IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 23, 2021, accepted April 9, 2021, date of publication April 22, 2021, date of current version May 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3074894

Efficient and Secure Bit-Level Chaos Security Algorithm for Orbital Angular Momentum Modulation in Free-Space Optical Communications

SHIMAA A. EL-MEADAWY[1], AHMED E. A. FARGHAL[2], HOSSAM M. H. SHALABY[3,4], (Senior Member, IEEE), NABIL A. ISMAIL[5], FATHI E. ABD EL-SAMIE[1,6], MOHAMMED ABD-ELNABY[7], AND WALID EL-SHAFAI[1,8]

[1]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoua University, Menouf 32952, Egypt
[2]Department of Electrical Engineering, Faculty of Engineering, Sohag University, Sohag 82524, Egypt
[3]Department of Electrical Engineering, Faculty of Engineering, Alexandria University, Alexandria 21544, Egypt
[4]Department of Electronics and Communication, Egypt-Japan University of Science and Technology, Alexandria 21934, Egypt
[5]Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoua University, Menouf 32952, Egypt
[6]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 84428, Saudi Arabia
[7]Department of Computer Engineering, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
[8]Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia

Corresponding author: Walid El-Shafai (eng.waled.elshafai@gmail.com)

This work was supported by Taif University Researchers Supporting Project Number (TURSP-2020/147), Taif university, Taif, Saudi Arabia.

ABSTRACT Currently, secure multimedia applications are becoming a very hot research topic, specifically over the Internet and wireless communication networks due to their rapid progress. Several researchers have implemented various chaotic image and video encryption algorithms to achieve data stability and communication security. This paper presents a novel bit-level video frame cryptosystem that is dependent on the piecewise linear chaotic maps (PWLCMs). It is implemented for orbital angular momentum (OAM) modulation over different turbulence channels. Firstly, the mathematical model for the bit error rate (BER) of OAM modulation is derived over the gamma-gamma turbulence channel. After that, a comparison between the theoretical results from Mathematica and the simulation results from MATLAB for different turbulence strengths, signal-to-noise ratios (SNRs), and propagation distance values is presented to assure that there is a perfect match. The proposed video cryptosystem is checked using entropy analysis, histogram testing, attack analysis, time analysis, correlation testing, differential analysis, and other quality and security evaluation metrics. The simulation results and the performance analysis confirm that the proposed cryptosystem is reliable and secure for video frame encryption, and communication with different turbulence conditions in free space.

INDEX TERMS PWLCM, multimedia security, free-space optics, gamma-gamma turbulence channel, orbital angular momentum.

I. INTRODUCTION

The photonics community is extremely concerned with achieving an excessive potential for data processing and resolving the crushing issue of unresolved bandwidth [1]. Multiplexing of a diversity of autonomous data channels is an exemplary way for improving both transmission capacity and spectral efficiency of lightwave communication systems. Different polarizations, wavelengths, or spatial channels can be positioned on the different data channels in consistency with multiplexing categories [2]. Recently, space division multiplexing (SDM), along with conventional multiplexing techniques, has gained much attention for capacity improvement in optical communication systems. Mode-division multiplexing (MDM) is a distinct SDM scenario, in which every mode can convey an independent data channel [3]. The SDM technology enhances the communication system capacity by transferring multiple parallel independent data streams. The SDM can be realized by transmitting various spatial modes on a multi-mode fiber or employing multiple nuclei on a multi-core fiber [4].

The associate editor coordinating the review of this manuscript and approving it for publication was San-Liang Lee.

The orbital angular momentum (OAM) is suggested to transmit multiple signals via free-space channels [5]–[7]. The orthogonality of OAM beams enables propagation without signal interference and allows simultaneous transmission of information on OAM modes. However, the transmitted OAM beams endure atmospheric turbulence (AT) in real-life communication scenarios, where there are spatial differences in the air refractive index. The OAM beam propagation in turbulent environments contributes to distortion of the phase front, beam spreading, and wandering. The signal power carried by a specific OAM mode is often transferred to other modes, leading to modal crosstalk. This modal crosstalk is mode-dependent and it destroys orthogonality between OAM modes, leading to loss discrepancies called mode-dependent losses, which cause system-level output degradations [8]. Various turbulence-induced irregularity alleviation techniques have been suggested for free-space communication. Turbulence mitigation can be accomplished either via adaptive optics (AOs) at the beam level or through digital signal processing (DSP), including channel coding and channel equalization techniques [8].

The rapid growth of the Internet and the emergence of smartphones with a large amount of secret information, particularly images, have lead to the emergence of security issues. However, due to the size of data and the large redundancy in raw images, conventional encryption algorithms, including international data encryption algorithm (IDEA), data encryption standard (DES), and advanced encryption standard (AES), may not be satisfactory for usage in image or video encryption [9]. Several different algorithms have been employed to eliminate image data leaks, including chaos theory [10]–[12], optical transformations [13]–[15], arbitrary grids [16], DNA coding [17], [18] and compressed sensing [19].

The key characteristic of chaotic technologies is their sensitivity to control parameters and primary conditions, which can be used for image or video diffusion, and confusion, to attain the required cryptographic properties [20], [21]. Image time or frequency domain encryption can be employed [22]. In some techniques, the pixel values of the image are manipulated in the time domain. In other ones, pixels are translated first to the frequency domain, and then the transformed coefficients can be modified [23]. Liu *et al.* in [24] provided a one-time key and a reliable chaotic image encryption method. In [25], Wang *et al.* proposed an algorithm based on the logistic map for color image encryption. The authors employed a combined strategy for the permutation and diffusion of the R, G, and B components to enhance the encryption efficiency. Several chaotic maps such as hyper-chaotic maps, quantum logistic maps, couplings of grid maps, and a chaotic fractional-order map were exploited to construct robust cryptosystems [26]–[30]. In [11], a block image encoding scheme was suggested based on composite chaotic maps and a dynamic arbitrary progress system. It is capable of removing the cyclic phenomena and avoiding the chosen plaintext attack, effectively. The authors of [31], and [32] implemented spatio-temporal non-contiguous coupled map gratings and spatial-temporal linear-nonlinear coupled map gratings with stronger dynamics than those of the logistic map or coupled map gratings. The results of simulation confirmed the effectiveness and security of those algorithms.

Due to the permutation advantages in the bit level, represented in the simultaneous adjustment of the value and pixel locations, several bit-level encryption algorithms were proposed [12], [33]–[36]. Xiang *et al.* recommended in [33] a discriminating image encryption scheme that encrypts the four upper bits in each pixel and leaves the four lower bits fixed. Zhu *et al.* suggested in [37] a bit-level permutation system that depends on Arnold cat map and a logistic map for image encryption. A logistic map creates the parameters of the Arnold cat map. As the upper four bit planes enclose almost all image information, they are autonomously confused, while the lower four bit planes are entirely permuted. However, Zhang *et al.* and Wang *et al.* found some shortcomings in Zhu's algorithm [35], [38]. Teng *et al.* developed also in [39] a self-adaptive encryption algorithm, but this algorithm has the same drawback as that of Zhu's algorithm.

A novel bit-level high-efficiency video coding (HEVC) encryption method based on cyclic shift, swapping, and piecewise linear chaotic maps (PWLCMs) is proposed in this paper to resolve the above-mentioned shortcomings. A PWLCM is configured with uniform invariant distribution, strong ergodicity, and few regular windows in its branching diagrams [36]. With these characteristics, the presented cryptosystem effectively withstands differential attacks.

To the best of our knowledge, it is the first time to study and evaluate upper bound and approximate upper bound expressions for the average BER of OAM modulation, considering the effects of gamma-gamma (GG) turbulence channel. Also, the effects of different turbulence strengths, SNR values, and propagation distances on OAM are considered. An efficient chaos-based HEVC cryptosystem for OAM modulation is proposed to overcome the shortcomings of the preceding algorithms and enhance the security levels of video streaming. The introduced cryptosystem provides low processing time and better efficiency in the presence of chosen-plaintext, known-plaintext, and statistical multimedia attacks. The robustness and ciphering performance of the proposed cryptosystem is improved as it allows column and row permutations at the same time.

The main contributions of this work are as follows:

- Derivation of closed-form expressions for the upper bound and approximate upper bound BER of OAM modulation for single-input single-output (SISO) transmission using 16 OAM states in the presence of the GG turbulence FSO channel.
- Achievement of perfect match between the theoretical analysis using Mathematica and the simulation analysis using MATLAB under different turbulence strengths, propagation distances, and SNR values.

- Introduction of an HEVC cryptosystem for OAM communication with more statistical analysis for a robust performance in the presence of different attacks, including known-plaintext attack, and chosen-plaintext attack.
- Study of the impact of different values of turbulence strength on the performance of the OAM communication system.
- As a proof of concept, transmission of several HEVC video frames is assessed, numerically. The security analysis is performed to prove the immunity to different types of potential attacks.

The structure of the paper is as follows. In Section II, we present the related work about different encryption techniques. In Section III, we describe, in detail, the theoretical analysis of OAM BER over a GG turbulence channel and also the configuration of the HEVC cryptosystem for OAM communication through this channel. In Section IV, both theoretical and simulation results are demonstrated, and also the performance analysis is presented. Finally, Section V is devoted to the conclusion.

II. RELATED WORK

In [40], the authors proposed a chaotic image encryption scheme applying two chaotic functions, which are sensitive to initial conditions. This scheme has the ability to encrypt original images with poor entropy values, and also it presents faster, simpler, and more secure encryption compared to other schemes. In [41], a method of optical image encryption employing gyrator random encoding and scrambling through a 3D chaotic map was proposed. Firstly, the scrambling is implemented to overwhelm the permuted image demerits. Then, the gyrator and spatial domains are exploited to perform a random encoding process to achieve robustness and good performance against multimedia attacks.

In [42], a 2-D chaotic Baker map with various operation modes was designed in the fractional Fourier domain. A permutation process is performed via the Baker map using three operation modes. An experimental study was presented to analyze this method. It has attractive security features, resistance to conventional attacks, and low computational cost. A self-adaptive diffusion-shuffling mechanism and a random deoxyribonucleic acid (DNA) method were suggested in [43]. The DNA is used to sequence the original image with random encoding rules to rearrange the original image pixels. The diffusion-shuffling process is then carried out for the encryption purpose. The properties of the original image affect the degree of diffusion-shuffling. Simulation results demonstrated that the system introduced in [43] is protected against conventional attacks, and it allows variable reuse for more effective real-time image encryption applications. The algorithm presented in [36] is based on a PWLCM, and it performs encryption in only one round. Simulation results and performance analysis verify reliability and security of this image encryption algorithm.

A 2D fractional Fourier transform (FrFT) based color image cryptosystem that depends on a 2D opto-logistic mapping (2D-LM) was presented and evaluated in [23]. This evaluation depends on visual inspection, entropy testing, histogram testing, quality measures, noise testing, and computational time analysis. In contrast to other works, the simulation results revealed superior performance. The algorithm in [44] depends on L-ary differential phase-shift keying multiple pulse position modulation (LDPSK-MPPM) that is protected by a discrete chaos mechanism in the physical layer. Device protection was tested for various forms of attacks, such as brute-force, differential, and statistical attacks by Monte Carlo (MC) simulations. A block-based opto-color cipher system depending on double random phase encoding (DRPE) with various block sizes was examined in [45]. The simulation results proved that this system is stable, reliable, and it has a good immunity to channel noise.

In [46], an FrFT-based LM color image cryptosystem was provided. Experimental results indicated that this cryptosystem is extremely secure and superior to other cryptosystems. The authors of [47] presented a study of the encryption efficiency of chaotic image block ciphering in the spatial and FrFT domains. The results demonstrated that the chaotic FrFT image encryption increases the confusion efficiency and produces a high non-linear relationship between plain and cipher images. Moreover, it has a high resistance to channel noise, and hence it can be effectively applied in noisy channel conditions. A color image cryptosystem based on RC6 with different operating modes was proposed in [48]. The simulation results reveal that this cryptosystem with cipher block chaining (CBC), cipher feedback (CFB), and the output feedback (OFB) modes can efficiently hide all color image information in images with few details, even in the presence of some input blocks with similar data. It also has a large efficiency in encrypting images in terms of security, encryption quality, and noise immunity.

Two robust hybrid watermarking techniques, namely the homomorphic-transform-based singular value decomposition (SVD) and the three-level discrete stationary wavelet transform (DSWT) for HEVC were introduced in [49]. The results prove that the hybrid fusion-encryption-watermarking system achieves a good perceptual quality with high peak signal-to-noise ratio (PSNR) values, less bit rates, high correlation coefficients with original frames, high information capacity, and high robustness without affecting the original 3D HEVC frame quality. A high-efficiency transmission and integrity assurance system based on HEVC was presented in [50]. This system is good and effective for verifying the integrity of HEVC frames through unsafe communication networks. This makes such cybersecurity framework appropriate, safe, and suitable for verification of multimedia integrity. A hybrid cryptosystem that combines DNA sequences, chaotic Arnold map and Mandelbrot sets for stable streaming of compressed HEVC was introduced in [51]. Substantial simulations and security analysis have been presented to ascertain robustness and security of this cryptosystem.

