) 1194 m, (e) 1196 m, (f) 1198 m, (g) 1200 m, (h) 1202 m, (i) 1204 m, and (j) 1206 m.

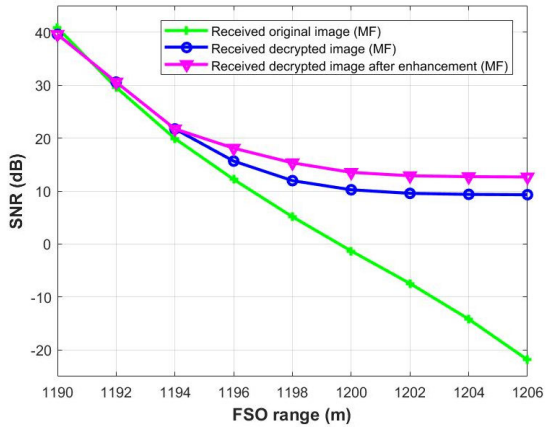


FIGURE 13. SNR versus various FSO ranges under MF condition.

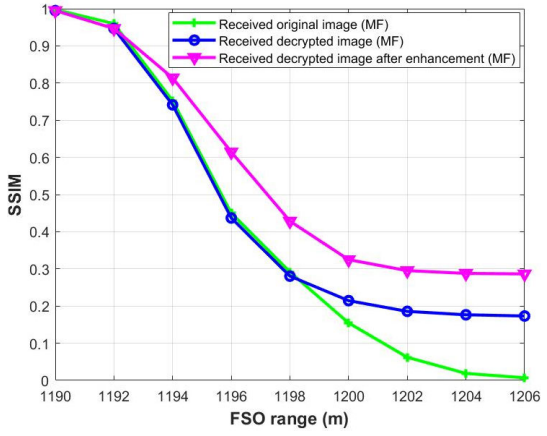


FIGURE 14. SSIM versus various FSO ranges under MF condition.

Moreover, Table 4 shows the comparison between proposed CFI algorithm and other algorithms. It can be seen that the variance values of the proposed algorithm are lower than other schemes. Therefore, the proposed scheme is more robust to resist the statistical attacks.

2) INFORMATION ENTROPY ANALYSIS

The uncertainty of the information of an image is measured using the entropy. It is also used to check the gray distribution value of the image. The values of information entropy fall between zero and eight, with 8 being the optimum value. As such, an encryption scheme is deemed effective when the image has an entropy close to eight. To calculate information entropy, Eq. (30) is used [18], [19], [43]:

$$E = \sum_{i=1}^{N-1} P(X_i) log_2 P(X_i) \tag{30}$$

where, N is the total number of (X), while $P(X_i)$ is the possibility of its occurrence. In Table 5 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, yielding the best of all the results other algorithm compared.

3) CORRELATION COEFFICIENT

Correlation analysis is undertaken to check for similarities between an encrypted image and its original version. Adjacent pixels are usually similar, thus there is a high correlation between them. This correlation can be broken by an effective encryption algorithm. As such, a low correlation value between adjacent pixels, i.e., zero or close, is a sign of an effective encryption scheme. Equation 31 is used to calculate the correlation coefficient for the three directions: vertical, horizontal, and diagonal [18], [19], [45]:

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{31}$$

where, r_{xy}, cov, $D(x)$, and $E(x)$ are the correlation coefficient, the covariance between pixel (x) and pixel (y), the variance, and the mean, respectively. As for (x) and (y), they represent the grayscale value of a specific pixel on the plaintext and on the encrypted text image, respectively.

TABLE 2. Received images under HF condition for FSO ranges from 941 m to 957 m.

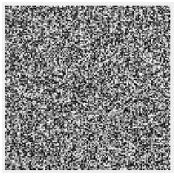
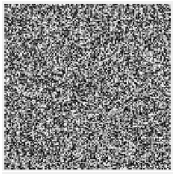
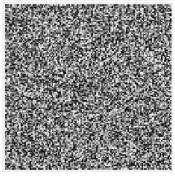
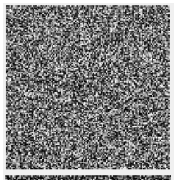
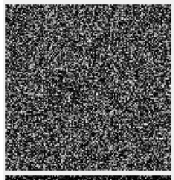
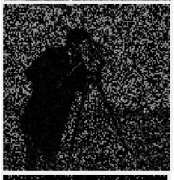
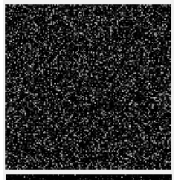
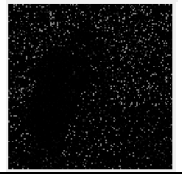
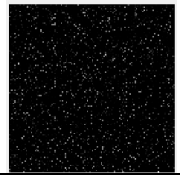
Received Images	When original image transmitted	When cipher image transmitted	After decrypting the received cipher image	Enhanced after applying filters
At 941 m				
At 943 m				
At 945 m				
At 947 m				
At 949 m				
At 951 m				
At 953 m				

Figure 19 shows the correlation between two adjacent pixels on the original and encrypted images, for the horizontal, vertical, and diagonal directions. When the cipher image is checked, the pixel correlation had become significantly smaller. Table 6 shows the correlation coefficients for images encrypted with the proposed scheme. In contrast, the correlation coefficient for original images was approximately one. As such, it can be concluded that the encryption algorithm proposed in this research has not only decreased the correlation coefficient but also brought its value close to zero (better than after applying other algorithms). This means that the suggested algorithm can cause a decrease in the correlation between two side by side pixels in the encrypted image.

