A Novel Chaotic Subcarriers Interleaving Approach for Secured OFDM Communication Systems

Một phương pháp xáo trộn hỗn loạn sóng mang con trong hệ thống thông tin bảo mật sử dụng công nghệ điều chế đa sóng mang trực giao

Nguyen Huu Long[1], To Thi Thao[2], Vu Nhat Minh[1], Hoang Minh Son[1], Vu Van Yem[1*]

[1] Hanoi University of Science and Technology – No. 1, Dai Co Viet Str., Hai Ba Trung, Ha Noi, Viet Nam

[2] Post and Telecommunications Institute of Technology – 122, Hoang Quoc Viet, Cau Giay, Ha Noi, Viet Nam

Received: March 31, 2016; accepted: August 26, 2016

Abstract

In this paper, we propose a chaotic interleaving approach for efficient data transmission with orthogonal frequency division multiplexing (OFDM). The subcarriers are interleaved with the proposed approach prior to the modulation step. The chaotic Baker map is used in the proposed interleaving approach. In addition to reducing Peak to Average Power Ratio (PAPR), the proposed chaotic interleaving approach adds a degree of encryption to the transmitted data. The performance of the proposed approach is evaluated by the transmission of bit stream over Gauss and Rayleigh channels with different modulation schemes.

Keywords: Digital Communications, Security, OFDM, Chaos, Interleaving.

Tóm tắt

Trong bài báo này, chúng tôi đề xuất một phương pháp xáo trộn hỗn loạn trong hệ thống thông tin số sử dụng công nghệ điều chế đa sóng mang trực giao. Các sóng mang con được xáo trộn theo cách đề xuất trước khi bước điều chế. Bản đồ hỗn loạn Baker được sử dụng trong phương pháp tiếp cận xáo trộn đề xuất. Ngoài việc để giảm tỉ số công suất đỉnh trên công suất trung bình, phương pháp xóa trộn hỗn loạn sóng mang đề xuất còn tăng độ bảo mật dữ liệu phát. Hiệu năng của phương pháp đề xuất được kiểm chứng thông qua việc truyền các chuỗi bit qua kênh Gauss và kênh Rayleigh cho các phương thức điều chế khác nhau.

Từ khóa: Thông tin số, Bảo mật, Điều chế đa sóng mang trực giao, Hỗn loạn, Xáo trộn.

1. Introduction

In recent years, both OFDM and chaotic algorithms have been widely developed for digital communication systems [1-8]. There are some chaotic communications systems have been proposed: chaotic modulation, chaotic masking, chaos shift keying (CSK) [4, 5, 6]. There are various researches proposing OFDM systems using chaotic algorithms [2,4,8]. However, those systems have showed several drawbacks. For instance, applying Discretized by Baker Map (DBM) in input bits [2, 8] introduces considerable delay since those bits are required to be buffered before Serial/Parallel step. Or as in [4], chaotic encryption systems might have higher BER than conventional systems.

Apparently, high correlation coefficient among QPSK symbols of OFDM signal leads to high Peak to Average Power Ratio (PARP). If the long correlation patterns of the in-phase and quadrature components are broken down, a reduction in the PAPR can be achieved [8]. Interleaving is an option to break these correlation patterns [9]. In this paper, we propose a chaotic subcarriers interleaving approach in which the chaotic Baker map is used to separately randomize the in-phase and quadrature components of the QPSK symbol. As a result, the correlation coefficient between two components is reduced. And then we propose an OFDM system applying DBM to subcarriers. Comparing to applying DBM on input bits, chaotic subcarriers avoids delay while maintains the same BER. Furthermore, the reduction in PAPR can be achieved because of lower correlation coefficient among modulated symbols.

The remained part of this paper is organized as follows. In section 2, the discretized baker map is presented. The OFDM system applying DBM to subcarriers is proposed in section 3 followed by correlation coefficient analysis in section 4. The simulated results are shown in section 5 and conclusions are given in section 6.

2. Discretized Baker Map

Fig.1 shows a square image consisting of NxN pixels. It is divided vertically into k rectangle-shaped

* Corresponding author: Tel.: (+84) 902280833
Email: yem.vuvan@hust.edu.vn

parts with size of p1, p2... pk respectively. The vector (p1, p2… pk) is call Baker key.

