Hindawi
Mobile Information Systems
Volume 2022, Article ID 4364706, 12 pages
https://doi.org/10.1155/2022/4364706

Research Article

Performance Enhancement of Bit-Level XOR Compressed Image OFDM Transmission Systems

Linlin Xue, Jianhong Lv, and Zhongpeng Wang

School of Information and Electronic Engineering, Zhejiang University of Science and Technology, Hangzhou 310023, China

Correspondence should be addressed to Zhongpeng Wang; wzp1966@sohu.com

Received 23 April 2022; Revised 23 July 2022; Accepted 30 July 2022; Published 27 August 2022

Academic Editor: Jose M. Barcelo-Ordinas

Copyright © 2022 Linlin Xue et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The bit error rate (BER) formula of the M-QAM system is derived under nonequally likely condition of the constellation points, from which improving the BER performance of the M-QAM system by optimizing the probability distribution of constellation points is identified. Based on the analysis, the bit-level XOR method is employed to encrypt the image data and modify the probability distribution of the constellation points. The simulation results show that bit-level XOR is helpful to obtain a better probability distribution of the 16-QAM system compared to that without bit XOR and hence can improve the BER performance of the proposed OFDM transmission system. Simulation results based on test images over the AWGN channel further confirm that the reliability of the OFDM transmission system and the reconstructed quality of the compressed image are both significantly enhanced using bit-level XOR operation.

1. Introduction

With the development of Internet of Things, increasing multimedia sources, such as video, image, and audio, need to be transmitted over wireless networks. Image data is one of the main multimedia sources. However, the unprocessed image data is usually very large. Hence, efficient compression of image data is necessary to reduce the storage space for transmission. Compressive sensing (CS) theory states that if a signal with a size of N is K-sparse ($K << N$) or compressible, it can be sampled below the Nyquist rate at the transmission side, while it can be exactly reconstructed with these samples of the signal at the receiver side [1]. CS technology has been widely applied in image compression, image encryption, and image wireless transmission [2, 3]. However, compared with the conventional compression method, such as JPEG and JPEG2000, image-based CS still has a significant gap in reconstruction quality [4]. How to improve the reconstruction quality of image is still an important issue in the field of image CS. Although some schemes have been proposed to improve the reconstruction quality for image CS framework [5–7], improving the CS performance by optimizing the property of modulated signal, which is transformed from the compressed image data, has been rarely studied, as far as we know. In this work, our goal is to improve the performance, in terms of reconstruction quality and bit error rate (BER) metrics, of the compressed image transmission system by optimizing the property of modulated signal using bit-level XOR operation, which can encrypt the image data and ensure the security of the system at the same time.

1.1. Related Works. In image wireless communication systems, the resulting data generated from image CS needs to be quantized and transformed into a bit stream and then mapped into digital modulation symbols in order to be transmitted over wireless channels. Orthogonal-frequency-division multiplexing (OFDM) is a physical layer transmission technique that is able to provide high data rates over multipath fading channels. There are many image transmission schemes for OFDM communication systems [8–12]. In [10], the authors studied the compressed image OFDM transmission based on the well-known EZW or SPIHT algorithms. Then to reduce the computational complexity of CS, the block compressed sensing (BCS) method was proposed [13–17]. In [15], the transmission performance of the block compressed-sensed image data over a wireless channel was researched, and the simulation results show that BCS with a proper block size can greatly reduce the computational complexity with a slight peak signal-to-noise ratio (PSNR) performance loss.

On the other hand, to protect sensitive personal information, images usually need to be encrypted before transmission. Many joint image compression-encryption algorithms have been proposed and investigated to ensure image security during transmission [18–20]. Generally, digital image encryption mainly consists of two phases: diffusion and permutation. Recently, the authors in [21] proposed double-image encryption based on convolutional neural network (CNN) and dynamic adaptive diffusion. The experiment results show the feasibility of the proposed scheme. In [22], for a range-gated laser imaging system, a joint compression and encryption scheme is proposed, in which the measurement matrix is constructed by the quantum cellular neural network (QCNN) hyperchaotic system. The simulation results show that the proposed scheme can achieve secure transmission of image data. In [22] and most other image encryption schemes, the key used is usually generated from chaotic systems. However, chaotic systems, especially high-dimensional chaotic systems, have the disadvantage of slow calculation speed. To solve this issue, the authors in [23] combined Least Squares Generative Adversarial Networks (LSGAN) with the chaotic system to produce a high-quality random number.

In addition, bit-level XOR operation is another commonly used image encrypted method [24–27], which has been extensively employed to further enhance the security of image encryption. Meanwhile, in recent years, the physical layer security approach has attracted widespread attention. Bit-level XOR operation is also used to enhance the security of the physical layer in wireless communication systems [28, 29]. However, in the above-mentioned image encryption schemes, the reliability performance of encrypted image over wireless communication system has seldom been considered. The effect of bit-level XOR operation on the reliability performance in a compressed image transmission system also has not been researched.

Recently, probabilistic shaping (PS), especially probabilistic amplitude shaping (PAS), has been used to improve the transmission reliability of optical communications [30, 31]. In the PS scheme, the constellation points with equidistant space are assigned different probabilities. In [32], the authors researched the reliability of the transmission of PS-based wireless communication systems over Rayleigh fading channels. In [33], PS enabled by precoding technique is used in a low-cost IM-DD system for optical access networks. These studied results all show that the transmission performance of the communication system can be optimized by PS. Inspired by the PS idea, we utilize bit-level XOR operation to encrypt the transmission data as well as optimize the probability distribution of the constellation points in order to improve both the security and reliability of the compressed image OFDM system.

1.2. Motivation and Contribution. In digital communication systems, the compressed image data is transformed into bit stream and then mapped into digital modulation signals, such as BPSK, QPSK, and M-QAM. In this work, bit-level XOR operation is employed on the bit stream, which is then mapped into square 16-QAM symbols. Generally, researchers mainly focus on the security of using bit-level XOR operation but rarely consider the impact of bit-level XOR operation on the transmission performance of the compressed image.

In fact, because of the bit-level XOR operation, the probability distribution of the constellation points is different from that without bit-level XOR. Moreover, through the simulation, we find that the probability distribution with bit-level XOR is better compared with that without bit-level XOR, which is beneficial to improving the performance of the OFDM communication system. We will study the effect of bit-level XOR on the BER and PSNR performances of a compressed image OFDM transmission system and aim to propose a method to improve the security and reliability of the compressed image OFDM system at the same time. The main contributions of this work are as follows:

(1) The mathematical model of an M-QAM system under nonequal probability distributions of constellation points was developed, based on which the BER formula of an M-QAM system was derived. The theoretical analysis shows that optimizing the distribution of the constellation points can improve the BER performance of the compressed image transmission system.

(2) Bit-level XOR operation was used to encrypt the bit stream generated from the BCS; meanwhile, this operation changes the probability distribution of constellation points of an M-QAM system. Through the simulation, we find that when bit XOR is employed, the probabilities of constellation points close to the origin are increased while the probabilities of the ones far away from the origin are decreased; this will lead to a reduction of the average transmit power. For the given transmit power, the reduction of average transmit power will increase the scaling factor and reduce the influence of noise on the whole constellation points. Hence, the transmission performance of the communication system will thus be improved.

(3) Simulations are carried out for the proposed compressed image OFDM system, and the results show that the BER performance and the image reconstructed quality of the OFDM system are significantly improved by using bit-level XOR operation when compared with that without bit-level XOR operation.

2. The Proposed System Principles

In this section, the BCS scheme [17] based on sparse discrete cosine transform (DCT) matrix with a partial DCT measurement matrix is introduced, and then an end-to-end compressed image transmission scheme is presented.

2.1. BCS Preliminaries. In BCS, the image with a size of $N \times N$ is divided into a number of nonoverlapping blocks with a size of $N_B \times N_B$, and the number of subblocks is $(N/N_B) \times (N/N_B)$.