4) DIFFERENTIAL ATTACK

The number of pixel change rate (NPCR) and the unified average changing intensity (UACI) are two measured metrics used to evaluate the difference between a specific bit in both the original and cipher images. NPCR is calculated by using Eq. (32), while Eq. (33) is used to calculate

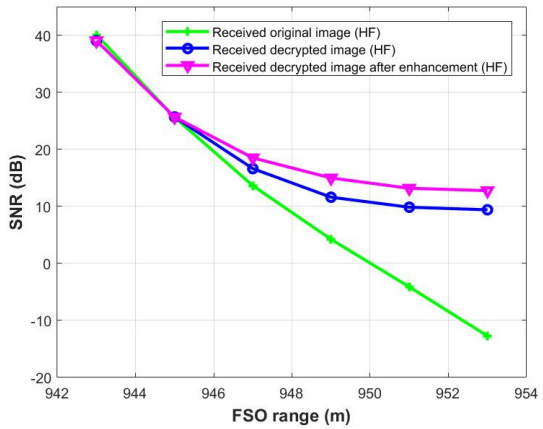


FIGURE 15. SNR versus various FSO ranges under HF condition.

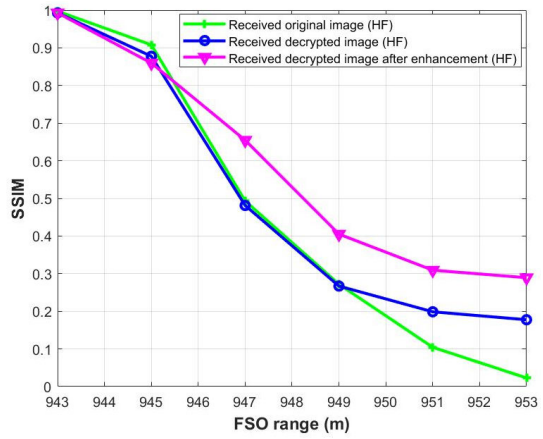


FIGURE 16. SSIM versus various FSO ranges under HF condition.

TABLE 3. Comparison between previous works and present work.

Reference	Ref [26]	Ref [27]	Ref [28]	Present work
Technique	OOK	OOK	QPSK	OOK
Encryption algorithm	NA	NA	NA	CFI
Weather condition (range)	MR (2640 m) HR (1925 m)	LF (1200 m) MF (550 m) HF (93 m)	LF (1400 m) MF (630 m) HF (320 m)	LF (1798 m) MF (1206 m) HF (320 m)
Enhancement techniques	Median filter	NA	NA	Median and high pass filters
Data rate	10 Gbps	10 Gbps	10 Gbps	10 Gbps

UACI [39], [46]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{32}$$

$$UACI = \frac{\sum_{i,j} E_1(i,j) - E_2(i,j)}{255 \times M \times N} \times 100\% \tag{33}$$

where, W is the width of the cipher image, while H is its height. $C_1(i,j)$ and $C_2(i,j)$ are representations of the cipher image, with the former prior to the single bit change, while the latter is after this change. Table 7 lists the values for both UACI and NPCR. It can be noted that they are close to the optimum values for each variable. In general, NPCR is 99.6094%, while UACI is 33.4635%. This shows the scheme's sensitivity to even slight modifications in the original image.

5) CONTRAST

The contrast measures the variation in intensity between neighboring pixels. An encryption scheme is effective when the value of contrast is high. Contrast can be calculated through Eq. 34 [19]:

$$Contrat = \sum |i-j|^2 P(i,j) \tag{34}$$

where, $p(i,j)$ marks the location of a specific pixel in the grey-level co-occurrence matrix (GLCM). Contrast values for images encrypted with the scheme in this study are shown in Table 8.

6) KEY SENSITIVITY ANALYSIS

Being sensitive towards its key makes the encryption scheme able to prevent brute-force attacks. Testing key sensitivity begins by encrypting an original image using a certain key, then applying a minuscule change to this key and using it to decrypt the encrypted image [48]. CFI's initial parameters, including the external key and the secret image, form the initial key for the encryption scheme. By changing the initial parameters of CFI, a change takes place in the specificity of the generated code. To begin, a single bit in the key is changed. This is followed by the application of Gaussian noise to the secret image. This minute change can lead to differences between plaintext and decrypted images. Figure 20 shows an original image and a decrypted version using the correct key, while the remaining two are also cipher images, but decrypted with incorrect keys. This algorithm proved to be sensitive to its key, as an insignificant change led to a decrypted image that is different from the original, which was never regained.

7) NIST TEST SUITE ANALYSIS

The NIST test is employed to assess the randomness of a binary sequence. This test comprises a set of 15 statistical tests grouped together. The condition for a sequence to be considered random is that the P-value for each individual test exceeds 0.01 [49]. Table 9 is presented, displaying the results of applying the NIST test to four fuzzy random sequences in comparison to a random sequence generated from a chaotic map. It is evident from the table that the tests were successfully passed by the sequences.

