Combining Quantum Key Distribution with Chaotic Systems for Free Space Optical Communications

Naveed Mahmud · Andrew MacGillivray · Apurva Rai · Jenna Patterson · Adam Gharaibeh · Esam El-Araby · Harry Shaw · Lavida Cooper

Received: 13 Oct. 2020 / Accepted: 06 Oct. 2021

Abstract In this work, we propose a Free-Space Optical (FSO) communication system that combines chaotic communications with Quantum Key Distribution (QKD) to achieve greater security and range compared to existing FSO techniques such as N-slit interferometers. We utilize Lorenz chaotic transmitter and receiver models, which are inherently auto-synchronizable, to generate chaotic signals used as data carriers. Data is transmitted securely over a classical channel using the Lorenz chaotic communication system, while a quantum channel is used for securely exchanging critical synchronization parameters via a combination of QKD and public-key cryptography protocols. Because FSO communications have been utilized by space agencies including NASA and ESA, we provide a concept of operations for a space mission combining chaotic communications and QKD to achieve an end-to-end encrypted Deep-Space optical communications link. Our experimental work includes successful real-time transmission of high-resolution single-spectral and multi-spectral images, measurement of bit-error-rate (BER) over a range of noise levels, and an evaluation of security and robustness of transmissions with dynamic reconfiguration of the chaotic systems.

Keywords Chaotic Communication · Quantum Key Distribution · FSO Security

1 Introduction

Free-Space Optical (FSO) communication is a common focus of research due to advantages in terms of higher bandwidth, lower cost, lower mass, and

N. Mahmud
Dept. of Electrical Engineering and Computer Science
University of Kansas
1520 W 15th St, Lawrence, KS 66045
Tel.: +1-929-386-6207
E-mail: naveed_923@ku.edu

lower power consumption compared to traditional Free-Space Radio-Frequency (FSRF) systems [1–3]. At the physical level, the high directionality and narrow beam widths of FSO communications make them harder to detect and intercept than broadcast-like FSRF communications [4, 5]. Propositions to further enhance the security of FSO communications have usually involved multi-beam N-slit interferometers, where the expected interference is predetermined. Using N-slit interferometer techniques, interception attempts cause the collapse of the interferometric pattern and the distortion or destruction of the signal [6, 7]. This technique has been demonstrated to work over propagation distances of practical interest (several kilometers) [8] for terrestrial applications and estimated to work over several thousand kilometers (2,000-10,000 km) [9,10] for space applications. Interferometric techniques, however, assume the availability of laser technology with low phase noise as well as minimal divergence of the collimated optical beam to achieve high quality and stability of the interference patterns. Such characteristics drive trade-offs between security and range when using inteferometric techniques at extreme distances, resulting in effective ranges that are too short for deep-space communication.

In this paper, we propose combining chaotic communications with Quantum Key Distribution (QKD) in order to improve security and synchronization in FSO communication. Chaotic models are attributed with particular features that make them suitable for highly secure communications. For instance, they display complex dynamic behaviors that are well defined, and have characteristics that include broadband noise-like signals, unpredictability, and sensitivity to initial conditions [11]. These behaviors and characteristics of chaotic signals make data synchronization and interception by eavesdroppers very difficult. Chaotic systems are also unstable, nonlinear and aperiodic in nature, but they offer a wideband signal, which can be thought of as spread spectrum, with multi-path fading resistance [12, 13]. Moreover, chaotic systems can be integrated with other formats/models such as On-Off Keying (OOK) as well as M-ary pulse position modulation (PPM) schemes which are suitable for deep space optical communications [14]. One caveat of chaotic systems is that synchronization of the chaotic models requires a common set of parameters to be shared between transmitter and receiver through a highly secure channel. The Rivest-Shamir-Adleman (RSA) algorithm [15] is a commonly used classical public-key cryptosystem whose security depends on the computational difficulty of factoring large integers. Quantum algorithms threaten that security, as recent works [16–19] have demonstrated that implementations of Shor's algorithm [20] will be able to factor large integers efficiently with a sufficiently powerful quantum computer. Conversely, quantum techniques like Quantum Key Distribution (QKD) are more robust and cannot be compromised by quantum computers. Any attempt at interception of the shared key destroys the data contained in it, thereby alerting the presence of an unintentional receiver. The unconditional security of QKD has been demonstrated in many previous works [21–23]. Therefore, we propose a scheme that uses a QKD-like protocol to secure the parameter synchronization in a chaotic communication system.

Our proposed design uses transmitter and receiver models based on auto-synchronous Lorenz chaotic systems [11] for use in FSO communications, suitable for both terrestrial and deep-space applications. We integrate an RSA based QKD protocol with pre-shared Huffman codeword dictionary, to securely communicate chaotic synchronization parameters between the transmitter and receiver via a quantum and/or classical channel. A realistic classical channel with Additive White Gaussian Noise (AWGN) is modeled for data communication. To minimize noise effects and improve the bit-error-rate (BER) of transmissions, we implement digital modulation and demodulation techniques including low-density-parity-check (LDPC) and quadrature-phase-shift-keying (QPSK). For experimental analysis, we send high-resolution, single/multi-spectral images encoded as binary non-return-to-zero (NRZ) data across the FSO communication channel and recover them at the receiver end. For higher security, the synchronization parameters of the transmitter and receiver are dynamically reconfigured for each transmission. This dynamic scheme secures both uplink and downlink FSO communications, which might contain control inputs or scientific data in a hypothetical space mission. Thus, future FSO space communications utilizing the outcome of our proposed work will allow for secure communications at distances from Mars to the outer planets and Kuiper belt (1.5 to 40 AU), benefiting missions such as the Ice Giants Decadal Study [24].

This paper is an extension to our previous work [25] where the initial scheme combining QKD with FSO communications was established, and details of that work is discussed in Section 2.3 "Related Work". The rest of the paper is organized such that Section 2 presents background information and related work. Section 3 describes the proposed communication scheme in detail. In Section 4, we provide a concept of operations for a practical space mission. The experimental work and analysis is presented in Section 5. Finally, Section 6 ends the paper with conclusions and future work.

2 Background and Related Work

2.1 Chaotic Communications

The system we propose leverages concepts introduced in previous works, specifically those focused on chaotic communications and synchronization [12, 26–28]. Chaotic systems, much like classical communication systems, require synchronization between a transmitter and receiver in order to establish successful communications. To recover a message in classical communications, e.g. FM, AM, ASK, FSK, etc., the receiver tunes to a carrier signal, which is a periodic waveform that the transmitter modulates in order to transmit information. Chaotic systems generalize this approach, using a chaotic, aperiodic carrier wave that offers a broad frequency spectrum over which data can be carried. The fundamental aperiodic nature of the chaotic carrier signal does not allow it to be stored in the receiver as a reference signal, which is detrimental

for coherent detection of the transmitted signal. The control and synchronization of chaotic systems have been studied over the past two decades [26–28] for potential applications in secure communication [12]. Pecora and Carroll in 1990 reported that certain chaotic systems possess a self-synchronization property [26]. They proved that a chaotic system is self-synchronizing if it can be decomposed into stable response subsystems. The stable response subsystems, when driven by a common signal from the original (drive) system, can then operate in auto synchrony with the drive system [26–28]. For example, they showed that the Lorenz chaotic system [11], usually called Lorenz attractor, is decomposable into two separate stable response subsystems that will each synchronize to the drive system when started from any initial condition [29,30] as shown in Fig. 1.

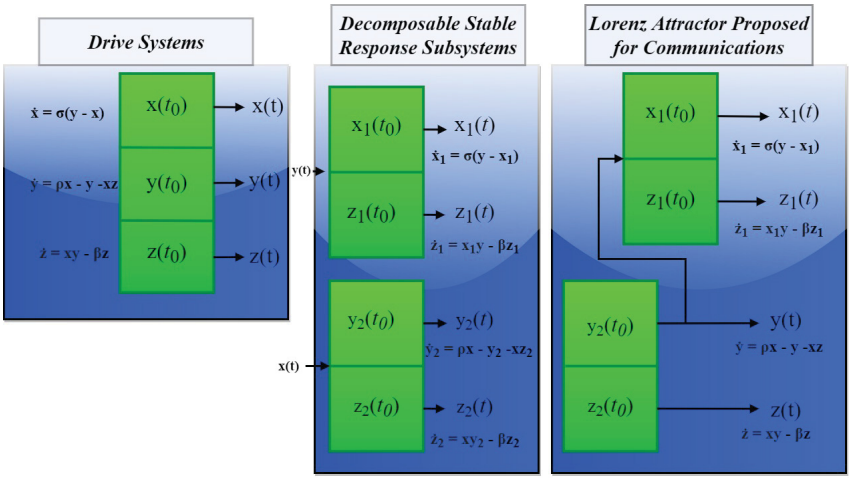


Fig. 1: Lorenz chaotic attractor and its decomposable response subsystems for chaotic communications.