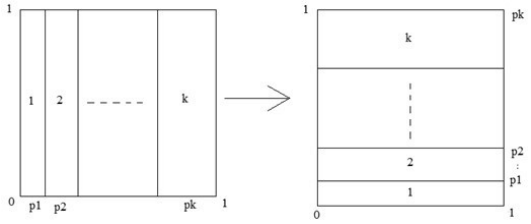


Fig. 1. Generalized Baker map

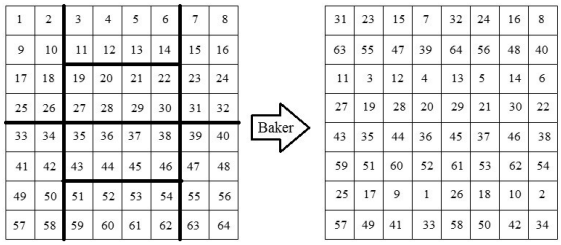


Fig. 2. Version A of DBM – key =(2, 4, 2)

DBM is commonly used in image encryption. In such applications, DBM is classified into two versions: A and B. In this paper, version A is concerned.

The formula of version A is:

$$B(x',y') = A\left(\frac{N}{p_i}(x - P_i) + y \bmod \frac{N}{p_i},\ \frac{p_i}{N}\left(y - y \bmod \frac{N}{p_i}\right) + P_i\right) \quad (1)$$

Where $P_i = p_1 + p_2 + \cdots + p_i$; $N = p_1 + p_2 + \cdots + p_k$; $P_i \le x < P_i + p_i$;

The chaotic interleaving is performed as follows:

- An NxN square matrix is divided into k vertical rectangles of height N and width p_i.
- These vertical rectangles are stretched in the horizontal direction and contracted vertically to obtain a p_i x N horizontal rectangle.
- These rectangles are stacked as shown in Figure 1, where the left one is put at the bottom and the right one at the top.
- Each p_i × N vertical rectangle is divided into p_i boxes of dimensions N=p_i × p_i containing exactly N points.
- Each of these boxes is mapped column by column into a row as shown in Fig. 2.

Fig.2 shows the case in which N = 8 with the Baker key equals to (2, 4, 2).

3. The proposed OFDM system

In this section, we use 8x8 matrix DBM as in Fig.2 in section II. The 1st element is mapped to the 31st, the 2nd to the 23rd…, and the 64th to the 34th.

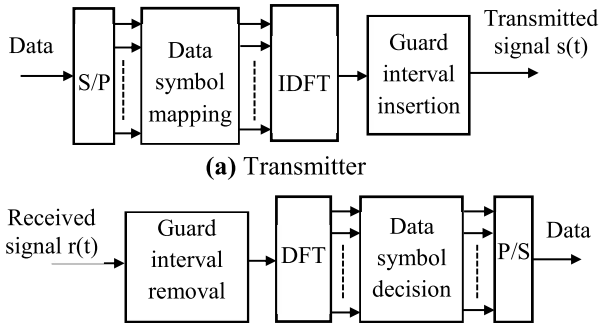


Fig. 3. A conventional OFDM system

Fig.3 is a simplified diagram of a conventional OFDM system. N is the number of subcarriers, c_k is the information symbol, f_k is the frequency of the subcarrier, T_s is the symbol period and s(t) is the OFDM signal.

The m[th] ($m \in [1, N]$) sample of s(t):

$$s_m = \sum_{k=1}^{N} c_k . e^{j2\pi f_k \frac{(m-1)T_s}{N}} \quad (2)$$

When N = 64, equation (2) becomes:

$$s_m = c_1 . e^{j2\pi f_1 \frac{(m-1)T_s}{N}} + c_2 . e^{j2\pi f_2 \frac{(m-1)T_s}{N}} + \cdots + c_{64} . e^{j2\pi f_{64} \frac{(m-1)T_s}{N}} \quad (3)$$

Applying DBM in subcarriers we have: f_1 maps to f_{31}, f_2 maps to f_{23}…, and f_{64} maps to f_{34} (mapping is shown in Fig.2). We get a new OFDM system and equation (3) becomes:

$$s_m = c_1 . e^{j2\pi f_{31} \frac{(m-1)T_s}{N}} + c_2 . e^{j2\pi f_{23} \frac{(m-1)T_s}{N}} + \cdots + c_{64} . e^{j2\pi f_{34} \frac{(m-1)T_s}{N}} \quad (4)$$

The *transformation* of transmitted signal from equation (3) to equation (4) is presented in Fig.4a and the reallocating subcarriers of received signal are shown in Fig.4b.

