Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 449-455, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.449.455

Chaotic Interleaving for Secured OFDM

N.R. Raajan, B. Monisha, R. Vishnupriya, Niranjana Rangarajan, G.N. Jayabhavani and C. Nishanthini
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

Corresponding Author: N.R. Raajan, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

ABSTRACT

An evolution on new discipline under nonlinear engineering was considered based on two facts: the first one is based on the higher order effects that takes place and plays more importance in current designs and the second one is focused mainly on non-linear behavior for the new upcoming designs. While considering for the latter one, the complexity of non-linear behavior in random manner is called "chaos", which is now applied for various areas like communications, physiology, signal processing. In this paper, we propose an effective method for improving the security in Orthogonal Frequency Division Multiplexing (OFDM) by the use fractals in the form of chaos.

Key words: OFDM, chaos, fractals, security, non-linearity

INTRODUCTION

Orthogonal Frequency Division Multiplexing (OFDM) is a digital modulation technique which uses Frequency Division Multiplexing (FDM) inherently. A multi-carrier superimpose outline which habituates orthogonal sub-carriers to tone digital signals by analogue steps was obtained by Quadrature Amplitude Modulation (Liu *et al*., 2006) technique.

Generally data for OFDM (Thenmozhi *et al.,* 2012) undergoes channel coding. It is generally convolution coding done after interleaving. Interleaving is the shuffling of data sequences in random yet a defined order. It helps to overcome the disadvantages of fading in the channel, because the error is spread out in the bit-stream and the decoder is not jammed because of concentration of errors in the sequences as would happen otherwise.

In Convolution coding Jenifer (Philomina *et al.,* 2012) each n-bit message symbol to be encoded is transformed into an m-bit symbol, where n/m is the code rate. This transformation is a function of the last k message symbols, where k is taken as the constraint length of the code. For performing this, k memory registers are considered each having an initial state of 0 unless specified to be otherwise. All the registers are operated upon at least once by a mod-2 adder which is governed by a polynomial equation. The output is taken when the last message symbol has passed through the shift register sequence fully.

The encoded message sequence is passed through serial to parallel converters and then modulated onto subcarriers using QAM. The QAM output is made secure against inter carrier interference by pilot carrier insertion. The signal is then converted from frequency to time domain by an effective implementation of IFFT (Raajan *et al.,* 2012a). This domain conversion facilitates easier appending of the last part of the signal onto the first part (i.e., cyclic prefix) by the process called guard interval insertion. This eliminates the problem of inter symbol interference thus disabling cross talk. This also helps in easier estimation of the signals.

Now the signal is passed through any channel like AWGN (Praveenkumar *et al.*, 2012) because it adds only white noise and for most part it is considered ideal as it does not lead to frequency selective fading or interference), or a Rayleigh channel and the transmission is complete.

In the reception part, the guard interval is removed from the received signal and then time to frequency domain transformation is done through FFT implementation. The pilot carriers are removed (Monisha *et al.*, 2012) and the signal devoid of pilot carriers is demodulated. The reception signal is converted from parallel to serial.

The serially converted signal is decoded using Viterbi algorithm. The output of the decoder is then de-interleaved to get the transmitted message signal. The OFDM in Fig. 1, transmission reception process is also shown in Fig. 1.

OFDM is chosen for security improvement because, of its flexible (Raajan *et al.*, 2011) digital processing and security can be implemented anywhere along the block. Because of the increase in the subscribers preferring OFDM recently, the need for privacy in communication (Arioua *et al.*, 2012) is mandatory.

The encryption is done at the physical layer (Tahir *et al.*, 2010) so there are no eavesdropping complications as it is done in the bit streams at the most lower level of OSI architecture. Chaos is chosen for encryption because it has a highly unpredictable and random-look nature. The chaos sequence is sensitive to variables' and parameters' changes and a small variation of any one of them changes the outputs considerably In this study, an effective method for improving the security in Orthogonal Frequency Division Multiplexing (OFDM) has been done. It adopts the use of fractals in the form of chaos which is used efficiently to counteract the malicious users in OFDM.