A bit-level image encryption algorithm based on PWLCM was presented in [36]. The simulation results and performance analysis in [36] reveal that this algorithm is effective and reliable for image encryption. Our previous work in [52] introduced an alternative effectual CNN architecture that is designed based on trial-and-error approach till getting the optimum network parameter and hyperparameter values to yield the best performance metrics of deep learning with three different optimizers. The objective is to obtain the optimal model through the 16 OAM-SK-FSO system using a 2D chaotic interleaver with Turbo and LDPC coded images. However, in this work, we consider the effects of GG turbulence channel and use both MATLAB and Mathematica, to obtain the upper bound and approximate upper bound expressions for the average BER of OAM using 16 states. In addition, to resolve the disadvantages of the preceding encryption algorithms and increase the security levels of video streaming, an effective chaos-based HEVC cryptosystem for OAM modulation is presented.

III. HEVC VIDEO FRAME ENCRYPTION FOR OAM MODULATION

The block diagram of the proposed cryptosystem for OAM modulation is depicted in Fig. 1. Firstly, the video frame is decomposed into eight bits by the binary bit-plane decomposition (BBD). After that, the bit planes are partitioned randomly into two similar groups [36]. In the presented model, the four upper and lower bit planes are selected as the two groups. Then, these two groups are transformed into two binary sequences: M_1 and M_2. The bit plane arrangements are set from left to right, top to bottom, and upper to lower bit planes in order to get M_1 and M_2 [36].

During the diffusion phase, to adjust the bit values in M_1 and M_2 and produce N_1 and N_2, confusion, cyclic shifts and XOR operations are employed. During the confusion phase, the binary elements in N_1 and N_2 are exchanged by employing the chaotic control map, and then we get K_1, and K_2. Finally, the ciphered video frames are obtained by arranging K_1 and K_2 into bit planes, and then combining all bit planes. N rounds are applied to further enhance the proposed cryptosystem performance [36]. The parameters and conditions of the unpredictable maps are used as secret keys. Before the confusion and diffusion phase, the creation of the two binary key-stream sequences is implemented using a secret key, $key_1 = (z_0, \delta_1)$. Let the size of the input video frame be $M \times N$. The preliminary parameters δ_1 and z_0 are adjusted to iterate the PWLCM for $N_0 + MN$ times, and remove the previous N_0 values to prevent harmful effects. The PWLCM is a map comprising several linear segments. It is defined as [36]:

$$z_i = F(z_{i-1}, \eta) = \begin{cases} \dfrac{z_{i-1}}{\eta}, & 0 < z_{i-1} < \eta \\ \dfrac{z_{i-1} - \eta}{0.5 - \eta}, & \eta \le z_{i-1} < 0.5 \\ F(1 - z_{i-1}, \eta), & 0.5 \le z_{i-1} < 1, \end{cases} \quad (1)$$

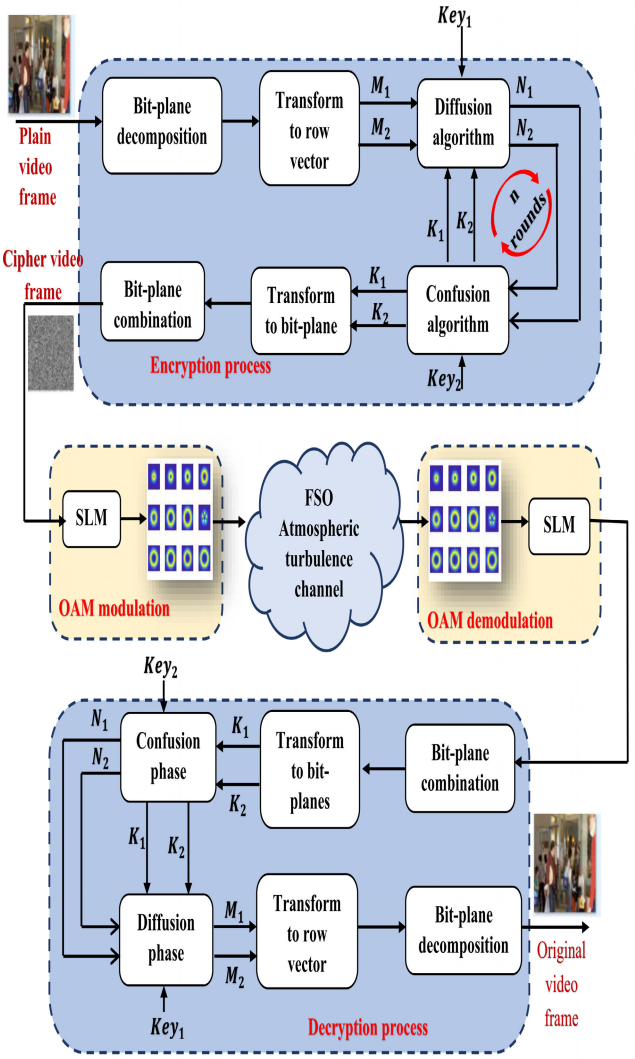


FIGURE 1. Block diagram of the proposed cryptosystem for OAM communication.

where the positive control parameter and initial conditions are $\eta \in [0, 0.5]$, and $z_i \in [0, 1]$, respectively. When the map lies in the entire parameter set, it is chaotic and it has no window in its bifurcation diagram [38].

The chaotic sequence has $M \times N$ elements, $Z = \{z_1, z_2, \cdots, z_{MN}\}$. The subsequent formula is used to convert $Z(i)$ to the integer sequence $Z_1(i)$ [36].

$$Z_1 = \text{mod}(\text{floor}(Z \times 10^{14}), 256) \quad (2)$$

A. DIFFUSION PHASE

This stage is performed by the following steps [36]:

1) Compute the sum of elements in M_2, and then obtain M_{11}, using the cyclic shift operation.

$$sum_1 = \sum_{i=1}^{L} M_2(i) \quad (3)$$

where L is the length of M_1 and M_2, $L = 4MN$, and M_{11} is the result of the M_1 matrix cyclic shift to the right by sum_1 bits.

2) Encrypt the first element in M_{11} using its last element, and the first elements in M_2 and n_1, according to:

$$N_1(1) = M_{11}(1) \oplus M_{11}(L) \oplus M_2(1) \oplus n_1(1) \tag{4}$$

3) Put $i = 2$, and encrypt the i^{th} element in M_{11} by the former element, and the i^{th} element in both M_2 and n_1, using:

$$N_1(i) = M_{11}(i) \oplus M_{11}(i-1) \oplus M_2(i) \oplus n_1(i) \tag{5}$$

4) Set $i = i + 1$ and return to step 3 until i reaches L. Use an identical method to encrypt M_2.

5) Calculate the sum of the elements in N_1, according to:

$$sum_2 = \sum_{i=1}^{L} N_1(i) \tag{6}$$

6) Get M_{22} using the cyclic shift operation. M_{22} is the cyclic shift of the M_2 matrix to the right by sum_2 bits.

7) Encrypt the first element in M_{22} by using its last element, and the first elements in N_1 and n_2, according to:

$$N_2(1) = M_{22}(1) \oplus M_{22}(L) \oplus N_1(1) \oplus n_2(1) \tag{7}$$

8) Set $i = 2$, and encrypt the i^{th} element in M_{22} by its former element, and the i^{th} element in N_1 and n_2 using:

$$N_2(i) = M_{22}(i) \oplus M_{22}(i-1) \oplus N_1(i) \oplus n_2(i) \tag{8}$$

9) Put $i = i + 1$, and return to step 8 until i reaches L.

B. CONFUSION PHASE

This phase is performed through the following steps [36]:

1) The sum of elements in N_1 and N_2 is computed as:

$$sum = \sum_{i=1}^{L} N_1(i) + N_2(i) \tag{9}$$

2) The secret key, $key_2(y_0, \delta_2)$ is used for the production of the chaotic sequences Y and Q, and the initial value s_0 is set according to:

$$s_0 = \mathrm{mod}\left(y_0 + \frac{sum}{L}, 1\right) \tag{10}$$

In order to prevent harmful effects, the chaotic system is iterated N_0+2L times and the previous N_0 values are omitted. The chaotic sequence has $2L$ elements, $S = \{s_1, s_2, \cdots s_{2L}\}$. The sequence S is split into two equal parts by the following two equations [36]:

$$\begin{aligned} S_1 &= \{s_1, s_2, \ldots\ldots.., s_L\} \\ S_2 &= \{s_{L+1}, s_{L+2}, \ldots\ldots.., s_{2L}\} \end{aligned} \tag{11}$$

Now, we use the following formula to transform S_1 and S_2 to the integer sequences Y and Q, where each sequence has a length L.

$$Y = \mathrm{mod}(\mathrm{floor}(S_1 \times 10^{14}), L) + 1$$

$$Q = \mathrm{mod}(\mathrm{floor}(S_2 \times 10^{14}), L) + 1 \tag{12}$$

3) Let $i = 1$, and exchange the binary elements in N_1 and N_2 according to:

$$\begin{aligned} \mathrm{temp} &= N_1(i) \\ N_1(i) &= N_2(Y(i)) \\ N_2(Y(i)) &= \mathrm{temp} \end{aligned} \tag{13}$$

4) Let $i = i + 1$; and go back to step 3 until i reaches L. Then, set $j = 1$; and switch the binary elements in N_1 and N_2 as follows:

$$\begin{aligned} \mathrm{temp} &= N_2(i) \\ N_2(i) &= N_2(Q(i)) \\ N_1(Q(i)) &= \mathrm{temp} \end{aligned} \tag{14}$$

5) Set $j = j + 1$, and go back to step 4 until j reaches L.

The encrypted k_1 and k_2 row vectors are then obtained. By transforming the sequences k_1 and k_2 into an MN video frame, the ciphered HEVC video frame is obtained.

C. OAM MODULATION AND DEMODULATION FOR FSO COMMUNICATION

The received signal after the turbulence channel is given by [5]:

$$y = \eta I x + N \tag{15}$$

where x is the transmitted encrypted data $\{0, 1\}$, I is the received irradiance, η is the optical-to-electrical conversion coefficient, N is the additive white Gaussian noise (AWGN) with zero mean and variance N_0.

The received irradiance is given by [5]:

$$I = \left| \int \chi(r, \phi, z).\chi^*(r, \phi, z) r dr d\phi \right|^2 \tag{16}$$

where $\chi(r, \emptyset, z)$ is the Laguerre Gaussian (LG) beam spatial distribution, and the equation that is used to measure the average bit error rate (ABER) is given by [8], [52]:

$$\begin{aligned} &\chi_{LG(l,p)}(r, \phi, z) \\ &= \frac{E}{\left(1 + \frac{z^2}{z_R^2}\right)^{1/2}} \cdot e^{-\frac{i\Upsilon r^2 z}{2\left(z^2 + z_R^2\right)}} \cdot e^{-\frac{r^2}{\omega^2(z)}} \\ &\cdot \left(\frac{r\sqrt{2}}{\omega(z)}\right)^{|l|} \cdot {L_p}^{|l|}\left(\frac{2r^2}{\omega^2(z)}\right) \\ &\cdot e^{-il\theta} \cdot e^{i\Upsilon z} e^{i(2p+|l|+1)\tan^{-1}\left(\frac{z}{z_R}\right)} \end{aligned} \tag{17}$$

where E is a normalization constant, r is the radial distance from z, l is the intertwined helical phase front, p is the radial index, (r, ϕ, z) are the cylindrical coordinates, $\Upsilon = 2\pi/\lambda$ is the wave number, λ is the optical wavelength, and ${L_p}^{|l|}$ is the generalized Laguerre polynomial. At a distance z, the beam radius of the standard Gaussian beam is given by [52]:

$$\omega(z) = \omega_0 \sqrt{1 + (z/z_R)^2} \tag{18}$$

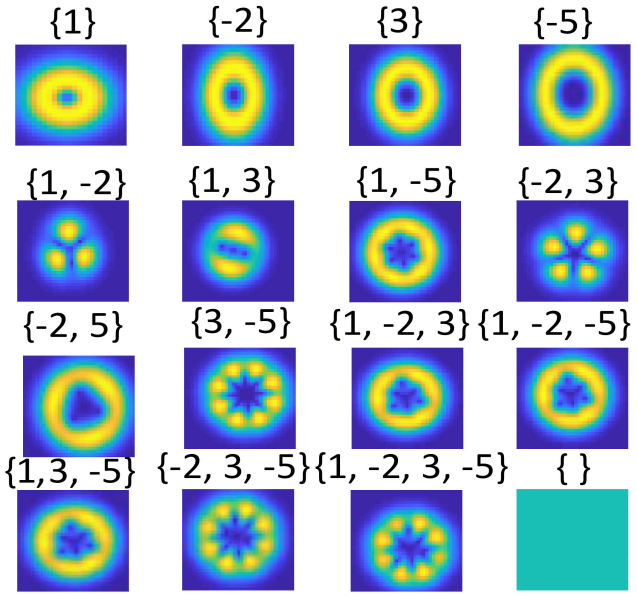


FIGURE 2. The used 16-ary OAM states.

Rayleigh range is obtained by [52]:

$$z_R = (\pi \omega_0^2)/\lambda \tag{19}$$

where ω_0 is the beam waist at $z = 0$.

