Journal of Optics
https://doi.org/10.1007/s12596-024-02253-7

RESEARCH ARTICLE

OptiFusion steganography method based on masking OFDM signal in Gaussian beam intensity

Kamal H. Kadem[1] · **Mohammed F. Mohammed**[1]

Received: 3 July 2024 / Accepted: 12 September 2024

Abstract

In free-space optical (FSO) communications, robust security is crucial. Multiple strategies, such as encryption and spatial diversity, are typically used. However, this research proposes optical steganography, which hides transmitted data rather than encrypting it. This study introduces "OptiFusion Steganography," a novel technology that uses the shape and intensity of Gaussian beams to hide data by masking an Orthogonal Frequency Division Multiplexing (OFDM) signal within the optical beam. Simulations tested the OptiFusion method under various atmospheric conditions and propagation distances, demonstrating its significant enhancement of FSO communication security, with resilience against both minor and severe turbulences.

Keywords Optical steganography · Free space · Gaussian Beam · Security · OFDM · Turbulences

Introduction

Free Space Optical (FSO) is a line-of-sight technology that uses lasers to provide optical bandwidth connections FSO is an optical communication technique that propagates the light in free space, which means air, outer space, vacuum, or something similar to wirelessly transmit data for telecommunication and computer networking [1]. FSO is a subset of OWC that Specializes in long-distance communication through free space. It's becoming a preferred choice over Radio Frequency (RF) communications, thanks to many advantages like no license requirement, broad bandwidth, and enhanced energy efficiency in addition to the inherent security and durability against external turbulence [2]. FSO communication system offers several advantages over the RF system. The major difference between FSO and RF communication arises from the large difference in the wavelength. For the FSO system, under clear weather conditions (visibility > 10 miles), the atmospheric transmission window lies in the near-infrared wavelength range between 700 nm and 1600 nm. The transmission window for the RF system lies between 30 mm and 3 m. Therefore, RF wavelength is thousands of times larger than optical wavelength. This high ratio of wavelength leads to some interesting differences between the two systems [3]. From the security perspective, FSO communications offer greater security than conventional RF due to the direct line of sight (LOS) required between the transmitter and receiver. This physical alignment ensures that only the intended recipient can access the signal, as any disruption in LOS halts transmission, preventing unauthorized interception. Nonetheless, they could be susceptible to interception by eavesdropping methods [4]. The challenge of ensuring secure communication in the presence of an external eavesdropper has been a fundamental issue in communications since Wyner first introduced the concept of the wiretap channel [5].

Despite the large range of strategies and conceptual frameworks used to ensure data security, hackers continue their efforts to illegally access data without permission. For that, any communication system must develop preventive measures, even for systems like FSO communications that inherently possess a degree of self-security. The necessity for ongoing development of security measures arises because methods of interception and penetration evolve concurrently with protective technologies. In FSO communication systems, many security techniques simpler or more

✉ Kamal H. Kadem
st.kamal.hussein.phd@ced.nahrainuniv.edu.iq

✉ Mohammed F. Mohammed
mohammed.al-temimi@nahrainuniv.edu.iq

[1] Department of Laser and Optoelectronics, College of Engineering, Al-Nahrain University, Jadriyah, Baghdad, Iraq

Published online: 10 October 2024

complex are utilized to prevent eavesdropping and interception as Encryption [6], Spatial Diversity [7], Temporal Diversity [8], and Quantum Cryptography [9].

In this study, we present a novel optical steganography to protect FSO communication that depends on masking data meant to be safeguarded within the transmission beam itself. Steganography, derived from the Greek word meaning "covered writing," refers to the art of hiding data to avoid detection. It encompasses various techniques aimed at concealing the existence of data in secret communications. These methods range from invisible inks and microdots to sequencing messages, digital signatures, and hidden channels in wide-spectrum communications [10]. Steganography is closely related to cryptography, both belonging to the realm of secret communication. Cryptography shields the content of a message through the use of encryption keys, ensuring its protection. On the other hand, steganography focuses on hiding the very presence of the message within a "cover" medium. While cryptography finds extensive usage in various everyday applications, both techniques have their respective domains of application and can potentially be combined for enhanced security measures. This trend highlights the increasing interest in merging or comparing these two disciplines within the research community. While the combination of multiple security mechanisms may appear advantageous, it is important to note that the suitability of combining cryptography with steganography can vary [11].

Optical steganography is a specialized branch of steganography that concentrates on hiding data within the optical spectrum or optical media [12]. It uses a variety of techniques that rely on hiding data, carrier waves, or beams in different ways. Some of these methods take advantage of the characteristics of the spectrum (phase, polarization, amplitude) to hide data in optical communications [13–15]. Like general steganography, optical steganography aims to secure communication by ensuring that only intended recipients are aware of the existence of the transmitted data and where is it hidden.

In this paper, we depended on the intensity and spatial profile of a Gaussian Beam (GB), coupled with Discrete Cosine Transform 2 (DCT2) and Inverse Discrete Cosine Transform 2 (IDCT2) algorithms developed. These tools were utilized to mask a digital Orthogonal Frequency Division Multiplexing (OFDM) signal within a segment of the Gaussian beam intensity. The masking of the OFDM signal can be controlled at any portion within the intensity profile of the Gaussian beam. This masking was executed without altering the beam's fundamental characteristics such as its shape and intensity. By meticulously adjusting the beam's profile and intensity before hiding the data, and subsequently restoring these parameters post-hiding, the original conditions of the optical beam were preserved. Upon reception, the hidden OFDM signal was precisely extracted from a specific segment of the Gaussian beam. This process involved isolating the segment carrying the OFDM signal from the remainder of the beam, and then decoupling the OFDM signal from the optical carrier. This method ensured that the original characteristics of the Gaussian beam both in shape and intensity remained unchanged, allowing for efficient and effective data retrieval. To validate the robustness of this approach, the system was tested under various atmospheric conditions that could potentially affect the beam's intensity and profile during transmission over different distances. These tests were crucial for assessing the impact of environmental factors on the integrity of the Gaussian beam and the consequent recovery of the OFDM signal and its data content. Additionally, a pseudo-random information source with 16-QAM modulation and OFDM technology was employed. The proposed system was modeled and simulated for optical steganography in Gaussian beam a 16-QAM-OFDM-FSO communication system with various weather conditions under the von Karman channel model by using Matlab R2022b Version 9.13.

The structure of this paper is organized as follows: Sect. 2 is a statement about the novel optical steganography method: comparison and advantages over existing techniques. Section 3 introduces the optifusion steganography design. Section 4 examines the Free Space Effects on Data Masking Beam. Sections 5 and 6 discuss the results and conclude the paper, respectively.

Novel optical steganography method: comparison and advantages over existing techniques

Our study introduces a novel method in optical steganography with significant potential for future development. This approach can be used as a standalone protection technique or combined with other security measures like encryption, beam shaping, and temporal or spatial diversity. Its flexibility and simplicity make it an effective way to enhance security at the physical layer of optical communication systems—a critical aspect [16]. Given the increasing reliance on optical communication technologies such as FSO and optical cables (fiber optic) and the current shortage of methods for hiding data within optical carriers, it is crucial to focus on developing and refining optical steganography. Advancing development and expansion in this field is equally important, if not more crucial, than other protection. By continuously exploring and enhancing these methods, we can better protect optical communication systems against potential threats from eavesdroppers.

It involves hiding the OFDM signal, which carries the data to be transmitted, within a small portion of the Gaussian beam. This concealment is achieved without altering or distorting the shape of the Gaussian beam, leaving no indication that the beam carries any hidden data. Since the OFDM signal is hidden in such a small part of the beam, it remains undetectable to potential eavesdroppers. Even if someone attempts to extract the data using conventional methods or a standard receiving device, they will not succeed because they would need to know the precise location of the OFDM signal within the Gaussian beam and this can only be determined using the OptiFusion Steganographic Decoder System that we designed and developed.