FRACTALS AND CHAOS

"Fractals" and "Chaos" are two examples of nonlinear approaches towards complex systems. Fractals (Chung and Ma, 2005) are mathematical sets that has fractal dimension to it and falls between integers. They exhibit the concept of being same from near as from far. Thus fractals can be thought of as a fragmented geometric shape that can be split into parts, each of those parts being approximately a reduced-size copy of the whole. They show properties of exact self-similarity/quasi self-similarity, or statistical self-similarity and they are recursive, that is the process by which they are created is repeated an infinite number of times.

Fractals are too irregular to be represented in Euclidean space (Raajan *et al.*, 2012b). They appear almost similar at all levels of magnification and are infinitely complex in nature. E.g. Natural objects that can be thought of as fractals are, clouds, animal coloration pattern, vegetables like cauliflower. Self-similar objects can be exceptions to fractals like a real line i.e., a straight Euclidean line.

A method to create a geometric fractal is, use a shape as the base and replace it with a motif shape that is recurring. Chaotic systems (dynamic) are related to fractalz (Raajan *et al.*, 2012a). It also called as displaying "butterfly effect" haos behavior gives rise to diverging outputs for small changes in initial conditions, which makes long term prediction of the state of a system difficult. Phase space existing objects of a dynamical system and parameter space objects for a family of systems are fractals. Chaos (Raajan *et al.*, 2012b) is in determinism which is objected in Laplace's world. It follows three important principles. They are:

- Sensitivity in extreme orders to initial conditions
- The cause and effect relationship are not proportional
- Nonlinearity

The Chaos system is generated using Chua's circuit. It is a simple electronic circuit that classic chaos behavior. It is also called "a paradigm for chaos" in the real world because of the ease in its construction.

It consists of standard components i.e., resistor, capacitor, inductor satisfying the following criteria in circuit form to result in chaotic behavior. The circuit must have:

- Non-linear elements (2 linear resistors, 2 diodes)
- Locally active elements (resistor)
- 3 or more energy-storage elements (2 capacitors, 1 inductor)
- Negative impedance converter (3 linear resistors, operational amplifier)

Applying the laws of electromagnetism, the working of Chua's circuit (Raajan *et al*., 2012a) can be modeled in the terms of nonlinear ordinary differential equations. It uses the following variables representing:

x(t) = Voltage across 1st capacitor used
y(t) = Voltage across 2nd capacitor used
z(t) = Intensity of electrical current in the inductor

The equations are:

$$\frac{dx}{dt} = \alpha[y - x - f(x)] \quad (1)$$

$$\frac{dy}{dt} = x - y + z \quad (2)$$

$$\frac{dz}{dt} = -\beta y \quad (3)$$

where, the function f(x) = electrical response of the nonlinear resistor, and the shape of it depends on the particular configuration of its components. The parameters α and β = particular values of the circuit components.

The output of such a Chua's circuit is used in the security improvement for data in an OFDM system. The output shown below is taken from a Chua's circuit, which is used in the OFDM transceiver data encryption. This is generated from the Simulink model of a Chua's system.

SECURITY PROVIDED BY FRACTALS FOR OFDM

The Chaos having fractal behaviour is used in data encryption (Zhang *et al*., 2011; Khan *et al*., 2007). Security given by chaos in convolutional coding (Zhou and Au, 2011) can be used to our advantage in the method of source coding which is followed here rather than the channel coding evolved from using convolutional codes in OFDM system as in Fig. 1.

The coordinates from the graphical plot of the chaotic system are taken in the form of a matrix with the x and y coordinates taken two columns separately initially and then appended into single row as in Fig. 2. The final index of the matrix is usually of the order 28000. The floating point values are converted to binary representation.