An enhanced mapping scheme is accomplished on the encrypted data through the usage of a reflecting SLM to get super-imposed OAM states. The SLM is equipped with a set of phase holograms for transforming continuous Gauss beams into super-imposed LG beams with various OAM states in different wavelength ranges. Through the mapping process, every quadruple bit is translated into a state from 16 states [52] as depicted in Fig. 2, and the binary representation of them is shown in Table 1 due to OAM beam orthogonality. Then, these orthogonal beams conveying the raw binary encrypted data are passed first through the AT channel, and then to the receiver. At the receiver, the inverse operation can be performed using the same device to transform an incoming OAM mode back to a Gaussian beam. The idea is to apply the conjugate mode sorting technique that is used to determine the OAM mode of a detected beam. The demapping scheme is implemented by multiplying the transmitted encrypted data with the conjugates of original beams. Finally, we apply the decryption process to recover the original video frames.

The channel used here is the GG turbulence channel, and its probability density function (pdf) is given by [53]:

$$f_I(I) = \frac{2(\alpha\beta)^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha)\Gamma(\beta)} \times I^{\frac{\alpha+\beta}{2}-1} \times K_{\alpha-\beta}\left(2\sqrt{\alpha\beta I}\right) \tag{20}$$

$$K_{\alpha-\beta}\left(\sqrt{\alpha\beta I}\right) = \frac{1}{2} G_{0,2}^{2,0}\left(\alpha\beta I \left| \begin{matrix} \cdot, \cdot \\ \frac{\alpha-\beta}{2}, \frac{\beta-\alpha}{2} \end{matrix} \right.\right) \tag{21}$$

TABLE 1. States of OAM and their binary representations.

States	Topological charge	Binary sequence
1	{1}	1000
2	{-2}	0100
3	{3}	0010
4	{-5}	0001
5	{1,-2}	1100
6	{1,3}	1010
7	{1,-5}	1001
8	{-2,3}	0110
9	{-2,-5}	0101
10	{3,-5}	0011
11	{1,-2,3}	1110
12	{1,-2,-5}	1101
13	{-2,3,-5}	0111
14	{1,3,-5}	1011
15	{1,-2,3,-5}	1111
16	Zeros	0000

$$f_I(I) = \frac{(\alpha\beta)^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha)\Gamma(\beta)} I^{\frac{\alpha+\beta}{2}-1} G_{0,2}^{2,0}\left(\alpha\beta I \left| \begin{matrix} \cdot, \cdot \\ \frac{\alpha-\beta}{2}, \frac{\beta-\alpha}{2} \end{matrix} \right.\right) \tag{22}$$

From the properties of Meier g function and the following equation [54], [55]:

$$z^{\rho}.G_{p,q}^{m,n}\left[\binom{a_p}{b_q}|z\right] = G_{p,q}^{m,n}\left[\binom{a_p+\rho}{b_q+\rho}|z\right] \tag{23}$$

it is derived that:

$$\begin{aligned} f_I(I) &= \frac{\alpha\beta^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha).\Gamma(\beta)}.I^{\frac{\alpha+\beta}{2}-1} \cdot G_{0,2}^{2,0}\left[\alpha\beta I \left| \begin{matrix} \cdot, \cdot \\ \frac{\alpha-\beta}{2}, \frac{\beta-\alpha}{2} \end{matrix} \right.\right] \\ &= \frac{\alpha\beta}{\Gamma(\alpha).\Gamma(\beta)}.G_{0,2}^{2,0}\left[\alpha\beta I \left| \begin{matrix} \cdot, \cdot \\ \alpha-1, \beta-1 \end{matrix} \right.\right] \end{aligned} \tag{24}$$

where α is the effective number of large-scale scattering eddies and β is the effective number of small-scale scattering eddies. The values of α and β are estimated with the help of the following equations [52]:

$$\begin{aligned} \alpha &= \left[\exp\left(0.49\rho_v^2/(1+1.11\rho_v^{12/5})^{7/6}\right) - 1\right]^{-1}, \\ \beta &= \left[\exp\left(0.51\rho_v^2/\left(1+0.69\rho_v^{12/5}\right)^{5/6}\right) - 1\right]^{-1} \end{aligned} \tag{25}$$

where $\rho_v^2 = 1.23 c_n^2 \, k_o^{\frac{7}{6}} l_p^{\frac{11}{6}}$ is the variance of the irradiance fluctuations, h is the normalized received irradiance, $\Gamma(\cdot)$ is the Gamma function, c_n^2 is the refractive index structure parameter, and l_p is the propagation distance.

The turbulence channel will therefore break the orthogonality of OAM modes and distort information transmission from the corresponding spatial OAM modes. The GG turbulence channel effect is included. At the receiver, the detection process is performed using the conjugate light field detection method. After demapping of all received data to different OAM states, the decryption process is performed. The decryption process is exactly the reverse of the encryption process [36], but with much attention to the reverse

cyclic shift order and swapping. After the decryption process, the original bit stream is obtained, and then transformed into the HEVC video frames. The OAM bit error rate is computed over the GG turbulence channel.

The instantaneous electrical SNR is given by [5]:

$$\gamma = (\eta I)^2/N_0 \tag{26}$$

The average electrical SNR is given by [5]:

$$\mu = (\eta E[I])^2/N_0 \tag{27}$$

The average SNR is given by:

$$\bar{\gamma} = \mu.\frac{E[I^2]}{E^2[I]} \tag{28}$$

To get the value of $E[I]$, the following expression is estimated [5], [55]:

$$E[I] = \int_0^\infty I.f_I(I)dI = \int_0^\infty I.\frac{\alpha\beta^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha).\Gamma(\beta)}.I^{\frac{\alpha+\beta}{2}-1} .G_{0,2}^{2,0}\left[\alpha\beta I\middle|\begin{matrix}\cdot,\cdot\\ \frac{\alpha+\beta}{2},\frac{-\alpha+\beta}{2}\end{matrix}\right]dI \tag{29}$$

From [54], [55], we have:

$$\int_0^\infty \tau^{\theta-1}.G_{p,q}^{m,n}\left[\tau z\middle|\begin{matrix}a_1,\ldots,a_n,a_{n+1}\ldots,a_p\\ b_1,\ldots,b_m,a_{m+1}\ldots,b_q\end{matrix}\right]d\tau = \frac{\prod_{k=1}^{m}\Gamma(\alpha+b_k).\prod_{k=1}^{n}\Gamma(1-\alpha-a_k)}{\prod_{k=n+1}^{p}\Gamma(\alpha+b_k).\prod_{k=m+1}^{q}\Gamma(1-\alpha-b_k)}.z^{-\theta} \tag{30}$$

After solving Eq.(29) according to Eq.(30), the value of $E[I]$ is obtained, and it is equal to 1.

To get the value of $E[I^2]$, the following expression is estimated [5], [55]:

$$E[I^2] = \int_0^\infty I^2.f_I(I)dI = \int_0^\infty I^2.\frac{\alpha\beta^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha).\Gamma(\beta)}.I^{\frac{\alpha+\beta}{2}-1} .G_{0,2}^{2,0}\left[\alpha\beta I\middle|\begin{matrix}\cdot,\cdot\\ \frac{\alpha+\beta}{2},\frac{-\alpha+\beta}{2}\end{matrix}\right]dI = \frac{(1+\beta).(1+\alpha)}{\alpha\beta} \tag{31}$$

$$\bar{\gamma} = \mu.\frac{E[I^2]}{E^2[I]} = \mu.\frac{(\alpha+1).(\beta+1)}{\alpha\beta} \tag{32}$$

Now, we can get the value of I as:

$$I = \sqrt{\frac{\gamma}{\mu}} \tag{33}$$

By applying this simple random variable transformation between I and γ, the resulting SNR PDF for the IM/DD technique is given as:

$$f_\gamma(\gamma) = \frac{\alpha\beta^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha).\Gamma(\beta)}.(\frac{\gamma}{\mu})^{\frac{\alpha+\beta}{4}-0.5}. \times G_{0,2}^{2,0}\left[\alpha\beta\sqrt{\frac{\gamma}{\mu}}\middle|\begin{matrix}\cdot,\cdot\\ \frac{\alpha+\beta}{2},\frac{-\alpha+\beta}{2}\end{matrix}\right] \tag{34}$$

The BER of K-OAM can be given by [56]:

$$\mathrm{BER}_{OAM}^{U} \le \frac{1}{K\log_2 K}.\sum_{i=1}^{K}\sum_{j=1}^{K}D_H(P_i,P_j).\mathrm{BEP}^{i\to j} \tag{35}$$

$$\mathrm{BEP}^{i\to j} = Q\left[|I_i - I_j|.\sqrt{\frac{\bar{\gamma}.\log_2 K}{2}}\right] \tag{36}$$

where $\mathrm{BEP}^{i\to j}$ is the bit error probability between symbols P_i and P_j, $D_H(P_i,P_j)$ is the Hamming distance between symbols P_i and P_j, $\bar{\gamma}$ is the average received SNR per bit, I_i and I_j are two independent and identically distributed channel gains, $Q(.)$ stands for the Gaussian q-function, and K is the number of applied OAM states.

The objective now is to get the value of $BEP^{i\to j}$. Assume that $U = |I_i - I_j|$, and $W = I_i - I_j$. Then $U = |W|$, where I_i and I_j are two independent random variables (RVs) characterized by the GG pdf.

The pdf of W is given by [56]:

$$f_W(W) = \begin{cases}\int_0^\infty f_{I_i}(W+I_i).f_{I_i}(I_i)dI_i, & \text{for } W \ge 0\\ \int_{-\infty}^0 f_{I_i}(W+I_i).f_{I_i}(I_i)dI_i, & \text{for } W < 0\end{cases} \tag{37}$$

The pdf of U is given by:

$$f_U(u) = f_W(u) + f_W(-u) \tag{38}$$

where $f_W(u) = f_W(W)$ for $W \ge 0$ and $f_W(-u) = f_W(W)$ for $W < 0$.

Now, Eq.(22), and Eq.(37) are used to get the value of $f_W(W)$:

$$f_W(W) = \int_0^\infty \frac{\alpha\beta}{\Gamma(\alpha).\Gamma(\beta)}.G_{0,2}^{2,0}\left[\alpha\beta(I_i+W)\middle|\begin{matrix}\cdot,\cdot\\ \alpha-1,\beta-1\end{matrix}\right] .\frac{\alpha\beta}{\Gamma(\alpha).\Gamma(\beta)}.G_{0,2}^{2,0}\left[\alpha\beta I_i\middle|\begin{matrix}\cdot,\cdot\\ \alpha-1,\beta-1\end{matrix}\right]dI_i \tag{39}$$

By putting $\alpha\beta I_i = I$, and $\alpha\beta dI_i = dI$,

$$f_W(W) = \frac{\alpha\beta}{(\Gamma(\alpha).\Gamma(\beta))^2}.\int_0^\infty G_{0,2}^{2,0}\left[(I+\alpha\beta W)\middle|\begin{matrix}\cdot,\cdot\\ \alpha-1,\beta-1\end{matrix}\right] .G_{0,2}^{2,0}\left[I\middle|\begin{matrix}\cdot,\cdot\\ \alpha-1,\beta-1\end{matrix}\right]dI \tag{40}$$

The solution for this integral can be found as [54], [56].

$$\int_0^\infty \tau^{\chi-1}.G_{u,v}^{s,t}\left[(\sigma+\tau\middle|\begin{matrix}c_1,\cdots,c_u\\ d_1,\cdots,d_v\end{matrix}\right] \times G_{p,q}^{m,n}\left[\omega\tau\middle|\begin{matrix}a_1,\cdots a_p\\ b_1,\cdots,b_q\end{matrix}\right]d\tau = \left\{\sum_{k=0}^{\infty}\frac{(-\sigma)^k}{k!}\right\} \times G_{p+v+1,q+u+1}^{m+t,n+s+1}\left[\omega\middle|\begin{matrix}a_1,\cdots,a_n\\ b_1,\cdots,b_m,\end{matrix}\right] \quad (41)$$

By comparison between Eq.(40), and Eq.(41), we get the following parameters: $\tau = I$, $\chi = 1, u, v = 0, 2, m, n = 2, 0, s, t = 2, 0, p, q = 0, 2, \sigma = \alpha\beta w, \omega = 1, d_v = b_q = \alpha - 1, \beta - 1$
At $W \geq 0$:

$$f_W(W) = f_W(u) = \frac{\alpha\beta}{(\Gamma(\alpha).\Gamma(\beta))^2}.\sum_{k=0}^{\infty}\frac{(-\alpha\beta.u)^k}{k!}. \times G_{3,3}^{2,3}\left[1\middle|\begin{matrix}0,\,1+k-\alpha,\,1+k-\beta\\ \alpha-1,\,\beta-1,\,k\end{matrix}\right] \quad (42)$$

Similar calculations can be obtained for $f_Z(-u)$, and the result shows that $f_W(u) = f_W(-u)$. Hence, the PDF of u will be:

$$f_u(u) = \frac{2\alpha\beta}{(\Gamma(\alpha).\Gamma(\beta))^2}.\sum_{k=0}^{\infty}\frac{(-\alpha\beta.u)^k}{k!}.G_{3,3}^{2,3}\left[1\middle|\begin{matrix}A\\ B\end{matrix}\right] \quad (43)$$

where $A = 0, 1+k-\alpha, 1+k-\beta$, and $B = \alpha-1, \beta-1, k$.

