micromachines

Article

High Spectrum Efficiency and High Security Radio-Over-Fiber Systems with Compressive-Sensing-Based Chaotic Encryption

Zhanhong Wang [1], Lu Zhang [1,*], Jiahao Zhang [1], Oskars Ozolins [2], Xiaodan Pang [1] and Xianbin Yu [1,*]

[1] College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China; zhanhongwang@zju.edu.cn (Z.W.); zhangjh914@zju.edu.cn (J.Z.); xipa@zju.edu.cn (X.P.)
[2] Institute of Photonics, Electronics and Telecommunications, Riga Technical University, 1048 Riga, Latvia; oskars.ozolins@rtu.lv
* Correspondence: zhanglu1993@zju.edu.cn (L.Z.); xyu@zju.edu.cn (X.Y.)

Abstract

With the increasing demand for high throughput and ultra-dense small cell deployment in the next-generation communication networks, spectrum resources are becoming increasingly strained. At the same time, the security risks posed by eavesdropping remain a significant concern, particularly due to the broadcast-access property of optical fronthaul networks. To address these challenges, we propose a high-security, high-spectrum efficiency radio-over-fiber (RoF) system in this paper, which leverages compressive sensing (CS)-based algorithms and chaotic encryption. An 8 Gbit/s RoF system is experimentally demonstrated, with 10 km optical fiber transmission and 20 GHz radio frequency (RF) transmission. In our experiment, spectrum efficiency is enhanced by compressing transmission data and reducing the quantization bit requirements, while security is maintained with minimal degradation in signal quality. The system could recover the signal correctly after dequantization with 6-bit fronthaul quantization, achieving a structural similarity index (SSIM) of 0.952 for the legitimate receiver (Bob) at a compression ratio of 0.75. In contrast, the SSIM for the unauthorized receiver (Eve) is only 0.073, highlighting the effectiveness of the proposed security approach.

Keywords: compressive sensing; radio-over-fiber; chaotic encryption

1. Introduction

As the demand for high capacity continues to grow in the next-generation wireless communication networks, high-frequency electromagnetic waves, such as millimeter waves (mmW) and terahertz waves (THz), have garnered significant attention. These frequencies offer broad bandwidth resources, which are crucial for meeting the capacity requirements of future networks [1]. However, their use in radio access networks (RANs) presents several challenges. On one hand, high-frequency communication can significantly enhance the throughput of radio remote units (RRUs), enabling the future 6G network to achieve peak rates of 1 Tb/s and user-experienced data rates of beyond 1 Gb/s [2]. On the other hand, these high-frequency waves experience greater path loss, necessitating ultra-dense deployment of RRUs to maintain coverage and performance [3]. Therefore, improving spectrum efficiency becomes essential for the optical fronthaul networks. Currently, the common public radio interface (CPRI) is widely used for optical fronthaul networks, particularly in Option 8 of the 3GPP function split options [4]. However, CPRI imposes high communication overhead, as it requires up to 15-bit quantization to maintain signal

Check for updates

Academic Editor: Xiaoguang Zhao

Received: 21 November 2025
Revised: 6 January 2026
Accepted: 6 January 2026
Published: 7 January 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

integrity, which results in significant bandwidth consumption and spectrum efficiency degradation [5]. This makes it clear that new methods are needed to improve the spectrum efficiency of optical fronthaul systems.

Several innovative strategies have been proposed to address this challenge. Analog radio-over-fiber (A-RoF) systems, for instance, have been experimentally implemented, as they require less bandwidth for transmission compared to digital signals [6,7]. However, analog signals are more susceptible to the nonlinear effects of optical fibers, necessitating complex nonlinear equalization algorithms that increase the demand for digital signal processing (DSP). Additionally, while data compression algorithms have been suggested to reduce transmission data volume, their effectiveness remains uncertain [8,9]. Digital–analog radio-over-fiber (DA-RoF) systems can enhance the signal-to-noise ratio (SNR) and support high-order modulation formats to improve spectrum efficiency, but they also require digital–analog hybrid transmission and complex signal recovery algorithms, which drive up deployment costs [10]. Alongside these technical challenges, security is a crucial concern for RANs. Due to the broadcast nature of the downlink in optical fronthaul networks, transmitted signals are vulnerable to eavesdropping by unauthorized receivers. In recent years, physical (PHY)-layer encryption techniques have been explored to provide more robust security than traditional media access control (MAC)-layer encryption [11,12]. One promising PHY-layer encryption method is chaotic encryption, which is favored for its high randomness and low implementation cost [13–16]. Recently, a CS-based chaotic encryption algorithm was proposed to improve the security performance of the communication system, embedding the chaotic encryption algorithm into the CS algorithm [17,18]. In addition, the performance of the spectrum efficiency is not discussed in these works.