8) CHI-SQUARE TEST ANALYSIS

In order to quantitatively assess the uniformity of gray pixel values, the analysis of the Chi-square test is performed. A smaller Chi-square value is indicative of a higher level of

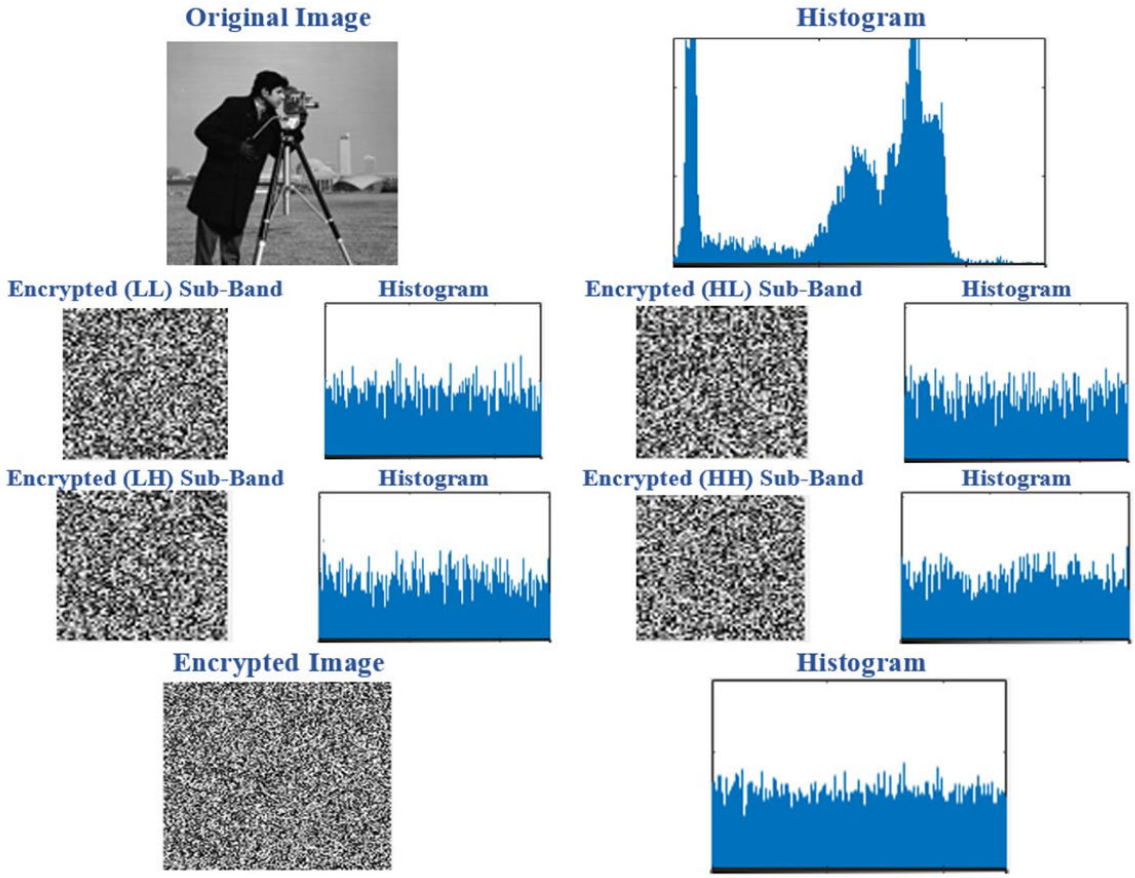


FIGURE 17. Histogram analysis for images resulting from each sub-band of the encryption.

TABLE 4. Variance values for the histogram analysis of different cipher images.

Algorithm	Images	Histogram Variance
Proposed work	Lena	223.5392
	Baboon	235.3325
	Cameraman	241.9827
	Boat	233.5642
	Truck	238.3369
	Peppers	245.5698
	Tree	250.0712
	Airplane	244.6245
Ref [39]	Lena	231.97
Ref [40]	Cameraman	269.0859
Ref [41]	Lena	853.37
Ref[42]	Peppers	898.98

TABLE 5. Information entropy analysis.

Algorithm	Images	Information entropy analysis
Proposed work	Lena	7.9985
	Baboon	7.9986
	Cameraman	7.9984
	Boat	7.9988
	Truck	7.9972
	Peppers	7.9987
	Tree	7.9952
	Airplane	7.9991
Ref [39]	Cameraman	7.9973
Ref [40]	Lena	7.9968
Ref [41]	Lena	7.9977
Ref [44]	Airplane	7.9971

uniformity in the grayscale distribution [19]. The results of the Chi-square test for the cipher images can be observed in Table 10.