The average bit error probability (ABEP) can be measured by [56]:

$$ABEP^{i\to j} = \int_0^\infty Q\left[u.\sqrt{\frac{\bar{\gamma}.\log_2 K}{2}}\right].f_u(u)du \quad (44)$$

$$Q(x) = \frac{1}{2}.erfc(\frac{x}{\sqrt{2}}) \quad (45)$$

where $erfc(.)$ is the complementary error function [56].
In our case, $x = u.\sqrt{\frac{\bar{\gamma}.\log_2 K}{2}}$.

$$ABEP^{i\to j} = \int_0^\infty \frac{1}{2}.erfc\left(\frac{u.\sqrt{\frac{\bar{\gamma}.\log_2 K}{2}}}{\sqrt{2}}\right).f_u(u)du = \times \int_0^\infty \frac{1}{2}.erfc\left(\frac{u.\sqrt{\frac{\bar{\gamma}.\log_2 K}{2}}}{\sqrt{2}}\right).\frac{2\alpha\beta}{(\Gamma(\alpha).\Gamma(\beta))^2}. \times \left\{\sum_{k=0}^{\infty}\frac{(-\alpha\beta.u)^k}{k!}.G_{3,3}^{2,3}\left[1\middle|\begin{matrix}A\\ B\end{matrix}\right]\right\}du \quad (46)$$

$$ABEP^{i\to j} = \frac{\alpha\beta}{(\Gamma(\alpha).\Gamma(\beta))^2}.\left\{\sum_{k=0}^{\infty}\frac{(-\alpha\beta)^k}{k!}.G_{3,3}^{2,3}\left[1\middle|\binom{A}{B}\right]\right\} \times \int_0^\infty (u)^k.erfc\left(\frac{u.\sqrt{\bar{\gamma}.\log_2 K}}{2}\right)du \quad (47)$$

It is shown that $\int_0^\infty (x)^{a-1}.\text{erfc}(bx)dx = \frac{\Gamma(\frac{a+1}{2})}{ab^a.\sqrt{\pi}}$ [56].
At $z = \int_0^\infty (u)^k.\text{erfc}(\frac{u.\sqrt{\bar{\gamma}.\log_2 K}}{2})du$, we have $a = k+1$, and $b = \frac{\sqrt{\bar{\gamma}.\log_2 K}}{2}$.

$$z = \frac{\Gamma(\frac{k+2}{2})}{(k+1).(\frac{\sqrt{\bar{\gamma}.\log_2 K}}{2})^a.\sqrt{\pi}} \quad (48)$$

$$ABEP^{i\to j} = \frac{\alpha\beta}{(\Gamma(\alpha).\Gamma(\beta))^2}.\sum_{k=0}^{\infty}\frac{(-\alpha\beta)^k}{k!}.G_{3,3}^{2,3}\left[1\middle|\begin{matrix}A\\ B\end{matrix}\right] \times \frac{\Gamma(\frac{k+2}{2})}{(k+1).(\frac{\sqrt{\bar{\gamma}.\log_2 K}}{2})^a.\sqrt{\pi}} \quad (49)$$

Now, to get the ABER, we use the following equation:

$$\text{ABER} = \frac{1}{K\log_2 K}.\sum_{i=1}^{K}\sum_{j=1}^{K}D_H(b_i,b_j).BEP^{i\to j} \quad (50)$$

The value of the Hamming distance is substituted by:

$$\frac{1}{K\log_2 K}.\sum_{i=1}^{K}\sum_{j=1}^{K}d_H(b_i,b_j) = \frac{K}{2} \quad (51)$$

The equation used to measure the ABER in the theoretical analysis is:

$$\text{ABER} = \frac{\alpha\beta.K}{2.(\Gamma(\alpha).\Gamma(\beta))^2}.\sum_{k=0}^{\infty}\frac{(-\alpha\beta)^k}{k!}.G_{3,3}^{2,3}\left[1\middle|\begin{matrix}A\\ B\end{matrix}\right] \times \frac{\Gamma(\frac{k+2}{2})}{(k+1).(\frac{\sqrt{\bar{\gamma}.\log_2 K}}{2})^{k+1}.\sqrt{\pi}} \quad (52)$$

IV. THEORETICAL RESULTS AND PERFORMANCE ANALYSIS

The proposed model efficiency is verified using both theoretical and simulation analysis under different values of turbulence strength, propagation distance, and SNR. The values of the parameters used in the analysis are $K = 16$, α= 11.6, 4.8, and 4.2, and β= 10.1, 1.9, and 1.4 for low, moderate, and strong turbulence strengths, respectively.

Figure 3 demonstrates the average BER versus SNR using different turbulence strengths. From this figure, it is noticed that there is an excellent match between theoretical results using Mathematica and simulation results using MATLAB. Also, the BER for low, moderate, and strong turbulence strengths reaches 10^{-7}, 10^{-5}, and 10^{-3} using 16 OAM states, respectively.

Figure 4 indicates the average BER versus propagation distance at different turbulence strengths with and without encryption. From this figure, it is noticed that increasing the propagation distance makes the BER increase for the different turbulence cases with and without encryption. At a distance of 400 m, the BER of OAM reaches 10^{-5}, 10^{-4}, and 10^{-3} using 16 OAM states for low, moderate, and strong turbulence, respectively. It is indicated from this figure that the implementation of HEVC encryption/decryption algorithm with OAM improves the performance of the system

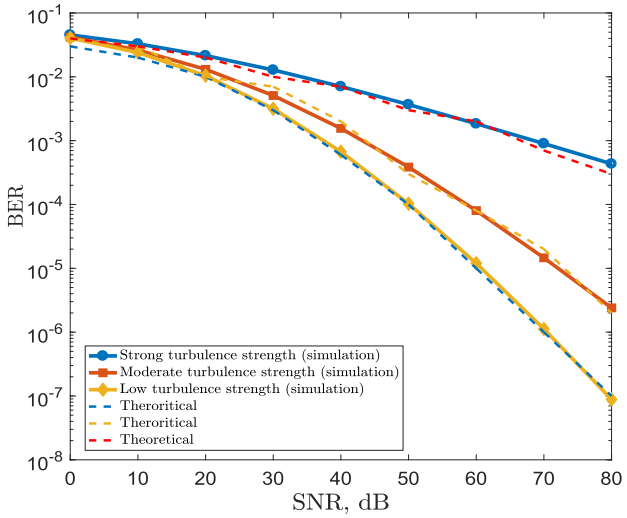


FIGURE 3. BER comparison between theoretical and simulation results at different SNR values.

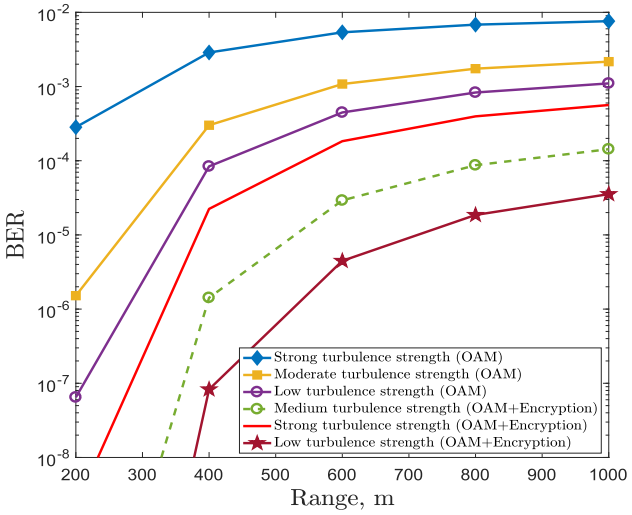


FIGURE 4. Simulated BER versus propagation distance for different turbulence strengths.

under different turbulence strengths at 400 m by nearly 3 orders of magnitude using 16 OAM states.

The performance analysis of the proposed system is discussed taking into consideration histograms, correlation coefficients, entropy, quality analysis, differential analysis, and other different security evaluation metrics [36]. In the simulations, 256 × 256 traditional 8-bit gray-scale video frames have been considered for testing.

A. CORRELATION ANALYSIS

In the horizontal, vertical, and diagonal directions, the adjacent pixels of the original video frame are strongly correlated. An ideal encryption algorithm should have a sufficiently low correlation between the encrypted video frame pixels to avoid any statistical attacks [36], [44]. The correlations of the adjacent pixels in the plain and encrypted video frames are evaluated and compared by arbitrarily picking 2000 pairs of adjacent pixels in every direction of the two video frames. The correlation distributions in the three directions of two neighboring pixels are demonstrated in Figs. (5–7). It is clear from the figures that the original video frame distributions for any two contiguous pixels are highly concentrated, which implies that these video frames have strong correlation between pixels. Due to the random distribution of adjacent pixels in the encrypted video frames, these video frames have low correlation. Furthermore, the mathematical formulas for determining the correlation coefficient R_{ab} for each pair is given by the subsequent equations [36], [45]:

$$R_{ab} = \frac{\text{cov}(a,b)}{\sqrt{D(a).D(b)}}$$

$$E(a) = \frac{1}{o}.\sum_{i=1}^{s} a_i$$

$$D(a) = \sum_{i=1}^{o} (a_i - E(a))^2$$

$$\text{cov}(a,b) = \frac{1}{o}.\sum_{i=1}^{o} (a_i - E(a)).(b_i - E(b)) \quad (53)$$

where a and b are the two adjacent video frame pixel gray-scale values, while o is the total number of selected video frame pixels. Table 2 demonstrates that the correlation coefficients of the original and encrypted video frames under different turbulence strengths are close to 1 and 0, respectively, in all three directions. From the obtained results, the proposed system achieves large confusion and diffusion.

B. HISTOGRAM ANALYSIS

The amount of confusion generated by the encryption scheme is estimated by histogram analysis. The histogram displays the pixel level distribution in a video frame. Ciphered video frame histograms must be distributed uniformly for highly reliable encryption techniques to withstand statistical attacks [36], [44]. The histograms of various original frames and the corresponding ciphered frames are displayed in Fig. 8, and all gray-scale values are uniformly distributed over the interval [0, 255]. The histograms of the decrypted video frames have been found to be entirely identical to those of the original video frames under low turbulence strengths. Under large turbulence strengths, the histograms of decrypted video frames differ from those of the original video frames. The histogram results confirm the ciphering/deciphering efficiency of the proposed system.

C. ENTROPY ANALYSIS

Information entropy is the most important measure of randomness in information theory. The equation used to measure the information entropy is [36]:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i).\log_2 \frac{1}{p(m_i)} \quad (54)$$

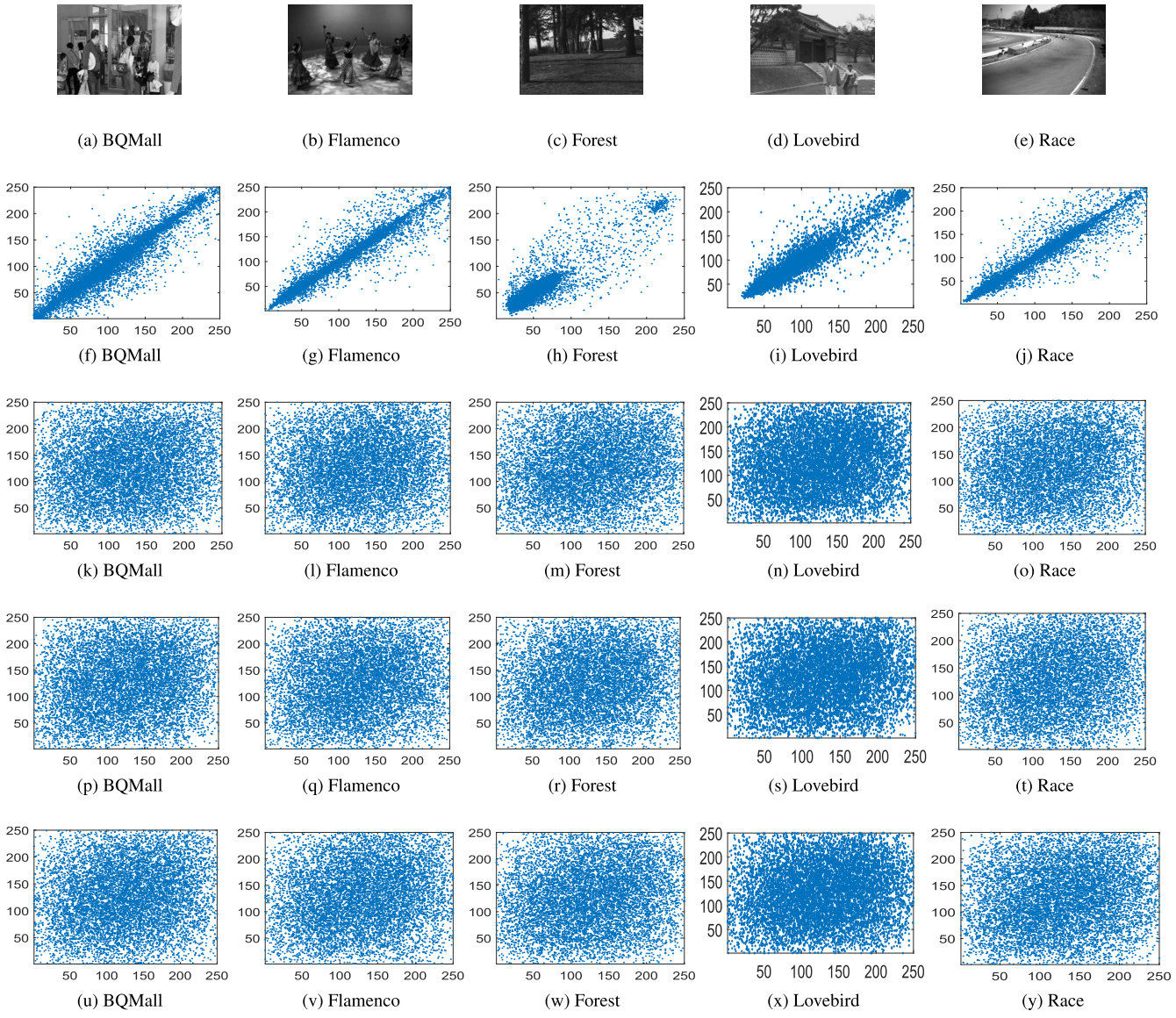


FIGURE 5. The diagonal correlation plots of different video frames and their corresponding ciphered video frames for: (a: e) original video frames and decrypted video frames under low turbulence strength.; (f: j) the corresponding correlation plots of original video frames; (k: o) encrypted video frames under low turbulence strengths; (p: t) encrypted video frames under moderate turbulence strengths; (u: y) encrypted video frames under strong turbulence strengths. The x, and y labels refer to the pixel gray-scale values at locations (x,y), and $(x+1,y+1)$, respectively.