In this paper, we present an approach that combines high spectrum efficiency with robust security by using the compressive sensing (CS)-based chaotic encryption algorithm in a radio-over-fiber (RoF) system. We generated a 16QAM-DMT signal and mapped it to an 8 Gbit/s BPSK signal via fronthaul quantization and transmitted it over 10 km of standard single-mode fiber (SSMF) at the C-band. A photonics-based method is used to generate the RF signal at 20 GHz. With the CS-based chaotic encryption algorithm, the system achieves quantization-error-free at a 6-bit quantization level, even with compression ratios (CR) of 0.25 and 0.5. Furthermore, the system's security is ensured, as demonstrated by the structural similarity index (SSIM) of 0.952 for the legitimate receiver (Bob) at a compression ratio of 0.75, indicating minimal loss of information. In contrast, the SSIM for the eavesdropper (Eve) is only 0.073 under the same conditions, highlighting the effectiveness of the proposed security method.

The remainder of the paper is organized as follows: Section 2 introduces the selected chaotic sequence and the principle of the algorithms. Section 3 explains the experiment setup for the 20 GHz RoF system, and Section 4 discusses the experiment results and optimizes the parameters of the algorithm. Finally, Section 5 concludes the paper with a summary of the research.

2. Principle

The architecture of the proposed RoF system is shown in Figure 1. The data is processed by the CS-based chaotic encryption algorithm at the BBU and then transmitted to multiple RRUs. At the RRUs, RF signals are generated and sent to the users. First, the amount of transmitted data is reduced, and a lesser quantization bit number will be used for the optical fronthaul network because of the CS algorithm. On top of that, because of the chaotic encryption, the legal receiver Bob can reconstruct the origin signal with minimal quality degradation, and the illegal receiver Eve obtains less effective information due to

the absence of the legal keys. Therefore, high spectrum efficiency and high security can be achieved in the proposed system.

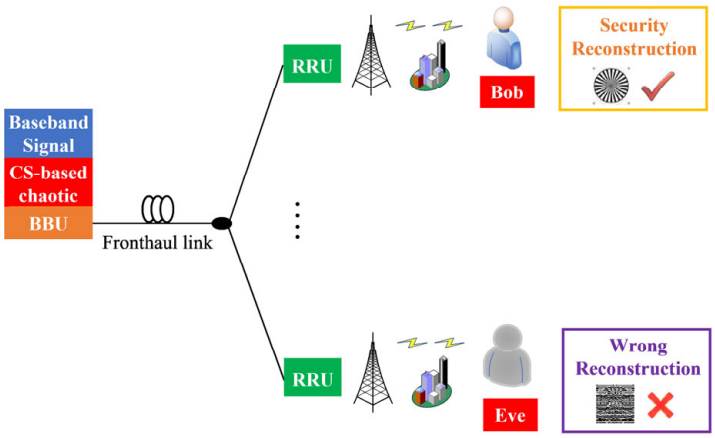


Figure 1. The architecture of the high-spectrum-efficiency and high-security RoF system.

A generalized algorithm block diagram is shown in Figure 2. The algorithm will be discussed in detail. First, the key is prestored in the BBU and the legal receivers. With the key, the chaotic sequence can be generated at the BBU. In the proposed system, the 2-dimensional logistic-sine-coupling map (2D-LSCM) is chosen as the chaotic sequence, which can be expressed as

$$\begin{cases} x_{i+1} = \sin(\pi(4\theta x_i(1-x_i) + (1-\theta)\sin(\pi y_i)) \\ y_{i+1} = \sin(\pi(4\theta x_i(1-x_i) + (1-\theta)\sin(\pi x_{i+1})) \end{cases}. \quad (1)$$

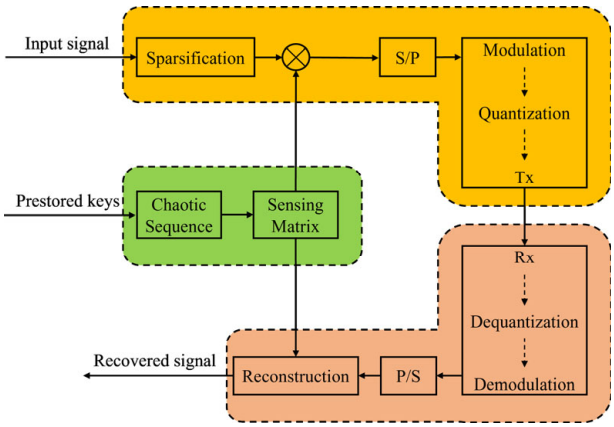


Figure 2. Schematic for the compressive-sensing-based chaotic encryption algorithm.