9) ROBUSTNESS TEST

The proposed algorithm was subjected to various attacks for testing purpose, such as salt and pepper noise and occlusion attack. In this study, the quality of the decrypted image is analyzed by measuring the Peak SNR (PSNR) and comparing it with the original plain-image. A higher PSNR value indicates minimal distortion in the plain image. The outcomes are listed in Table 11 which shows the PSNR values of the decrypted images as the encrypted images are attacked by various image operations. The robustness of the proposed algorithm is explained by the results shows that the decrypted images are still identifiable in spite of the cipher-image

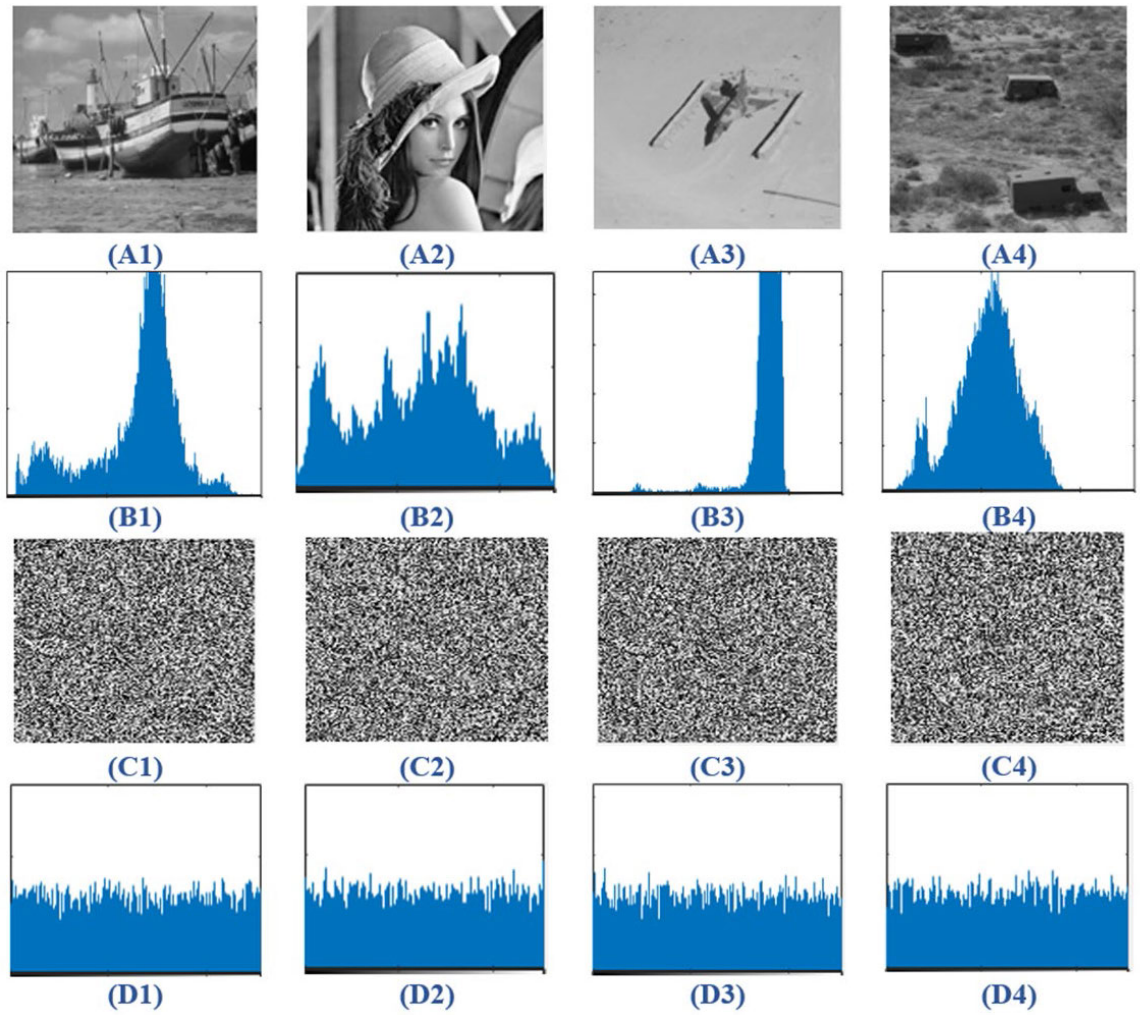


FIGURE 18. Histogram of original and encrypted images; (A1) - (A4) The original images; (B1) - (B4) The histogram of original images; (C1) - (C4) The encrypted images; (D1) - (D4) The histogram of encrypted images.

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
Proposed work	Lena	0.9729	2.0557e-04	0.9463	0.00045	0.9402	0.00063
	Baboon	0.8736	0.00024	0.8261	0.00013	0.8132	0.00076
	Cameraman	0.9592	0.00043	0.9335	0.00035	0.9452	0.00172
	Boat	0.9268	0.00057	0.9452	0.0045	0.9152	0.00342
	Truck	0.9477	0.00012	0.8955	0.00092	0.8745	0.00136
	Peppers	0.9634	7.0325e-04	0.9704	9.0256e-04	0.9014	0.00035
	Tree	0.9682	7.6542e-04	0.9451	0.00028	0.9312	0.00284
	Airplane	0.9166	0.000345	0.9318	6.7686e-04	0.9621	0.00253
Ref [39]	Lena	NA	0.002	NA	-0.0005	NA	-0.0009
Ref [40]	Cameraman	NA	0.02245	NA	-0.00744	NA	0.00388
Ref [41]	Peppers	NA	-0.0009	NA	0.0044	NA	0.00019
Ref [44]	Airplane	NA	0.0385	NA	0.0546	NA	0.0132

being distorted. Test result shows when the encrypted image is added salt and pepper noise as displayed in Fig. 20, as well as occlusion attack shown in Fig. 21, we can still decrypt the encrypted image. PSNR can be measured as the following