Based on Pecora and Carroll's findings [26–28], Cuomo and Oppenheim [29,30] proposed chaos synchronization as a means for communication. In one of their discussed approaches, chaotic signal masking, the noise-like chaotic signal $x(t)$ generated at the transmitter is added to the input data signal $d(t)$ and then transmitted over the communication channel. For signal masking, it is assumed that the power level of the input data signal $d(t)$ is significantly lower than that of the chaotic signal $x(t)$. For this technique, regenerating the chaotic carrier at the receiver end [29,30] is essential for synchronization. The error between the received signal and the regenerated carrier could then be used for recovering the original data signal $d(t)$.

2.2 Quantum Key Distribution

Quantum Key Distribution (QKD) is a highly secure key distribution system that enables two parties to share a secret key using the properties of quantum mechanics. By relying on physics, rather than the computational difficulty of a cryptographic algorithm, the security of QKD surpasses that of conventional cryptography and key distribution systems [21–23]. QKD works by encoding a private key as conjugate bases of a quantum state (or qubits) and transmitting it over a quantum channel [22]. Even if the quantum channel is intercepted, a theoretical eavesdropper will not be able to distinguish between code qubits and check qubits, and will inevitably have to measure both [22]. Due to fundamental characteristics of quantum mechanics, measurement of these qubits will alter their states. Thus, after the key is received, the transmitter can reveal the location of the check qubits, and the receiver can determine the likelihood of the message having been intercepted based on how many qubits have been corrupted [22]. If the likelihood of interception is high, communication is aborted and the key distribution process must be restarted. After the key is successfully shared between the two transmitting and receiving parties, the transmitting side can start encrypting messages with the shared key and broadcasting them, while the receiving party decrypts the message with the key known only to them.

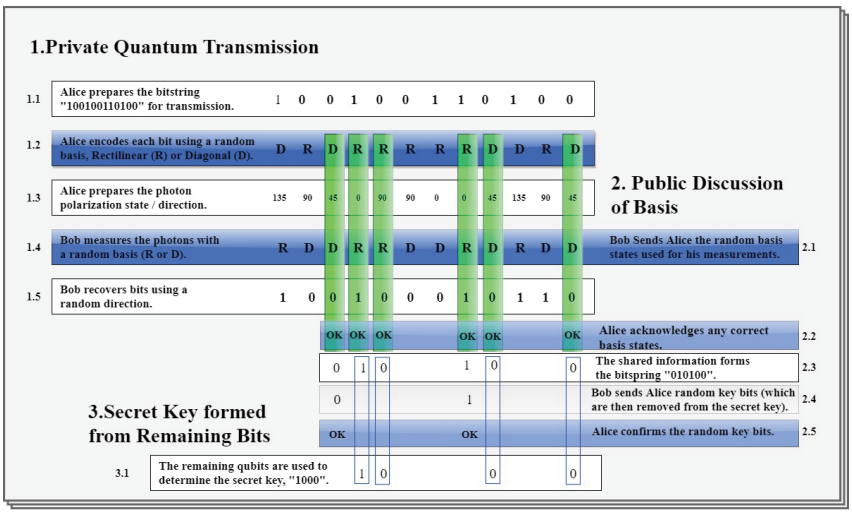


Fig. 2: Quantum transmission via BB84 protocol that uses four polarization directions and two non-orthogonal bases.

The first secure QKD protocol [31] was introduced by Bennett and Brassard in 1984 (and was thus dubbed 'BB84'). In their protocol, photon polarization states are used to transmit key information through a quantum channel in combination with an insecure public channel. The key information is encoded as non-orthogonal quantum states, which in the case of photons are polarization directions of 0, 45, 90 and 135 degrees. To begin key distribution with the BB84 protocol, the transmitter 'Alice' encodes each data bit on one of two polarization bases, i.e., Rectilinear R or Diagonal D, and uses either pair, i.e., (0, 90) or (45, 135), of polarization states/directions to encode each bit. The receiver 'Bob' can use either one of the two polarization bases to measure the received photon and recover the data bits, resulting in Bob having a 50% chance to recover the correct bits. After all photons are measured by Bob, both Alice and Bob communicate over a public channel, with Alice sending the basis of each photon she had sent and Bob sending the basis of each of his measurements. They eliminate the measurement bits whose basis did not match, and create a key with the remaining bits. To detect the presence of an eavesdropper, Bob and Alice can agree upon a pre-shared subset of the key bits, e.g., one third, and match that with their measured bits. If no errors are detected then they commence encryption of their data with the shared key and can securely transmit over the classical channel. Fig. 2 illustrates the above BB84 protocol example.

2.3 Related Work

Extended work on chaotic communication [32–35] has been reported since its introduction by Cuomo and Oppenheim [29, 30]. Despite the potential use of chaos in secure communications, there are known limitations when applied in a real system. The major problem in designing chaos-based secure communication systems can be stated as how to send an encrypted message from the transmitter (drive system) to the receiver (response system) over a public channel while achieving security, maintaining privacy, and providing good noise rejection [35]. Specifically, small parameter mismatches and noise may bring about irreversible synchronization errors due to large distortions present in the synchronization manifold, known as attractor bubbling [36]. Moreover, bit-error-rate (BER) of the synchronized chaos communication may be higher than alternative secure communication approaches. This is because chaotic systems continuously generate non-redundant information and have a positive Kolmogorov-Sinai entropy [35]. Overcoming these limitations should be achieved, in practice, using either analog or digital hardware [35] in a robust form that can achieve, to some degree, perfect reconstruction of the transmitted signal at the receiver end. Several attempts were made to improve the design of chaos-based secure communication systems and many techniques were developed [32, 35]. Similar research work investigating the combination of chaotic systems with FSO communication has been demonstrated [37]. For example, Annovazzi-Lodi et al. [37] proposed an optical configuration of semi-

conductor lasers which are injected with a third driving signal to gain chaotic synchronization. This methodology and hardware setup has some limitations that were avoided in our proposed work. In their work, the lasers were configured based on the Lang Kobayashi model [38], which is not inherently auto-synchronizable and necessitates external injection from a third laser. The external laser used optical reflectors to create the synchronizing signal which is impractical or infeasible in a long-distance communication system. Our proposed work based on the auto-synchronizing Lorenz model eliminates the need for such an extra costly hardware.

There have been many notable demonstrations of QKD in FSO communications. Marcikic et al. [39] demonstrated a QKD system utilizing polarization entangled photon pairs. Schmitt-Manderbach et al. [40] presented an experimental evaluation of the BB84 protocol over a 144 km FSO link using weak coherent lasers. Hughes et al. [41] demonstrated a similar implementation of BB84 over a 10 km FSO channel in both daytime and nighttime. The work in [42] analyzes that the probability of information leakage in the FSO channel associated with an eavesdropper detecting backflash photons, increases at a logarithmic rate. They demonstrated results that could be useful in system design so that the probability of information leakage is minimized as much as possible. The analysis derived in [43] proposes a new QKD protocol that can be implemented on standard FSO systems. This protocol utilizes Subcarrier Intensity Modulation/Binary Phase Shift Keying (SIM/BPSK) and Dual Threshold/Direct Detection (D-T/DD) receivers with an Avalanche Photodiode (APD). The analysis also shows that QKD function can be achieved based on the pulse-based signal level of a laser beam as in the standard optical systems.

The work in [44] combined QKD with chaotic systems in an effort to improve the performance of the QKD system. Their methodology is different from ours as they are using the chaotic system to generate the secure keys for QKD to achieve higher QKD bit rate. Our proposed methodology uses QKD to enhance the security of the chaotic communications system by securely exchanging chaotic synchronization parameters. A system similar to what we have proposed was presented in [45], that combined a chaotic cryptographic model with QKD. However, the QKD model used in that work was very simplistic and not elaborated in detail. Moreover, there was no discussion of application of the proposed scheme. In our work, we present a highly secure communication scheme for Free-Space Optics that provides improved and auto-synchronized communication by combining QKD with chaotic systems. Details of the QKD model and the chaotic parameter exchange protocol are presented. We also provide a practical concept of operations for an FSO space mission where the proposed scheme can be applied. While QKD is used to secure key distribution, additional security is provided by the chaotic Lorenz models in the classical communication channel to protect the data from intruding attacks. The use of chaotic signal masking in data transmission also eliminates the cost of employing computationally intensive encryption/decryption techniques and reduces hardware complexity and cost.