Here, x_1, y_1 and θ are chosen as the keys, where $\theta \in [0, 1]$, $x_1, y_1 \in (0, 1)$. Compared to other sequences, such as the Logistic map and the Lorenz system, 2D-LSCM exhibits hyperchaotic properties over a larger range, with better chaotic performance and lower computational complexity [19]. Then utilizing the keys, the sensing matrix **B** for the compressive sensing can be obtained. According to mathematical theory, the matrix **B** needs to meet the restricted isometry property (RIP) condition for signal reconstruction at the receiver. The random circular matrix (RCM) is utilized in our system to meet the condition because of its simplicity [20]. The cyclic characteristic of RCM is

$$\begin{aligned} \mathbf{B}(j,1) &= \lambda \cdot \mathbf{B}(j-1,n) \\ \mathbf{B}(j,2:n) &= \lambda \cdot \mathbf{B}(j-1,1:n-1), \end{aligned} \quad (2)$$

where $2 \leq j \leq m$, $\lambda > 1$. The first line of $\mathbf{B}$ can be set as the corresponding number of the average of x_n and y_n. For the input transmitted signal, it needs to be sparsified by orthonormal basis decomposition due to the condition for compressive sensing. For example, an $n \times 1$ vector $\mathbf{x}$ can be decomposed as

$$\mathbf{x} = \sum_{k=1}^{n} \psi_k s_k = \boldsymbol{\psi}\mathbf{s}, \tag{3}$$

where $\boldsymbol{\psi}$ is the orthonormal basis of $\mathbf{x}$, and $\mathbf{s}$ is an $n \times 1$ sparse vector. For multimedia signals such as images, the frequency domain matrix is sparse because of low high-frequency components, and the sparsification can be completed by time-frequency transform directly, such as Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). Among them, the range of matrix elements obtained after DCT can be represented using only 14 binary digits, which is smaller than the 18 bits of DWT and the 31 bits of FFT [17]. Therefore, in algorithm design, DCT is adopted for sparsification to reduce data volume. Then the vector $\mathbf{x}$ is multiplied by an $m \times n$ measurement matrix $\boldsymbol{\Phi}$ for low-dimensional mapping, which can be expressed as

$$\mathbf{y} = \boldsymbol{\Phi}\mathbf{x} + \mathbf{e} = \boldsymbol{\Phi}\boldsymbol{\psi}\mathbf{s} + \mathbf{e} = \mathbf{B}\mathbf{s} + \mathbf{e}, \tag{4}$$

where $\mathbf{B}$ is the $m \times n$ sensing matrix obtained by a chaotic sequence. Here $\mathbf{y}$ is an $m \times 1$ matrix, and the CR is defined as m/n. Then after parallel serial conversion, the signal is modulated and quantized by the BBU and then transmitted to RRU for frequency conversion.

At the legal receiver, the keys are prestored and the chaotic sensing matrix $\mathbf{B}$ can be cloned. In fact, the problem of solving $\mathbf{s}$ can be transformed into an optimization problem [21], which is

$$\begin{aligned} &\min ||\mathbf{s}||_0 \\ &\text{subject to } ||y - Bs||_2 \leq \varepsilon_e, \end{aligned} \tag{5}$$

where ε_e is the energy of the sampling noise. It is difficult to solve the NP-hard problem by an analytical method. The smooth l_0 method can be used in this scene [22]. This method uses a Gaussian function to fit the l_0-norm of vector $\mathbf{s}$, converting it into a smooth continuous function for optimization. The Gaussian function is

$$f_\sigma(s_i) = 1 - \exp(-\frac{s_i^2}{2\sigma^2}), \tag{6}$$

where σ is the smoothness factor. Then the l_0-norm of vector $\mathbf{s}$ is

$$\|\mathbf{s}\|_0 = \lim_{\sigma \to \infty} F_\sigma(s_i) = \lim_{\sigma \to \infty} (n - \sum_{i=1}^{n} f_\sigma(s_i)). \tag{7}$$

Because of the smooth, continuous characteristic, gradient descent can be utilized to find the minimum point of l_0-norm. The initial vector is the multiplication of the pseudo-inverse of the matrix $\mathbf{B}$ and the measurement vector $\mathbf{y}$. After several iterations, the algorithm convergence is achieved, and the sparsest solution of the problem in Equation (5) is obtained. However, because of a lack of knowledge of the keys, the chaotic sensing matrix cannot be cloned correctly at the illegal receiver Eve. Therefore, Eve can obtain less effective information, and the security of the RoF system is ensured.