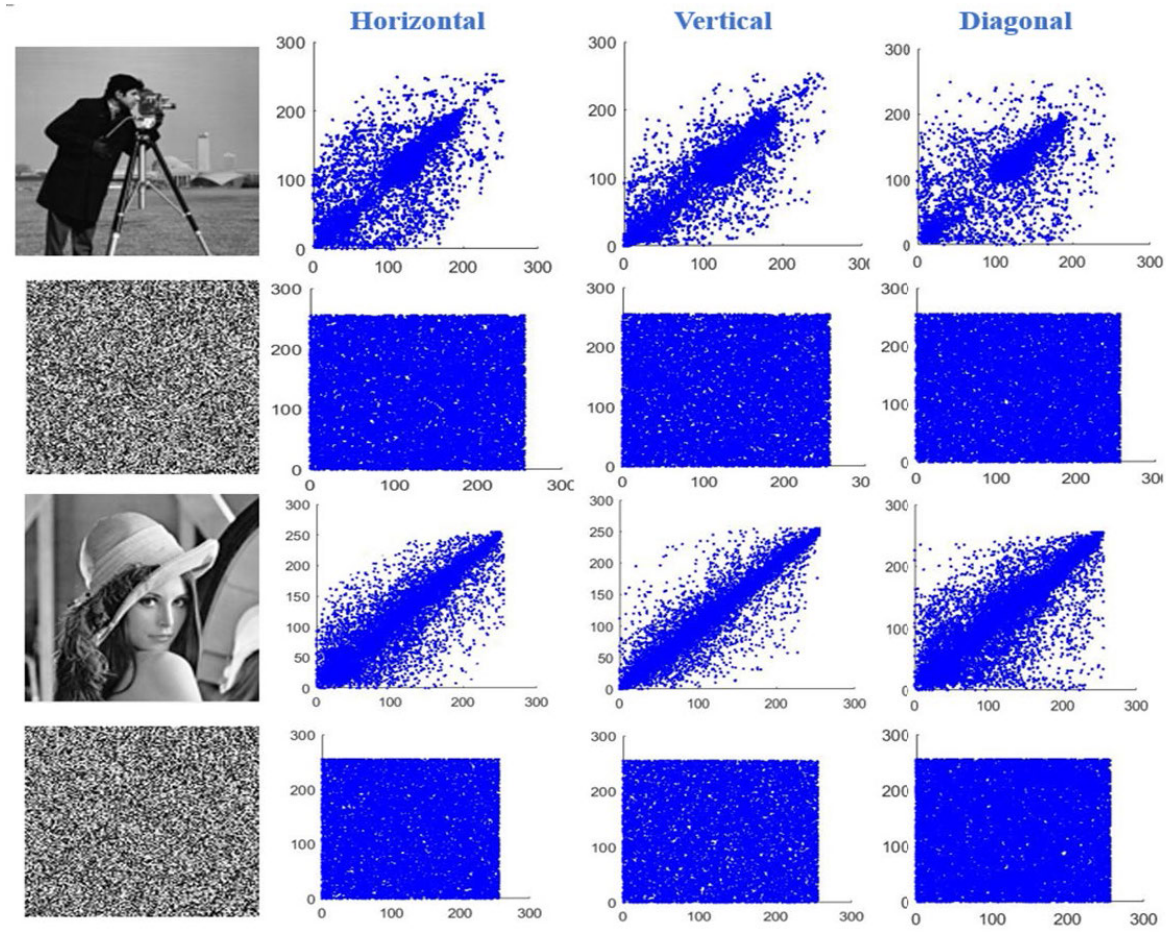


FIGURE 19. Correlation of two adjacent pixels of the original and its encrypted image.

TABLE 7. npcr and uaci for different images.

Algorithm	Images	NPCR	UACI
Proposed work	Lena	99.61	33.44
	Baboon	99.58	33.45
	Cameraman	99.61	33.46
	Boat	99.59	33.43
	Truck	99.62	33.45
	Peppers	99.57	33.42
	Tree	99.62	33.44
	Airplane	99.63	33.42
Ref[39]	Cameraman	99.65	33.60
Ref[40]	Lena	99.62158	33.56123
Ref[47]	Cameraman	99.5575	33.4745

TABLE 8. Contrast of cipher images.

Algorithm	Images	Contrast
Proposed work	Lena	10.83668
	Baboon	10.79885
	Cameraman	10.86529
	Boat	10.80353
	Truck	10.85690
	Peppers	10.7845
	Tree	10.8536
	Airplane	10.86511

formula [50]:

$$PSNR = 10\log\left[\frac{M \times N \times 255^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}[P(i,j) - D(i,j)]^2}\right] \quad (35)$$

where M and N represent the length and width of the image, respectively. $P(i,j)$ represents the pixel value of an original image, and $D(i,j)$ represents the pixel value of the decrypted image.