TABLE 2. Correlation coefficients between the original and encrypted video frames under different turbulence strengths.

Cases	Diagonal					Horizontal					Vertical				
	BQM.	Flam.	For.	Love.	Race.	BQM.	Flam.	For.	Love	Race.	BQM.	Flam.	For.	Love.	Race.
Original	0.929	0.944	0.943	0.945	0.946	0.942	0.983	0.981	0.984	0.986	0.979	0.967	0.966	0.959	0.972
Low	0.078	0.097	0.121	0.055	0.119	0.327	0.322	0.444	0.365	0.325	0.351	0.336	0.392	0.422	0.381
Moderate	0.023	0.098	0.158	0.09	0.179	0.431	0.322	0.366	0.378	0.343	0.367	0.352	0.338	0.411	0.271
Strong	0.095	0.065	0.138	0.094	0.194	0.335	0.349	0.39	0.338	0.367	0.388	0.39	0.393	0.341	0.342

where m is the information source, n is the number of required bits to represent the symbol m_i, and $p(m_i)$ is probability of the symbol m_i.

When all pixels are distributed equally, the maximum entropy in the 8-bit gray scale will be 8 [36], [45]. As the entropy approaches the optimum value of 8, the ciphered video frame cannot be decrypted by an attacker. Eq. (54) is used to calculate the information entropy of the plain video frames and the corresponding encrypted video frames. The results are shown in Table 3. From this table, it is evident that the estimated ciphered video frame entropies are close to the ideal values, which means that there is very little possibility of unintended information leakage.

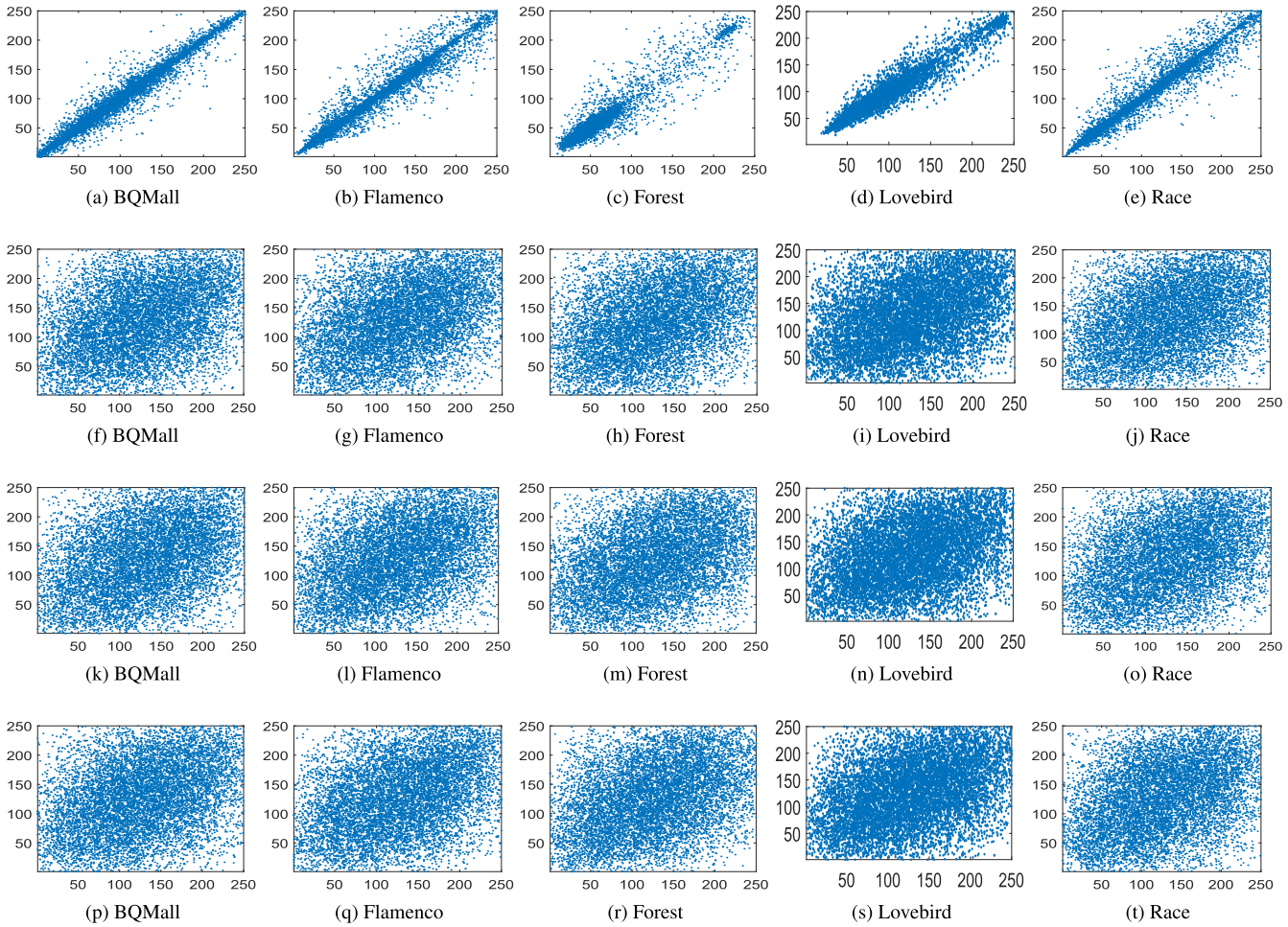


FIGURE 6. The horizontal correlation plots of different video frames and their corresponding ciphered video frames for: (a: e) original video frames; (f: j) encrypted video frames under low turbulence strengths; (k: o) encrypted video frames under moderate turbulence strengths; (p: t) encrypted video frames under strong turbulence strengths. The *x*, and *y* labels refer to the pixel gray-scale values at locations (x,y), and $(x+1,y+1)$, respectively.

TABLE 3. Information entropy.

Video frames	Original-video frame	Low	Moderate	Strong
BQMall	7.68	7.87	7.87	7.87
Flamenco	7.55	7.87	7.87	7.87
Forest	7.55	7.87	7.87	7.87
Lovebird	7.55	7.87	7.87	7.87
Race	7.55	7.95	7.95	7.95

D. DIFFERENTIAL ATTACKS

A good cryptosystem should guarantee that any minor changes to the plain video frame will make substantial variations in the encrypted video frame to withstand differential attacks. The number of pixel changes rate (NPCR) and unified average change intensity (UACI) are typically utilized for differential attack analysis. Eqs (55)– (57) describe these definitions [36], [44], [45].

$$\text{NCPR} = \sum_{i,j} \frac{D(i,j)}{M \times N} \times 100\% \tag{55}$$

$$\text{UACI} = \sum_{i,j} \frac{|v_1(i,j) - v_2(i,j)|}{M \times N \times 255} \tag{56}$$

where v_1 and v_2 are two identical video frames with size $M \times N$, and $D(i,j)$ is defined as:

$$D(i,j) = \begin{cases} 0 & v_1(i,j) = v_2(i,j) \\ 1 & v_1(i,j) \neq v_2(i,j) \end{cases} \tag{57}$$

After computing the UACI and NPCR values, the impacts of a 1-bit variation in the plain video frame on the corresponding ciphered video frames are tested and given in Table 4. As observed from the table, the proposed HEVC cryptosystem gives an NPCR over 99.6% and a UACI over 33.4%. These findings show that the proposed cryptosystem can efficiently resist differential attacks.

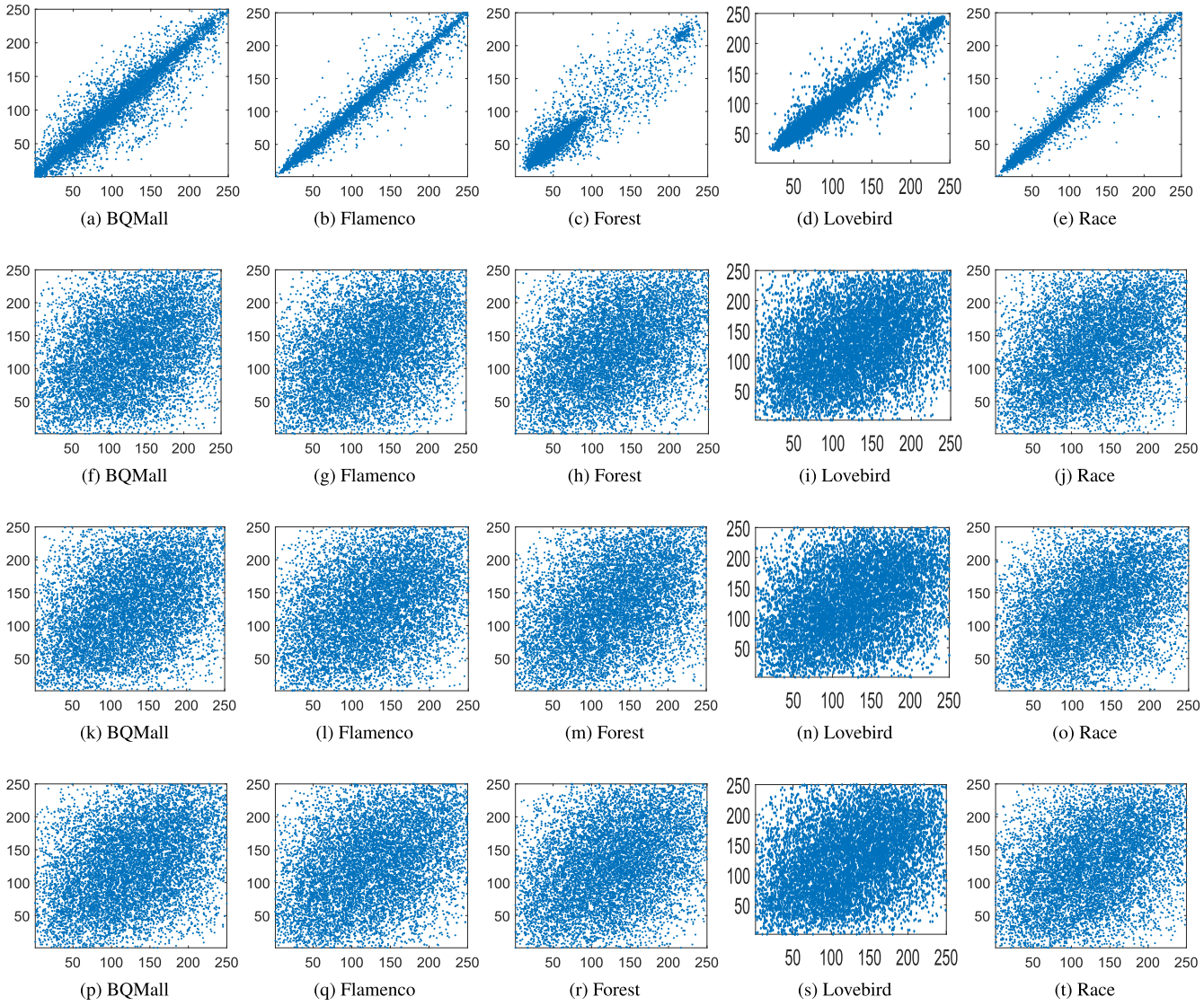


FIGURE 7. The vertical correlation plots of different video frames and their corresponding ciphered video frames for: (a: e) original video frames; (f: j) encrypted video frames under low turbulence strengths; (k: o) encrypted video frames under moderate turbulence strengths; (p: t) encrypted video frames under strong turbulence strengths. The *x*, and *y* labels refer to the pixel gray-scale values at locations (*x*,*y*), and ($x+1$,$y+1$), respectively.