Our previous work [25] prototyped the initial scheme of QKD protocol securing chaotic communications. We demonstrated feasibility of the scheme and evaluated its security by transmitting single-spectral images, with an eavesdropper trying to intercept the transmission. In this work, we show higher security of the scheme by experimentally performing dynamic reconfiguration of the chaotic transmitter and receiver models during transmission. We also evaluate the proposed scheme using higher-resolution data, as well as test the robustness of the system by transmission of multi-spectral images. We show that high security is maintained by the combination of QKD and chaotic models for every frequency band of the transmitted multi-spectral image, in the presence of an unintentional receiver trying to intercept each image band.

3 Proposed Communication System Combining Chaotic Systems with QKD

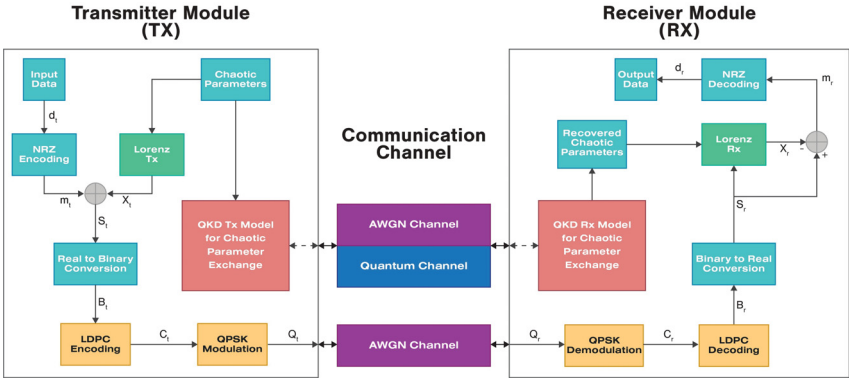


Fig. 3: Chaotic communication system secured by QKD.

Fig. 3 shows our proposed system for chaotic communications with QKD. The system operates by, beginning with the QKD transmitter (TX) side, exchanging the chaotic synchronization parameters with the receiver (RX) module in a two-way BB84-like protocol via both classical and quantum channels. On the receiver side (RX), the QKD RX model recovers the chaotic parameters and supplies them to the synchronizable Lorenz chaotic receiver, see Fig. 3. Data transmission from the transmitter side commences after the parameter exchange is complete. The input message data d_t is converted to a binary non-return-to-zero (NRZ) format m_t. The noise-like chaotic signal x_t generated by the Lorenz transmitter along with message data are added together to form the transmission signal S_t. This transmission signal is then converted to pure binary format B_t. Constituting the chaotically masked message, the binary data is supplied to a low-density-parity-check (LDPC) module

which performs forward error correction by adding redundancy to the data. The encoded signal C_t undergoes quadrature-phase-shift-keying (QPSK) digital modulation before being broadcast on the Additive White Gaussian Noise (AWGN) communication channel in complex form Q_t. On the receiver side, see Fig. 3, the received complex signal undergoes QPSK demodulation, LDPC decoding, and binary to real conversion. S_r, the converted signal given as the driving signal to the synchronizable Lorenz receiver, equipped with the synchronization parameters from the QKD RX model, can regenerate a chaotic signal x_r like the one from the Lorenz TX. The regenerated signal is used for recovering the NRZ message data m_r which is then converted to its original format by an NRZ decoder. The operations of the Lorenz TX, RX, and the QKD parameter exchange models are discussed in the subsequent sections.

3.1 Chaotic Transmitter and Receiver

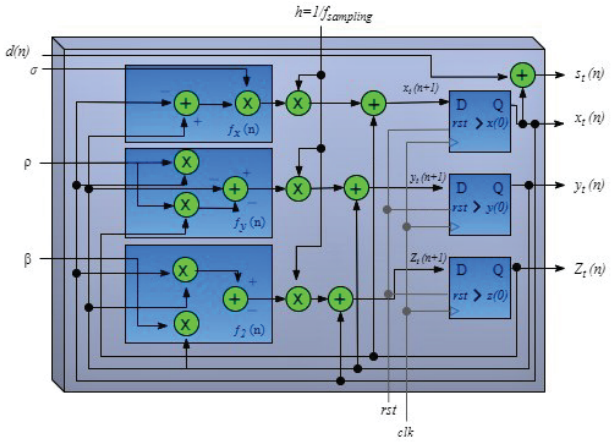
The design of the Lorenz attractor for both the transmitter and receiver was based on Cuomo and Oppenheim's work [29, 30]. The transmitted signal $S_t(t) = x_t(t) + d_t(t)$, see Fig. 3, is obtained through the masking of the input data signal $d_t(t)$ with the generated chaotic state signals $x_t(t)$. The initial conditions $x(0)$, $y(0)$ and $z(0)$, essential for synchronization and accurate data reconstruction, along with the parameters of the transmitter σ, ρ, β, and the received signal $S_r(t)$ are used by the receiver to regenerate the chaotic carrier [29, 30] $x_r(t)$. The original data $d_r(t)$, see Fig. 3, is reconstructed by means of the error signal $m_r(t)$, which is the difference between the received signal $S_r(t)$ and the regenerated carrier $x_r(t)$. Within the design process of the simulation models for the transmitter and the receiver, the differential equations (1) and (2) were discretized using the Euler and First Order Runge-Kutta (RK) approximations. The utilization of higher order RK resulted in negligible improvements in accuracy, and thus 1^{st} order RK approximation was adopted for its simpler implementation and lower hardware cost.

$$\left.\begin{aligned} \dot{x}_t &= \sigma(y_t - x_t) \\ \dot{y}_t &= \rho x_t - y_t - x_t z_t \\ \dot{z}_t &= x_t y_t - \beta z_t \end{aligned}\right\} \begin{array}{c}\text{Lorenz Chaotic Transmitter} \\ \text{where } d(t) \text{ is the input} \\ \text{data signal and } x_t(t) \\ \text{is the carrier signal}\end{array} \tag{1}$$

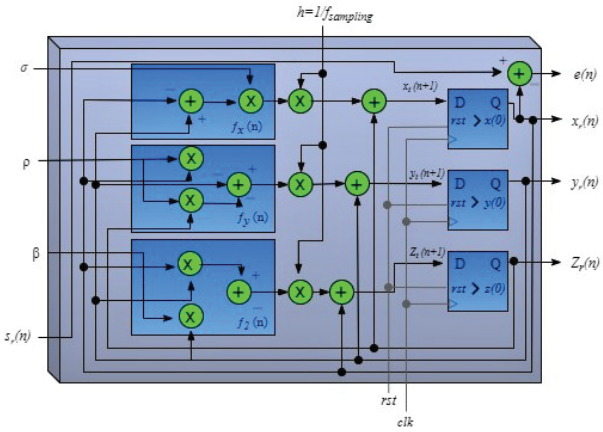
$$\textit{and, } s_t(t) = x_t(t) + d(t)$$

$$\left.\begin{aligned} \dot{x}_r &= \sigma(y_r - x_r) \\ \dot{y}_r &= \rho s_r - y_r - s_r z_r \\ \dot{z}_r &= s_r y_r - \beta z_r \end{aligned}\right\} \begin{array}{c}\text{Synchronized Lorenz Chaotic} \\ \text{Receiver where } s_r(t) \text{ is the} \\ \text{received signal and } x_r(t) \text{ is the} \\ \text{regenerated carrier signal}\end{array} \tag{2}$$

Signal masking of the data signal with chaotic carrier signal was simply implemented as $S_t(t) = d_t(t) + x_t(t)$. Fig. 4, illustrates the digital models derived from RK approximation of (1) and (2). Modeling the transmitter and receiver was performed by the discretization of the time domain as $t = n.\Delta t =$



(a) Chaotic transmitter model.



(b) Chaotic receiver model.

Fig. 4: The proposed communication scheme's transmitter and receiver hardware models.

$n.h$, where n is the discrete time (sample) index and h is the sample time step or the reciprocal of the sampling frequency $f_{sampling}$. The transmitter model with the input parameters σ, ρ, β, the input data $d(n)$, the sampling time step h, the output chaotic signals $x_t(n)$, $y_t(n)$, $z_t(n)$, and the output transmitted signal $s_t(n) = x_t(n) + d(n)$ is shown in Fig. 4a. Configured with the chaotic parameters, the receiver in Fig. 4b receives the transmitted signal. The receiver generates chaotic signals $x_r(n)$, $y_r(n)$, $z_r(n)$ using the received parameters and recovers an error signal $e(n) = s_r(n) - x_r(t)$, which is used to reconstruct the original data $d(n)$. Consisting of subcomponents f_x, f_y, and

f_z, the transmitter and receiver implement the Lorenz operations described in (1) and (2).