Let x_i^j with a size of $N_B \times 1$ denote the i-th column of the j-th block image. An image signal is usually sparse in some sparse bases, such as discrete wavelet transform (DWT) and DCT; the original signal x_i^j can be transformed into a sparse signal s_i^j by using a sparse matrix Ψ_B with a size of $N_B \times N_B$. The transformation can be expressed as

$$x_i^j = \Psi_B s_i^j. \tag{1}$$

Then the measurement process of BCS can be expressed as [34]

$$\begin{aligned} y_i^j &= \Phi_B \Psi_B s_i^j \\ &= A s_i^j, \end{aligned} \tag{2}$$

where $i = 1, 2, \ldots, N_B$, Φ_B, is the measurement matrix with a size of $M_B \times N_B$, and the matrix $A = \Phi_B \Psi_B$ with a size of $M_B \times N_B$ is called the sensing matrix. After all block images are measured, the obtained compressed data vectors form a matrix Y with a size of $M_B \times N_B$, which can be expressed as

$$Y = \begin{bmatrix} y_1 & y_2 & \cdots & y_{N_B} \end{bmatrix}. \tag{3}$$

In the receiver side, the sparse signal s_i^j can be recovered by solving the following optimization problem:

$$\hat{s}_i^j = \begin{cases} \min\limits_{s_i^j \in R^N} & \left\| s_i^j \right\|_1 \\ \text{subject.to.} & y_i = \Phi_B x_i^j = \Phi_B \Psi_B s_i^j, \end{cases} \tag{4}$$

where $i = 1, \ldots N$

With the recovered sparse signal, the i-th column of the j-th block image can be reconstructed via $\hat{x}_i^j = \Psi_B \hat{s}_i^j$. Thus, the entire j-th block image data can be formed as $X^j = \begin{bmatrix} \hat{x}_1^j & \hat{x}_2^j & \cdots & \hat{x}_{N_B}^j \end{bmatrix}$. After all block images are reconstructed, the whole original image can in turn be recovered. There are many reconstructed algorithms that can be used to solve (4); in this work, the orthogonal matching pursuit (OMP) [35] is employed. Additionally, in this work, the conventional DCT matrix with a size of $N_B \times N_B$ is used as the sparse basis matrix Ψ_B, and the partial DCT matrix with a size of $M_B \times N_B$ is used as the measurement matrix Φ_B, which will be introduced in the following.

2.2. Partial DCT Measurement Matrix. Similar to [17], a partial chaotic DCT matrix is utilized to serve as the measurement matrix in the BCS scheme. A conventional DCT matrix can be expressed as

$$F_{N \times N} = \left[f_{i,j} \right]_{N \times N}, \tag{5}$$

where $F(i)$ denotes the i-row vector of the matrix; $f_{i,j}$ denotes the i-row and j-column element of the matrix $F_{N \times N}$ and is defined as

$$f_{i,j} = \beta(k) \cos\left(\frac{\pi k (2n+1)}{2N} \right), \quad 0 < n,\ k < N-1, \tag{6}$$

where $\beta(k)$ is defined as

$$\beta(k) = \begin{cases} \dfrac{1}{\sqrt{2}}, & k = 0, \\ 1, & k = 1, 2, \ldots, N-1. \end{cases} \tag{7}$$

The partial DCT measurement matrix is obtained by randomly selecting M rows from the conventional DCT matrix $F_{N \times N}$, and the detailed process is as follows.

First, a Logistic map is employed to generate the key sequence and scramble the conventional DCT matrix. The Logistic map is defined as follows [36]:

$$x_{n+1} = \mu x_n (1 - x_n), \tag{8}$$

where $3.569945627 < \mu \le 4$ is the control parameter and $x_n \in [0, 1]$. Based on (8), an integer vector $a = \begin{bmatrix} a(1) & a(2) & \ldots & a(B) \end{bmatrix}$ can be obtained according to the following formula:

$$a(n) = \left(\operatorname{mod}\left(\operatorname{floor}(x_n + 100) \times 10^{10} \right), N \right) + 1, \tag{9}$$

where $\operatorname{floor}(x)$ returns the values of x to the nearest integers less than or equal to x and $\operatorname{mod}(z, N)$ returns the remainder of z divided by N.

Then a row scrambling operation is done to the matrix F using the chaotic vector a, and the obtained scrambled DCT matrix can be expressed as

$$\hat{F}_{N \times N} = \begin{bmatrix} F(a(1)) & F(a(2)) & \cdots & F(a(N)) \end{bmatrix}^T. \tag{10}$$

Finally, the former M $(M < N)$ rows of the matrix $\hat{F}_{N \times N}$ are reserved to form a new matrix, which is used to serve as the partial DCT measurement matrix. It can be expressed as

$$\Phi = \hat{F}_{M \times N} = \begin{bmatrix} F(a(1)) & F(a(2)) & \cdots & F(a(M)) \end{bmatrix}^T. \tag{11}$$

Based on the above method, we can obtain a measurement matrix Φ_B with a size of $M_B \times N_B$ for the BCS framework.

2.3. Compressed Image OFDM Transmission System. Figure 1 shows the compressed image OFDM transmission system. The main steps of signal processing in the transmitter are summarized as follows:

Step 1. Block image compressed sampling: an image is divided into many nonoverlapping blocks with a size of $N_B \times N_B$. Each block is processed according to (2) using the same sparse DCT matrix Ψ_B and partial DCT measurement matrix Φ_B.

Step 2. The compressed image data is quantized and transformed into a bit stream. The quantifying operation is according to the following formula:

$$P_{i,j} = \operatorname{floor}\left(\frac{255 \times \left(P_{i,j} - \min \right)}{(\max - \min)} \right), \tag{12}$$

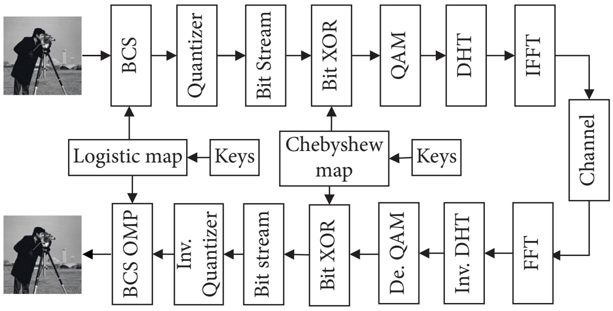


FIGURE 1: The compressed image OFDM transmission system.

where max and min denote the maximum value and minimum value of the measurement data matrix and $P_{i,j}$ represents the i-row and j-column element of the matrix.

Step 3. Bit-level XOR encryption: let $m = [m_0,\ m_1\ \cdots,\ m_K]$, $k = [k_0,\ k_1\ \cdots,\ k_K]$, and $c = [c_0,\ c_1\ \cdots,\ c_K]$ be the information bit steam, the key bit stream, and the encrypted bit stream, respectively, and then the bit-level XOR encryption can be expressed as

$$c = m \oplus k, \tag{13}$$

where $\oplus$ denotes the XOR operation. In this work, we employ the Chebyshev map [37] to generate the key bit stream k.

Step 4. Precoding operation: the encrypted bit stream is mapped into a square 16-QAM symbol stream and forms a symbol vector $S = [S(1)\ \ S(2)\ \ \ldots\ \ S(N_{\text{data}})]$. Then, the 16-QAM symbol vector is precoded by a Discrete Hartley transform (DHT) precoding matrix P according to reference [38], and the resulting precoded signal vector can be expressed as $X = PS$.

Step 5. IFFT operation: the precoded signal is processed by an IFFT unit to produce a time domain OFDM signal.

In the receiver side, the corresponding inverse operations, such as FFT, inverse DHT precoding, and inverse quantization, are employed. Finally, the original image is recovered by OMP (orthogonal matching pursuit) reconstructed algorithm.