TABLE 4. NPCR and UACI performance.

Video frames	NCPR			UACI		
	Low	Moderate	Strong	Low	Moderate	Strong
BQMall	0.996	0.996	0.996	0.334	0.334	0.334
Flamenco	0.996	0.996	0.996	0.334	0.334	0.334
Forest	0.996	0.996	0.996	0.334	0.334	0.334
Lovebird	0.996	0.996	0.996	0.334	0.334	0.334
Race	0.996	0.996	0.996	0.334	0.334	0.334

E. PSNR, SSIM, AND FSIM

Peak signal-to-noise ratio (PSNR) is used to assess the robustness of the proposed system. It is measured between the original and decoded OAM video frames. Structural similarity index (SSIM) is used to estimate the similarity between plain and decrypted OAM video frames. Feature similarity index (FSIM) is the SSIM Fourier form. The FSIM can build a complete similarity index by distributing various weights to various visual quality components to assess the video quality. It is necessary for the three parameters to get high and low values for decryption and encryption, respectively [36], [45]. From Table 5, it is demonstrated that the estimated PSNR, SSIM, and FSIM of the encrypted video frames have low values, which ensures that the suggested HEVC cryptosystem is effective.

$$\mathrm{MSE} = \frac{1}{M.N}.\sum_{a=1}^{M}\sum_{b=1}^{N}[\rho(x,y)-\varrho(x,y)]^2 \tag{58}$$

$$\mathrm{PSNR} = 10\log\frac{(2^n-1)^2}{MSE} \tag{59}$$

$$\mathrm{SSIM} = \frac{(2\epsilon_I\epsilon_D+v_1)(2\tau_{ID}+v_2)}{(\epsilon_I^2+\epsilon_D^2+v_1)(\tau_I^2+\tau_D^2+v_2)} \tag{60}$$

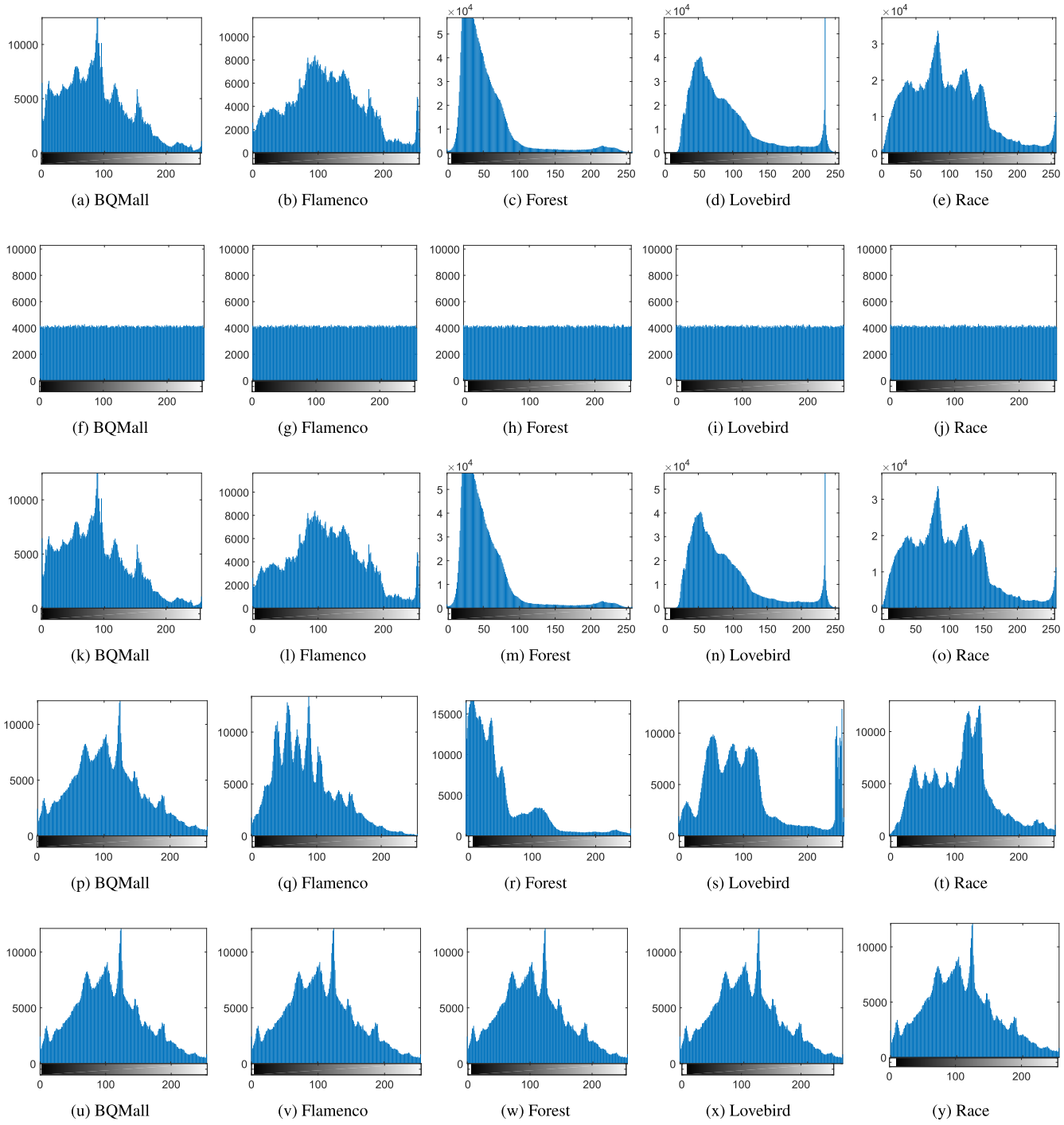


FIGURE 8. Histogram analysis. (a: e) The different original video frame histograms; (f: j) the different encrypted video frame histograms; (k: o) the different decrypted video frame histograms under low turbulence strengths;(f: j) the different decrypted video frame histograms under moderate turbulence strengths;(u: y) the different decrypted video frame histograms under strong turbulence strengths.

$$\text{FSIM} = \frac{\sum_{x\in v} o_l(x).pv_m(x)}{\sum_{x\in v} pv_m(x)} \tag{61}$$

where ρ is the plain video frame, ϱ is the decrypted video frame, n is the number of bits per pixel, ϵ_I is the average of the input video frame, ϵ_D is the average of decrypted (D) image, τ_D^2 and τ_I^2 correspond to the variances of decrypted and plain video frames, τ_{ID} signifies the covariance of plain and decrypted video frames, and v is the video frame in the spatial domain.

F. EDGE DETECTION ANALYSIS

The proposed HEVC cryptosystem with OAM modulation should secure the information from the burglars on the edges

TABLE 5. PSNR, SSIM, and FSIM performance metrics.

Images	PSNR			SSIM			FSIM		
	Low	Mod	Strong	Low	Mod	Strong	Low	Mod	Strong
BQMall	9.8	9.9	9.9	0.42	0.34	0.34	0.42	0.34	0.34
Flamenco	9.8	9.8	9.8	0.33	0.33	0.33	0.33	0.33	0.33
Forest	9.9	9.9	9.9	0.34	0.34	0.34	0.34	0.34	0.34
Lovebird	9.9	9.9	9.9	0.34	0.34	0.34	0.34	0.34	0.34
Race	9.8	9.8	9.8	0.34	0.34	0.34	0.34	0.34	0.34

of OAM video frames. The visible distortion for the ciphered video frames using the recommended cryptosystem can be computed by the distortion on the video frame edges [36]. The mathematical equation of the edge differential ratio (EDR) is computed as the edge distortion by Eq. (62). Table 6 shows that the EDR values between the enciphered and the original video frames are close to 1, ensuring the total difference between enciphered and original video frames. For the original, encrypted and decrypted video frames, Figure 9 displays the Laplacian of Gaussian edge detection. The edges of the enciphered video frames are totally different from those of the original video frames. It is also found that the detected edges are the same as those found in the original and decrypted video frames at low turbulence strengths, but the performance gets slightly worse, when the turbulence strength increases. These results show the superiority of the proposed HEVC cryptosystem.

$$\mathrm{EDR} = \frac{\sum_{i,j=1}^{N} |\mu(i,j) - \bar{\mu}(i,j)|}{\sum_{i,j=1}^{N} |\mu(i,j) + \bar{\mu}(i,j)|} \tag{62}$$

where $\mu(i,j)$, and $\bar{\mu}(i,j)$ are the detected edge pixel values of the plain and encrypted video frames, respectively.

TABLE 6. EDR performance metrics values.

Video frames		BQMall	Flamenco	Forest	Lovebird	Race
EDR	Low	0.879	0.902	0.905	0.91	0.907
	Moderate	0.905	0.902	0.905	0.91	0.907
	Strong	0.905	0.902	0.905	0.91	0.907

G. HISTOGRAM DEVIATION (D_H) AND IRREGULAR DEVIATION (D_I)

The ciphering accuracy of the proposed cryptosystem is evaluated by measurement of the maximum deviation from the histogram (D_H) of the plain and the ciphered video frames. D_I metric is used to reveal the ciphering quality of the proposed cryptosystem by calculating the maximum irregular deviation from an ideal encryption process [36], [45]. The results of the (D_H) and (D_I) values as depicted in Table 7 are low, meaning that the ciphered and original video frames are uncorrelated.

$$D_H = \frac{\frac{\theta_0+\theta_{255}}{2} + \sum_{i=1}^{254} \theta_i}{MN}$$
$$D_I = \frac{\sum_{i=1}^{255} |H(i) - M_H|}{MN} \tag{63}$$

TABLE 7. Histogram deviation (D_H) and irregular deviation (D_I).

Video frames	D_H			D_I		
	Low	Moderate	Strong	Low	Moderate	Strong
BQMall	0.392	0.477	0.477	0.0034	0.0034	0.0034
Flamenco	0.48	0.48	0.48	0.0031	0.0031	0.0031
Forest	0.46	0.46	0.46	0.0035	0.0035	0.0035
Lovebird	0.47	0.47	0.47	0.0032	0.0032	0.0032
Race	0.47	0.47	0.47	0.0034	0.0034	0.0034

TABLE 8. The entropies of the original and ciphered black and white images.

Image entropies			
All white images	Ciphered images	All black images	Ciphered images
0	7.99	0	7.99

TABLE 9. Processing times for the different encrypted video frames.

Cipher video frames computation processing time (Sec)				
BQMall.	Flamenco.	Forest.	Lovebird.	Race.
1.4	1.34	1.32	1.26	1.35

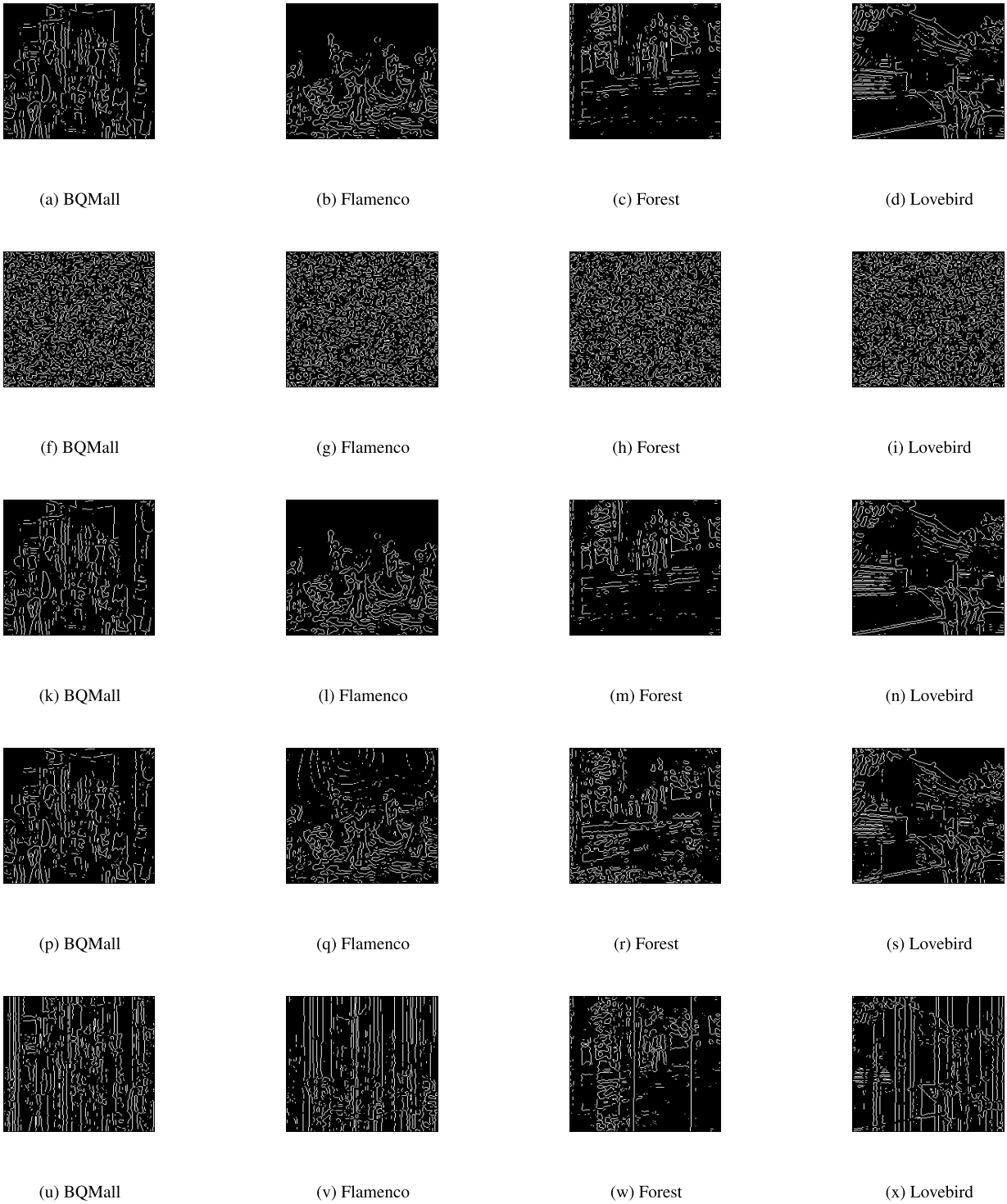
where θ_i is the absolute difference at the gray level i, M_H is the histogram value, and H is the difference video frame histogram.