https://doi.org/10.3390/mi17010080

3. Experimental Setup

The setup for the proof-of-concept experiment is illustrated in Figure 3. A 64 × 64 image signal, labeled 'testpat1', is chosen as the input signal. First, the image signal undergoes a sparse transformation using DCT, followed by processing with the CS-based chaotic encryption algorithm. The resulting compressed signal is then modulated into a 16-QAM signal. Next, the signal is converted into a DMT signal through subcarrier mapping and IFFT, with 2048 IFFT points. Of these, 800 subcarriers are used to carry the 16-QAM signal, while another 800 subcarriers carry the complex conjugate of the 16-QAM signal. The DMT signal is subsequently quantized and remapped to a BPSK signal for optical fronthaul transmission.

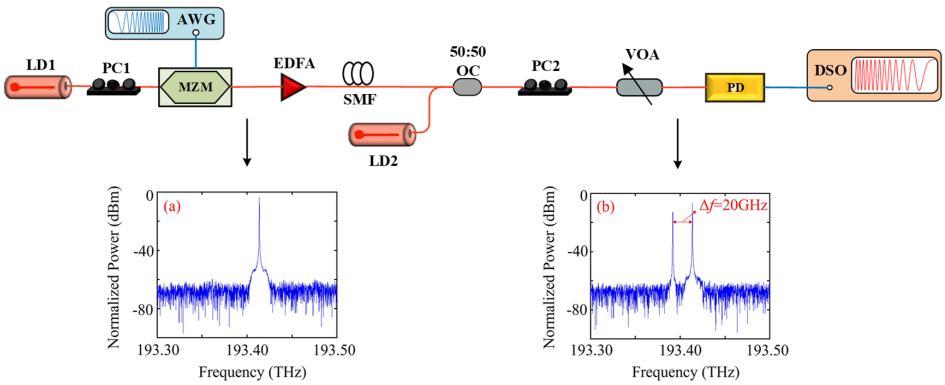


Figure 3. Experimental setup of the proposed RoF system. Inset: (**a**) the normalized optical spectrum after MZM, (**b**) the normalized optical spectrum before PD.

For the optical transmission, intensity modulation is employed. The output wavelength of laser diode LD1 (100 kHz linewidth) is set to 1500.00 nm, and the laser is modulated by a Mach-Zehnder Modulator (MZM, EOSpace, 40-GHz bandwidth). An 8 Gbps total signal is generated by an arbitrary waveform generator (AWG, Keysight M8195A, 64 GSa/s) to drive the MZM. The modulated laser is then amplified by an erbium-doped fiber amplifier (EDFA) to increase the power budget. After traveling through 10 km standard single-mode fiber (SSMF), the signal is coupled with a local oscillator (LO) laser from LD2 (100 kHz linewidth), which operates at a wavelength of 1550.16 nm, using a 50:50 coupler. A variable optical attenuator (VOA) is used to control the input power to the photodiode (PD, 40 GHz bandwidth). In the PD, the 20 GHz RF signal is generated via photo-mixing and transmitted through an RF cable. The RF signal is captured by a digital storage oscilloscope (DSO, Keysight DSOX93204A, 80 GSa/s) for offline DSP.

The signal recovery process follows these steps in the DSP flow. First, the signal is resampled at 64 GSa/s from DSO and converted to baseband through digital down-conversion. Due to the free-running characteristics of the two laser diodes, frequency offset (FO) can impact communication performance. The FO is estimated using a digital phase-locked loop [23], and synchronization is achieved via a cross-correlation algorithm. To compensate for dispersion, a 4-tap feedforward equalizer is employed, followed by a decision feedback equalizer with four feedforward taps and three feedback taps [24]. After equalization, the BPSK signal is recovered, and dequantization and demodulation are performed to retrieve the compressed signal. The sparsest solution to the optimization problem is found using the greedy descent algorithm, with 40 iterations and a step size of 1.01. The original signal is then reconstructed through IDCT.

4. Results and Discussion

The transmission performance of the proposed RoF system is shown in Figure 4. The bit error rate (BER) is evaluated by comparing the transmitted and received BPSK signals. Given the non-Gaussian distribution of the actual transmission signal, the robustness of the system is critical. The results show that the BER improves with increasing optical power at the photodiode (PD). The system maintains a BER below the hard-decision forward error correction (HD-FEC) threshold of 3.8×10^{-3} [25] when the optical power exceeds -4 dBm, and error-free transmission is achieved when the optical power exceeds 0 dBm. The BPSK constellation diagram in Figure 3 further demonstrates the performance.