3. Error Probability Analysis

3.1. Error Probability Analysis under Equally Likely Condition. In general, the theoretical error probability formula of an M-QAM communication system is obtained by assuming that the transmitted M-QAM symbols are equally likely and the additive noise n follows the Gaussian probability distribution function; that is, $p(x) = (1/\sqrt{2\pi\sigma^2})e^{-(x-\mu)^2/2\sigma^2}$ with $\mu = 0$ and $\sigma^2 = (N_0/2)$. In this case, the symbol error rate (SER) P_e for the M-QAM system can be written as follows [39]:

$$P_e = \frac{4(\sqrt{M}-1)}{\sqrt{M}} Q\left(\sqrt{\frac{3E_s}{(M-1)N_0}}\right). \tag{14}$$

When the 16-QAM modulation format is used, M is equal to 16.

Figure 2 shows the square 16-QAM signal constellation under Gray's rule. Let the points along the I axis be $\{-3d,\ -d,\ d\ \ 3d\}$ and the points along the Q axis be the same, and then each constellation point can be expressed as $s_i = s_i^I + js_i^Q$, where $s_i^I, s_i^Q \in \{-3d,\ -d,\ d\ \ 3d\}$. In this case, the 16-QAM alphabet can be expressed as $\Gamma = \{\pm d \pm jd,\ \pm d \pm j3d,\ \pm 3d \pm jd,\ \pm 3d \pm j3d\}$, where $d = \sqrt{E_s/10}$. When the constellation points have equal probability, the average energy/symbol of the 16-QAM constellation is given by

$$\begin{aligned} E_s &= \frac{1}{16}\sum_{i=0}^{M-1} \left\|s_i\right\|^2 \\ &= \sum_{i=1}^{16} d^2 \times \left(\left(s_i^I\right)^2 + \left(s_i^Q\right)^2\right) \\ &= 10d^2. \end{aligned} \tag{15}$$

Inserting (15) into (14), the SER of 16-QAM under equally likely condition can further be expressed as

$$P_e = \frac{4(\sqrt{M}-1)}{\sqrt{M}} Q\left(\sqrt{\frac{3\times 10d^2}{(M-1)N_0}}\right). \tag{16}$$

3.2. Error Probability Analysis under Nonequally Likely Condition. Recently, the researched results for PS [32, 33] show that the reliable performance of M-QAM systems can be improved by assigning different probabilities to the M-QAM constellation points. In this case, the probability distribution of M-QAM constellation points becomes nonequally likely. The SER of the 16-QAM system under a nonequally likely condition can be derived by using a similar method to that of an equally likely condition.

From Figure 2, it can be seen that the probability of error of 16-QAM constellation points can be divided into three cases [40]: first, four points that are inside (◇), with each point having four nearest neighbors; second, four points that are in the corner (Δ), with each point having two nearest neighbors; third, four points that are not inside or in the corner (O), with each point having three nearest neighbors.

For the first case (s_5, s_7, s_{13}, and s_{15}), the probability of error of each point can be expressed as

$$\begin{aligned} P_e(s_i) &= P_y\left(\frac{n \ge d}{2}\right) + P_x\left(\frac{n \ge d}{n \ge d}\right) \\ &\quad - P_x\left(\frac{n \ge d}{2}\right) \times P_y\left(\frac{n \ge d}{2}\right) \\ &= 2Q\left(\frac{d}{2\sigma}\right) - Q^2\left(\frac{d}{2\sigma}\right). \end{aligned} \tag{17}$$

For the second case (s_0, s_2, s_8, and s_{10}), the probability of error of each point can be expressed as

$$
\begin{aligned}
P_e(s_i) &= 2P_y\left(\frac{n \geq d}{2}\right) + P_x\left(\frac{n \geq d}{2}\right) \\
&\quad - 2P_x\left(\frac{n \geq d}{2}\right) \times P_y\left(\frac{n \geq d}{2}\right) \\
&= 3Q\left(\frac{d}{2\sigma}\right) - 2Q^2\left(\frac{d}{2\sigma}\right).
\end{aligned}
\tag{18}
$$

For the third case (s_1, s_3, s_4, s_6, s_9, s_{11}, s_{12}, and s_{14}), the probability of error of each point can be expressed as

$$
\begin{aligned}
P_e(s_i) &= 2P_y\left(\frac{n \geq d}{2}\right) + 2P_x\left(\frac{n \geq d}{2}\right) \\
&\quad - 4P_x\left(\frac{n \geq d}{2}\right) \times P_y\left(\frac{n \geq d}{2}\right) \\
&= 4Q\left(\frac{d}{2\sigma}\right) - 4Q^2\left(\frac{d}{2\sigma}\right).
\end{aligned}
\tag{19}
$$

Therefore, the theoretical SER of the nonequally likely 16-QAM system can be expressed as

$$
P_e = \sum_{i=o}^{M-1} P_e(s_i) \times p(s_i), \tag{20}
$$

where $p(s_i)$ denotes the occurrence probability of the transmitted symbol s_i. Based on (20), it can be seen that SER is related to the probability distribution of constellation points $p(s_i)$. When $p(s_i)$ is given, the SER of a 16-QAM system can be calculated according to (20).

On the other hand, the average energy/symbol of the 16-QAM constellation E_s under nonequally likely condition can be obtained by

$$
E_s = \sum_{i=0}^{M-1} \left\| s_i \right\|^2 p(s_i). \tag{21}
$$

From (21), we can see that the average energy/symbol of the 16-QAM constellation is also related to the probability distribution of constellation points $p(s_i)$.

3.3. Effect of Bit-Level XOR on SER of the Proposed System.

Bit-level XOR has been employed to achieve secure CS and enhance the security of the physical layer signals. However, the effect of bit-level XOR on the SER of the compressed image transmission has seldom been studied. In this work, the key generated from the Chebyshev map is used for the bit-level XOR operation. The Chebyshev map is defined as follows [37]:

$$
y_{n+1} = \cos(w\mathrm{arccos}\, y_n), \tag{22}
$$

where $w \geq 20$ is the control parameter and $y_n \in [-1, 1]$. Based on (22), a key bit stream $k = [\, k_0,\ k_1\ \cdots,\ k_K \,]$ can be generated according to the following formula:

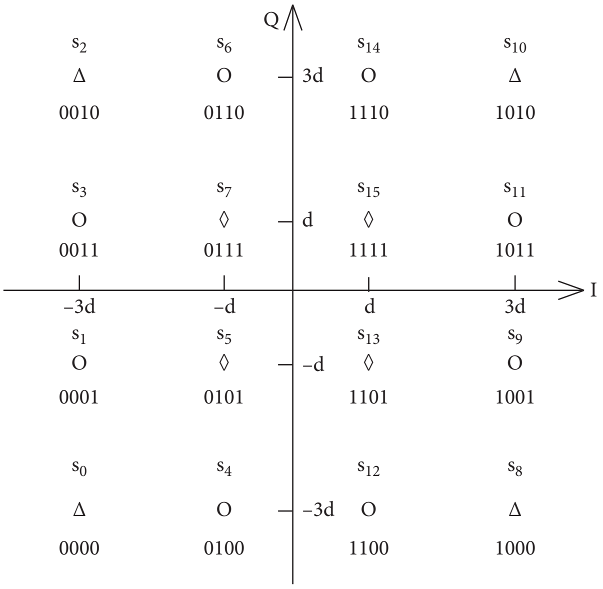


Figure 2: 16-QAM constellations with Gray's rule.

$$
k_n = \begin{cases} 1, & y_n \geq 0, \\ 0, & y_n \leq 0. \end{cases} \tag{23}
$$

The resulting key stream is used to encrypt the information bit stream generated from the image CS by using a bit-level XOR operation.