H. KEY SENSITIVITY ANALYSIS

The cryptosystem should be sensitive to the used key. The chaotic map has the major benefit of providing significant and vital keyspace and great sensitivity to preliminary conditions. The video frames are encrypted with the correct key values during the simulation tests [36]. The key sensitivity efficiency in the proposed algorithm is tested by decrypting the different video frames with the right keys and with keys having slight modifications in the values of δ and z_0 [45]. So, if the primary input boundary values vary slightly, a massive change would occur at the output, and the video frame is irretrievable. Hence, the encrypted video frames cannot be decrypted, accurately. Therefore, the encrypted video frames, decrypted video frames and their histograms are shown in the Fig. 10 to verify the key sensitivity performance of the proposed HEVC cryptosystem with accurate and inaccurate secret key values. It is evident from these results that the proposed cryptosystem is highly sensitive to the case of a tiny shift in the secret key.

I. CHOSEN-PLAINTEXT AND KNOWN-PLAINTEXT ATTACK ANALYSIS

This section discusses the ability of the proposed HEVC cryptosystem to withstand selected-plaintext and known-plaintext attacks. Two different kinds of images have been used to verify if the proposed cryptosystem is robust enough to withstand these attacks [36], [45]. The first examined image is white, and the other examined image is black. The results of the two images are shown in Fig. 9. It is shown that no useful knowledge from the ciphered images can be reliably accessed. Thus, the proposed cryptosystem



(a) BQMall (b) Flamenco (c) Forest (d) Lovebird

(f) BQMall (g) Flamenco (h) Forest (i) Lovebird

(k) BQMall (l) Flamenco (m) Forest (n) Lovebird

(p) BQMall (q) Flamenco (r) Forest (s) Lovebird

(u) BQMall (v) Flamenco (w) Forest (x) Lovebird

FIGURE 9. Edge detection outcomes for: (a: e) original video frame edges; (f: j) encrypted video frame edges; (k: o) decrypted video frame edges under low turbulence strength; (p: t) decrypted video frame edges under moderate turbulence strength; and (u:y) decrypted video frame edges under strong turbulence strength.

offers greater resilience to such attacks. Table 8 also gives the entropies of the original black and white ciphered images, which assures the efficiency of the proposed cryptosystem.

J. COMPUTATION PROCESSING TIME

The proposed HEVC cryptosystem introduces lower encryption times for the whole analyzed video frames as shown in Table 9, which illustrates its applicability.

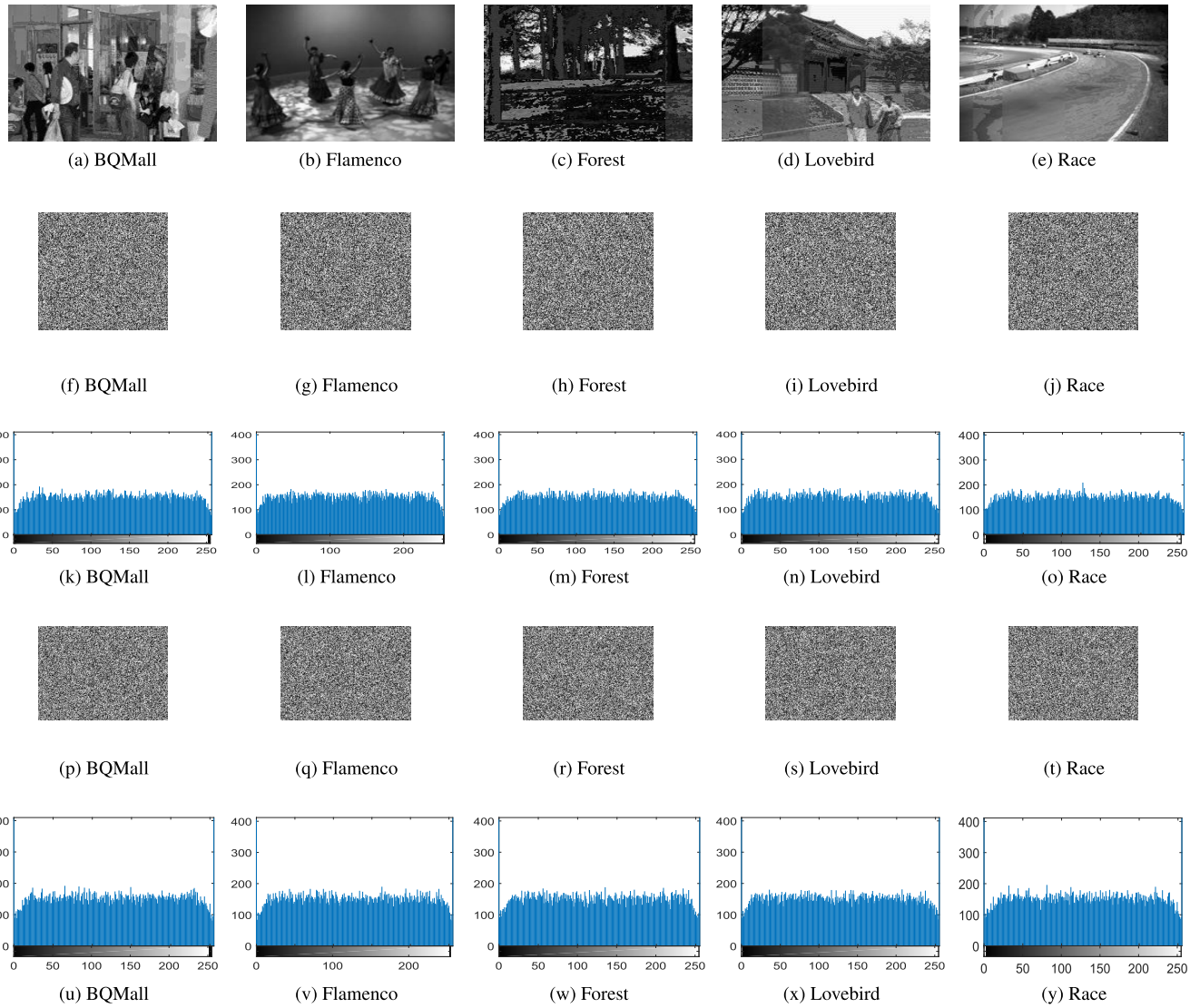


FIGURE 10. The key sensitivity test for different video frames: (a: e) The different decrypted video frames under moderate turbulence strength; (f: j) Different decoded video frames with $\delta_1 + 10^{-16}$; (k: o) Histograms of different decoded video frames with $\delta_1 + 10^{-16}$; (p: t) Different decoded video frames with $z_0 + 10^{-16}$;(u: y) Histograms of different decoded video frames at $z_0 + 10^{-16}$.

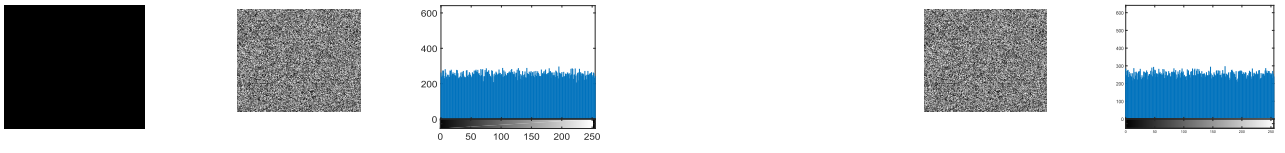


FIGURE 11. Experimental results for: (a: c) black image; (d: f) white image.

V. CONCLUSION AND FUTURE WORK

A closed-form expression for the upper bound of OAM BER has been derived, and it has been studied for FSO systems under GG turbulence channel. The proposed model is analyzed under different turbulence conditions and different SNR values. The obtained results indicate that there is a perfect match between analytical and simulation results from Mathematica and MATLAB, respectively. From the obtained results, it is indicated that the BER of OAM reaches nearly 10^{-7}, 10^{-5}, and 10^{-3} for low, moderate, and strong turbulence channel, respectively. The paper also offered a secure HEVC cryptosystem for OAM communication through GG turbulence channel model. Various experiments were implemented and carried out using five standard HEVC video frames by employing security key indicators such as visual inspection, entropy testing, histogram testing, computational

processing analysis, cipher quality measures, turbulence testing, and differential testing. The simulation and experimental results ensure that the proposed cryptosystem allows statistical ciphering with effective confusion, good channel turbulence immunity, and high robustness to different attacks. This study demonstrates the security and reliability of the proposed HEVC cryptosystem against various types of attacks.

As a future work, it would be interesting to consider the performance of OAM with different deep learning (DL) techniques in order to enhance the classification and prediction performance of the model and overcome the defects of OAM modulation. In addition, a further theoretical analysis can be conducted to approximate the performance of OAM with other modulation techniques and then test the theoretical and the simulation results using other simulators (e.g., RSoft optSIM). Additionally, we are interested in studying different DL techniques with other different security algorithms. We can also study various encryption/decryption algorithms with OAM-DL systems to improve the efficiency and reliability of these systems.

ACKNOWLEDGMENT

The authors would like to acknowledge the support received from Taif University Researchers Supporting Project Number (TURSP-2020/147), Taif university, Taif, Saudi Arabia.

REFERENCES

[1] 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.

[2] A. H. Gnauck, P. J. Winzer, S. Chandrasekhar, X. Liu, B. Zhu, and D. W. Peckham, "Spectrally efficient long-haul WDM transmission using 224-Gb/s polarization-multiplexed 16-QAM," *J. Lightw. Technol.*, vol. 29, no. 4, pp. 373–377, Feb. 15, 2011.

[3] W. Zhang, S. Zheng, X. Hui, R. Dong, X. Jin, H. Chi, and X. Zhang, "Mode division multiplexing communication using microwave orbital angular momentum: An experimental study," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1308–1318, Feb. 2017.

[4] D. J. Richardson, J. M. Fini, and L. E. Nelson, "Space-division multiplexing in optical fibres," *Nature Photon.*, vol. 7, no. 5, pp. 354–362, May 2013.

[5] E.-M. Amhoud, B. S. Ooi, and M.-S. Alouini, "A unified statistical model for atmospheric turbulence-induced fading in orbital angular momentum multiplexed FSO systems," *IEEE Trans. Wireless Commun.*, vol. 19, no. 2, pp. 888–900, Feb. 2020.

[6] A. E. Willner, J. Wang, and H. Huang, "A different angle on light communications," *Science*, vol. 337, no. 6095, pp. 655–656, Aug. 2012.

[7] A. Trichili, K.-H. Park, M. Zghal, B. S. Ooi, and M.-S. Alouini, "Communicating using spatial mode multiplexing: Potentials, challenges, and perspectives," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3175–3203, 2019.

[8] E. M. Amhoud, A. Trichili, B. S. Ooi, and M.-S. Alouini, "OAM mode selection and space–time coding for atmospheric turbulence mitigation in FSO communication," *IEEE Access*, vol. 7, pp. 88049–88057, 2019.

[9] S. Li, G. Chen, A. Cheung, B. Bhargava, and K.-T. Lo, "On the design of perceptual MPEG-video encryption algorithms," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 2, pp. 214–223, Feb. 2007.

[10] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, Nov. 2010.

[11] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.

[12] X.-Y. Wang, S.-X. Gu, and Y.-Q. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Opt. Lasers Eng.*, vol. 68, pp. 126–134, May 2015.

[13] J.-X. Chen, Z.-L. Zhu, Z. Liu, C. Fu, L.-B. Zhang, and H. Yu, "A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains," *Opt. Exp.*, vol. 22, no. 6, pp. 7349–7361, Mar. 2014.