To showcase the capabilities, potential, and advantages of our proposed concealment method, it is essential to compare it with the latest methods introduced recently, as well as with the most effective optical steganography techniques.

A recent study on optical steganography in FSO communications involved hiding the OFDM signal within a CW laser and then using a steganographic encoder to insert an image, known as a cover image, onto the CW laser carrying the OFDM signal. This approach results in a CW laser that carries an image concealing the OFDM signal. Strengths include improved BER performance and resilience under adverse weather conditions, while weaknesses might involve potential vulnerability to advanced steganalysis techniques and increased computational complexity [17]. When comparing this method to our approach, we observe that both methods leverage the OFDM signal due to its advantageous properties, including the ability to increase the amount of transmittable data. However, the use of a cover image creates an opportunity for eavesdroppers to attempt to extract the hidden data. In contrast, our method eliminates this vulnerability by providing no visible environment or context for the eavesdropper to target. The Gaussian beam appears empty, without any indication that it carries data, images, or anything else.

One of the ways effective methods of optical steganography in FSO communication is Spectral-Polarization Coding (SPC) Optical Code-Division Multiple Access (OCDMA) systems to hide a stealth signal within a public BPSK channel. The technique uses pulse broadening and balanced detection to hide the stealth signal, making it virtually undetectable in the public channel. Strengths include enhanced security and minimal interference with public channels. Weaknesses involve complexity in implementation and potential challenges in synchronization and decoding under varying conditions [18]. What was also found in this method is that hidden signal and noise can negatively impact the overall network. In contrast, in our method the stealth signal (OFDM signal) does not affect on the Gaussian beam that carries it in order not to be detected, this is done by relying on hiding the stealth signal in a portion of the Gaussian beam. This is done using the developed (DCT2) algorithms that are compatible with optical beams, which work to stretch and compress the OFDM signal to fit the masking location in the optical beam.

Another idea that relies on optical steganography is “hiding” a low-power optical beam within a high-power beam. This is achieved by employing orthogonal spatial modes specifically, orbital angular momentum (OAM) modes for co-axial transmission of the strong and weak beams. Despite sharing the same frequency band and polarization, the strong and weak beams can be effectively separated with minimal crosstalk due to their spatial orthogonally, making the weak beam difficult to detect without prior knowledge of the transmission scheme [19]. Our proposed method is simpler as it does not require multiple laser sources or separate high- and low-energy beams. Instead, it uses a single beam that is split into two beams. However, our method is Similar to this method in terms of concealment strength, as extracting the hidden data requires knowledge of both the transmission and reception scheme.

This method demonstrated effectiveness in fiber optic communications, but FSO communications still need development and it depends on using wide-band spontaneous emission light sources, such as those from amplified spontaneous emission (ASE), to achieve FSO stealth communication. The signal is hidden within the phase randomness of the wideband noise and can only be recovered by authorized receivers using pre-shared keys that match optical delays at both the transmitter and receiver. This method offers robust physical layer security, effective protection against eavesdropping, and the ability to use existing light sources without extra power. However, it requires precise synchronization and delay matching, has a limited transmission distance, and may be vulnerable to jamming attacks [20, 21]. In contrast, our method is more straightforward and allows for a longer propagation distance. It is also more reliable in extracting the OFDM signal from the transmitting beam, with a lower likelihood of data loss compared to this method, where the risk of losing data is higher in this method due to interference between the noise carrying the data, the noise generated by the transmitters, and the noise present in the FSO medium.

We find that the most important advantages of our method are its simplicity, low complexity, and effectiveness, as it relies on a single laser source with the flexibility of hiding the OFDM signal since its location within the Gaussian beam is unknown and variable. The use of OFDM technology increases the amount of hidden data that can be transmitted and strengthens the method due to the inherent advantages of OFDM technology. Additionally, this method is adaptable for use with other optical beams, as it depends on the shape and intensity of the beam. There are also other strengths, previously mentioned when comparing our method with other approaches in research focused on protecting data in FSO communications through data hiding. A key criticism of our method, which requires further development on this side, is the data loss caused by severe weather conditions. This results in a significantly reduced propagation distance in free space while attempting to preserve the integrity of the transmitted data.

OptiFusion steganography design

The innovative concept of hiding data within an optical beam involves embedding a signal, originating from OFDM, into a segment of the optical beam's intensity. This is accomplished by splitting the original beam into two fractions: one that conveys data and the other that remains devoid of any data. These fractions are subsequently merged, ensuring the recombined beam closely mirrors the original in both shape and intensity, displaying no apparent alterations. Because more than one integration process is performed in this method, we suggest naming it "OptiFusion Steganography". The OptiFusion method setup includes the OptiFusion Steganographic Encoder in the transmitter system and the OptiFusion Steganographic Decoder in the receiver system. These systems are explained in detail as follows:

OptiFusion steganographic encoder system

The experimental setup for the OptiFusion Steganography method in the Transmitter System, as illustrated in Fig. 1, includes a continuous laser source. Specifically, it employs a laser diode operating at a wavelength of 1550 nm to produce a Gaussian beam. This beam is then amplified to increase its intensity. Followed by the application of an advanced discrete cosine transform algorithm (DCT2) developed to fit the Gaussian beam, where this algorithm finely tunes the beam's intensity, facilitating the compression of OFDM signal within the Gaussian beam for more efficient data hidden.

The Gaussian beam is meticulously split into two segments using a divider, with special consideration for the dimensions of each segment. Notably, the smaller the portion of the beam designated for data concealment, the higher the effectiveness of the hiding process. This segmentation process is crucial and adjusts based on the volume of data that needs to be concealed. Essentially, the larger the quantity of data to be hidden, the greater the portion of the beam used for data concealment. Conversely, when the data size is smaller, the segment of the beam carrying the data reduces, resulting in a larger portion of the beam remaining empty, this case is more efficient for hiding data, as it optimizes the use of space within the beam according to the data size.

Subsequently, the lesser of the two beams undergo modulation in a Mach-Zehnder Modulator (MZM), where it is infused with a digital OFDM signal. This signal is enriched with randomly generated data, encoded using the 16-QAM modulation technique to fully leverage the inherent advantages of OFDM and enhance the Proposed technology efficiency. Following modulation, the beam, now carrying the digital OFDM signal, is recombined with its counterpart, which remains devoid of concealed data. This reintegration is performed with precision, ensuring the newly formed beam retains the original shape and intensity of the initial laser output, thereby concealing any evidence of the data transmission. The beam, now a composite of both beams, is subsequently passed through a modified inverse discrete cosine transform (IDCT2) followed by an attenuator to fine-tune the beam's intensity. This ensures the emergent beam from the system mirrors the initial input from the laser diode in both form and function, conspicuously free of any signs of the hidden data.

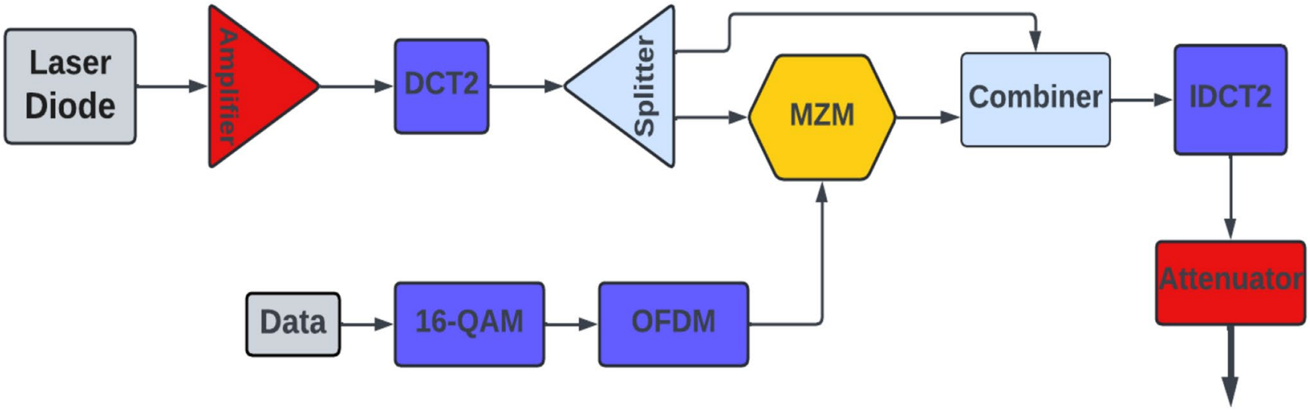

Fig. 1 Simulation of OptiFusion Steganographic Encoder System in the Transmitter

OptiFusion steganographic decoder system

In the receiver system, the process of extricating the hidden OFDM signal and subsequently demodulating it to unveil the data involves several meticulously executed steps as in Fig. 2.