In our simulation experiment, a test image with a size of 256 × 256 is firstly compressively sampled with a compressive ratio of 0.75, and the generated data is transformed into information bit stream. Then per K-bit information bits are grouped to form a bit vector $m = [\, m_0,\ m_1\ \cdots,\ m_K \,]$. The length of the key stream and the length of information bit vector are both fixed at 2048. Next, each information bit vector is encrypted to form an encrypted bit vector c according to the bit-level XOR operation of (13). Finally, the encrypted bit stream c is transformed into a 16-QAM symbol stream according to the 16-QAM constellations with Gray's rule.

In the following, we will investigate the effect of bit-level XOR on the SER of 16-QAM communication systems for different compressed image data. Four test images with a size of 256 × 256, as shown in Figure 3, are used to generate the compressed image data.

First, the probability distributions of the 16-QAM constellation points for different compressed image data with and without bit-level XOR are obtained, as shown in Table 1, where "w/" denotes "with bit-level XOR operation" and "w/o" denotes "without bit-level XOR operation." It can be seen that the probability distribution of the 16-QAM symbols directly generated from the compressed image is nonequally likely. When bit-level XOR is employed to the image data, the probability of each 16-QAM symbol further changes, leading to a new probability distribution.

To intuitively show the change of the probability distribution when bit-level XOR operation is applied, Figures 4 and 5 give the probability distributions of the 16-QAM

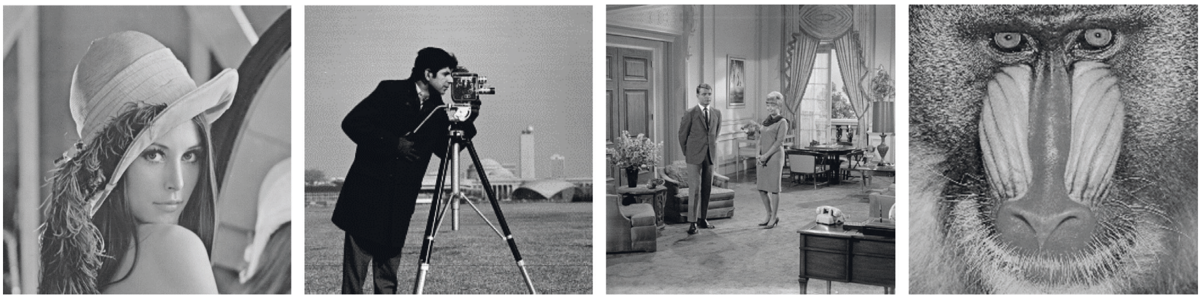


Figure 3: Four test images used in the simulations. "Lena," "Cameraman," "Couple," and "Mandrill" (from left to right).

Table 1: Probability distribution of the 16-QAM constellation points for images with and without bit XOR operation.

Image P (si)	Lena		Cameraman		Couple		Mandrill	
	w/o	w/	w/o	w/	w/o	w/	w/o	w/
P (s_0)	0.4752	0.1832	0.5505	0.1922	0.5205	0.1803	0.4358	0.1737
P (s_1)	0.0551	0.021	0.0368	0.0154	0.0491	0.0215	0.0603	0.0252
P (s_2)	0.0494	0.0154	0.0381	0.0148	0.0328	0.0133	0.0391	0.0141
P (s_3)	0.0247	0.0208	0.0138	0.0171	0.0233	0.0215	0.0289	0.0294
P (s_4)	0.0383	0.0123	0.0432	0.0145	0.0281	0.0112	0.0393	0.0147
P (s_5)	0.0085	0.0092	0.0064	0.0074	0.0077	0.0083	0.0134	0.0141
P (s_6)	0.0179	0.0061	0.0125	0.0049	0.0135	0.0054	0.0187	0.0084
P (s_7)	0.0198	0.0511	0.0115	0.0286	0.0189	0.0446	0.0242	0.0606
P (s_8)	0.0483	0.0185	0.0258	0.0100	0.0448	0.0195	0.0610	0.0250
P (s_9)	0.0058	0.0172	0.0046	0.0118	0.0051	0.0128	0.0080	0.0180
P (s_{10})	0.0086	0.0081	0.0070	0.0060	0.0087	0.0082	0.0143	0.0139
P (s_{11})	0.0118	0.0370	0.0141	0.0420	0.0109	0.0276	0.0144	0.0388
P (s_{12})	0.0195	0.0242	0.0159	0.0134	0.0221	0.0245	0.0300	0.0301
P (s_{13})	0.0150	0.0488	0.0144	0.0377	0.0127	0.0315	0.0136	0.0379
P (s_{14})	0.0203	0.0548	0.0148	0.0365	0.0228	0.0521	0.0265	0.0632
P (s_{15})	0.1819	0.4724	0.1907	0.5476	0.1791	0.5175	0.1725	0.4329

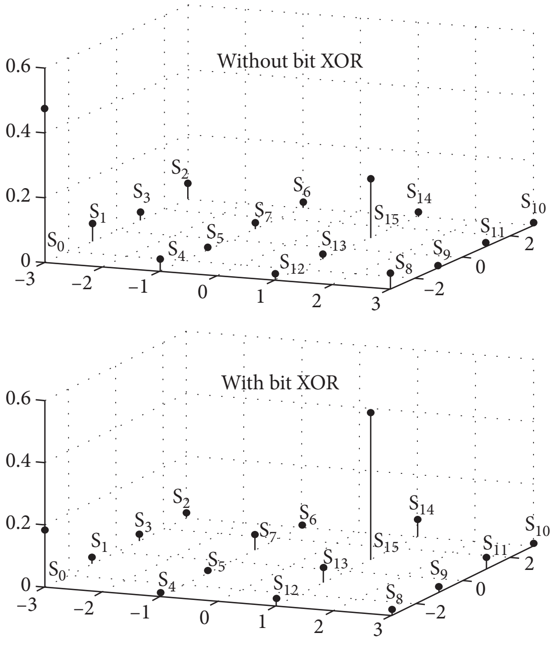


Figure 4: The probability distribution of the 16-QAM constellation for Lena image.

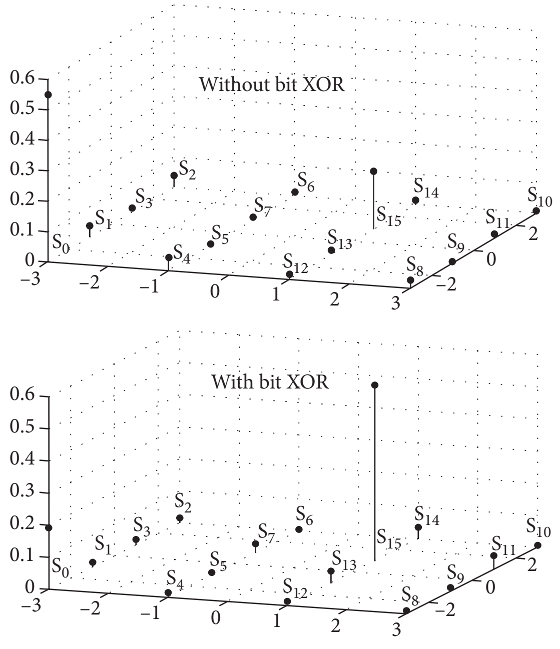


Figure 5: The probability distribution of the 16-QAM constellation for Cameraman image.

constellation points for “Lena” image and “Cameraman” image, respectively. The probability distribution figures for the two images are similar. From Figures 4 and 5, we can see that, compared with the case without bit XOR operation, the probability of low energy symbols with bit-level XOR operation is significantly increased; this will lead to a reduction of the average signal power according to (21). This means that, under the same transmit power, the Euclidean distance between constellation points will increase, and the effect of noise on the whole constellation points will thus be reduced. As a result, the BER performance of the compressed image OFDM system with bit XOR can be improved compared with that of the system without bit XOR.

Based on the probability distributions of 16-QAM constellation points, the BER performance curves of the 16-QAM transmission system for compressed “Lean” and “Cameraman” with and without bit XOR are obtained according to (16) and (20), as shown in Figure 6. The theoretical BER curve and the BER curve for random bits are also given in Figure 6 for comparison.