The proposed OFDM system is presented in the Figure 5.

"IDFT with DBM" block and "DFT with DBM" block which allocate subcarriers based on DBM are implemented as described in Fig.4.

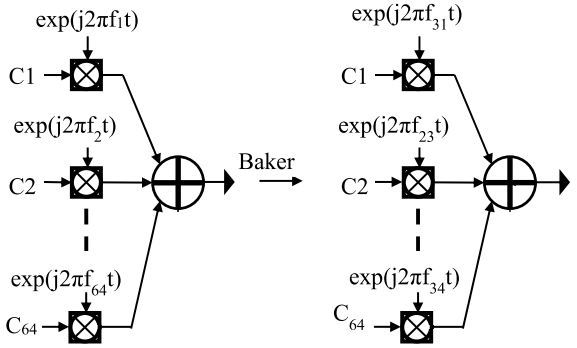
In case there are more than 64 subcarriers (128, 256…), the subcarriers are divided into smaller groups of 64 subcarriers and processed as above.

In an OFDM transmission, the transmission of cyclic prefix does not carry 'extra' information. The signal energy is spread over time $T_d + T_{CP}$ whereas the bit energy is spread over the time T_d.

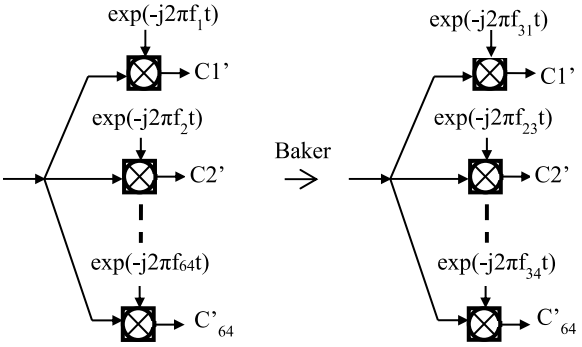
$$E_s.(T_d + T_{CP}) = E_b.T_d \quad (5)$$

Simplifying:

$$E_s = \frac{T_d}{T_d+T_{CP}} E_b \quad (6)$$

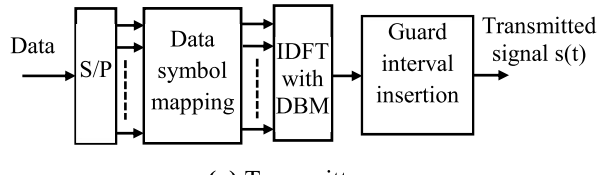


(a) Subcarriers in transmitter of the conventional OFDM system and the proposed OFDM system

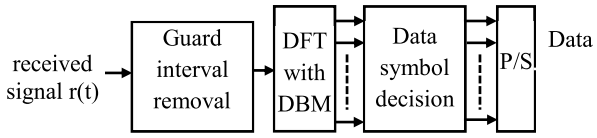


(b) Subcarriers in receiver of the conventional OFDM system and the proposed OFDM system

Fig. 4. Mapping subcarriers



(a) Transmitter



(b) Receiver

Fig. 5. The proposed OFDM system

In addition, not all the available subcarriers from the DFT are used for data transmission. Typically, some subcarriers are left unused to ensure spectrum roll off. Assume that among N subcarriers, the number of used subcarriers is n. We have:

$$E_s = \frac{n}{N} E_b \quad (7)$$

Combining the impacts of prefix (equation (6)) and unused subcarriers (equation (7)), the relation between symbol energy and the bit energy is:

$$\frac{E_s}{N_0} = \frac{E_b}{N_0}.\left(\frac{T_d}{T_d+T_{CP}}\right).\frac{n}{N} \quad (8)$$

Thus:

$$\frac{E_s}{N_0}[dB] = \frac{E_b}{N_0}[dB] + 10 * \log\left(\frac{T_d}{T_d+T_{CP}}\right) + 10 * \log\frac{n}{N} \quad (9)$$

Then:

$$SNR[dB] = E_s/N_0\,[dB] - 10 * \log\frac{n}{N} \quad (10)$$

Theoretical BER:

$$P_e = 2 * Q\left(\frac{E_s}{N_0}\right) \quad (11)$$

From (9) and (11), we can see that BER of OFDM using QPSK does not depend on the order of symbols or subcarriers.