Finally, we can say that the pros of using the proposed cipher image transmission in the FSO channel are multi-faceted. It not only ensures the protection of data during transmission but also significantly enhances the image quality. This is evident through the positive values achieved for SSIM and SNR, which are crucial indicators of image quality. Moreover, the method allows encrypted images to be transmitted over longer distances in FSO channels, making it suitable for various applications. The CFI algorithm

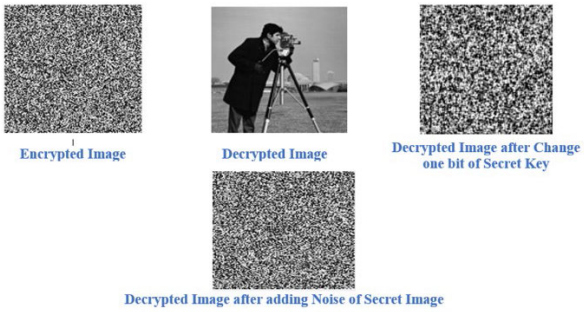


FIGURE 20. Results of key sensitivity of the proposed image cryptosystem.

TABLE 9. Nist test results of four fuzzy random sequences.

Test Index	P-Value (Four Random Sequences)				Ref [49]
	C_1	C_2	C_3	C_4	
Longest Run of Ones	0.91585	0.97487	0.84585	0.90599	0.21330
Run Test	0.90637	0.97487	0.84323	0.86737	0.12232
Serial Test	0.98561	0.36220	0.95348	0.98561	0.35048
Random Excursions Variant	0.80090	0.91173	0.98649	0.943345	NA
Random Excursions	0.62753	0.64709	0.88813	0.98657	NA
Non-overlapping Template	0.94337	0.89983	0.53946	0.56090	0.73991
Frequency Test within blocks	0.97248	0.95122	0.94912	0.92422	0.73991
Frequency Test	0.97088	0.950552	0.93091	0.92488	0.53414
Cumulative Sum Reverse	0.90814	0.98391	0.88219	0.98657	0.91141
Cumulative Sum	0.69632	0.92263	0.75526	0.82771	0.91141
Approximation Entropy	0.98561	0.92317	0.89249	0.76820	0.53414
Linear Complexity	0.67358	0.98052	0.48469	0.31854	0.73991
Rank Test	0.74190	0.550428	0.0.681248	0.576146	0.91141

TABLE 10. Chi-square test of cipher images.

Algorithm	Images	Chi-Square Test
Proposed work	Lena	219.4652
	Baboon	223.3592
	Cameraman	233.9254
	Boat	225.2398
	Truck	230.3365
	Peppers	233.6541
	Tree	235.6982
	Airplane	228.4456

adds another layer of strength to the system by providing efficacy against attacks and robust security measures. However, it's important to note that there are some limitations to consider. While the method extends the transmission range

TABLE 11. Psnr of decrypted image after different operations.

Tests	PSNR (dB)
Salt and Pepper Noise (0.005)	37.0784
Salt and Pepper Noise (0.05)	27.2505
Salt and Pepper Noise (0.1)	24.4869
Occlusion (First Block)	47.1456
Occlusion (Second Block)	26.0965
Occlusion (Third Block)	18.8177

FIGURE 21. Decrypted images under salt and pepper noise with (a) 0.005, (b) 0.05, and (c) 0.1.

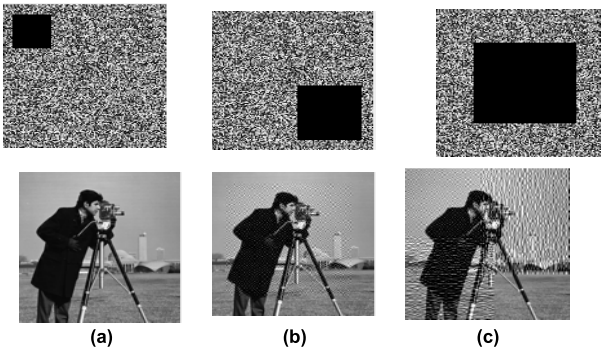


FIGURE 22. Occlusion attacks analysis results (a) first block, (b) second block, and (c) third block.

in FSO, it may still require further enhancement to optimize image quality. This is achieved through the application of median and high pass filters, which, while effective, add an additional processing step to the system.

VII. CONCLUSION

An effective and secure image encryption based on CFI algorithm is proposed and used in the transmission of images over FSO channel under foggy weather condition. The algorithm is characterized by high level of confidentiality and complexity. Several metric analyses are investigated to validate that the proposed cryptosystem has high level of resistance against any attacks. These analyses are correlation coefficient, histograms, entropy, contrast, differential attacks, and key sensitivity analysis. Furthermore, median and high pass filters are used after employing decryption process to improve the visuality of the received image. The impact of different attenuations caused by various levels of fog on the optical signal that carries the images during travelling in free space is considered. Additionally, the system performance is investigated when plain and cipher images are transmitted.

The SNR, FSO link range, and SSIM are metrics used in the evaluation of the system. The results demonstrated that the images received when they are encrypted has better quality. As an example, the decrypted image has a SNR of approximately 12 dB at 1789 m in LF channel while for the original image received, the same SNR is achieved at 1784 m. Moreover, using filters after decryption making an enhancement to the received image. As an example, for MF channel, the SSIM value increased from 0.18 to 0.29 for FSO channel span of 1206 m. Consequently, our proposed image transmission can be used in military services that required high speed and secure transmission and in areas where the implementation of optical fibers is costly and difficult.