Figure 2 Simulation of OptiFusion Steganographic Decoder System in the Receiver.

Initially, as the beam makes its entry into the system, its intensity is enhanced by an amplifier. Following amplification, this intensified beam is methodically divided into two parts through the use of a splitter. These parts are then subjected to distinct processing paths: one part is routed directly towards a discrete cosine transform process (DCT2), while the other part is first modulated in intensity before it, too, proceeds to undergo DCT2 processing. This step is crucial for preparing the beam for the subsequent extraction of data. After undergoing DCT2, the beams are again partitioned, this time mirroring the original segmentation executed within the transmission system, ensuring that the resultant beam fragments are congruent with their initial subdivisions.

These segmented beams are then ingeniously combined using a combiner, where the beam that traversed the intensity modulator is subtracted from its counterpart that bypassed modulation. This subtraction technique is pivotal for isolating the embedded OFDM signal from the rest of the optical beam. The optical beam, now stripped of its excess optical components and retaining the OFDM signal, is funneled into a specialized device designed for this precise separation a Mach-Zehnder Interferometer (MZI). Finally, data is extracted from the OFDM signal through the demodulation process of 16-QAM-OFDM.

Examine of OptiFusion steganography: (operational efficiency and data integrity)

To validate the efficacy of our innovative OptiFusion steganography method, which embeds data in the intensity profile of an optical beam to both transmit and protect it from unauthorized detection, we meticulously evaluate the beam's shape and intensity. This examination is conducted both before and after the incorporation of the OFDM signal into the optical beam, with a comparison of the two conditions. Figure 3 illustrates that, in comparing the Gaussian beam with and without hidden data in both 2D and 3D representations, there is no change in the intensity or shape of the Gaussian beam after embedding the hidden data using the OptiFusion steganography method.

This consistency plays a pivotal role in obscuring the presence and location of the hidden data from potential interceptors or eavesdroppers. The inability of conventional analysis methods to detect any alterations in the beam ensures that unauthorized parties cannot extract the hidden data without extensive knowledge of the specific techniques, mechanisms, and algorithms used for data hiding.

Another method for evaluating the OptiFusion steganography technique is through a Back-to-Back (BTB) test simulation. In this setup, the system's transmitter and receiver telescopes are directly connected, eliminating any external interference or intermediaries. This arrangement simulates an ideal transmission environment, free from common distance-related impairments such as signal loss, dispersion, and nonlinearity, allowing us to assess the system's optimal performance. This evaluation aims to benchmark the system's capabilities before considering additional variables like transmission distance or fluctuating weather conditions, as shown in Fig. 4. The results of this simulation are