From Figure 6, we can see that the compressed image transmission with bit XOR provides a 2.3 dB SNR gain to that without bit XOR at BER of 10^{-3} level. In addition, the BER of the 16-QAM system for random bits is the same as the theoretical BER, as the probability distribution for random bits is nearly equally likely. Most important, the BER performance of the 16-QAM for compressed images with bit-level XOR is better than the theoretical BER of the 16-QAM system.

Therefore, besides the improvement in security, the bit-level XOR operation is also helpful to optimize the probability distribution of the 16-QAM system. This will in turn improve the BER performance and the reconstructed quality of the proposed compressed image OFDM transmission system, which will be confirmed by the following simulation experiments.

4. Simulations and Results Analysis

In this section, BER and PSNR performances are studied for the proposed OFDM system. For concise display of the simulated curves, only “Lean” image and “Cameraman” image with a size of 256 × 256 are used in the simulation; nevertheless, similar results are obtained for other images, such as “Couple” and “Mandrill.” The main system parameters used in the simulation are given in Table 2. “Lean” images and “Cameraman” image are first compressively sampled and then transmitted over the Addition Gaussian White Noise (AWGN) channel. The size of each block image is 16 × 16.

4.1. Comparison of BER and PSNR Performances. The PSNR is usually employed to evaluate the quality of the reconstructed image in the CS framework and is defined as

$$\text{PSNR} = 10 \cdot \log_{10}\left(\frac{M_1 \times N_1 \times 255^2}{\text{MSE}}\right), \tag{24}$$

where the mean square error (MSE) is defined as

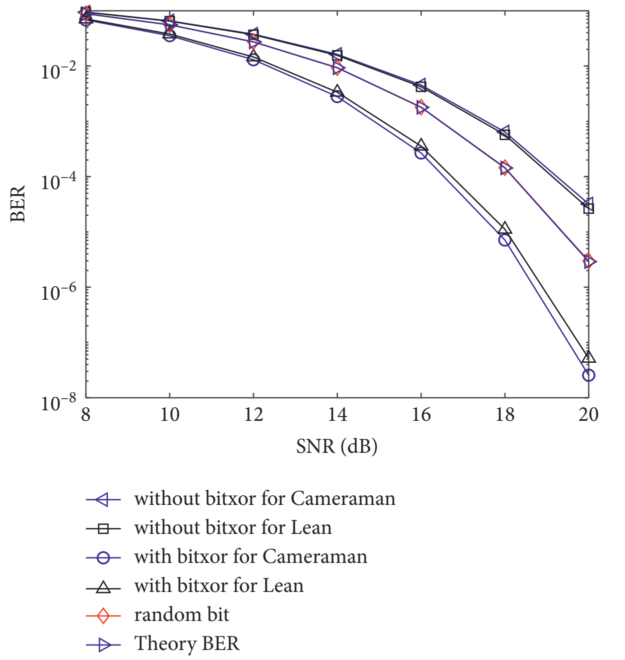


Figure 6: BER performance of a 16-QAM system for different probability distributions of constellation points.

Table 2: System parameters used in the simulation.

Modulation	16-QAM
Number of subcarriers	256
Length of cyclic prefix	32
Number of data subcarriers	192
Number of pilot symbols	8
Channel	AWGN
Logistic map, x_0 and μ	$0.33 + 10^{-15}$, 4
Chebyshev map, x_0 and w	$0.33 + 10^{-15}$, 20
Subblock size	16 × 16

$$\text{MSE} = \frac{1}{M_1 \times N_1} \sum_{i=0}^{M_1-1} \sum_{j=0}^{N_1-1} \left(P(i,j) - Q(i,j)\right)^2, \tag{25}$$

where M_1 and N_1 are the numbers of pixels of horizontal and vertical coordinates of the image, respectively; $P(i,j)$ and $Q(i,j)$ represent the gray matrices of the original image and the reconstructed image, respectively.

In the simulation experiments, the original image is processed by BCS based on DCT sparse matrix and chaotic partial DHT measurement matrix. After BCS, the resulting data is quantized and transformed into a bit stream. In the signal transmission phase, the DHT precoding method is used to reduce the PAPR of the OFDM signal. In the simulation, a slight level of clipping is used, and the clipping ratio λ, which is defined as (26), is set to be 12.

$$\lambda = \frac{A^2}{P_{av}}, \tag{26}$$

where A^2 represents the predefined peak power threshold and P_{av} represents the average power of the signal before clipping.

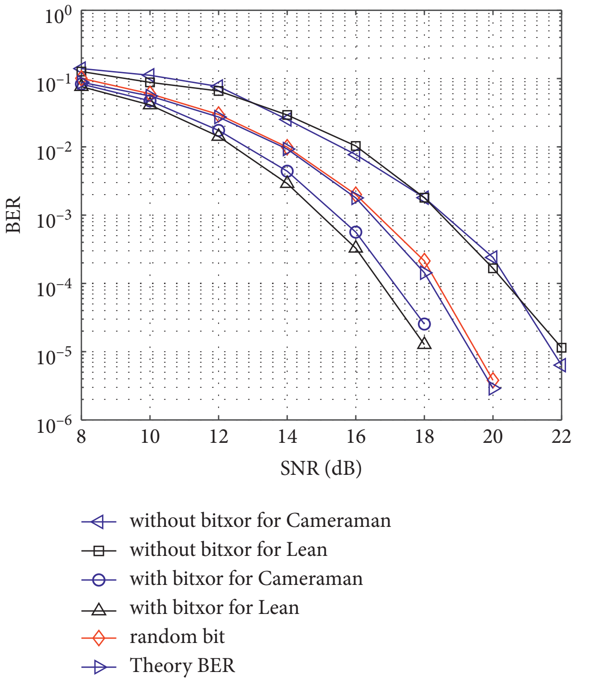


Figure 7: BER performance of the compressed images in the proposed system over the AWGN channel.

Figure 7 shows the BER performance of the compressed images over AWGN channels, where a 16-QAM modulation format is used. The compressive ratio is fixed at 0.75. It can be seen that bit-level XOR can improve the BER performance of the proposed DHT precoded OFDM system in AWGN channels. At BER = 10^{-3} case, the bit-level XOR in the proposed system can obtain approximately 3.5 dB gain when compared to that without bit-level XOR. In addition, the performance enhancement of the compressed "Lena" image is more significant compared with that of the compressed "Cameraman" image.

Figure 8 shows the PSNR performance of the compressed images in the proposed system over the AWGN channel. It can be seen that bit-level XOR can improve the reconstructed quality of the image transmitted in the proposed compressed image transmission system. When SNR is smaller than 18 dB, using bit XOR in the proposed system can obtain a 10 dB gain when compared to that of the case without bit XOR for "Cameraman" image. When SNR is higher than 18 dB, the gain obtained by using the bit XOR becomes small. For "Lena" image, when SNR is higher than 12 dB, the PSNR performance with bit-level XOR is better than that without bit XOR, and at SNR = 18 dB, the bit XOR method can obtain a 5 dB PSNR gain. Similar to the "Cameraman" test image, when SNR is higher than 18 dB, the gains obtained by using bit-level XOR become small.

Figure 9 depicts the relationship between the PSNR and the compression ratio in the proposed OFDM system with an SNR of 18 dB. For "Lena" image, using bit XOR can obtain about 3 dB gain at a compressive ratio of 0.5. For "Cameraman" image, using bit XOR can obtain about 4 dB gain at a compressive ratio of 0.7. Therefore, the bit XOR used in the proposed precoded OFDM transmission system can improve both the BER and PSNR performances over the AWGN channel.