REFERENCES

[1] 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.

[2] *Cisco Annual Internet Report (2018–2023); White Paper*, Cisco Syst., San Jose, CA, USA, 2022. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[3] (Feb. 2021). *Cisco Visual Networking Index: Forecast and Trends 2017–2022*. [Online]. Available: https://cloud.report/whitepapers/ciscovisual-networking-index-forecast-and-trends-2017-2022/9017

[4] 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, Jan. 2023, doi: 10.1002/dac.5426.

[5] E. Leitgeb, "Future applications of optical wireless and combination scenarios with RF technology," in *Proc. 40th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, Opatija, Croatia, 2017, pp. 404–406, doi: 10.23919/MIPRO.2017.7973457.

[6] M. Z. Chowdhury, Md. T. Hossan, A. Islam, and Y. M. Jang, "A comparative survey of optical wireless technologies: Architectures and applications," *IEEE Access*, vol. 6, pp. 9819–9840, 2018, doi: 10.1109/ACCESS.2018.2792419.

[7] 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.

[8] T. Richter, E. Palushani, C. Schmidt-Langhorst, R. Ludwig, L. Molle, M. Nolle, and C. Schubert, "Transmission of single-channel 16-QAM data signals at terabaud symbol rates," *J. Lightw. Technol.*, vol. 30, no. 4, pp. 504–511, Feb. 15, 2012, doi: 10.1109/JLT.2011.2174029.

[9] P. T. Dat, A. Kanno, N. Yamamoto, and T. Kawanishi, "Seamless convergence of fiber and wireless systems for 5G and beyond networks," *J. Lightw. Technol.*, vol. 37, no. 2, pp. 592–605, Jan. 15, 2019, doi: 10.1109/JLT.2018.2883337.

[10] M. Singh, A. Atieh, M. H. Aly, and S. A. A. El-Mottaleb, "120 Gbps SAC-OCDMA-OAM-based FSO transmission system: Performance evaluation under different weather conditions," *Alexandria Eng. J.*, vol. 61, no. 12, pp. 10407–10418, Dec. 2022, doi: 10.1016/j.aej.2022.03.070.

[11] N. A. M. 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.

[12] 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.

[13] 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.

[14] A. Malik and P. Singh, "Comparative analysis of point to point FSO system under clear and haze weather conditions," *Wireless Pers. Commun.*, vol. 80, no. 2, pp. 483–492, Jan. 2015, doi: 10.1007/s11277-014-2022-6.

[15] 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," *Proc. SPIE*, vol. 4214, pp. 26–37, Feb. 2001, doi: 10.1117/12.417512.

[16] X. Chen, Q. Wang, L. Fan, and S. Yu, "A novel chaotic image encryption scheme armed with global dynamic selection," *Entropy*, vol. 25, no. 3, p. 476, Mar. 2023, doi: 10.3390/e25030476.

[17] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "A novel color image encryption based on fractional shifted Gegenbauer moments and 2D logistic-sine map," *Vis. Comput.*, vol. 39, no. 3, pp. 1027–1044, Jan. 2022, doi: 10.1007/s00371-021-02382-1.

[18] 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.

[19] 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.

[20] 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.

[21] S. Du and G. Ye, "IWT and RSA based asymmetric image encryption algorithm," *Alexandria Eng. J.*, vol. 66, pp. 979–991, Mar. 2023, doi: 10.1016/j.aej.2022.10.066.

[22] 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.

[23] 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.

[24] Y.-G. Yang, B.-P. Wang, Y.-L. Yang, Y.-H. Zhou, W.-M. Shi, and X. Liao, "A visually meaningful image encryption algorithm based on adaptive 2D compressive sensing and chaotic system," *Multimedia Tools Appl.*, vol. 82, no. 14, pp. 22033–22062, Jun. 2022, doi: 10.1007/s11042-021-11656-8.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] G. Kaur and G. Singh, "Performance analysis of SAC-OCDMA in free space optical medium using MD and DDW code," in *Proc. 2nd Int. Conf. Recent Adv. Eng. Comput. Sci. (RAECS)*, Chandigarh, India, Dec. 2015, pp. 1–6, doi: 10.1109/RAECS.2015.7453295.

[30] M. Moghaddasi, S. Seyedzadeh, I. Glesk, G. Lakshminarayana, and S. B. A. Anas, "DW-ZCC code based on SAC–OCDMA deploying multi-wavelength laser source for wireless optical networks," *Opt. Quantum Electron.*, vol. 49, no. 12, Dec. 2017, Art. no. 393, doi: 10.1007/s11082-017-1217-y.

[31] 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.