4. Correlation coefficient analysis

Interleaving subcarriers following DBM means that symbols after QPSK also are interleaved likewise. If there are 64 subcarriers, the number of symbols of an OFDM symbol is also 64. These symbols are mapped following DBM and considered as an 8x8 array. The correlation coefficient is calculated as follow:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (12)$$

$$E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \quad (13)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (14)$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - E(y))^2 \quad (15)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (16)$$

$$\gamma_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (17)$$

Table 1. Correlation coefficients of two adjacent symbols of an OFDM symbol

	conventional OFDM	proposed OFDM
horizontal	0.1442	0.0703
vertical	0.0959	0.0736

Table 1 presents the correlation coefficient values of two horizontally, vertically and diagonally adjacent symbols of first 128 bits data. The correlation analysis indicates that the proposed OFDM system is

better since all the values are tending towards zero correlation.

5. Simulation results

The simulations are conducted to compare the performance of the proposed OFDM system to the conventional OFDM system. In the simulations, signal is transmitted using conventional OFDM and proposed OFDM over an additive white Gaussian noise (AWGN) as well as Rayleigh fading channels. QPSK is used for baseband modulation. There are 64 subcarriers and guard interval length equals to a quarter of the symbol duration. The simulation result of conventional OFDM and OFDM with chaotic subcarriers under AWGN channel is shown in Fig.6.

It shows that there is little difference in BER between the proposed OFDM and conventional OFDM system and it matches well to theoretical one. This means that mapping subcarriers do not deplete signal's quality. However, the proposed chaotic interleaving approach, apparently, adds a degree of encryption to the system.

In addition to AWGN channel, we also investigate our proposed method under the effect of Rayleigh fading. Fig.7 shows the comparison among BER of theoretical analysis, OFDM chaotic and conventional OFDM. The simulation uses QPSK modulation with 64 subcarriers. We can see clearly from Fig. 7 that there is very small difference of BER between two systems, which indicates that chaotic-subcarriers do not reduce the precision of transmitting signals.

In Fig.8, we analyze the influences of number of subcarriers on BER under Rayleigh fading channel. Due to the fact that an equalizer is applied at receiver and Doppler Effect is neglected, there are minor differences among schemes.

Lastly, we examine the proposed method under different modulation schemes. The results of 4-QAM, 16-QAM and 64-QAM in Rayleigh fading are compared with theoretical values in Fig.9.

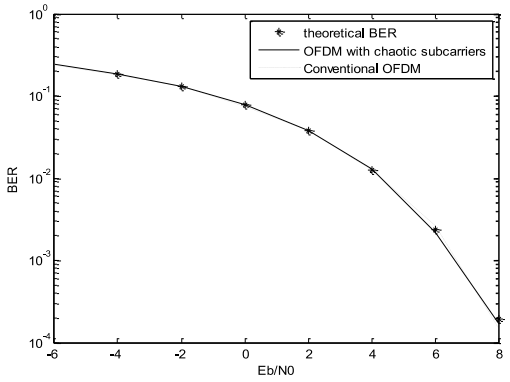


Fig.6. Theoretical BER, BER of conventional OFDM and OFDM with chaotic subcarriers under AWGN channel

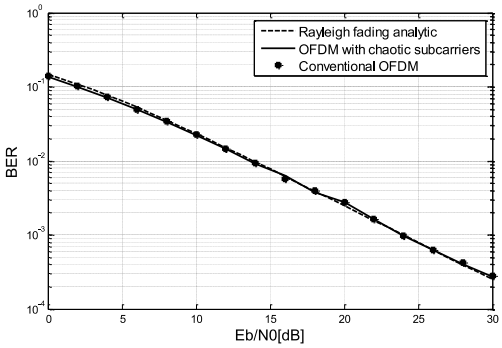


Fig. 7. Theoretical BER, BER of conventional OFDM and OFDM with chaotic subcarriers under Rayleigh channel