3.2 QKD Model for Exchange of Critical Synchronization Parameters

The QKD model is critical for securely establishing the FSO chaotic communications link with exchange of the set of synchronization parameters, $\mathbb{Z}$ where

$$\mathbb{Z} = \{\sigma, \rho, \beta, x(0), y(0), z(0)\} \tag{3}$$

The synchronization parameters are signed real numbers. A transmitter (Alice) and receiver (Bob) will exchange the parameters using quantum communications, i.e., encoded as quantum bits (qubits) [22], from the set of signed real numbers. Given

$$\psi = p_0 \left|0\right\rangle + p_1 \left|1\right\rangle \tag{4}$$

such that the binary representation of $\mathbb{Z}$ can be mapped to either basis/symbol state, where p_i represents the probability of each symbol, and ψ_i is the basis set with a total probability p given by

$$p = \sum_i p_i = 1 \tag{5}$$

and probability density function $\rho^{'}$

$$\rho^{'} = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| \tag{6}$$

Alice and Bob utilize a quantum communications model that is agnostic to the quantum basis and mode of quantum communication. The quantum codebook is created from a user specified basis set ψ. The user can specify pure states, mixed states or a combination of pure and mixed states. The basis set operates upon a positive semi-definite matrix created from the user-provided chaotic parameters. For the minimum basis set, the set of synchronization parameters are transformed into a set of matrices $A = \{A_0, A_1, A_2\}$, such that

$$A_0 = \begin{bmatrix} \sigma & 0 \\ 0 & \rho \end{bmatrix}, A_1 = \begin{bmatrix} \beta & 0 \\ 0 & x(0) \end{bmatrix}, A_2 = \begin{bmatrix} y(0) & 0 \\ 0 & z(0) \end{bmatrix}$$

Alice and Bob use the RSA algorithm to generate a key pair, consisting of one private key and one public key. Details of the function of the RSA algorithm can be found in [15]. Alice and Bob possess a public encryption key $\{e, n\}$ and a private decryption key $\{d, n\}$ with a common factor n. For any integer message M, where $M < n$ and M is an integer representation of each non-zero entry in matrix set A, Alice generates an encrypted message C using the public key $\{e, n\}$ as described in (7), and Bob decrypts C back to M using the private key $\{d, n\}$ as described in (8).

$$C = M^e * mod(n) \tag{7}$$

$$M = C^d * mod(n) \tag{8}$$

3.3 Pre-shared Secrets and Huffman Codewords

Alice and Bob share pre-established RSA key pairs, (e, n) and (d, n), along with protocols for the establishment of new pairs. It is assumed that both Alice and Bob share knowledge about the quantum basis and are using identical hardware and software for coding and decoding qubits. The physical implementation of said hardware determines the quantum coding basis for Alice and Bob. Using simple basis offers lower levels of security. Higher orders of quantum basis offer better security against brute force eavesdropping or sequence analysis. Alice and Bob can share a set of secret symbol probabilities S, as in (9), for the construction of a second codebook. This set of probabilities can then be used to derive the second codebook that is a binary Huffman dictionary of variable length codewords H as defined in (10). The probabilities in S determine the number of bits for each word in W. As shown in Fig. 5, combinations of W are formed to develop the encryption protocol.

$$S = \{s_0, s_1, ..., s_n\} \tag{9}$$

$$H = \{W_0, W_1, ..., W_n\} \tag{10}$$

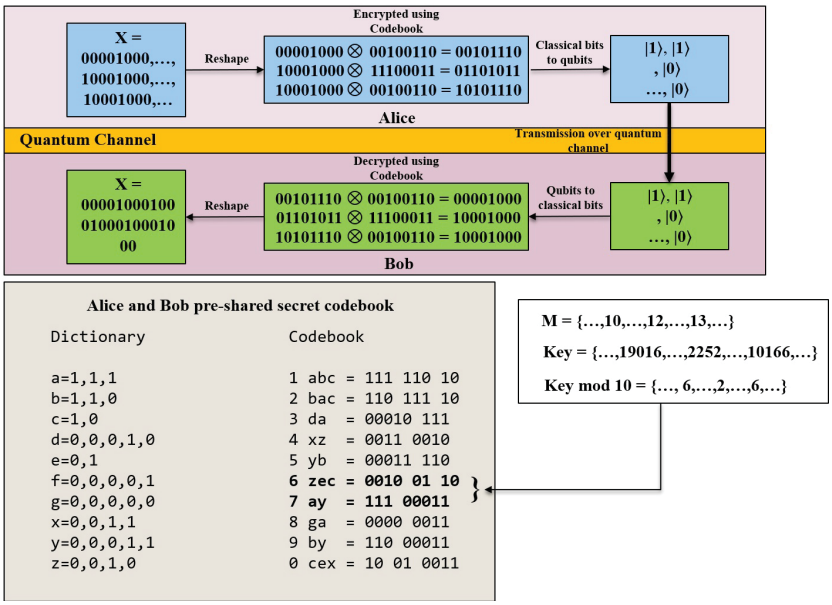


Fig. 5: Preshared codebook for encrypting/decrypting data. It is assumed that position of the codewords were randomized by Alice and Bob.

The simplest implementation would be a two qubit codeword possibility. In this case, a brute force attack on the quantum exchange by Eve will lead to approximately 50% of the qubits being identified correctly. Through further sequence analysis, Eve can determine that there are only two quantum codewords and also determine the frequency of each appearing as the codeword. Alice, however, has coded the classical qubits into another codeword dictionary where the qubit exchange determines the selection of the codewords from that dictionary as shown in Fig. 5. Thus, another limiting factor in a successful Man-In-The-Middle (MITM) impersonation attack is codeword recovery. This approach has the following advantages:

1. The synchronization parameters are exchanged twice. The first exchange helps establish the quantum keys and the second exchange sends the encrypted parameters as quantum bits.
2. If Eve is able to intercept the first transmission of qubits she has no more idea than Bob on how the qubits can be interpreted. Unless Eve can fully impersonate Bob the forward information from Alice is meaningless.
3. Alice and Bob can compare the two exchanges of qubits for inferring information about the quality of the quantum link and potential existence of an eavesdropper.

With X denoting a 24-bit sequence within Alice's synchronization parameters, the generation of M is established from the Alice-Bob matches of the qubit basis. Alice uses the RSA algorithm on M to generate the Key as has been previously established. The Key holds the encrypted positions of the matches represented by M. The pre-shared probabilities S have been used by Alice and Bob to generate the Huffman dictionary H, as shown in Fig. 5. In this example, the 24-bit sequence X has been decomposed into three 8-bit words. All valid combinations of codewords in this case are concatenated codewords of length 8-bits. The XOR encryption operation is performed on the 8-bit words as well. In this example the valid symbols are $\{a, b, c, d, e, f, x, y, z\}$ resulting in a valid codeword combination set of $\{abc, bac, da, xz, yb, zec, ay, ga, by, cex\}$. When we have m valid codewords in H, Alice and Bob can use the Key mod m to select the 8-bit codewords for the XOR encryption operation. Alice and Bob are free to setup this approach using as many codewords as they deem necessary in H, and then establish the Hamming distance between each code. Alice and Bob also determine the length of X and its decomposition which, need not be 8-bits in length but, can be any arbitrary length that they deem fit.

Fig. 6 depicts the proposed protocol for exchanging the chaotic synchronization parameters along with the corresponding TX/RX models. In the first step Alice encodes the synchronization parameters into a classical binary format, translates them to qubits, and then transmit them to Bob using the quantum basis that was pre-established. In the second step, Alice receives and compares Bob's results, encrypts the matches M to make the quantum encryption key Key as shown in Fig. 5 and Fig. 6. In the third step Alice transmits the Key to Bob. In the fourth step, Alice encrypts the synchroniza-

tion parameters using the Key and the pre-shared Huffman dictionary H as described in (10). Alice then translates and transmits the associated qubits to Bob. Using the pre-shared Huffman dictionary H and the Key, Bob then decodes the qubits. Fig. 5 elucidates this concept in detail.