[32] 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.
[33] P. S. Pati and P. Krishnan, "Modelling of OFDM based RoFSO system for 5G applications over varying weather conditions: A case study," *Optik*, vol. 184, pp. 313–323, May 2019, doi: 10.1016/j.ijleo.2019.03.031.
[34] 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.
[35] 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.
[36] 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.
[37] A. Durdu, "Image transfer with secure communications application using a new reversible chaotic image encryption," *Multimedia Tools Appl.*, May 2023, doi: 10.1007/s11042-023-15707-0.
[38] 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.
[39] M. Ahmad, S. Agarwal, A. Alkhayyat, A. Alhudhaif, F. Alenezi, A. H. Zahid, and N. O. Aljehane, "An image encryption algorithm based on new generalized fusion fractal structure," *Inf. Sci.*, vol. 592, pp. 1–20, May 2022, doi: 10.1016/j.ins.2022.01.042.
[40] M. Demirtaş, "A novel multiple grayscale image encryption method based on 3D bit-scrambling and diffusion," *Optik*, vol. 266, Sep. 2022, Art. no. 169624, doi: 10.1016/j.ijleo.2022.169624.
[41] 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 Appl.*, vol. 82, no. 22, pp. 33637–33662, Mar. 2023, doi: 10.1007/s11042-023-14607-7.
[42] A. Toktas, U. Erkan, S. Gao, and C. Pak, "A robust bit-level image encryption based on Bessel map," *Appl. Math. Comput.*, vol. 462, Feb. 2024, Art. no. 128340, doi: 10.1016/j.amc.2023.128340.
[43] 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.
[44] X. Liu and C. Liu, "Quantum image encryption scheme using independent bit-plane permutation and baker map," *Quantum Inf. Process.*, vol. 22, no. 6, p. 262, Jun. 2023, doi: 10.1007/s11128-023-04026-w.
[45] 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.
[46] S. W. Jirjees, F. F. Alkalid, and W. F. Shareef, "Image encryption using dynamic image as a key based on multilayers of chaotic permutation," *Symmetry*, vol. 15, no. 2, p. 409, Feb. 2023, doi: 10.3390/sym15020409.
[47] S. Alharbi, A. Elsonbaty, A. A. Elsadany, and F. Kamal, "Nonlinear dynamics in the coupled fractional-order memristor chaotic system and its application in image encryption," *Math. Problems Eng.*, vol. 2023, pp. 1–23, Apr. 2023, doi: 10.1155/2023/8994299.
[48] S. Mansoor and S. A. Parah, "HAIE: A hybrid adaptive image encryption algorithm using chaos and DNA computing," *Multimedia Tools Appl.*, vol. 82, no. 19, pp. 28769–28796, Feb. 2023, doi: 10.1007/s11042-023-14542-7.
[49] K. Sathya, V. Sarveshwaran, T. Subhika, and M. D. Devi, "Security analyses of random number generation with image encryption using improved chaotic map," *Proc. Comput. Sci.*, vol. 215, pp. 432–441, Jan. 2022, doi: 10.1016/j.procs.2022.12.045.
[50] 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 Fractional*, vol. 7, no. 10, p. 734, Oct. 2023, doi: 10.3390/fractalfract7100734.

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 articles 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.

AMIRA G. MOHAMED (Student Member, IEEE) received the degree in electrical engineering from the Faculty of Engineering, Alexandria University, Egypt, 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, in 2017 and 2021, respectively. She is currently a Lecturer with the Electronics and Communication Department, AIET. Her research interests include image processing, steganography, cryptography, and information security.

ABDELLAH CHEHRI (Senior Member, IEEE) received the master's degree from Université Nice-Sophia-Antipolis-Eurecom, France, and the Ph.D. degree from Laval University, Québec. He is currently an Associate Professor with the Department of Mathematics and Computer Science, Royal Military College of Canada (RMC), Kingston, ON, Canada. He is the coauthor of more than 250 peer-reviewed publications in established journals and conference proceedings sponsored by established publishers, such as IEEE, ACM, Elsevier, and Springer. He is a member of the IEEE Communication Society, the IEEE Vehicular Technology Society (VTS), and the IEEE Photonics Society. He has served for roughly 30 conference and workshop program committees. He served as a guest editor/an associate editor for several well-reputed journals.

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*.

AHMAD ATIEH received the B.Sc. degree in electrical engineering from Yarmouk University, Jordan, in 1985, the M.Sc. degree in electrical engineering from the Jordan University of Science and Technology, in 1987, and the Ph.D. degree in electrical engineering from the University of Ottawa, Canada, in 1997.

He was with the National Research Council of Canada; JDS Uniphase Inc.; BTI Systems Inc., Canada; Taibah University, Madinah, Saudi Arabia; and The University of Jordan, Amman, Jordan. He is currently the VP of Optiwave Systems Inc., Canada. He has contributed more than 135 technical papers in different refereed journals and conferences. He holds over 32 issued patent and patent pending. His current research interests include optical fiber communication systems, including optical fiber characterization, optical amplifiers, nonlinear fiber optics, optical communication transmission systems, and free-space optical communication systems.

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 an Associate Professor with the Electrical Engineering Department, College of Engineering, Prince Sattam bin Abdulaziz University. He is also the Dean Assistant of the Quality and Development. His research interests include computer networks, wireless communications networks, optical communications, and cryptography systems.

MEDIEN ZEGHID received the Ph.D. degree in information and communication, sciences and technologies from the University of South Brittany, Lorient, France, in 2011. He was an Assistant Professor with the Department of Electronic Engineering, Higher Institute of Applied Sciences and Technology, Sousse University, Tunisia, from 2012 to 2014. 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 the crypto-systems, image and video coding, and optical communication.