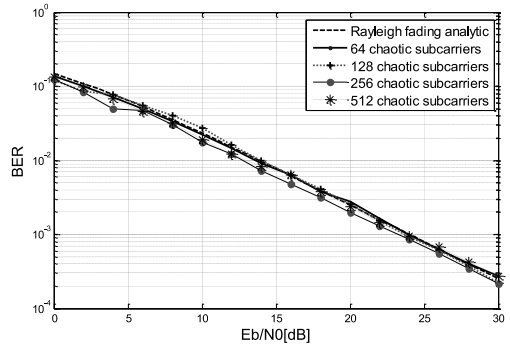


Fig. 8. Theoretical BER and BER of OFDM chaotic with different number of subcarriers under Rayleigh channel

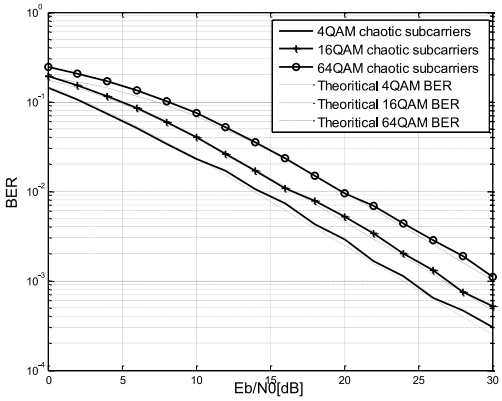


Fig. 9. Theoretical BER and BER of OFDM chaotic with different modulation schemes under Rayleigh channel

As illustrated in the figure, the BER of OFDM chaotic schemes are consistent with theoretical analysis which suggests that even with varying modulation schemes, chaotic mapping still maintains the reliability while improves the security of the signal.

6. Conclusion

We propose in this paper an OFDM system using chaotic subcarriers based on DBM to improve the privacy and security of communication using OFDM. Through theoretical analysis and simulation, we have pointed out that the proposed OFDM system not only maintains transmission quality but also adds a degree of encryption to the system. Besides, no any additional delay caused by buffers for chaotic interleaving as many other proposed methods.

References

[1] Y.Mao, G.Chen, S.Lian, "A novel fast image encryption scheme based on 3D chaotic Baker maps," Int. J. Bifurcation Chaos, Vol. 14, No. 10 (2004), p. 3613-3624.

[2] E.M.El-Bakary, O.Zahran, S.A.El-Dolil, F.E.Abd El-Samie, "Chaotic Maps: A tool to enhance the performance of OFDM Systems," International Journal of Communication Networks and Information Security, Vol. 1, No. 2, August 2009.

[3] F.Huang, Y.Feng, "Security analysis of image encryption based on two-dimensional chaotic maps and improved algorithm," Frontiers of Electrical and Electronic Engineering in China, Volume 4, Issue 1, p.5-9.

[4] D.Luengo, Ignacio Santamaría, "Secure Communications Using OFDM with Chaotic Modulation in the Subcarriers," Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st, p.1022-1026 Vol.2.

[5] M. P. Kennedy, R. Rovatti, and G. Setti, Eds., "Chaotic Electronics in Telecommunications," CRC Press, 2000.

[6] F.C.M.LauandC.K.Tse, "Chaos-Based Digital Communication Systems," Berlin: Springer-Verlag, 2003.

[7] S.K.Kadari, B.S.B.Raju, N.X.Quyen, "Digital image encryption based on chaotic behavior of a modified tent map," ISAST transactions on computer and intelligent system, No.1, Vol.4, 2012 (ISSN 1798-2448).

[8] N.F. Soliman, A.A. Shaalan, S. El-Rabaie, and F.E. Abd El-samie, "Peak power reduction of OFDM signals using chaotic Baker map," In proceedings IEEE International Conference on Computer Engineering & Systems, 2009. ICCES 2009, p.593-598.

[9] A.D. S. Jayalath and C. Tellambura, "The Use of Interleaving to Reduce the Peak-to-Average Power Ratio of an OFDM Signal," In Proceedings IEEE Global Telecommunications Conference, 2000, pp. 82-86, San Francisco, CA.