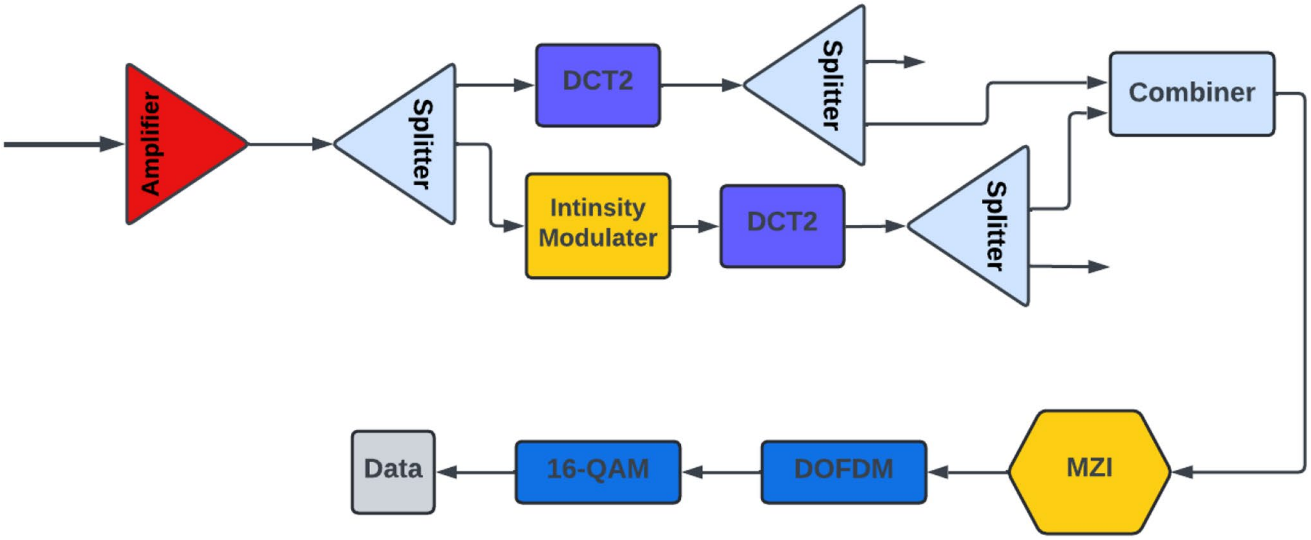

Fig. 2 Simulation of OptiFusion Steganographic Decoder System in the Receiver

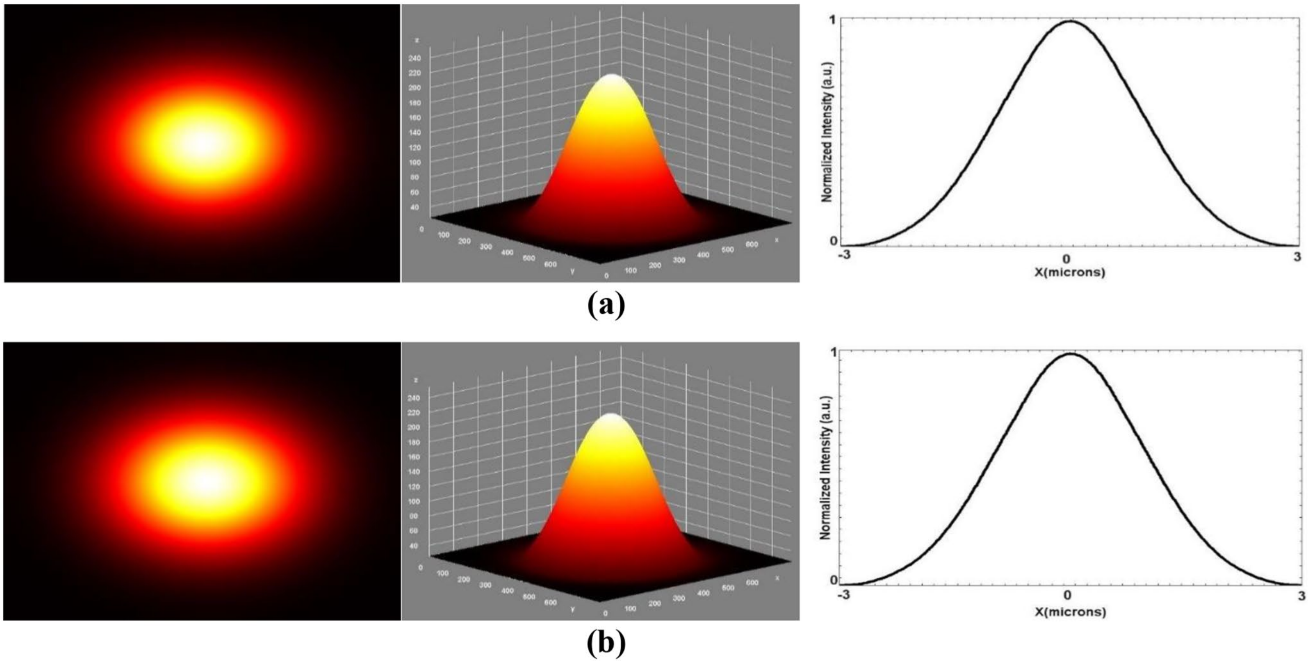

Fig. 3 A Gaussian beam (GB): (**a**) without OptiFusion Steganography and (**b**) with it. The left column displays intensity profiles, the middle shows 3D intensity profiles, and the right presents intensity distribution

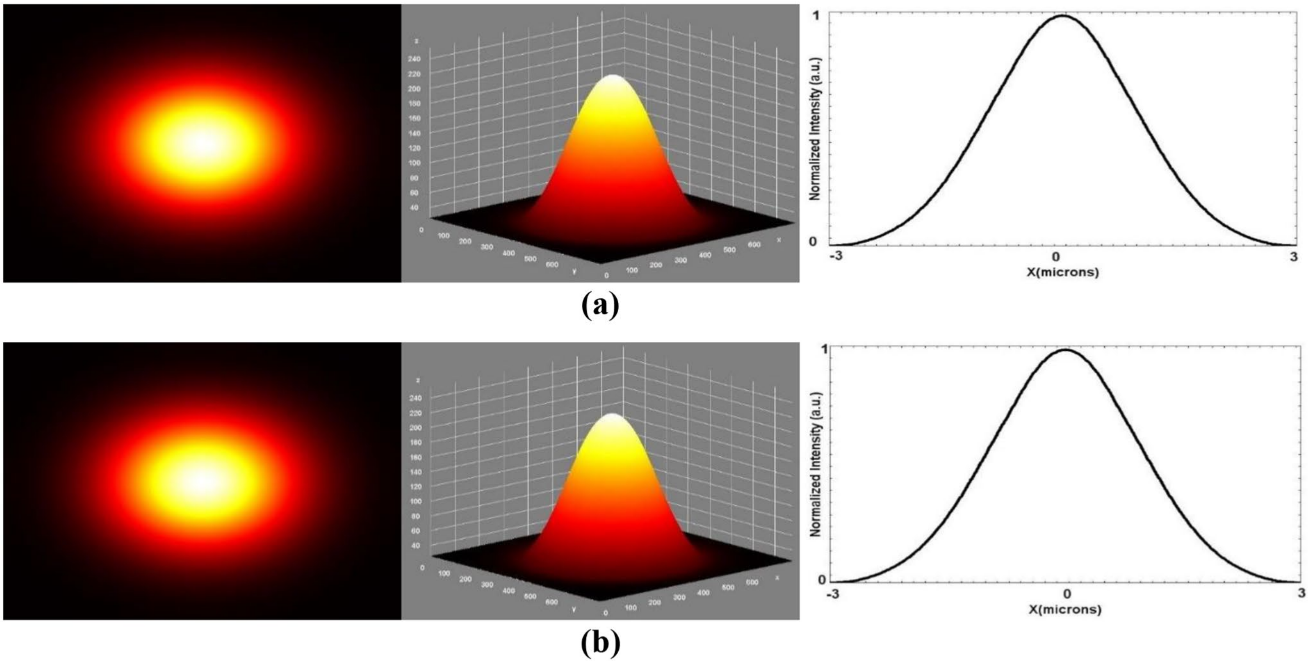

Fig. 4 A Gaussian beam (GB): (**a**) exiting the transmitter and (**b**) entering the receiver. The left column displays intensity profiles, the middle shows 3D intensity profiles, and the right presents intensity distribution

promising, indicating a high degree of similarity between the transmitted and received Gaussian beam signals in terms of both shape and amplitude.

Figure 4 shows a Gaussian beam (GB): (a) exiting the transmitter and (b) entering the receiver. The left column displays intensity profiles, the middle shows 3D intensity profiles, and the right presents intensity distribution.

Notably, there is no discernible evidence within the beam to suggest that it carries hidden data. Moreover, the extraction of hidden data within the receiving system is achieved flawlessly, with no observable loss or degradation. This approach demonstrates the system's ability to maintain the integrity of the Gaussian beam and securely retrieve hidden data, highlighting its robustness in an idealized simulation free from real-world propagation challenges.

Free space effects on data masking beam

To assess the effectiveness of the proposed system in maintaining the integrity of data hidden within Gaussian beams over varying distances in free space, it's essential to analyze the impact of atmospheric parameters on beam spread. Understanding these parameters, particularly atmospheric turbulence the most critical factor validates and enhances the system's performance. It is essential to examine the influence of atmospheric turbulence on the propagation of Gaussian beams and thoroughly comprehend how distortions, caused by turbulent variations in the refractive index, substantially alter the characteristics of this Gaussian beam during their passage through the atmosphere [22].

This study examines the impact of turbulence using the modified von Kármán Spectrum model (MVKS), which accounts for both inner and outer scale effects, as described in Eq. 1 [23]

$$\Phi_n\left(k\right) = 0.033C_n^2\frac{e^{-\frac{k^2}{k_m^2}}}{\left(k^2+k_o^2\right)^{\frac{11}{6}}} \qquad 0 \leq\ k \gg\ \infty \tag{1}$$

Where C_n^2 is the index of refraction structure parameter, also called the structure constant C_n^2 typically ranges from $10^{-17}m^{-2/3}$ or less for conditions of "weak turbulence" to $10^{-13}m^{-2/3}$ when the turbulence is "very strong.",k is the wave number, $k_m = 5.92/l_o$ is an equivalent unbounded wavenumber corresponding to the inner scalel_0, and $k_o = 2\pi\ /L_0$ outer scale L_0. The atmospheric refractive index variation is characterized as a stochastic process. In the research, atmospheric turbulence is generated through simulation by using a method involving random phase screens. This method models the effects of turbulence on Gaussian beam propagation by introducing phase distortions that simulate the random fluctuations in the atmospheric refractive index. The random phase screens are strategically placed along the propagation path of the modulated optical beam.

The simulation incorporates one or more phase screens that randomly alter the phase of the transmitted Gaussian beam. These screens are placed at certain locations between the transmitter and the receiver. The Gaussian beam is transmitted through these phase screens. As the beam passes through each screen, its phase is altered, simulating the effect of traveling through a turbulent medium. The effect of turbulence on the wave is analyzed using a combination of Fourier transforms and the Kirchhoff-Fresnel integral. This analytical approach helps in understanding how phase distortions impact the amplitude and phase of the Gaussian beam, thereby affecting the hidden data they carry [24]. This style allows for a detailed study of how atmospheric turbulence can affect the propagation of optical beams, particularly focusing on the distortions introduced to the phase and amplitude of the beams, which are critical for optical communication technologies.

Through meticulous modeling and simulation, we delve into analyzing the OptiFusion Steganography performance by placing the beam emerging from it under the influences of atmospheric from weak to strong passing through moderate turbulence, as well as the effect of propagation distances in free space, as in Fig. 5.

Figure 5 Overview of propagation of a Gaussian beam in free space, based on the OptiFusion Steganography method, with the effects of turbulence.