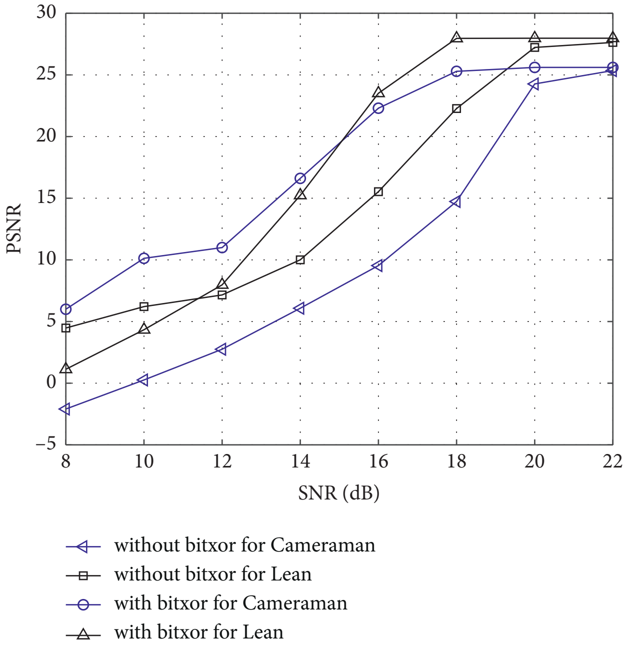


Figure 8: PSNR performance of the compressed images in the proposed system over the AWGN channel.

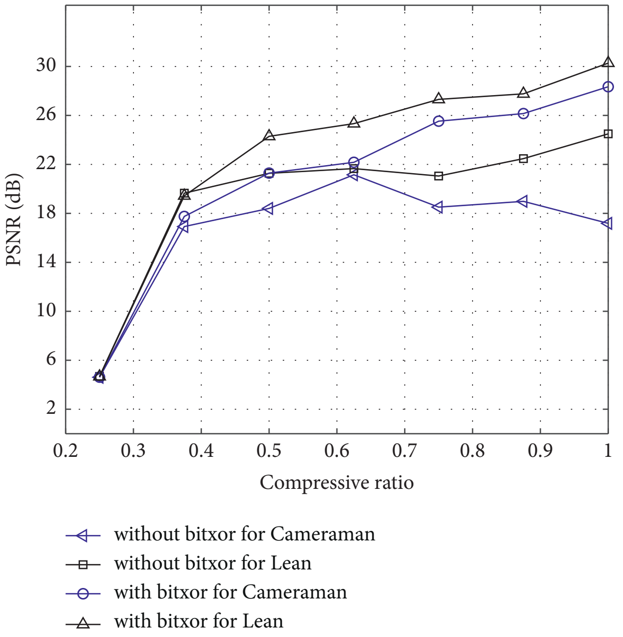
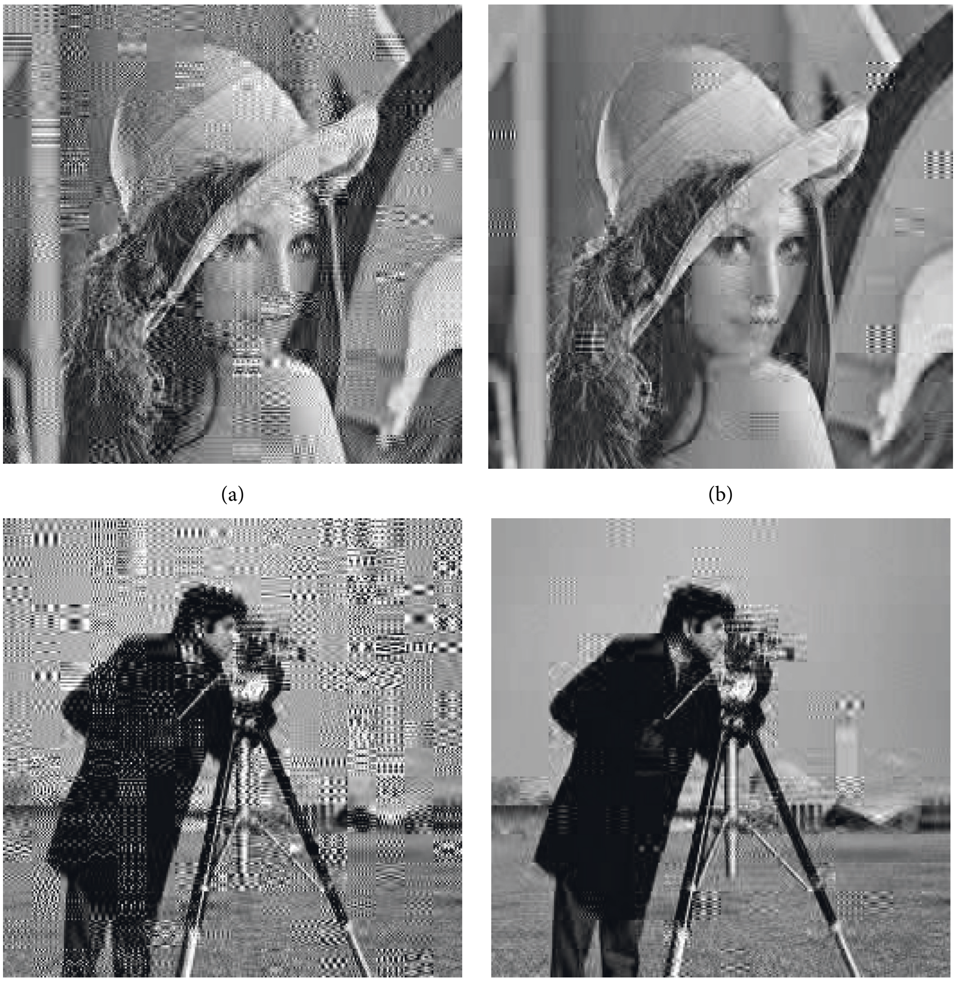


Figure 9: PSNR with a compressive ratio of the compressed images in the proposed system over the AWGN channel.

Figure 10 shows the reconstructed images of our proposed system under SNR of 17 dB and a compressive ratio of 0.75. The reconstructed quality of both images when bit XOR is used in the transmitter is much better than that without bit XOR, which further confirms the performance enhancement of using bit-level XOR operation in the compressed image OFDM transmission system.


(a)

(b)

(c)

(d)

Figure 10: Reconstructed images at SNR of 17 dB. (a) Reconstructed “Lena” image without bit XOR. (b) Reconstructed “Lena” image with bit XOR. (c) Reconstructed “Cameraman” image without bit XOR. (d) Reconstructed “Cameraman” image with bit XOR.

4.2. Influence of Block Size on System Performance. In this section, we evaluate the effect of different block sizes on the proposed system performance in terms of BER and PSNR metrics. For image-based CS, to reduce the computational complexity, the BCS scheme is usually used. The idea of BCS is that a whole image is divided into many small non-overlapping image blocks, and each image block is sampled column by column using a small measurement matrix. The results in the previous work [17] show that choosing a proper block size is helpful to improve the reconstruction performance of the image-based CS. In the following experiments, image “Lean” with a size of 256 × 256 is used to serve as the test image, and the compressive ratio is fixed at 0.75. The BER and PSNR performance of BCS is evaluated over the AWGN channel under four different block sizes, 128×128, 64×64, 32×32, and 16×16. All block images are sampled using the same measurement matrix and recovered using the same OMP algorithm.