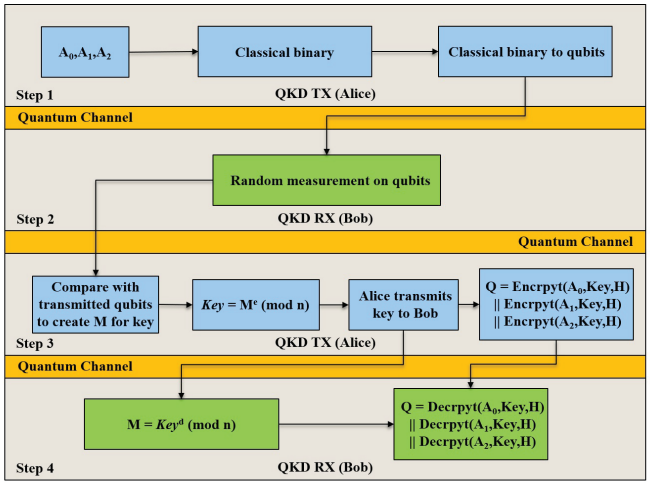


Fig. 6: Proposed QKD models for exchanging chaotic parameters.

4 Utilization of Proposed System for Space Missions

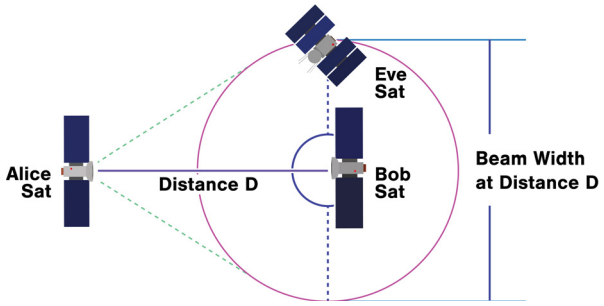


Fig. 7: Orbital Configuration of AliceSat, BobSat, and EveSat where AliceSat transmitting beam is oriented towards BobSat. We assume AliceSat and Bobsat are boresight aligned. EveSat is undetected by AliceSat, BobSat, or Earth Optical Ground Station, although within the AliceSat transmit beam.

In Fig. 7, the proposed chaotic communication scheme with QKD parameter exchange is used to exchange data between AliceSat and BobSat in an orbital configuration via space-to-space optical communications link. 10 cm optics at 1550 nm transmit wavelength (similar to the Lunar Laser Communications Demonstration - LLCD [46]) create a beamwidth approximately 6 km in diameter at an approximate earth-lunar distance of 400,000 km. The eavesdropper, EveSat, must be within that area to have a line-of-sight (LOS) with good link characterstics to be able to impersonate BobSat as shown in Fig. 7. For comparison, refer to the GRACE mission that flew twin spacecraft in tandem 220 km apart from one another, to study key changes in Earth's waters, ice sheets and the solid Earth [47]. Given the nature of this space application, the two most probable attacks are Man-In-The-Middle (MITM) attacks, where, EveSat tries to impersonate BobSat, and blinding attacks in which EveSat attempts to disable AliceSat and BobSat. The latter is beyond the scope of this paper and the main focus of this paper is towards MITM attacks. In MITM, EveSat's main attack goal is to impersonate BobSat by intercepting and decoding the data being exchanged between AliceSat and BobSat without being identified.

4.1 Pre-launch Requirements

The set of pre-shared secrets must be established alongside a strong authentication protocol to minimize the likelihood of a successful MITM attack. Since AliceSat and BobSat are using RSA encryption, they will establish their private and public keys as described in previous sections. Both AliceSat and BobSat also share a classical Huffman dictionary of binary codewords which will be mapped to the encrypted key parameters.

AliceSat and BobSat will establish a series of authentication and key exchange procedures depending upon the space-to-space orbital drivers (two free-flying independent spacecraft, orbiter-to-relay, etc.). Once authentication is complete the two can utilize a quantum communication channel for all forms of data exchange. The initial quantum key exchange protocol can be used for re-keying if deemed necessary.

4.2 Link Security

Following are the factors that contribute to link security:

1. EveSat's required proximity to either AliceSat or BobSat.
2. AliceSat and BobSat's known orbital dynamics.
3. Chaotic communication's inherent spread spectrum nature.
4. The weak link of sending the synchronization parameters as cleartext is addressed with the quantum coding of synchronization parameters.
5. The RSA encryption of the key parameters reconciling the correct matches of BobSat and AliceSat quantum basis.

On a two-qubit scheme, security is enhanced through maximizing randomization of inputs in a BB84-like key distribution scheme [48]. Provided that the eavesdropper cannot use knowledge of one state to derive knowledge of the remaining states security can also be improved by increasing the orders of complexity of the quantum basis [48]. However, this will result in more complex hardware and software. A sophisticated attack on the binary coding schemes that analyzes the distribution of measurement responses with EveSat's own application of quantum basis can be a possibility. A good countermeasure to this would be to increase the modularity of the quantum basis and the complexity of encryption protocols as permitted by the budget and schedule. The basic security scheme shown in this paper, combined with the constraints on the eavesdropper to attack this space-to-space free space optical link would be useful if installed in a National Institute of Standards and Technology (NIST) - moderate security environment, which is also easily extendable to the NIST-high security environment [49].

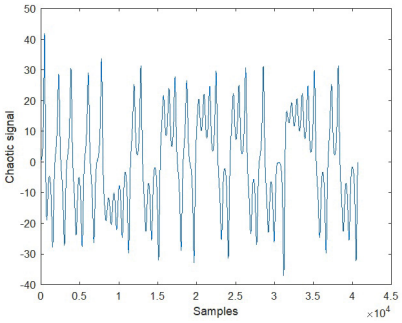
5 Experimental Work

We evaluated the performance of the proposed communication scheme through the experimental work described in this section. We tested the accuracy of the quantum key and chaotic parameter exchange by performing real-time data transmission and recovery across an AWGN channel model. High-resolution, single spectral and multi-spectral images were used as the input data. The noise tolerance of the system was investigated by measuring the transmission bit error rate (BER) for varying values of channel signal-to-noise-ratio (SNR). The quality of the reconstructed image was also evaluated by measuring the percentage error in pixels, $error_{pixels}$, given by (11), between the original transmitted image and the reconstructed image at the receiver. MATLAB version 2020A was used for design and simulation purposes.

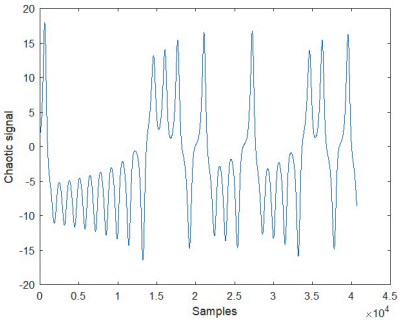
$$error_{pixels} = \frac{\sum_{i=0}^{rows-1} \sum_{j=0}^{cols-1} |pixel_{i,j}^{RX} - pixel_{i,j}^{TX}|}{rows \times cols} \tag{11}$$

5.1 Single-spectral Image Transmission

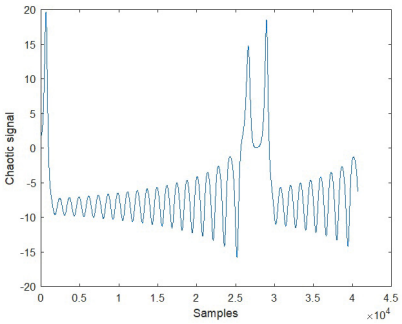
To ensure that the set of chaotic parameters are not predictable, they are usually varied dynamically during transmission. Therefore, the proposed chaotic system with QKD was tested for image transmission using different sets of chaotic parameters. Table 1 shows four sets of chaotic synchronization parameters that are typically used for chaotic systems [12]. Different sets of orthogonal basis was also used for each configuration, shown in Table 1. The experimental results showed that the QKD model was able to successfully exchange each set of chaotic parameters between the chaotic transmitter and receiver with 100% accuracy.