Our focus extends to understanding the general impact of free-space characteristics and the propagation distance of the Gaussian beam on data hidden efficacy. By systematically investigating these factors, the study aims to not only propose a groundbreaking method for data hiding within the Gaussian beam but also to thoroughly evaluate its resilience and reliability under diverse environmental conditions and distances. This comprehensive analysis is pivotal in demonstrating the method's potential applicability and robustness in real-world optical communication scenarios, where

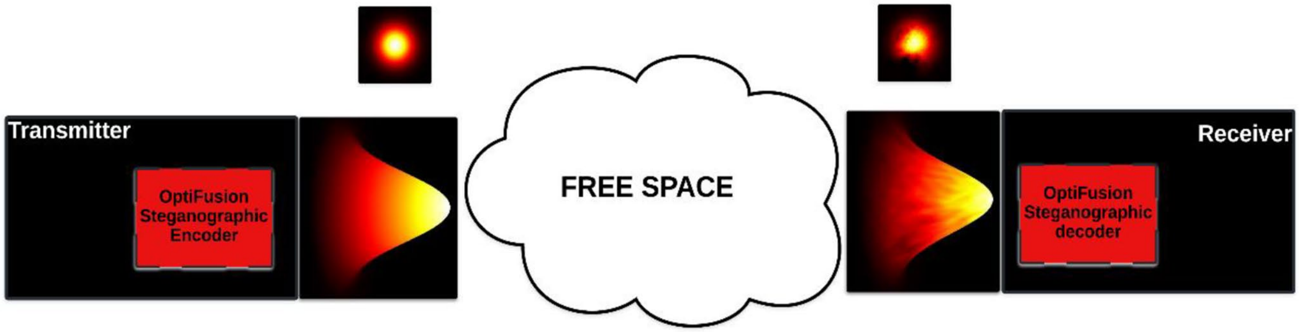
Transmitter
OptiFusion Steganographic Encoder
FREE SPACE
Receiver
OptiFusion Steganographic decoder

Fig. 5 Overview of propagation of a Gaussian beam in free space, based on the OptiFusion Steganography method, with the effects of turbulence

atmospheric turbulence and propagation distances play critical roles in system performance.

In this section, we analyze the effect of atmospheric turbulence on a Gaussian beam at two different intensity levels (weak and strong) over free-space propagation distances ranging from 1 m to more than 10 km. Figure 6 shows the impact of weak turbulence, with a turbulence strength of$C_n^2 = 10^{-17}$, on the beam's shape and intensity across various distances. The analysis of the Gaussian beam intensity profiles and the status of the embedded data demonstrates that the beam not only preserves its embedded data over distances exceeding 10 km but also maintains its structural integrity, remaining largely unaffected by minor disturbances in free space.

Under strong turbulence conditions withC_n^2=10^{-13}, significant distortion occurs, and the Gaussian beam begins to lose its original shape. The beam cannot withstand the effects of strong turbulence, limiting its propagation to less than 100 m before the embedded data becomes unrecoverable, as shown in the bottom row of Fig. 6.

Result analysis

The proposed Optifusion method, when integrated into an optical communication system, seeks to enhance data security by masking the transmitted data within the intensity profile of the Gaussian beam. To evaluate the Optifusion method, we conduct a direct comparison of two scenarios: In the first scenario, the beam carries the OFDM signal conventionally, using a standard method. In the second scenario, the OFDM signal is hidden within the Gaussian beam using the Optifusion method. Both scenarios were tested across identical atmospheric conditions and transmission mediums, with propagation distances ranging from 1 m to 10 km. The reason we chose these long distances for testing, is that in the long-range communications, data loss typically increases due to Accumulated weather disturbances increasing and optical communication systems modifications complexity. However, the Optifusion method does not require modifications when the transmission distance increases. In fact, as the propagation distance increases, the inherent blurring effect of Optifusion enhances data protection.

As regards the Channel State Information (CSI) about the interaction between the Gaussian beam and various atmospheric disturbances, from weak to strong passing through the moderate. This CSI helps us assess the strengths and limitations of the Optifusion method, determining its robustness and ability to maintain data integrity over different propagation distances. Key performance indicators Signal-to-Noise Ratio (SNR) and Bit Error Rate (BER) were computed for the optical communication system with and without the Optifusion method. By examining these metrics, we gained insight into the effectiveness of Optifusion in preserving and concealing data. All results and figures were generated using MATLAB Version 9.13.

In Fig. 7a, b, and c, we present the calculated SNR values for a Gaussian beam, both with and without OptiFusion, across varying atmospheric turbulence levels: weak, moderate, and strong, characterized by turbulence strengths of Cn^2 = 10^{-17}, 10^{-15}, and 10^{-13}, respectively. The figures illustrate the performance of both the standard Gaussian beam, which

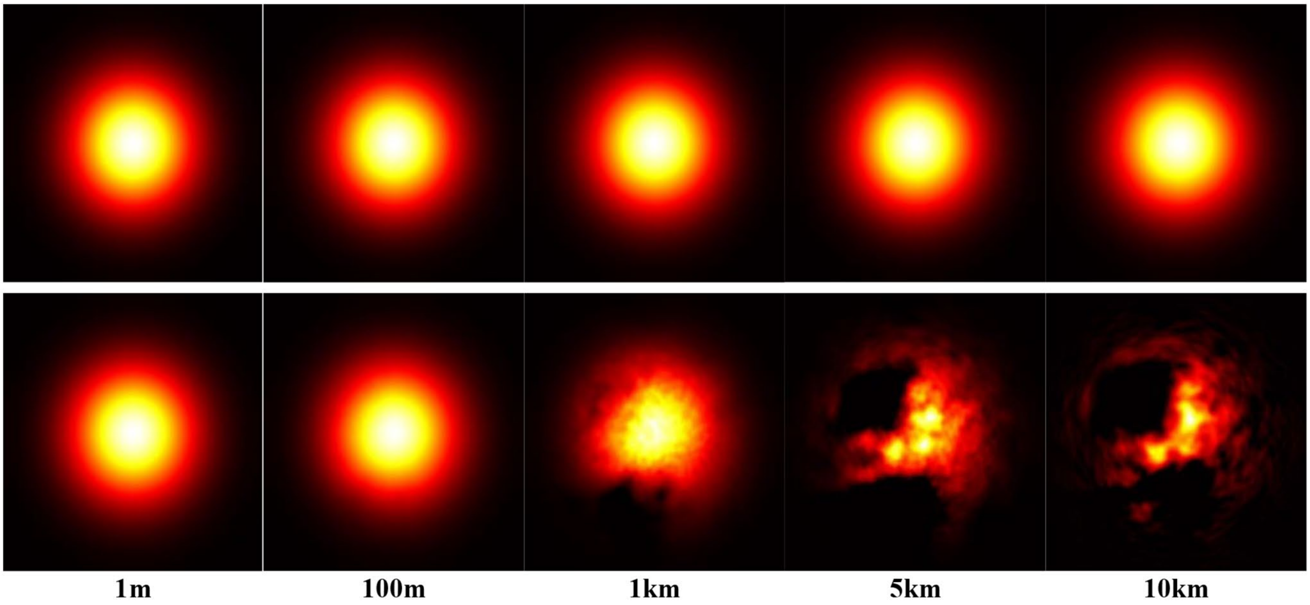

Fig. 6 GB simulations: the top row under weak turbulence and the bottom row under strong turbulence. Columns display beam intensity profiles at distances of 1m, 100m, 1km, 5km, and 10km