Figure 11 shows the effect of block size on the BER performance of the proposed compressed image transmission system using bit-level XOR. It can be seen that the BER

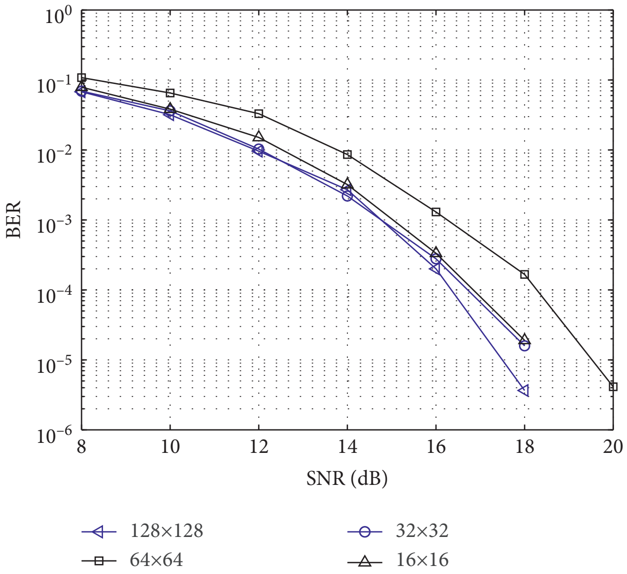


Figure 11: BER performance of the compressed image in the proposed system over the AWGN channel.

performance of BCS with a block size of 64 × 64 is the worst, while the difference in BER performance for the other three block sizes is very small, especially when SNR is less than 16 dB.

In addition, the effect of block size on PSNR performance is also evaluated under four different block sizes, as shown in Figure 12. We can see that the PSNR performance of the image BCS scheme with a block size of 64 × 64 is also the worst among the four block sizes when the SNR value is less than 20 dB, while the PSNR performance with a block size of 16 × 16 is the best.

4.3. Computational Complexity Analysis of BCS Scheme. To evaluate the computational complexity of image-based CS, both CS encoder and CS decoder need to be considered.

For the whole image CS, the original image is compressively sampled according to $y = \Phi\Psi s$. The size of the sparse basis matrix Ψ is $N \times N$, and the size of the measurement matrix Φ is $M \times N$ $(M < N)$. To obtain the sampled signal y, the required number of additions and multiplications is given by

$$\begin{aligned} T_{\text{add}} &= N^2(N-1) + M \times (N-1) \\ &= \left(N^2 + M\right)(N-1), \end{aligned} \tag{27}$$

$$T_{\text{mul}} = N^3 + M \times N. \tag{28}$$

On the other hand, for the BCS scheme, the original image is divided into a number of nonoverlapping block images with a size of $N_B \times N_B$, and the number of block images is $(N/N_B) \times (N/N_B)$. The size of the measurement matrix in BCS is $M_B \times N_B$ $(M_B < N_B)$. To finish one block image CS, the required number of additions and multiplications is given by

$$\begin{aligned} T_{B,\text{add}} &= N_B^2(N_B-1) + M_B \times (N_B-1) \\ &= \left(N_B^2 + M_B\right)(N_B-1), \\ T_{B,\text{mul}} &= N_B^3 + M_B \times N_B. \end{aligned} \tag{29}$$

Therefore, for the whole image, the required total number of additions and multiplications using BCS is given by

$$\begin{aligned} T_{\text{all},B,\text{add}} &= \frac{N^2}{N_B^2\left(\left(N_B^2 + M_B\right)(N_B-1)\right)} \\ &= N^2\left(\frac{1+M_B}{N_B^2}\right)(N_B-1), \end{aligned} \tag{30}$$

$$\begin{aligned} T_{\text{all},B,\text{mul}} &= \frac{N^2}{N_B^2\left(N_B^3 + M_B \times N_B\right)} \\ &= N^2\left(\frac{N_B + M_B}{N_B}\right). \end{aligned} \tag{31}$$

Based on the above analysis, the computational complexity for the whole image CS and block image CS can be evaluated, respectively. Take a test image with a size of 256 × 256 as an example; if we assume $N = 256$, $M = 192$, $N_B = 16$, and $M_B = 12$, the computational complexity of the whole image CS needs 16760640 additions and 16826368 multiplications according to (27) and (28). Similarly, the BCS scheme with a block size of 16 × 16 requires 1029120 additions and 1097728 multiplications according to (30) and (31). Moreover, the BCS requires less storage space than that of the whole image CS due to the small size of the sparse basis matrix and measurement matrix in the BCS scheme.

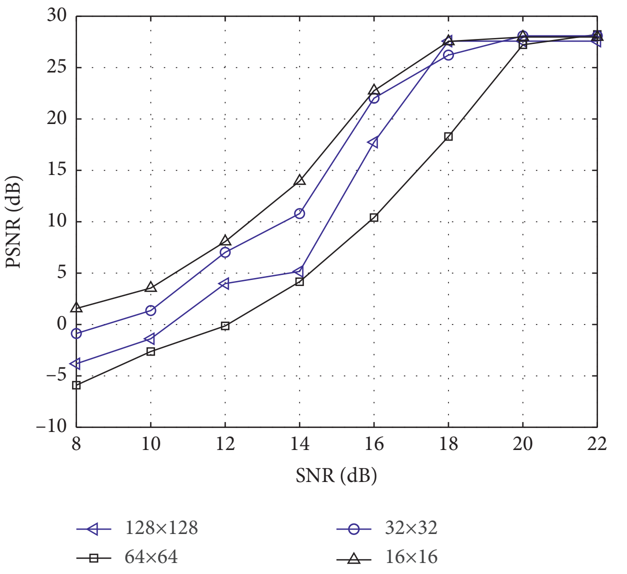


Figure 12: PSNR performance of the compressed image in the proposed system over the AWGN channel.

On the other hand, the BCS scheme can also significantly reduce the computational complexity of the CS decoder. In this work, we use the same OMP reconstruction algorithms for different block sizes of image for a fair comparison. The computational complexity of the CS decoder mainly depends on the complexity of OMP strategies. The standard OMP always runs through K iterations to finish the recovery. For the whole image CS scheme, the complexity of OMP is roughly $O(\text{KMN})$ [41,42]. Thus, for the BCS scheme, the complexity of OMP is roughly $(N^2/N_B^2) \cdot O(K_B M_B N_B)$, where $K_B << N_B$. Hence, the complexity of the decoder in the BCS scheme can be reduced compared with the whole image CS.

Therefore, to achieve high performance of BCS with low computational complexity, the block size needs to be properly selected. In our simulation case, we find that the BCS with a block size of 16 × 16 can obtain both good BER and good PSNR performance with low computational complexity. These experiment results are consistent with the previous work in [17].

5. Conclusions

In our work, the BER formula of a 16-QAM system under a nonequally likely condition is derived and analyzed, from which we can see that the BER performance of the 16-QAM system can be improved by optimizing the probability distribution of the constellation points. Based on the theoretical results, bit-level XOR operation is employed to encrypt the image data and optimize the probability distribution of the 16-QAM constellation points. The simulation shows that the bit-level XOR is helpful to obtain better probability distribution of the 16-QAM system compared with that without bit XOR and hence can improve the BER performance of the proposed OFDM transmission system. Simulations of BER and PSNR performance for test images over the AWGN channel further confirms the former theoretical analysis. In this paper, we mainly focus on the effect of bit-level XOR on the BER performance and the reconstructed quality of the compressed image in the OFDM transmission system. In the near future, we would consider how to combine bit-level XOR with other types of physical layer security to further enhance the security and reliability of compressed image transmission systems.

Data Availability

The data are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Key Laboratory of Universal Wireless Communications (BUPT), Ministry of Education China under KFKT-2020103, by the Zhejiang Provincial Key Natural Science Foundation of China under LZ21F010001, and by National Natural Science Foundation of China under 61405178.

References

[1] E. Candes and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 21–30, Mar. 2008.

[2] A. S. Unde and P. P. Deepthi, "Design and analysis of compressive sensing-based lightweight encryption scheme for multimedia IoT," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 1, pp. 167–171, 2020.

[3] Z. Chen, X. Hou, X. Qian, and C. Gong, "Efficient and robust image coding and transmission based on scrambled block compressive sensing," *IEEE Transactions on Multimedia*, vol. 20, no. 7, pp. 1–1621, 2017.

[4] Z. Chen, X. Hou, L. Shao et al., "Compressive sensing multi-layer residual coefficients for image coding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 4, pp. 1109–1120, 2020.

[5] K. Q. Dinh and B. Jeon, "Iterative weighted recovery for block-based compressive sensing of image/video at a low subrate," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 27, no. 11, pp. 2294–2308, 2017.