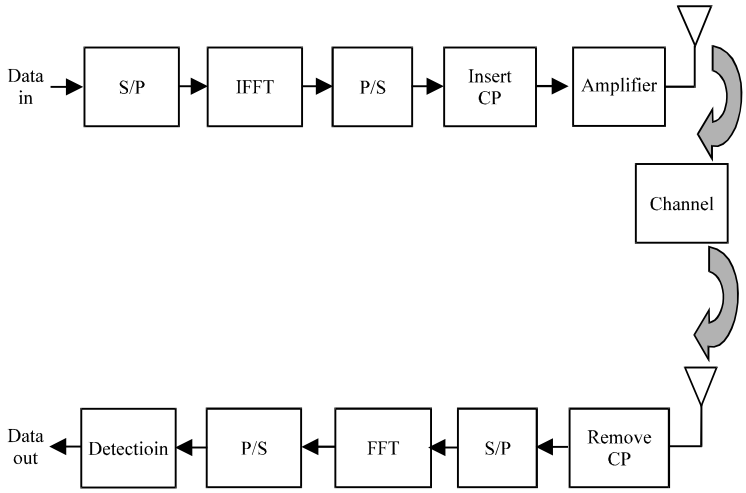

Fig. 1: General block diagram of OFDM transceiver

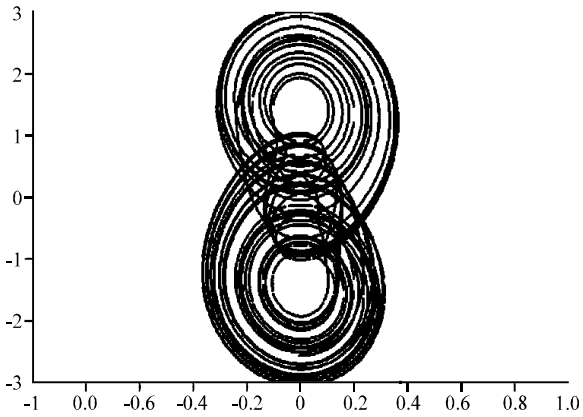

Fig. 2: Chaotic behavior using the sequence

The data bits (Amirtharajan and Rayappan, 2012) are interleaved mutually to achieve shuffling and to immunize it against usual channel interference parameters. The set of interleaved data bits are Exclusively-OR with the chaos binary coordinates. The chaos sequence without the data bits are concatenated by XOR operation using random PN sequences. This is then sent through the OFDM transceiver block. The chaos sequence is kept as the confidential key with the transmitter and at the receiver it is used in the decryption process. This is illustrated in Fig. 3.

LEVEL OF SECURITY

In our analysis, we consider key size as 64 bits (binary values), total length of the bit considered are combination of 450 times of chaos input signal taken. Hence the size of the key space was considered for the factor of combination of twice power of key size taken to the product of the combination of chaos signal (input signal). If the time requires for the retrieval of input chaotic signal for one value of the key in the key space is taken as 10^{-3} sec (Amirtharajan and Rayappan, 2012), then the time taken for retrieving its original input signal by considering all the possible keys in the total key space is given as 10.13×10^{1008} years in accordance with Kallam *et al.* (2011).

Algorithm:

Step 1: Generate PN sequence of length 64 bits and chaos sequence as input signal
Step 2: Generate key of size 64 bits using key division and distribution algorithm in chaos signal
Step 3: Obtain encrypted signal by xor both message sequence and chaos sequence
Step 4: Encrypted signal gets converted into fractals, and then transmit that signal as an input for OFDM system
Step 5: Receive encrypted fractals signal from OFDM system and then convert that one as chaos based sequence
Step 6: Decrypt that chaos signal to obtain transmitted PN sequence

In spite of showing improvement in security at such levels after attack by potential malicious users, the bit error rate and signal to noise ratio graph has not steeply deteriorated as compared to BER graphs from normal OFDM transceiver systems as shown in Fig. 4. It is evident that message 2 will give more secure than message 1.