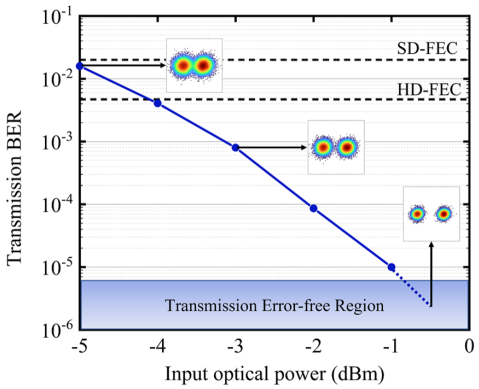


Figure 4. The transmission performance of the proposed RoF system.

The spectrum efficiency of the system is discussed. To ensure a fair comparison, spectral efficiency is evaluated under two conditions: one using the CS-based chaotic encryption algorithm and the other with traditional encryption but without CS. In both cases, the input power to the photodiode (PD) is set to 5 dBm to achieve error-free transmission. With the CS-based algorithm, the amount of transmitted data is significantly reduced. For instance, when the CR is 0.5, the number of symbols per subcarrier in a frame decreases from 20 to 9. This reduction allows the system to transmit twice the amount of data in the same transmission bandwidth. Similarly, when the CR is 0.25, nearly four times the amount of data can be transmitted. However, it is important to note that a lower CR can lead to greater signal degradation during reconstruction. This represents a trade-off between spectrum efficiency and signal quality.

The effect of fronthaul quantization is also examined in our experiment. Figure 5 shows the BER performance of the system with different CR values. Since the system achieves error-free transmission, the focus is on estimating the effect of transmission errors. With the CS algorithm, the quantization BER improves compared to the case without CS, meaning that fewer quantization bits are required in the RoF system. As a result, the system's spectrum efficiency is further enhanced. This improvement is because the CS algorithm reduces signal redundancy and the amplitude of the DMT signal [26], allowing the signal to be represented with fewer quantization bits. However, the quantization BER degrades as the CR increases since lower CR values eliminate more redundant information from the sparse signal. Notably, error-free quantization can be achieved when the CR is 0.25 or 0.5, demonstrating the effectiveness of the CS-based approach in reducing the required quantization bits while maintaining signal integrity.

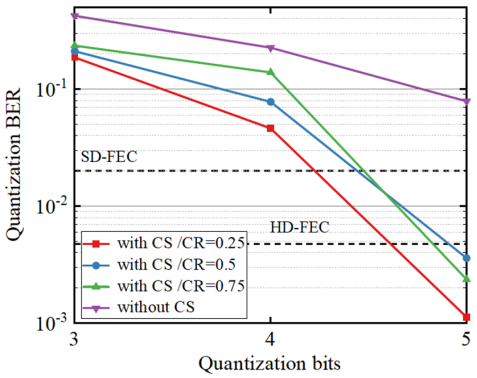


Figure 5. The quantization BER performance under different fronthaul quantization bit numbers when error-free transmission is achieved.

Then the security of the system is verified. The SSIM performance and the quality of the reconstructed images are shown in Figure 6 and Table 1. The legal keys (x_1 = 0.6, y_1 = 0.7, θ = 0.8) are prestored in Bob (x_1 = 0.7, y_1 = 0.7, θ = 0.8), and there are only incorrect keys in Eve. As a result, Bob, the legitimate receiver, can successfully reconstruct the image using the correct decryption keys, while Eve, the unauthorized receiver, cannot. When the CR is 0.75, the SSIM between Alice and Bob reaches 0.952, indicating only minimal quality degradation due to the CS-based chaotic encryption algorithm. In contrast, the SSIM between Alice and Eve remains close to 0, meaning that Eve is unable to extract meaningful information from the reconstructed image. Then the situation of perturbation is also considered. Here, the disturbance is set to 10^{-14}, and the SSIM of Eve is 0.033 with CR = 0.5 and 0.028 with CR = 0.75, confirming the sensitivity to the keys. With the sensitivity of the chaotic sequency is 10^{-14}, the key space can be calculated as $(10^{14})^3 = 10^{42}$, which is sufficient to prevent attacks from Eve. This demonstrates that the CS-based chaotic encryption algorithm effectively ensures the security of the RoF system, preventing unauthorized access.