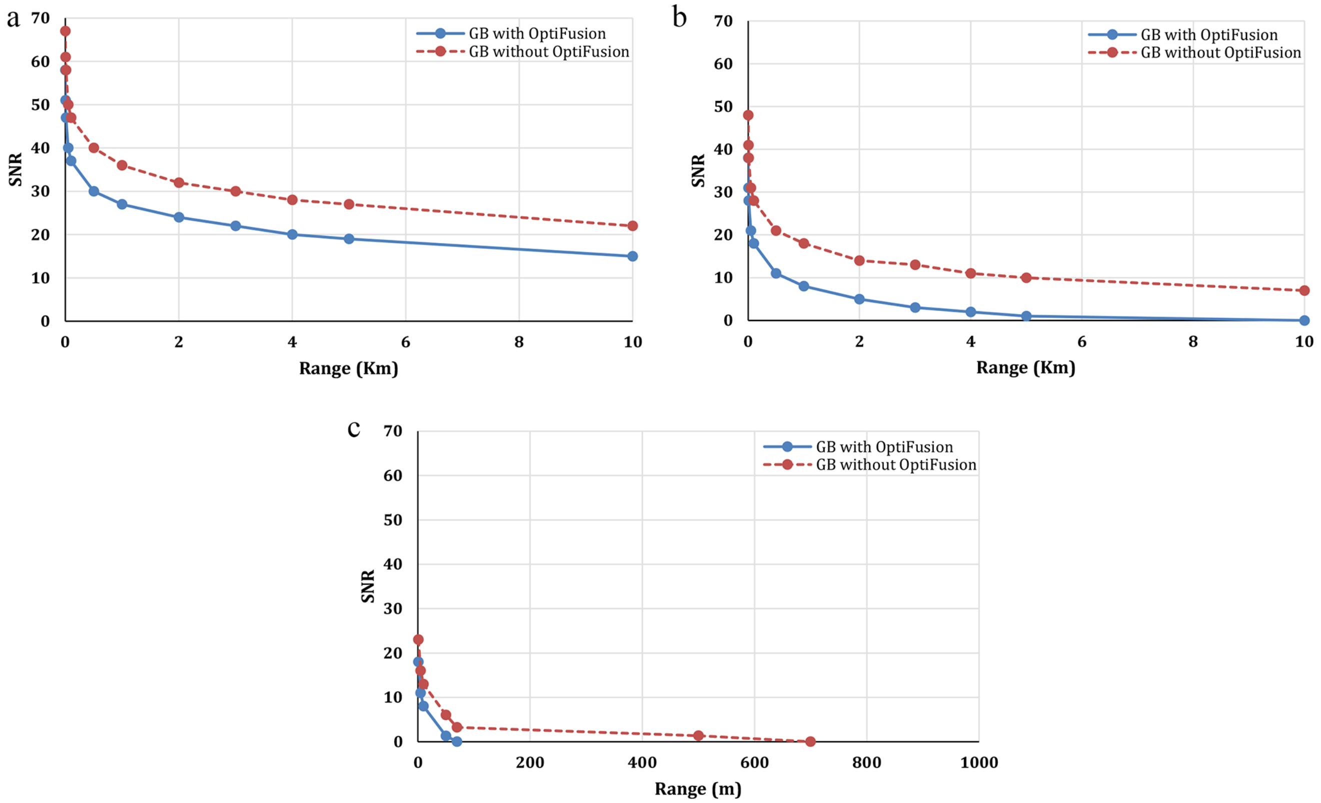

Fig. 7 **a**. SNR for GB in weak turbulences $C_n^2 = 10^{-17}$. **b**. SNR for GB in moderate turbulences $C_n^2 = 10^{-15}$. **c**. SNR for GB in strong turbulences $C_n^2 = 10^{-13}$.

carries data visibly, and the OptiFusion-enabled Gaussian beam, which employs a data-hiding mechanism, and over different propagation distances.

Figure 7a, the comparison focuses on the SNR performance of the Gaussian beam under weak atmospheric turbulence over varying distances. From the figure, it is clear that while both systems (with and without OptiFusion) experience attenuation with increasing distance, the Gaussian beam with OptiFusion maintains stable SNR performance, even though it slightly lags behind the system without OptiFusion. This behavior is consistent with the integration of optical steganography techniques, which can introduce some overhead affecting SNR. Despite this, the GB with OptiFusion continues to provide effective beam transmission over a distance of 10 km.

The choice of 10 km as the maximum propagation distance for this analysis stems from its importance in long-range optical communication systems. It serves as a standard reference point for comparison with other methods in the field, while also demonstrating the system's ability to maintain beam integrity over extended distances. While further distances could be explored more than 10 km, the analysis of these results shows that under weak turbulence, the OptiFusion method performs efficiently in maintaining data transmission quality. This result has promising implications for future research and practical implementations of the OptiFusion technique.

In Fig. 7b, The SNR decreases as the moderate turbulence, showing a steeper decline in the SNR for the Gaussian beam with OptiFusion than the Gaussian beam without it. This behavior is similar to the previous analysis, where OptiFusion impacts the beam quality due to the data-hiding process. Still, here, the effects are more pronounced under moderate turbulence conditions. The Gaussian beam without OptiFusion maintains a higher SNR throughout the propagation distance, with better beam quality at shorter ranges. However, both systems experience significant attenuation as distance increases, with the SNR for the OptiFusion system dropping more quickly. By the time the range reaches around 10 km, the SNR for the OptiFusion-enabled system approaches zero, indicating that the beam becomes nearly indistinguishable from noise at these distances under moderate turbulence. However, under moderate turbulence, OptiFusion can maintain well transmission.

Under weak atmospheric conditions, the Gaussian beam with OptiFusion showed more resilience over long distances, maintaining a higher SNR compared to its performance under moderate disturbances. Moderate Turbulence causes a more severe degradation of the SNR, especially for the system utilizing OptiFusion. This suggests that while

OptiFusion is effective for secure transmission under weak disturbances, its performance decreases but it's still effective as atmospheric conditions worsen.

In strong turbulence, as depicted in Fig. 7c, the Gaussian beams with/without the optifusion method show no distortion in the shape or attenuation over very short distances. This indicates the Gaussian beam with the OptiFusion Steganography method can preserve data integrity over short distances.in harsh conditions, extending the range toward 1 km leads to irreversible data loss, despite all Gaussian beams maintaining their general structure. After the critical distance of 1 km, all Gaussian beam in general starts to exhibit physical distortions, and before this point, the SNR values drop sharply, signaling heavily degraded beam quality. We notice in Fig. 7c when comparing the Gaussian beam with and without OptiFusion values that the SNR of the Gaussian beam with the OptiFusion method is slightly lower due to the OptiFusion method. However, even within these short distances, attenuation is rapid due to strong free-space turbulences. As the propagation distance increases to 70 m, the Gaussian beam with the optifusion method experiences approach zero SNR. However, the Gaussian beam without the optifusion method can propagate to 700 m before the SNR value approaches zero. Indicating total beam loss and an inability to maintain transmission quality under such extreme conditions to Long propagation distance. Compared to previous scenarios involving weak and moderate turbulence, where the Gaussian beam with OptiFusion exhibited better performance over longer distances, the strong turbulence scenario in Fig. 7c results in the Gaussian beam with/without the optifusion method rapidly deteriorating.

Although OptiFusion is effective for hiding data, its performance in maintaining beam quality weakens over longer distances, particularly under strong turbulence when compared to the standard Gaussian beam. This demonstrates the necessity for improved strategies to lessen the impact of atmospheric disturbances in optical communication systems utilizing techniques like OptiFusion.

The results indicate that while OptiFusion is promising in weak and moderate turbulence environments, its performance declines sharply in the presence of stronger turbulence. To address these limitations, future research should prioritize the development of advanced solutions such as adaptive optics or error correction methods to better handle severe atmospheric conditions and enhance the operational range of the OptiFusion method in challenging environments.