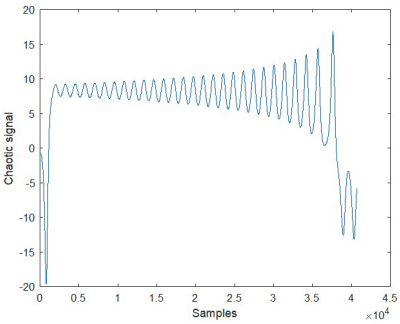
(a) Chaotic signal x_t with Configuration A



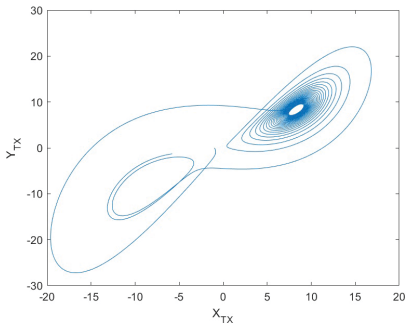
(b) Chaotic signal x_t with Configuration B



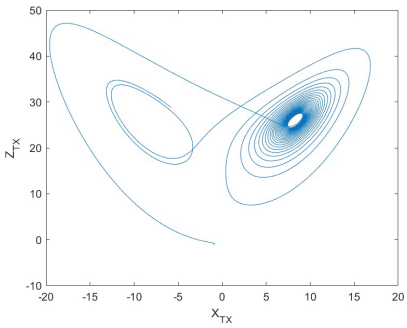
(c) Chaotic signal x_t with Configuration C



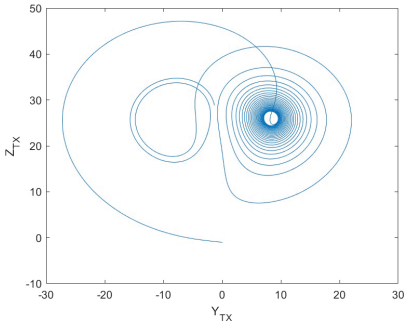
(d) Chaotic signal x_t with Configuration D



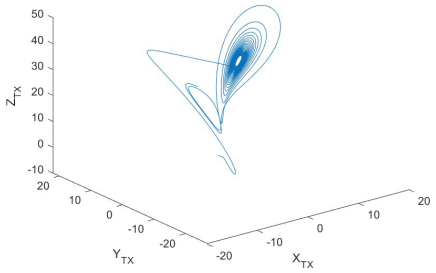
(e) Lorenz attractor chaotic signals y_t and x_t for configuration A



(f) Lorenz attractor chaotic signals z_t and x_t for configuration A



(g) Lorenz attractor chaotic signals z_t and y_t for configuration A



(h) Phase diagram of Lorenz attractor for configuration A.

Fig. 8: Chaotic carrier signals generated by synchronized Lorenz attractor TX and RX for different configurations.

Config.	Sigma	Rho	Beta	X(0)	Y(0)	Z(0)	Basis	Parameters recovered
A	16.0	64.0	4.0	1.0	0	0	[1,0;0,1]	Yes
B	10.0	27.0	2.677	1.77	2.89	4.56	[1,0;0,1]	Yes
C	10.0	28.0	2.677	2	1	1	[-0.5275,-0.8496;-0.8496,0.5275]	Yes
D	10.0	27.0	2.677	-1	0	-1	[-0.5275,-0.8496;-0.8496,0.5275]	Yes

Table 1: Four sets of typical Lorenz chaotic parameters.

With the Lorenz TX and RX configured with different sets of parameters, the attractors generated different forms of random, noise-like chaotic carrier signals. This is demonstrated in Figs. 8a-8d for each of the configurations in Table 1. A sampling frequency of 2 KHz was used by the Lorenz TX and RX. Figs. 8e-8h show the phase diagrams of the chaotic signals for the first configuration set (Configuration A). These plots show that the Lorenz attractor, configured with a specific parameter configuration and initial conditions, generates chaotic signals that are sensitive to the initial conditions within a particular phase space region of the attractor.

(a) Original image (512 × 512 pixels) transmitted by Alice using parameters $\sigma = 10, \rho = 54, \beta = 4$.

(b) Reconstructed image by Bob using recovered parameters $\sigma = 10, \rho = 54, \beta = 4$ and 0% pixel error.

(c) Reconstructed image by Eve using incorrect parameters $\sigma = 10, \rho = 45.6, \beta = 14$ and 98.4652% pixel error.

Fig. 9: Transmission of a 512 × 512 pixels image between Alice and Bob at SNR = 0.1 dB, with interception attempted by Eve.

A grayscale image of size 512 × 512 pixels transmitted by AliceSat and reconstructed at BobSat for SNR = 0.1 dB is shown in Fig. 9. Results show a 0% error in pixels between the original and reconstructed image. Also shown is a third image reconstructed by an unintentional intercepting RX, EveSat. We assume that EveSat has knowledge of the communication scheme we are using and is able to perform techniques such as LDPC decoding, QPSK demodulation, NRZ decoding, etc. to reconstruct the image data. However, to successfully intercept any data from this scheme EveSat has to know the chaotic parameters shared by AliceSat and BobSat, and due to the high security provided by QKD, EveSat has no way of acquiring those parameters.

Thus, EveSat proceeds with a randomly configured/synchronized Lorenz RX to try and capture the transmitted signal and regenerate the message. The intercepted image, shown in Fig. 9c, was reconstructed with 98.465% error in pixels. Thus it is concluded that EveSat cannot obtain any useful data from the intercepted signal since it cannot obtain synchronization parameters from the quantum channel and synchronize with the chaotic transmitter.

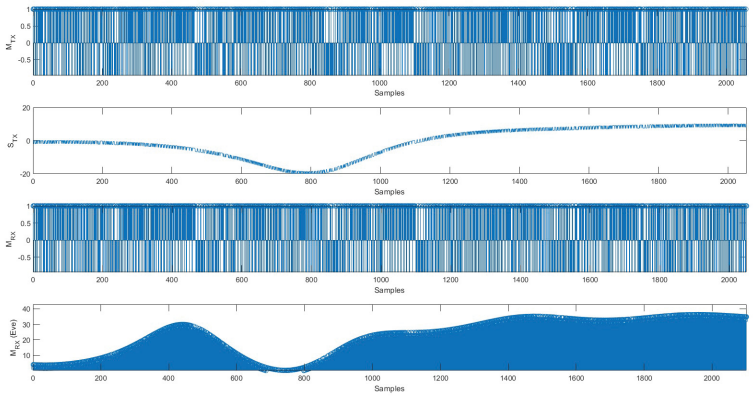
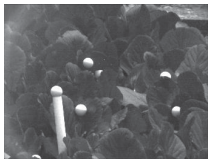


Fig. 10: Experimental data of transmission of a 512×512 pixels image between Alice and Bob, with interception attempted by Eve. M_{TX} is the transmitted binary NRZ data, S_{TX} is the chaotic transmitted signal masked with binary data, M_{RX} is the binary NRZ data correctly recovered by Bob, and M_{RX}(Eve) is the binary NRZ data incorrectly recovered by Eve.

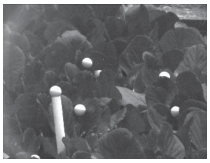
The transmitted image encoded as binary NRZ data, M_{TX} is shown in Fig. 10 over a range of 2000 sample points. Also shown is the signal, S_{TX} which is the generated chaotic signal masked with the binary NRZ data and transmitted over a noisy AWGN channel model. M_{RX} is the reconstructed binary NRZ data from the error signal and correctly recovered by Bob, and M_{RX}(Eve) is the data recovery attempted by EveSat from the intercepted data, see Fig. 10. As EveSat does not use a correctly configured Lorenz receiver, the chaotic signal generated at EveSat's receiver is not synchronized with the transmitted signal data, which distorts the error signal resulting in poor and inaccurate recovery of the binary data. These results further validate the use of QKD for securing FSO transmissions.

5.2 Multi-spectral Image Transmission

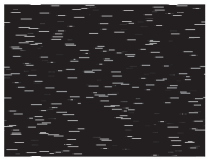
To extensively test the proposed communication system, we used multi-spectral radiance images, collected in a previous study [50]. The images were obtained in 2003 from rural and urban scenes in Minho, Portugal with the help of



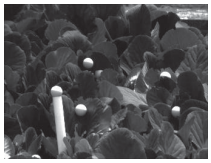
(a) Image transmitted by Bob at 400 nm frequency band.



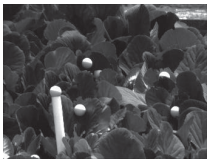
(b) Image received by Alice at 400 nm frequency band with 0% pixel error.



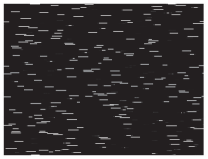
(c) Image intercepted by Eve during transmission with 98.3759% pixel error.



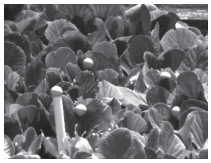
(d) Image transmitted by Bob at 500 nm frequency band.



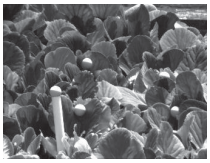
(e) Image received by Alice at 500 nm frequency band with 0% pixel error.



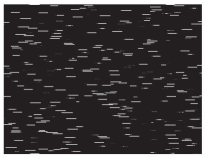
(f) Image intercepted by Eve during transmission with 98.1341% pixel error.



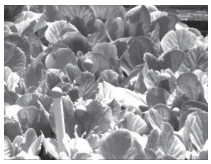
(g) Image transmitted by Bob at 600 nm frequency band.



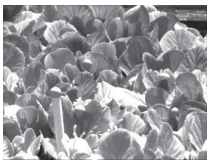
(h) Image received by Alice at 600 nm frequency band with 0% pixel error.