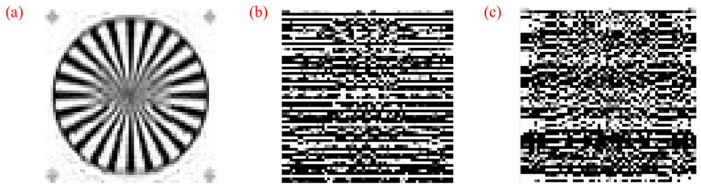


Figure 6. Images recovered by (**a**) Bob and (**b**) Eve with incorrect keys (x_1, y_1, θ) = (0.7, 0.7, 0.8) and (**c**) Eve with incorrect keys (x_1, y_1, θ) = ($0.6 + 10^{-14}$, 0.7, 0.8) when CR = 0.5.

Table 1. The SSIM between the image transmitted and the one recovered with 6-bit quantization.

Receiver	CR = 0.5	CR = 0.75
Bob	0.877	0.952
Eve [(x_1, y_1, θ) = (0.7, 0.7, 0.8)]	0.052	0.073
Eve [(x_1, y_1, θ) = ($0.6 + 10^{-14}$, 0.7, 0.8)]	0.033	0.028

The optimized parameters for the smooth l_0 method are also discussed. The SSIM performance of Bob with different iteration numbers is illustrated in Figure 7. For iteration numbers, the step size is set as 1.01, and the CR is set as 0.5. From the results, we found that there is not much difference in SSIM performance under different iteration times. When the iteration number is small, SSIM performance has slightly improved with its improvement. Afterwards, the algorithm converges and SSIM performance gradually stabilizes. Since the improvement is not very significant, the iteration number can be

reduced to lower the algorithm complexity and meet real-time communication requirements. In fact, the complexity of the compressive sensing algorithm is approximately $O(N)$, which is completely acceptable for real-time communication [17]. Based on existing deductions, the initial smooth factor for the compressive sensing algorithm may be chosen about two to four times the maximum absolute value of the obtained sources. In the proof-of-concept experiment, we set the factor to two times the maximum absolute value to ensure mathematical interpretability.

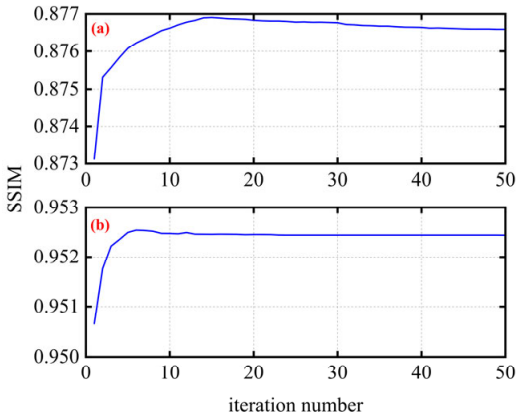


Figure 7. The SSIM performance under different iteration numbers of the smooth l_0 method with (**a**) CR = 0.5 and (**b**) CR = 0.75.

The selection of CR also has a significant impact on the signal reconstruction performance of Bob. The SSIM performance of Bob under different CRs is shown in Figure 8. Clearly, when the CR is less than 0.5, the SSIM performance significantly decreases. There are two main reasons for this result. Firstly, the DCT of the image signal is not a strictly sparse matrix, and there are still small coefficients at high frequencies. When the number of samples is reduced, the effective sparsity of the matrix remains unchanged, making it difficult for the algorithm to distinguish between the main components and noise based on redundant information. On the other hand, the observation process of CS is accompanied by noise. When the CR decreases, the number of elements in the matrix also decreases. Due to the diffusion effect of matrix multiplication, the SNR of each sampling point decreases. Therefore, to ensure the signal quality reconstructed by Bob, it is best to choose a CR greater than 0.5. And adaptive adjustment algorithms can be further adopted to balance the computational complexity and signal reconstruction quality.

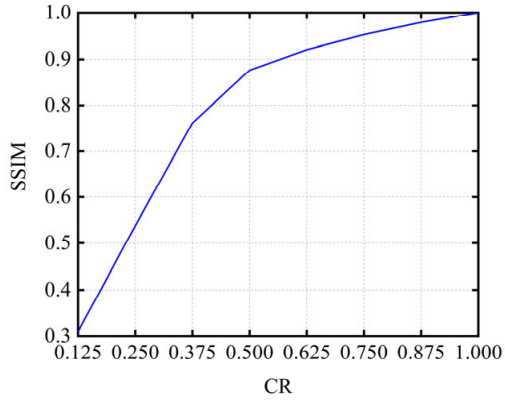


Figure 8. The SSIM between Alice and Bob under different CR conditions.