We present in Fig. 8a, b, and c, the BER calculations for the same scenarios and atmospheric conditions, similar to the SNR analysis shown earlier. This comparison highlights the performance of the Gaussian beam with and without the OptiFusion method in terms of data preservation and loss. Figure 8a displays the BER of the Gaussian beam under weak turbulence. As depicted both the Gaussian beam with and without the OptiFusion method maintain very low BER values over extended distances, surpassing 10 km. This indicates a high level of accuracy in data transmission, even across long distances, which suggests the robustness of the OptiFusion Steganography method in preserving data integrity when environmental disturbances are minimal. Comparing this with the previous figures that focused on SNR, we observe a similar trend. The weak turbulence scenario continues to support the Gaussian beam's ability to maintain its structure and data integrity, whether or not OptiFusion is applied. The performance of the OptiFusion method in these conditions, as indicated by the minimal increase in BER, reinforces its suitability for environments with relatively stable atmospheric conditions. This demonstrates that the method can effectively hide data while sustaining high transmission quality over significant distances in weak turbulence.

In Fig. 8b, the BER is plotted against the transmission range under moderate weather conditions, illustrating how beam degradation increases due to increases the turbulence. As the distance increases, the BER for both the Gaussian beam with and without the OptiFusion method gradually rises. The Gaussian beam with the OptiFusion method, encounters limitations in these conditions. The sharp increase in BER when using OptiFusion suggests that, although it may offer benefits under different circumstances, its performance in moderate weather is lower compared to the system without it.

Figure 8c, the BER is presented for the Gaussian beams under strong turbulence conditions. The results show that the Gaussian beam faces significant challenges in maintaining data integrity over longer distances in such harsh environments.

High BER values are observed even at short transmission ranges, indicating a considerable rise in transmission errors due to the turbulent atmosphere. While earlier analyses highlighted the Gaussian beam's ability to maintain its shape, the data here emphasizes that the data it carries is increasingly vulnerable to loss under these harsh conditions, leading to a sharp rise in BER. This behavior highlights the optifusion method's limitations in such environments, as it cannot adequately compensate for the increased error rate.

The analysis of Fig. 8 starkly illustrates the dependency of the OptiFusion Steganography method's performance on the atmospheric conditions during transmission. While the technology excels in environments with weak turbulence, ensuring long-distance data integrity, its performance drops significantly in strong turbulence, limiting its effectiveness to much shorter distances. The main reason for this is that

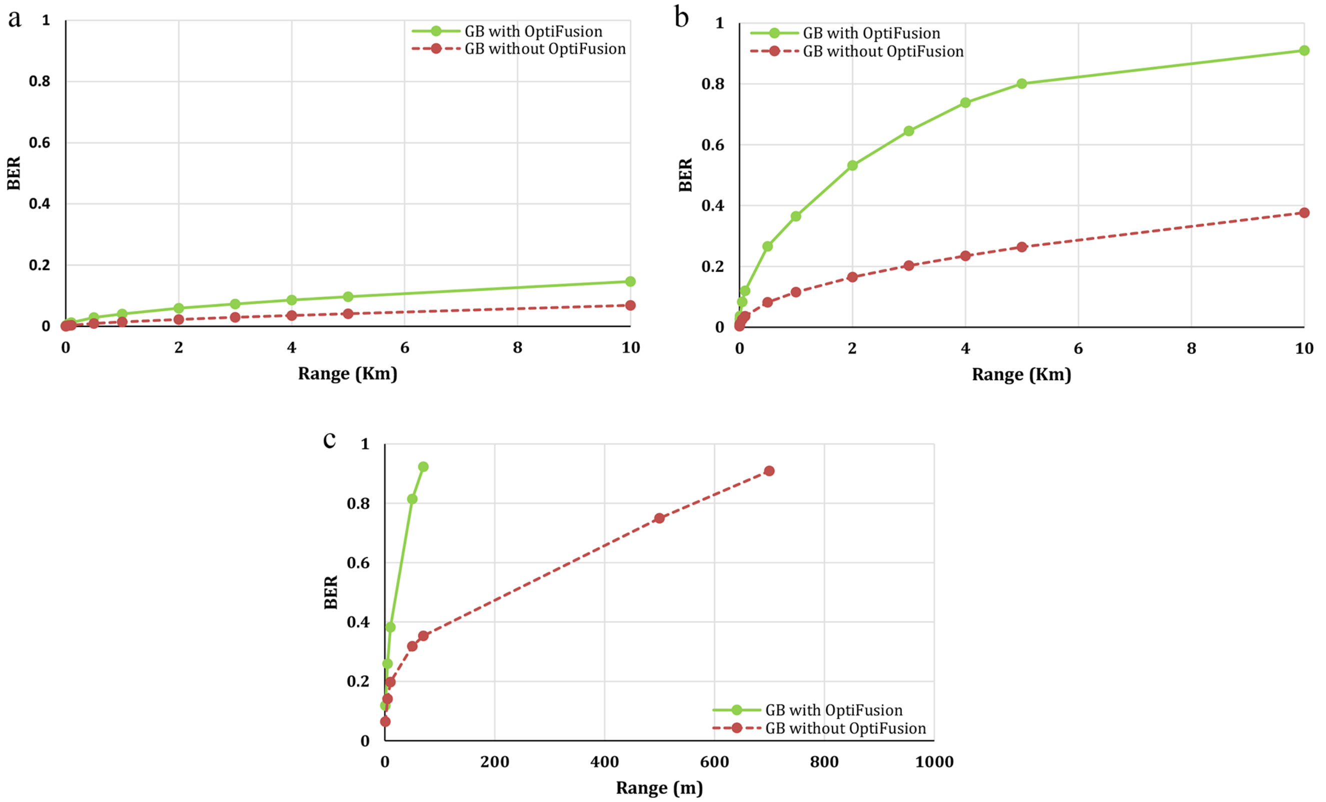

Fig. 8 **a**. BER for GB in weak turbulences $C_n^2 = 10^{-17}$. **b**. BER for GB in moderate turbulences $C_n^2 = 10^{-15}$. **c**. BER for GB in strong turbulences $C_n^2 = 10^{-13}$.

the OptiFusion Steganography method relies on the intensity and shape of the Gaussian beam to hide data which is affected by strong atmospheric disturbances in free-space optical communications, which therefore affects the data inside this intensity of the Gaussian beam.

The relationship between the BER and SNR for the Gaussian beam with the OptiFusion Steganography method across various levels of turbulence is illustrated in Fig. 9. Under weak and moderate turbulences, the Gaussian beam exhibits excellent performance, with favorable BER and SNR values. This demonstrates the beam's robustness in stable conditions, allowing for effective data transmission over long distances with minimal errors, which is ideal for normal operational settings in FSO communication.

However, when examining the same metrics under strong turbulence, the Gaussian beam's performance deteriorates rapidly. There is a swift increase in data loss over short propagation distances, accompanied by significant beam distortion. This decline indicates that the Gaussian beam lacks the necessary resilience to withstand severe disturbances. As turbulence levels increase, the BER rises and the SNR rate decreases, leading to compromised beam integrity and reduced data transmission effectiveness.

This highlights the need to improve the OptiFusion method when using Gaussian beams for masking data and long-range propagation under severe atmospheric turbulence. Two potential solutions include utilizing alternative optical beam types, such as OAM beams or non-diffracting beams, which better preserve their intensity and shape in turbulent conditions. Another option is to integrate adaptive optics or error correction techniques into the optical communication system to enhance performance in challenging environments. These approaches offer valuable directions for future research, while OptiFusion continues to perform effectively in weak to moderate conditions without requiring adjustments.

Figure 9 Relationship between BER and SNR in various turbulence for a propagation distance from 1 m to 10 km.