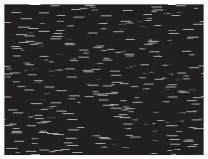
(i) Image intercepted by Eve during transmission with 98.1852% pixel error.



(j) Image transmitted by Bob at 700 nm frequency band.



(k) Image received by Alice at 700 nm frequency band with 0% pixel error.



(l) Image intercepted by Eve during transmission with 98.1852% error.

Fig. 11: Multi-spectral image recovered successfully by Bob after transmission by Alice at SNR = 0.1 dB and different frequency bands 400 nm, 500 nm, 600 nm, and 700 nm.

Chaotic parameter configs.	Multi-spectral image bands	Parameters recovered
B	band-1, (400nm)	Yes
C	band-2, (410nm)	Yes
D	band-3, (420nm)	Yes
C	band-4, (430nm)	Yes
A	band-5, (440nm)	Yes
D	band-6, (450nm)	Yes
A	band-7, (460nm)	Yes
B	band-8, (470nm)	Yes
C	band-9, (480nm)	Yes
D	band-10, (490nm)	Yes
B	band-11, (500nm)	Yes
C	band-12, (510nm)	Yes
D	band-13, (520nm)	Yes
A	band-14, (530nm)	Yes
A	band-15, (540nm)	Yes
A	band-16, (550nm)	Yes
B	band-17, (560nm)	Yes
B	band-18, (570nm)	Yes
D	band-19, (580nm)	Yes
A	band-20, (590nm)	Yes
C	band-21, (600nm)	Yes
A	band-22, (610nm)	Yes
D	band-23, (620nm)	Yes
A	band-24, (630nm)	Yes
C	band-25, (640nm)	Yes
D	band-26, (650nm)	Yes
B	band-27, (660nm)	Yes
A	band-28, (670nm)	Yes
A	band-29, (680nm)	Yes
B	band-30, (690nm)	Yes
B	band-31, (700nm)	Yes
A	band-32, (710nm)	Yes
D	band-33, (720nm)	Yes

Table 2: Randomized Lorenz chaotic parameter configurations for multi-spectral image transmission.

embedded neutral probe spheres. On each sphere, the spectra of the local illumination at 17 sample points were extracted in each scene and a total of 1904 chromaticity coordinates and correlated color temperatures (CCTs) derived [50]. During acquisition, these images were sampled in a wavelength range of 400-720 nm at 10 nm intervals. Each image cube has an effective resolution of $1344 \times 1024 \times 33$ (1344×1024 pixels of spatial resolution and 33 bands of spectral resolution). An image used for transmision in our experiments is sampled at different frequency bands and shown in Figs. 11a to 11l. The multi-spectral image was sampled at each frequency band and then transmitted to Alice, while an unintentional receiver, Eve, intercepts and captures the data in the classical AWGN channel. For each transmission, the chaotic parameters of Bob were reconfigured dynamically by choosing a random configuration, see Table 2, from the configurations shown in Table 1, and communicated to Alice via the QKD protocol. This was done to ensure complete randomness and to disable the Eavesdropper from possibly 'guessing' the correct configuration during transmission. For every configuration, the chaotic parameters were successfully recovered at the receiver and the transmitted images were recovered with 100% accuracy. However, Eve is not able to intercept and recover any

useful data at any of the frequency bands, as demonstrated by Figs. 11c, 11f, 11i, and 11l. This shows that the proposed system is secure and robust while transmitting a higher volume of data at multiple frequency bands.

5.3 Variation of Channel Noise

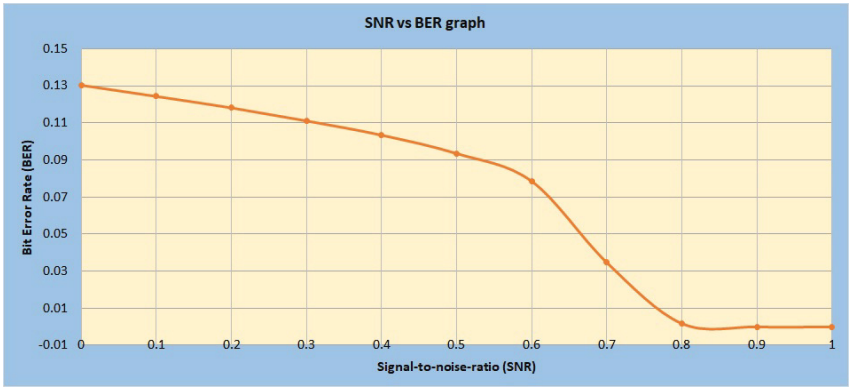


Fig. 12: Variation of bit error rate (BER) as a function of signal-to-noise-ratio (SNR).

To evaluate the noise tolerance of the system, the noise in the AWGN channels between the TX and RX was varied from SNR range of 0 dB to 40 dB and the bit error rate (BER) was measured. Fig. 12 shows the variation over the range 0 to 1 dB during transmission of the image at the 700 nm spectral band. Beyond 1 dB, the error rate was constantly zero. The results showed that the system can reject channel noise for a wide range of SNR ($>$ 0.8 dB). Accurate recovery of the data was possible even for very low SNR, e.g., 0.1 dB, see Figs. 9, 11, and 12.

6 Conclusions and Future Work

In this work, we demonstrated a scheme to secure free-space optical (FSO) communications by combining chaotic communication, using a Lorenz attractor, and a quantum key distribution (QKD) protocol. We propose increasing security of this scheme by dynamic reconfiguration of critical model parameters during transmission. The proposed scheme is evaluated via simulation, and results show that the system is noise-tolerant and feasible for transmission of high-resolution, single and multi-spectral data in FSO communications. Furthermore, the results indicate that the combination of chaotic systems and

QKD provide high security, because the chaotic carriers provide inherent security in the classical channel, while QKD secures the quantum channel data. We conclude that secure sharing of chaotic parameters between the transmitter and the receiver via QKD is feasible and increases efficiency and security of FSO communication. Future work will focus on hardware implementations, interfacing with free-space optics, and deployment to future space relays.

References

1. B. Edwards, "Overview of the Laser Communications Relay Demonstration Project," in *SpaceOps 2012 Conference*. Reston, Virigina: American Institute of Aeronautics and Astronautics, jun 2012, http://arc.aiaa.org/doi/10.2514/6.2012-1261897 Last Accessed: October 2020.
2. L. Mohon, "Laser communications relay demonstration (lcrd)," Jul 2015, https://www.nasa.gov/mission_pages/tdm/lcrd/index.html Last Accessed: October 2020.
3. "Nasa laser communications mission passes major review milestone," Jul 2015, https://www.nasa.gov/centers/goddard/news/releases/2012/12-074.html Last Accessed: October 2020.
4. Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, *Optical Wireless Communications: System and Channel Modelling with MATLAB*, 1st ed. USA: CRC Press, Inc., 2012.
5. H. Kaushal and G. Kaddoum, "Free space optical communication: challenges and mitigation techniques," *arXiv preprint arXiv:1506.04836*, 2015.
6. F. Duarte, "Secure interferometric communications in free space," *Optics Communications*, vol. 205, no. 4-6, pp. 313–319, may 2002, https://linkinghub.elsevier.com/retrieve/pii/S0030401802013846 Last Accessed: October 2020.
7. F. J. Duarte, "Secure interferometric communications in free space: enhanced sensitivity for propagation in the metre range," *Journal of Optics A: Pure and Applied Optics*, vol. 7, no. 1, pp. 73–75, jan 2005, http://stacks.iop.org/1464-4258/7/i=1/a=011?key=crossref.616bacd140853552d182f5d29863ef76 Last Accessed: October 2020.
8. F. J. Duarte, T. S. Taylor, A. M. Black, W. E. Davenport, and P. G. Varmette, "N -slit interferometer for secure free-space optical communications: 527 m intra interferometric path length," *Journal of Optics*, vol. 13, no. 3, p. 035710, mar 2011, http://stacks.iop.org/2040-8986/13/i=3/a=035710?key=crossref.8687d80f67af655c33a5427f848bc9a3 Last Accessed: October 2020.
9. F. J. Duarte and T. S. Taylor, "Quantum entanglement physics secures space-to-space interferometric communications," *LASER FOCUS WORLD*, vol. 51, pp. 54–58, 2015.
10. D. Boroson, "Optical Communications: A Compendium of Signal Formats, Receiver Architectures, Analysis Mathematics, and Performance Characteristics," Defense Technical Information Center (DTIC), Tech. Rep., 2005, https://apps.dtic.mil/docs/citations/ADA439968 Last Accessed: October 2020.
11. E. N. Lorenz, "Deterministic Nonperiodic Flow," *Journal of the Atmospheric Sciences*, vol. 20, no. 2, pp. 130–141, mar 1963, https://journals.ametsoc.org/jas/article/20/2/130/16956/Deterministic-Nonperiodic-Flow Last Accessed: October 2020.
12. A. Riaz and M. Ali, "Chaotic Communications, their applications and advantages over traditional methods of communication," in *2008 6th International Symposium on Communication Systems, Networks and Digital Signal Processing*. IEEE, jul 2008, pp. 21–24, http://ieeexplore.ieee.org/document/4610808/ Last Accessed: October 2020.
13. T. Mehtap and H. Oğraş, "Performing Modulation Scheme of Chaos Shift Keying with Hyperchaotic Chen System," in *Proceedings of the 6th International Advanced Technologies Symposium (IATS'11)*, 2011, pp. 54–58.
14. D.-s. Shiu and J. M. Kahn, "Differential pulse-position modulation for power-efficient optical communication," *IEEE transactions on communications*, vol. 47, no. 8, pp. 1201–1210, 1999.
15. W. Stallings, *Cryptography and Network Security: Principles and Practice (6th Edition)*, 6th ed. Upper Saddle River: Pearson, 2013.