5. Conclusions

In this paper, we propose a novel method that utilizes a CS-based chaotic encryption algorithm to enhance both spectrum efficiency and security of the RoF system. Regarding spectrum efficiency, the CS algorithm reduces the amount of transmitted data, and the system achieves quantization-error-free at only a 6-bit quantization level with the proposed algorithm. In terms of security, an SSIM of 0.952 for Bob at a CR of 0.75 is achieved, indicating minimal information loss. In contrast, under the same condition, the SSIM for Eve is only 0.073, confirming the effectiveness of the algorithm. On this basis, the parameters are optimized and explored to further reduce computational complexity.

Author Contributions: Conceptualization, Z.W. and L.Z.; methodology, Z.W. and L.Z.; software, Z.W. and J.Z.; validation, Z.W. and J.Z.; formal analysis, Z.W. and L.Z.; investigation, Z.W. and L.Z.; resources, L.Z. and X.Y.; data curation, Z.W.; writing—original draft preparation, Z.W.; writing—review and editing, Z.W., L.Z., X.P., O.O., and X.Y.; supervision, L.Z. and X.Y.; project administration, L.Z., X.P., O.O., and X.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China (62471433); the Sweden's Innovation Agency (VINNOVA) funded project (2024-02451); the strategic innovation program Smarter Electronic Systems—a joint venture by Vinnova, Formas, and the Swedish Energy Agency A-FRONTAHUL project (2023-00659).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Dataset available on request from the authors.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Xiao, M.; Mumtaz, S.; Huang, Y.; Dai, L.; Li, Y.; Matthaiou, M.; Karagiannidis, G.K.; Bjornson, E.; Yang, K.; I, C.-L.; et al. Millimeter Wave Communications for Future Mobile Networks. *IEEE J. Select. Areas Commun.* **2017**, *35*, 1909–1935. [CrossRef]
2. Rasti, M.; Taskou, S.K.; Tabassum, H.; Hossain, E. Evolution Toward 6G Multi-Band Wireless Networks: A Resource Management Perspective. *IEEE Wirel. Commun.* **2022**, *29*, 118–125. [CrossRef]
3. Hemadeh, I.A.; Satyanarayana, K.; El-Hajjar, M.; Hanzo, L. Millimeter-Wave Communications: Physical Channel Models, Design Considerations, Antenna Constructions, and Link-Budget. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 870–913. [CrossRef]
4. Common Public Radio Interface, Interface Specification V7.0. 2015. Available online: https://www.cpri.info/downloads/CPRI_v_7_0_2015-10-09.pdf (accessed on 5 January 2026).
5. Liu, X.; Zeng, H.; Chand, N.; Effenberger, F. Efficient Mobile Fronthaul via DSP-Based Channel Aggregation. *J. Light. Technol.* **2016**, *34*, 1556–1564. [CrossRef]
6. Nimura, S.; Tanaka, K.; Ishimura, S.; Nishimura, K.; Inohara, R.; Tsuritani, T.; Suzuki, M. 10.51-Tbit/s Multi-Channel IF-over-Fiber Transmission with SDM/WDM/SCM for beyond-5G Mobile Fronthaul Accommodating Ultra-High-Density Antennas. *J. Opt. Commun. Netw.* **2023**, *15*, C263. [CrossRef]
7. Maximidis, R.; Vagionas, C.; Kalfas, G.; Leiba, Y.; Miliou, A.; Pleros, N. A 51 Gb/s Reconfigurable mmWave Fiber-Wireless C-RAN Supporting 5G/6G MNO Network Sharing. *J. Light. Technol.* **2023**, *41*, 4705–4712. [CrossRef]
8. Qiao, R.; Jiang, T.; Yu, W. Learning-Based Fronthaul Compression for Uplink Cloud Radio Access Networks. In Proceedings of the ICC 2023—IEEE International Conference on Communications, Rome, Italy, 28 May–1 June 2023; pp. 5928–5933.
9. Grönland, A.; Klaiqi, B.; Gelabert, X. Learning-Based Latency-Constrained Fronthaul Compression Optimization in C-RAN. In Proceedings of the 2023 IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Edinburgh, UK, 6–8 November 2023; pp. 134–139.
10. Zhang, C.; Zhu, Y.; He, B.; Lin, J.; Liu, R.; Xu, Y.; Yi, L.; Zhuge, Q.; Hu, W.; Hu, W.; et al. Clone-Comb-Enabled High-Capacity Digital-Analogue Fronthaul with High-Order Modulation Formats. *Nat. Photonics* **2023**, *17*, 1000–1008. [CrossRef]
11. Argyris, A.; Syvridis, D.; Larger, L.; Annovazzi-Lodi, V.; Colet, P.; Fischer, I.; García-Ojalvo, J.; Mirasso, C.R.; Pesquera, L.; Shore, K.A. Chaos-Based Communications at High Bit Rates Using Commercial Fibre-Optic Links. *Nature* **2005**, *438*, 343–346. [CrossRef]
12. Kodama, T.; Nakagawa, N.; Kataoka, N.; Wada, N.; Cincotti, G.; Wang, X.; Miyazaki, T.; Kitayama, K.-I. Secure 2.5 Gbit/s, 16-Ary OCDM Block-Ciphering with XOR Using a Single Multi-Port En/Decoder. *J. Light. Technol.* **2010**, *28*, 181–187. [CrossRef]