[6] L. Wang, X. Wu, and G. Shi, "Binned progressive quantization for compressive sensing," *IEEE Transactions on Image Processing*, vol. 21, no. 6, pp. 2980–2990, 2012.

[7] X. Song, X. Peng, J. Xu, G. Shi, and F. Wu, "Distributed compressive sensing for cloud-based wireless image transmission," *IEEE Transactions on Multimedia*, vol. 19, no. 6, pp. 1351–1364, 2017.

[8] I. Eldokany, E. S. M. El-Rabaie, S. M. Elhalafawy et al., "Efficient transmission of encrypted images with OFDM in the presence of carrier frequency offset," *Wireless Personal Communications*, vol. 84, no. 1, pp. 475–521, 2015.

[9] H. Song and K. R. Liu, "Robust progressive image transmission over OFDM systems using space-time block code," *IEEE Transactions on Multimedia*, vol. 4, no. 3, pp. 394–406, 2002.

[10] A. Bouchemel, D. Abed, and A. Moussaoui, "Enhancement of compressed image transmission in WMSNs using modified <tex-math notation=LaTeX>μ </tex-math> -nonlinear transformation," *IEEE Communications Letters*, vol. 22, no. 5, pp. 934–937, 2018.

[11] K. Dharavathu and S. A. Mosa, "Efficient transmission of an encrypted image through a MIMO-OFDM system with different encryption schemes," *Sensing and Imaging*, vol. 21, no. 1, p. 13, 2020.

[12] Z. P. Wang, Z. Y. Ye, X. M. Wang, and Z. N. Zhai, "Image transmission in an OFDM VLC system using symbol scrambling and chaotic Walsh-Hadamard precoding," *Optoelectronics Letters*, vol. 15, no. 4, pp. 284–287, 2019.

[13] A. Pramanik, A. Kashyap, and S. P. Maity, "Study on sampling matrices for far-end image reconstruction by block compressed sensing," in *Proceedings of the 2015 IEEE International WIE Conference on Electrical and Computer Engineering*, pp. 346–349, Dhaka, Bangladesh, December 2015.

[14] A. Kashyap, A. Pramanik, and S. P. Maity, "On Block Compressed Sensing far end reconstruction using OFDM," in *Proceedings of the 2015 Third International Conference on Image Information Processing (ICIIP)*, pp. 162–167, Waknaghat, India, December 2015.

[15] H. H. Zhao, P. L. Rosin, Y. K. Lai, J. H. Zheng, and Y. N. Wang, "Adaptive gradient-based block compressive sensing with sparsity for noisy images," *Multimedia Tools and Applications*, vol. 79, no. 21-22, pp. 14825–14847, 2020.

[16] A. S. Unde and D. Pp, "Rate-distortion analysis of structured sensing matrices for block compressive sensing of images," *Signal Processing: Image Communication*, vol. 65, pp. 115–127, 2018.

[17] Z. P. Wang, "Secure image transmission in wireless OFDM systems using secure block compression-encryption and symbol scrambling," *IEEE Access*, vol. 7, pp. 126985–126997, 2019.

[18] G. Kuldeep and Q. Zhang, "Design prototype and security analysis of a lightweight joint compression and encryption scheme for resource-constrained IoT devices," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 165–181, 2022.

[19] A. S. Unde and P. P. Deepthi, "Design and analysis of compressive sensing-based lightweight encryption scheme for multimedia IoT," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 1, pp. 167–171, 2020.

[20] M. Yamaç, M. Ahishali, N. Passalis, J. Raitoharju, B. Sankur, and M. Gabbouj, "Multi-level reversible data anonymization via compressive sensing and data hiding," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1014–1028, 2021.

[21] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, "Double image encryption algorithm based on neural network and chaos," *Chaos, Solitons & Fractals*, vol. 152, Article ID 111318, 2021.

[22] jinqing Li, Y. sheng, X. Di, and Y. Mu, "Range-gated laser image compression and encryption scheme based on bidirectional diffusion," *Optoelectronics Letters*, vol. 17, no. 10, pp. 0630–0635, 2021.

[23] Z. Man, J. Li, X. Di et al., "A novel image encryption algorithm based on least squares generative adversarial network random number generator," *Multimedia Tools and Applications*, vol. 80, no. 18, pp. 27445–27469, 2021.

[24] L. H. Gong, K. D. Qiu, C. Z. Deng, and N. R. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Optics & Laser Technology*, vol. 115, pp. 257–267, 2019.

[25] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of image ciphers with permutation-substitution network and chaos," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 6, pp. 2494–2508, 2021.

[26] L. Qu, H. He, and F. Chen, "On the security of block permutation and Co-XOR in reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 3, pp. 920–932, 2022.

[27] S. Sun, "A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling," *IEEE Photonics Journal*, vol. 10, no. 2, pp. 1–14, Article ID 7201714, 2018.

[28] F. Huo and G. Gong, "XOR encryption versus phase encryption, an in-depth analysis," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 4, pp. 903–911, 2015.

[29] M. Y. Li, G. M. Zhang, G. B. Li, H. X. Li, and X. Zhang, "Secure transmission algorithm based on subcarrier sorting and XOR operation in OFDM systems," in *Proceedings of the 2018 IEEE International Conference On Communication Systems (ICCS)*, pp. 147–151, Chengdu, China, December 2018.

[30] F. Buchali, F. Steiner, G. Bocherer, L. Schmalen, P. Schulte, and W. Idler, "Rate adaptation and reach increase by probabilistically shaped 64-QAM: an experimental demonstration," *Journal of Lightwave Technology*, vol. 34, no. 7, pp. 1599–1609, 2016.

[31] T. Wiegart, F. Da Ros, M. P. Yankov, F. Steiner, S. Gaiarin, and R. D. Wesel, "Probabilistically shaped 4-PAM for short-reach IM/DD links with a peak power constraint," *Journal of Lightwave Technology*, vol. 39, no. 2, pp. 400–405, 2021.

[32] Y. Yao, K. X. Xiao, B. Xia, and Q. J. Gu, "Design and analysis of rotated-QAM based probabilistic shaping scheme for Rayleigh fading channels," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3047–3063, 2020.

[33] J. Ma, M. Chen, K. Q. Wu, and J. He, "Performance enhancement of probabilistically shaped OFDM enabled by precoding technique in an IM-DD system," *Journal of Lightwave Technology*, vol. 37, no. 24, pp. 6063–6071, 2019.

[34] R. Ponuma and R. Amutha, "Encryption of image data using compressive sensing and chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 11857–11881, 2019.

[35] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4655–4666, 2007.

[36] A. Kanso and N. Smaoui, "Logistic chaotic maps for binary numbers generations," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2557–2568, 2009.

[37] T. Geisel and V. Fairen, "Statistical properties of chaos in Chebyshev maps," *Physics Letters A*, vol. 105, no. 6, pp. 263–266, 1984.

[38] R. N. Bracewell, "Discrete hartley transform," *Journal of the Optical Society Of America*, vol. 73, no. 12, pp. 1832–1835, 1983.

[39] J. G. Proakis, *Digital Communications*, McGraw-Hill, New York, NY, USA, 1995.

[40] J. R. Barry, E. A. Lee, and D. G. Messerschmitt, *Digital Communication*, Kluwer, Boston, MA, USA, 3rd edition, 2004.

[41] N. Fu, L. Cao, and X. Peng, "A modified orthogonal matching algorithm using correlation coefficient for compressed sensing," in *Proceedings of the 2011 IEEE International Instrumentation and Measurement Technology Conference*, pp. 1–5, Hangzhou, China, May 2011.

[42] D. Needell and J. A. Tropp, "Cosamp: iterative signal recovery from incomplete and inaccurate samples," *Applied and Computational Harmonic Analysis*, vol. 26, no. 3, pp. 301–321, 2009.