16. M. H. Amin, N. G. Dickson, and P. Smith, "Adiabatic quantum optimization with qudits," *Quantum Information Processing*, 2013.
17. "Ibm quantum experience," https://quantum-computing.ibm.com/ Last Accessed: October 2020.
18. N. Xu, J. Zhu, D. Lu, X. Zhou, X. Peng, and J. Du, "Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System," *Physical Review Letters*, vol. 108, no. 13, p. 130501, mar 2012, https://link.aps.org/doi/10.1103/PhysRevLett.108.130501 Last Accessed: October 2020.
19. N. S. Dattani and N. Bryans, "Quantum factorization of 56153 with only 4 qubits," nov 2014, http://arxiv.org/abs/1411.6758 Last Accessed: October 2020.
20. P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press, 1994, pp. 124–134, http://ieeexplore.ieee.org/document/365700/ Last Accessed: October 2020.
21. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of Quantum Key Distribution Using d-Level Systems," *Physical Review Letters*, vol. 88, no. 12, p. 127902, mar 2002, https://link.aps.org/doi/10.1103/PhysRevLett.88.127902 Last Accessed: October 2020.
22. P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters*, vol. 85, no. 2, pp. 441–444, jul 2000, https://link.aps.org/doi/10.1103/PhysRevLett.85.441 Last Accessed: October 2020.
23. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Physical Review A*, vol. 78, no. 4, p. 042333, oct 2008, https://link.aps.org/doi/10.1103/PhysRevA.78.042333 Last Accessed: October 2020.
24. W. Hubbard, "Ice giants decadal study," *Vision and Voyages for Planetary Science in the Decade 2013*, vol. 2022, pp. 1–40, 2010.
25. N. Mahmud, E. El-Araby, H. Shaw, and L. Cooper, "Securing and auto-synchronizing communication over free-space optics using quantum key distribution and chaotic systems," in *Quantum Communications and Quantum Imaging XVI*, vol. 10771. International Society for Optics and Photonics, 2018, p. 107710U.
26. L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, feb 1990, https://link.aps.org/doi/10.1103/PhysRevLett.64.821 Last Accessed: October 2020.
27. T. Carroll and L. Pecora, "Synchronizing chaotic circuits," *IEEE Transactions on Circuits and Systems*, vol. 38, no. 4, pp. 453–456, apr 1991, http://ieeexplore.ieee.org/document/75404/ Last Accessed: October 2020.
28. L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals," *Physical Review A*, vol. 44, no. 4, pp. 2374–2383, aug 1991, https://link.aps.org/doi/10.1103/PhysRevA.44.2374 Last Accessed: October 2020.
29. K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Physical Review Letters*, vol. 71, no. 1, pp. 65–68, jul 1993, https://link.aps.org/doi/10.1103/PhysRevLett.71.65 Last Accessed: October 2020.
30. K. M. Cuomo, "Analysis and synthesis of self-synchronizing chaotic systems," Ph.D. dissertation, Massachusetts Institute of Technology, 1994.
31. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, dec 2014, https://linkinghub.elsevier.com/retrieve/pii/S0304397514004241 Last Accessed: October 2020.
32. T. Yang, "A survey of chaotic secure communication systems," *Int. J. Comp. Cognition*, vol. 2, pp. 81–130, 2004.
33. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 7066, pp. 343–346, nov 2005, http://www.nature.com/articles/nature04275 Last Accessed: October 2020.
34. L. Illing, "Digital communication using chaos and nonlinear dynamics," *Nonlinear Analysis: Theory, Methods & Applications*, vol. 71, no. 12, pp. e2958–e2964, dec 2009,

https://linkinghub.elsevier.com/retrieve/pii/S0362546X0900902X Last Accessed: October 2020.
35. A. A. Zaher and A. Abu-Rezq, "On the design of chaos-based secure communication systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 9, pp. 3721–3737, sep 2011, https://linkinghub.elsevier.com/retrieve/pii/S1007570411000037 Last Accessed: October 2020.
36. T. Kapitaniak, Y. Maistrenko, and C. Grebogi, "Bubbling and riddling of higher-dimensional attractors," *Chaos, Solitons & Fractals*, vol. 17, no. 1, pp. 61–66, jul 2003, https://linkinghub.elsevier.com/retrieve/pii/S0960077902004472 Last Accessed: October 2020.
37. V. Annovazzi-Lodi, G. Aromataris, M. Benedetti, and S. Merlo, "Secure Chaotic Transmission on a Free-Space Optics Data Link," *IEEE Journal of Quantum Electronics*, vol. 44, no. 11, pp. 1089–1095, nov 2008, http://ieeexplore.ieee.org/document/4674656/ Last Accessed: October 2020.
38. R. Lang and K. Kobayashi, "External optical feedback effects on semiconductor injection laser properties," *IEEE Journal of Quantum Electronics*, vol. 16, no. 3, pp. 347–355, mar 1980, http://ieeexplore.ieee.org/document/1070479/ Last Accessed: October 2020.
39. I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Free-space quantum key distribution with entangled photons," *Applied Physics Letters*, vol. 89, no. 10, p. 101122, sep 2006, http://aip.scitation.org/doi/10.1063/1.2348775 Last Accessed: October 2020.
40. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," *Physical Review Letters*, vol. 98, no. 1, p. 010504, jan 2007, https://link.aps.org/doi/10.1103/PhysRevLett.98.010504 Last Accessed: October 2020.
41. R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New Journal of Physics*, vol. 4, pp. 43–43, jul 2002, http://stacks.iop.org/1367-2630/4/i=1/a=343?key=crossref.d7b8b45f84c813d48668b496880b2be8 Last Accessed: October 2020.
42. J. Kupferman and S. Arnon, "Zero-error attacks on a quantum key distribution fso system," *OSA Continuum*, vol. 1, no. 3, pp. 1079–1086, 2018.
43. P. V. Trinh, T. V. Pham, N. T. Dang, H. V. Nguyen, S. X. Ng, and A. T. Pham, "Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver," *IEEE Access*, vol. 6, pp. 4159–4175, 2018.
44. D. Jiang, Y. Chen, X. Gu, L. Xie, and L. Chen, "Efficient and universal quantum key distribution based on chaos and middleware," *International Journal of Modern Physics B*, vol. 31, no. 2, p. 1650264, 2017.
45. K. Cho and T. Miyano, "Chaotic cryptography using augmented lorenz equations aided by quantum key distribution," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 2, pp. 478–487, 2015.
46. D. Boroson, B. Robinson, D. Burianek, D. Murphy, and F. Khatri, "The lunar laser communication demonstration (llcd)," 2014, https://alumni.jhu.edu/sites/default/files/inline-images/NASA-LasercomTalk-JHU-Aerospace-Affinity-June-11th-2014.pdf, Last Accessed: October 2020.
47. "Grace (gravity recovery and climate experiment)," https://directory.eoportal.org/web/eoportal/satellite-missions/g/grace Last Accessed: October 2020.
48. H.-W. Li, Z.-Q. Yin, S. Wang, Y.-J. Qian, W. Chen, G.-C. Guo, and Z.-F. Han, "Randomness determines practical security of BB84 quantum key distribution," *Scientific Reports*, vol. 5, no. 1, p. 16200, dec 2015, http://www.nature.com/articles/srep16200 Last Accessed: October 2020.
49. NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.
50. S. M. Nascimento, K. Amano, and D. H. Foster, "Spatial distributions of local illumination color in natural scenes," *Vision research*, vol. 120, pp. 39–44, 2016.