Conclusion

This research introduces an innovative optical steganography model using Gaussian beams in free-space optical (FSO) communications to enhance physical layer security. By leveraging the shape and intensity of Gaussian beams, the OptiFusion Steganography method effectively hides and transmits data. Theoretical exploration and simulations demonstrate its effectiveness in secure data transmission over various distances and atmospheric conditions. In

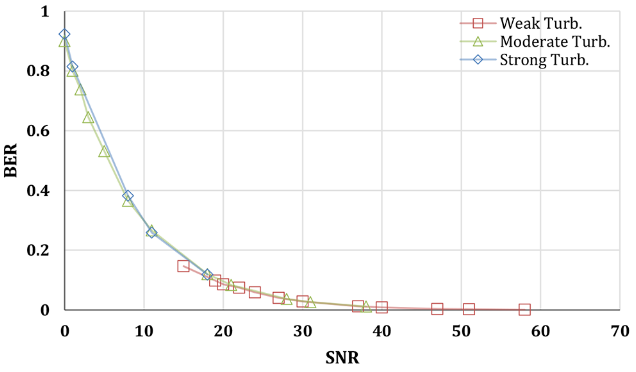

Fig. 9 Relationship between BER and SNR in various turbulence for a propagation distance from 1m to 10 km.

weak and moderate atmospheric turbulence, the technology maintains low bit error rates (BER) and high signal-to-noise ratios (SNR) over long distances, exceeding 10 km, proving its efficacy in stable or moderately disturbed environments. However, in strong turbulence, while the beam retains its shape, it experiences rapid data loss and significant BER increase over shorter distances, highlighting its limitation under severe conditions.

The integration of advanced modulation techniques like 16-QAM and OFDM with Gaussian beams also enhances data transfer and provides additional protection against eavesdropping, increasing system security.

This study highlights the promising potential of the Opt-iFusion Steganography method for securing optical communications, showcasing its capability to enhance the security and reliability of FSO systems under varying atmospheric conditions. Further research is recommended to refine and maximize this technology by improving algorithms, incorporating additional components, or exploring different types of optical beams. These advancements could enable its application under severe weather conditions, where it currently faces challenges over long distances while remaining effective over shorter distances.

References

1. A.G. Alkholidi, K.S. Altowij, Free space optical communications—Theory and practices. IntechOpen (2014). https://doi.org/10.5772/58884
2. M. Mukherjee, Wireless communication—moving from RF to optical, in: Proceedings of the 10th INDIACom; 2016 3rd International Conference on Computing for Sustainable Global Development (IEEE, 2016), pp. 1079–1086. https://doi.org/10.1109/INDIACom.2016.37465
3. H. Kaushal, G. Kaddoum, Free space optical communication: Challenges and mitigation techniques, IntechOpen, (2017). https://doi.org/10.5772/65724
4. X. Sun, I.B. Djordjevic, Physical-layer security in orbital angular momentum multiplexing free-space optical communications. IEEE Photon J. **8**, 7901110 (2016). https://doi.org/10.1109/JPHOT.2016.2520878
5. A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J., **54**(8), 1355–1387 (1975). https://doi.org/10.1002/j.1538-7305.1975.tb02040.x
6. H. Endo, M. Fujiwara, M. Kitamura, T. Ito, M. Toyoshima, Y. Takayama, H. Takenaka, R. Shimizu, N. Laurenti, G. Vallone, P. Villoresi, T. Aoki, M. Sasaki, Free-space optical channel estimation for physical layer security. Opt. Express. **26**, 24567–24578 (2018). https://doi.org/10.1364/OE.26.024567
7. Q. Huang, D. Liu, Y. Chen, Y. Wang, J. Tan, W. Chen, J. Liu, N. Zhu, Secure free-space optical communication system based on data fragmentation multipath transmission technology. Opt. Express. **26**, 13536–13542 (2018). https://doi.org/10.1364/OE.26.013536
8. J. Ji, B. Wu, J. Zhang, M. Xu, K. Wang, Design and investigation of 10 GB/s FSO wiretap channel using OCDMA time-diversity reception. IEEE Photon J. **12**, 7903212 (2020). https://doi.org/10.1109/JPHOT.2020.2985747
9. P.V. Trinh, T.V. Pham, N.T. Dang, H.V. Nguyen, S.X. Ng, A.T. Pham, Design and security analysis of quantum key distribution protocol over free-space optics using the dual-threshold direct-detection receiver. IEEE Access. **6**, 4159–4171 (2018). https://doi.org/10.1109/ACCESS.2018.2800291
10. J. Kour, D. Verma, Steganography techniques—a review paper. Int. J. Emerg. Res. Manag Technol. **3**, 132–135 (2014)
11. I. Haverkamp, D.K. Sarmah, Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis. Int. J. Inf. Secure. (2024). https://doi.org/10.1007/s10207-024-00853-9
12. C.-T. Yen, J.-F. Huang, W.-Z. Zhang, Hiding stealth optical CDMA signals in public BPSK channels for optical wireless communication. Appl. Sci. **8**(10), 1731 (2018). https://doi.org/10.3390/app8101731
13. X. Hong, D. Wang, L. Xu, S. He, Demonstration of optical steganography transmission using temporal phase coded optical signals with spectral notch filtering. Opt. Express. **18**, 12415–12420 (2010). https://doi.org/10.1364/OE.18.012415
14. Y. Chen, R. Wang, T. Fang, T. Pu, P. Xiang, H. Zhu, J. Zheng, Stealth transmission of temporal phase en/decoded polarization-modulated-code-shift-keying OCDMA signal over synchronous digital hierarchy network with asynchronous detection. Opt. Eng. **53**, 066103 (2014). https://doi.org/10.1117/1.OE.53.6.066103
15. H. Zhu, R. Wang, T. Pu, T. Fang, P. Xiang, J. Zheng, W. Wu, Optical steganography of code-shift-keying OCDMA signal based on the incoherent light source. IEEE Photon J. **7**, 6801607 (2015). https://doi.org/10.1109/JPHOT.2015.2432072
16. Q. Liu, M.P. Fok, Bio-inspired photonics – marine hatchet fish camouflage strategies for RF steganography. Opt. Express. **29**, 2587 (2021). https://doi.org/10.1364/OE.414091
17. S. Sahoo, C. Panda, U. Bhanja, Performance evaluation of an OFDM-FSO-steganography model, in 2023 International Conference on Microwave, Optical, and, C. Engineering, (ICMOCE), IEEE, 2023, pp. 1–6. https://doi.org/10.1109/ICMOCE57812.2023.10166349
18. C.-T. Yen, J.-F. Huang, W.-Z. Zhang, Hiding stealth optical CDMA signals in public BPSK channels for optical wireless communication. Appl. Sci. **8**, 1731 (2018). https://doi.org/10.3390/app8101731
19. H. Song, A. Almaiman, H. Song, Z. Zhao, R. Zhang, K. Pang, C. Liu, L. Li, K. Manukyan, S. Zach, N. Cohen, M. Tur, A.E. Willner, Hiding a low-intensity 50-Gbit/s QPSK free-space OAM Beam using an orthogonal co-axial high-intensity 50-Gbit/s QPSK beam. Appl. Opt. (2020). https://doi.org/10.1364/AO.396386

20. Y. Qi, B. Wu, Free-space optical stealth communication based on wideband noise. Front. Opt. Laser Sci. (2018). https://doi.org/10.1364/FIO.2018.FW5B.5
21. Y. Qi, J. Li, C. Wei, B. Wu, Free-space optical stealth communication based on wide-band spontaneous emission. Opt. Continuum. **1**, 11 (2022). https://doi.org/10.1364/OPTCON.441727
22. L. Burger, I.A. Litvin, A. Forbes, Simulating atmospheric turbulence using a phase-only spatial light modulator. S Afr. J. Sci. **104**, 129–134 (2008)
23. L.C. Andrews, M. Beason, Laser beam propagation in random media: New and advanced topics, SPIE (2022)
24. M.R. Chatterjee, F.H.A. Mohamed, Diffractive propagation and recovery of modulated (including chaotic) electromagnetic waves through the uniform atmosphere and modified von Karman phase turbulence, Proc. SPIE **9833**, 98330F (2016). https://doi.org/10.1117/12.2228909

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.