[14] M. R. Abuturab, "An asymmetric single-channel color image encryption based on Hartley transform and gyrator transform," *Opt. Lasers Eng.*, vol. 69, pp. 49–57, Jun. 2015.

[15] M. Joshi, C. Shakher, and K. Singh, "Image encryption and decryption using fractional Fourier transform and radial Hilbert transform," *Opt. Lasers Eng.*, vol. 46, no. 7, pp. 522–526, Jul. 2008.

[16] T.-H. Chen, K.-H. Tsao, and Y.-S. Lee, "Yet another multiple-image encryption by rotating random grids," *Signal Process.*, vol. 92, no. 9, pp. 2229–2237, Sep. 2012.

[17] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Opt. Lasers Eng.*, vol. 56, pp. 83–93, May 2014.

[18] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.

[19] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," *Opt. Laser Technol.*, vol. 62, pp. 152–160, Oct. 2014.

[20] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, Jan. 2011.

[21] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons Fractals*, vol. 40, no. 5, pp. 2191–2199, Jun. 2009.

[22] E. A. Naeem, M. M. A. Elnaby, N. F. Soliman, A. M. Abbas, O. S. Faragallah, N. Semary, M. M. Hadhoud, S. A. Alshebeili, and F. E. A. El-Samie, "Efficient implementation of chaotic image encryption in transform domains," *J. Syst. Softw.*, vol. 97, pp. 118–127, Nov. 2014.

[23] O. S. Faragallah, H. S. El-Sayed, A. Afifi, and W. El-Shafai, "Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform," *Opt. Lasers Eng.*, vol. 137, Feb. 2021, Art. no. 106333.

[24] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.*, vol. 59, no. 10, pp. 3320–3327, May 2010.

[25] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.

[26] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," *Nonlinear Dyn.*, vol. 69, no. 4, pp. 2079–2087, Sep. 2012.

[27] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 4, pp. 394–400, Jan. 2008.

[28] X.-J. Tong, "Design of an image encryption scheme based on a multiple chaotic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 7, pp. 1725–1733, Jul. 2013.

[29] A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 12, pp. 4653–4661, Dec. 2012.

[30] J. Zhao, S. Wang, Y. Chang, and X. Li, "A novel image encryption scheme based on an improper fractional-order chaotic system," *Nonlinear Dyn.*, vol. 80, no. 4, pp. 1721–1729, Jun. 2015.

[31] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft Comput.*, vol. 26, pp. 10–20, Jan. 2015.

[32] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.

[33] T. Xiang, K.-W. Wong, and X. Liao, "Selective image encryption using a spatiotemporal chaotic system," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 17, no. 2, Jun. 2007, Art. no. 023115.

[34] C. Fu, B.-B. Lin, Y.-S. Miao, X. Liu, and J.-J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Opt. Commun.*, vol. 284, no. 23, pp. 5415–5423, Nov. 2011.

[35] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011.

[36] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.
[37] Z.-L. Zhu, W. Zhang, K.-W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Inf. Sci.*, vol. 181, no. 6, pp. 1171–1186, Mar. 2011.
[38] X. Wang and H.-L. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Opt. Commun.*, vol. 342, pp. 51–60, May 2015.
[39] L. Teng and X. Wang, "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive," *Opt. Commun.*, vol. 285, no. 20, pp. 4048–4054, Sep. 2012.
[40] E. Yavuz, R. Yazıcı, M. C. Kasapbaşı, and E. Yamaç, "A chaos-based image encryption algorithm with simple logical functions," *Comput. Electr. Eng.*, vol. 54, pp. 471–483, Aug. 2016.
[41] J.-X. Chen, Z.-L. Zhu, C. Fu, and H. Yu, "Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains," *Opt. Commun.*, vol. 341, pp. 263–270, Apr. 2015.
[42] H. M. Elhosany, H. E. Hossin, H. B. Kazemian, and O. S. Faragallah, "C9. Chaotic encryption of images in the fractional Fourier transform domain using different modes of operation," in *Proc. 29th Nat. Radio Sci. Conf. (NRSC)*, Apr. 2012, pp. 223–235.
[43] J. Chen, Z.-L. Zhu, L.-B. Zhang, Y. Zhang, and B.-Q. Yang, "Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption," *Signal Process.*, vol. 142, pp. 340–353, Jan. 2018.
[44] A. E. Elfiqi, H. S. Khallaf, S. F. Hegazy, A. Elsonbaty, H. M. H. Shalaby, and S. S. Obayya, "Chaotic polarization-assisted *L* DPSK-MPPM modulation for free-space optical communications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 9, pp. 4225–4237, Sep. 2019.
[45] O. S. Faragallah, M. A. Alzain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, and B. Soh, "Block-based optical color image encryption based on double random phase encoding," *IEEE Access*, vol. 7, pp. 4184–4194, 2019.
[46] O. S. Faragallah, M. A. AlZain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, and B. Soh, "Secure color image cryptosystem based on chaotic logistic in the FrFT domain," *Multimedia Tools Appl.*, vol. 79, nos. 3–4, pp. 2495–2519, Jan. 2020.
[47] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-Sayed, E. A. Naeem, M. A. Alzain, J. F. Al-Amri, B. Soh, and F. E. A. El-Samie, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," *IEEE Access*, vol. 8, pp. 42491–42503, 2020.
[48] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-Sayed, M. A. Alzain, J. F. Al-Amri, and F. E. A. El-Samie, "Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications," *IEEE Access*, vol. 8, pp. 103200–103218, 2020.
[49] W. El-Shafai, E.-S.-M. El-Rabaie, M. El-Halawany, and F. E. A. El-Samie, "Efficient multi-level security for robust 3D color-plus-depth HEVC," *Multimedia Tools Appl.*, vol. 77, no. 23, pp. 30911–30937, Dec. 2018.
[50] O. S. Faragallah, A. Afifi, H. S. El-Sayed, M. A. Alzain, J. F. Al-Amri, F. E. A. El-Samie, and W. El-Shafai, "Efficient HEVC integrity verification scheme for multimedia cybersecurity applications," *IEEE Access*, vol. 8, pp. 167069–167089, 2020.
[51] A. Alarifi, S. Sankar, T. Altameem, K. C. Jithin, M. Amoon, and W. El-Shafai, "A novel hybrid cryptosystem for secure streaming of high efficiency H.265 compressed videos in IoT multimedia applications," *IEEE Access*, vol. 8, pp. 128548–128573, 2020.
[52] S. A. El-Meadawy, H. M. Shalaby, N. A. Ismail, F. E. A. El-Samie, and A. E. Farghal, "Free-space 16-ary orbital angular momentum coded optical communication system based on chaotic interleaving and convolutional neural networks," *Appl. Opt.*, vol. 59, no. 23, pp. 6966–6976, 2020.
[53] H. G. Sandalidis, T. A. Tsiftsis, and G. K. Karagiannidis, "Optical wireless communications with heterodyne detection over turbulence channels with pointing errors," *J. Lightw. Technol.*, vol. 27, no. 20, pp. 4440–4445, Oct. 15, 2009.
[54] A. P. Prudnikov, I. A. Brychkov, and O. I. Marichev, *Integrals and Series: Special Functions*, vol. 3. Boca Raton, FL, USA: CRC Press, 1986.
[55] C. Fox, "The *G* and *H* functions as symmetrical Fourier kernels," *Trans. Amer. Math. Soc.*, vol. 98, no. 3, pp. 395–429, 1961.
[56] A. Jaiswal, M. R. Bhatnagar, and V. K. Jain, "Performance of optical space shift keying over gamma–gamma fading with pointing error," *IEEE Photon. J.*, vol. 9, no. 2, pp. 1–16, Apr. 2017.

SHIMAA AEL-MEADAWY received the B.Sc. and M.Sc. degrees in electrical engineering from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2013 and 2017, respectively. She is currently pursuing the Ph.D. degree in electrical engineering. She is currently an Assistant Lecturer with the Department of Electrical Engineering, Faculty of Electronic Engineering, Menoufia University. Her current research interests include optical communications, deep learning (DL) applications and computer vision, deep neural networks, information theory, elastic optical networks, image and video signal processing, efficient 2D video/3D multi-view video coding, multi-view video plus depth coding, 3D multi-view video coding and transmission, quality of service and experience, digital communication techniques, speech processing, and security algorithms.

AHMED E. A. FARGHAL received the B.Sc. (Hons.) and M.Sc. degrees from Menoufia University, Menoufia, Egypt, in 2006 and 2011, respectively, and the Ph.D. degree from the Egypt-Japan University for Science and Technology, Egypt, in 2015, all in electrical engineering. In 2007, he joined the Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, and was promoted to the position of a Lecturer Assistant, in 2011. From November 2014 to July 2015, he joined Kyushu University, Fukuoka, Japan, as a Special Research Student. From 2015 to 2018, he was with the Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, as an Assistant Professor. He is currently with the Department of Electrical Engineering, Faculty of Engineering, Sohag University, Sohag, Egypt. His research interests include optical CDMA, all-optical networks, QoS provisioning in optical networks, elastic optical networking, green optical networks, and nano-optoelectronic devices.

HOSSAM M. H. SHALABY (Senior Member, IEEE) was born in Giza, Egypt, in 1961. He received the B.S. and M.S. degrees from Alexandria University, Alexandria, Egypt, in 1983 and 1986, respectively, and the Ph.D. degree from the University of Maryland at College Park, in 1991, all in electrical engineering. In 1991, he joined the Department of Electrical Engineering, Alexandria University, and was promoted to a Professor, in 2001. From 1996 to 1998, he was with the Department of Electrical and Computer Engineering, International Islamic University Malaysia, and from 1998 to 2001, he was with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. From December 2000 to December 2004, he was an Adjunct Professor with the Faculty of Sciences and Engineering, Department of Electrical and Information Engineering, Laval University, Quebec, QC, Canada. From 2007 to 2010, he worked as a Consultant with SysDSoft Company, Alexandria, Egypt. From 2010 to 2016, he was the Chair of the Department of Electronics and Communications Engineering (ECE), Egypt-Japan University of Science and Technology (E-JUST), New Borg EL-Arab City, Egypt. Since 2017, he has been on leave from Alexandria University, where he is currently a Professor with the Department of ECE, School of Electronics, Communications, and Computer Engineering, E-JUST. His research interests include optical communications, silicon photonics, optical CDMA, and quantum information theory. He has been serving as a Student Branch Counselor for the IEEE E-JUST Student Branch, since 2020.

NABIL A. ISMAIL received the Ph.D. degree in computer engineering from Durham University, in 1983. From August 2006 to August 2008, he was the Dean of the Faculty of Computers and Information, Menoufia University. He is currently a Professor of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University. His main research interests include deep learning applications and computer vision, tomography, computer security, computer architecture, elliptic curve cryptography, processor design, light-power smart devices, security applications, EIT algorithms, and multi-core/many-core parallel programming.

FATHI E. ABD EL-SAMIE received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees from Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. Since 2005, he has been a Teaching Staff Member with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. His current research interests include image enhancement, image restoration, image interpolation, super-resolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications. He was a recipient of the Most Cited Paper Award from the *Digital Signal Processing* journal, in 2008.

MOHAMMED ABD-ELNABY received the B.S., M.S., and Ph.D. degrees in electronic engineering from Menoufia University, Menouf, Egypt, in 2000, 2004, and 2010, respectively. Since 2010, he has been a Teaching Staff Member with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. Since 2015, he has also been working as an Associate Professor with the Department of Electronics and Electrical Communication, Faculty of Electronic Engineering, Menoufia University. He has coauthored about 69 articles in international journals and conference proceedings. His research interests include wireless resource management, MAC protocols, cognitive radio, cooperative communication, the IoT, 5G communication, NOMA, and D2D communication.

WALID EL-SHAFAI was born in Alexandria, Egypt. He received the B.Sc. degree (Hons.) in electronics and electrical communication engineering from the Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt, in 2008, the M.Sc. degree from the Egypt-Japan University of Science and Technology (E-JUST), in 2012, and the Ph.D. degree from the Faculty of Electronic Engineering, Menoufia University, in 2019. Since January 2021, he has been joined as a Postdoctoral Research Fellow with the Security Engineering Lab (SEL), Prince Sultan University (PSU), Riyadh, Saudi Arabia. He is currently working as a Lecturer and an Assistant Professor with the Department of Electronics and Communication Engineering (ECE), FEE, Menoufia University. His research interests include wireless mobile and multimedia communications systems, image and video signal processing, efficient 2D video/3D multi-view video coding, multi-view video plus depth coding, 3D multi-view video coding and transmission, quality of service and experience, digital communication techniques, cognitive radio networks, adaptive filters design, 3D video watermarking, steganography, encryption, error resilience and concealment algorithms for H.264/AVC, H.264/MVC, and H.265/HEVC video codecs standards, cognitive cryptography, medical image processing, speech processing, security algorithms, software defined networks, the Internet of Things, medical diagnoses applications, FPGA implementations for signal processing algorithms and communication systems, cancellable biometrics and pattern recognition, image and video magnification, artificial intelligence for signal processing algorithms and communication systems, modulation identification and classification, image and video super-resolution and denoising, cybersecurity applications, malware and ransomware detection and analysis, deep learning in signal processing, and communication systems applications. He also serves as a reviewer for several international journals.