13. Bi, M.; Fu, X.; Zhou, X.; Zhang, L.; Yang, G.; Yang, X.; Xiao, S.; Hu, W. A Key Space Enhanced Chaotic Encryption Scheme for Physical Layer Security in OFDM-PON. *IEEE Photonics J.* **2017**, *9*, 1–10. [CrossRef]
14. Cui, M.; Chen, Y.; Zhang, C.; Liang, X.; Wu, T.; Liu, S.; Wen, H.; Qiu, K. Chaotic RNA and DNA for Security OFDM-WDM-PON and Dynamic Key Agreement. *Opt. Express* **2021**, *29*, 25552. [CrossRef] [PubMed]
15. Zhang, W.; Zhang, C.; Chen, C.; Zhang, H.; Qiu, K. Brownian Motion Encryption for Physical-Layer Security Improvement in CO-OFDM-PON. *IEEE Photonics Technol. Lett.* **2017**, *29*, 1023–1026. [CrossRef]
16. Hu, Z.; Chan, C.-K. A 7-D Hyperchaotic System-Based Encryption Scheme for Secure Fast-OFDM-PON. *J. Light. Technol.* **2018**, *36*, 3373–3381. [CrossRef]
17. Wu, T.; Zhang, C.; Chen, Y.; Cui, M.; Huang, H.; Zhang, Z.; Wen, H.; Zhao, X.; Qiu, K. Compressive Sensing Chaotic Encryption Algorithms for OFDM-PON Data Transmission. *Opt. Express* **2021**, *29*, 3669. [CrossRef]
18. Zhong, Q.; Guo, Z.; Liu, B.; Ren, J.; Mao, Y.; Wu, X.; Wu, Y.; Zhao, L.; Sun, T.; Ullah, R. Block Compressive Sensing Chaotic Embedded Encryption for MCF-OFDM Transmission System. *Opt. Express* **2022**, *30*, 21774. [CrossRef]
19. Hua, Z.; Jin, F.; Xu, B.; Huang, H. 2D Logistic-Sine-Coupling Map for Image Encryption. *Signal Process.* **2018**, *149*, 148–161. [CrossRef]
20. Rauhut, H.; Romberg, J.; Tropp, J.A. Restricted Isometries for Partial Random Circulant Matrices. *Appl. Comput. Harmon. Anal.* **2012**, *32*, 242–254. [CrossRef]
21. Qaisar, S.; Bilal, R.M.; Iqbal, W.; Naureen, M.; Lee, S. Compressive Sensing: From Theory to Applications, a Survey. *J. Commun. Netw.* **2013**, *15*, 443–456. [CrossRef]
22. Mohimani, H.; Babaie-Zadeh, M.; Jutten, C. A Fast Approach for Overcomplete Sparse Decomposition Based on Smoothed l^0 Norm. *IEEE Trans. Signal Process.* **2009**, *57*, 289–301. [CrossRef]
23. Sari, H.; Moridi, S. New Phase and Frequency Detectors for Carrier Recovery in PSK and QAM Systems. *IEEE Trans. Commun.* **1988**, *36*, 1035–1043. [CrossRef]
24. Belfiore, C.A.; Park, J.H. Decision Feedback Equalization. *Proc. IEEE* **1979**, *67*, 1143–1156. [CrossRef]
25. Takiguchi, K. 40 Gsymbol/s Channel-Based Nyquist Wavelength Division Multiplexing Communication in a Terahertz-Band Using Optical-Domain Reception Signal Processing. *OSA Contin.* **2020**, *3*, 2308. [CrossRef]
26. Azarnia, G.; Sharifi, A.A.; Emami, H. Compressive Sensing Based PAPR Reduction in OFDM Systems: Modified Orthogonal Matching Pursuit Approach. *ICT Express* **2020**, *6*, 368–371. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.