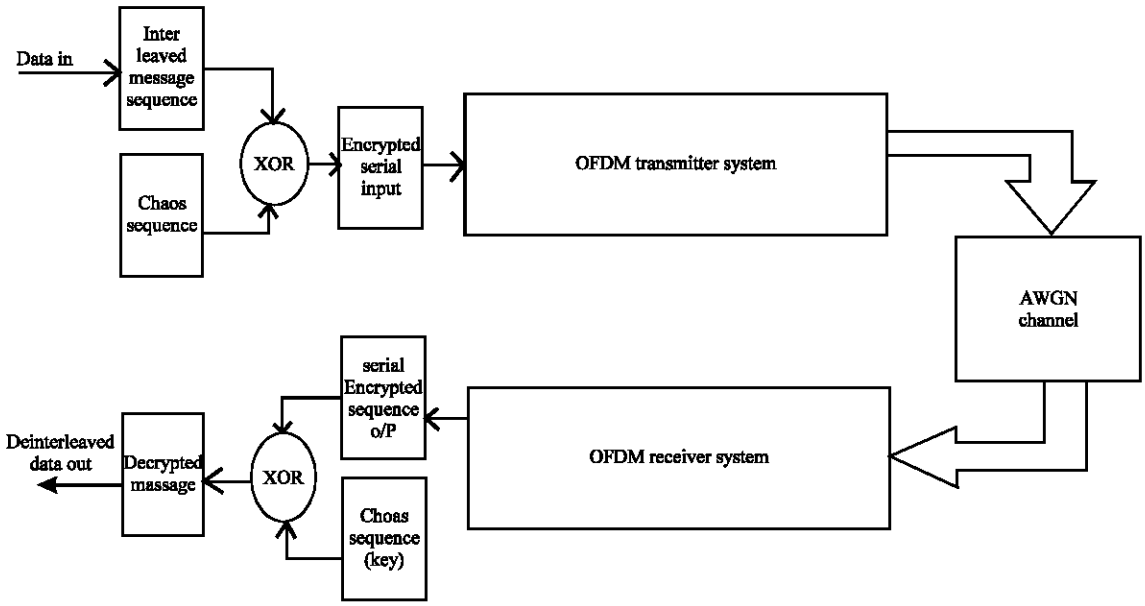

Fig. 3: Flow diagram of chaos based secured OFDM system

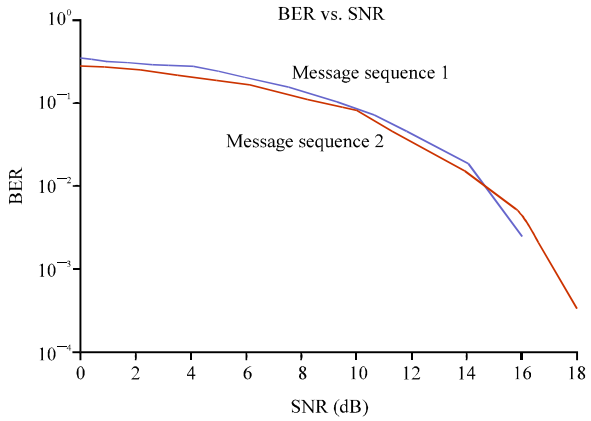

Fig. 4: Graph of SNR vs. BER-To substantiate performance

CONCLUSION

We have concluded that Orthogonal Frequency Division Multiplexing (OFDM) technique using data encrypted by fractals in chaotic form has enhanced the security, which is substantiated by the performance, bit error rate and the level of security results shown above. By concatenating the input with the random sequence of Fractals in the form of Chaotic Systems, in the initial part as source coding and then interleaving but still maintaining orthogonality, the security improvement is shown by the time taken to retrieve the information without the key, which amounts to years.

REFERENCES

Amirtharajan, R. and J.B.B. Rayappan, 2012. An intelligent chaotic embedding approach to enhance stego-image quality. Inf. Sci., 193: 115-124.

Arioua, M., S. Belkouch and M.M. Hassani, 2012. Efficient 16-points FFT/IFFT architecture for OFDM based wireless broadband communication. Inf. Technol. J., 11: 118-125.

Chung, K.W. and H.M. Ma, 2005. Automatic generation of aesthetic patterns on fractal tilings by means of dynamical systems. Chaos Solitons Fractals, 24: 1145-1158.

Kallam, R.B., S.U. Kumar and A.V. Babu, 2011. A new framework for scalable secure block cipher generation using color substitution and permutation on characters, numbers, images and diagrams. Int. J. Comput. Appl., 20: 37-42.

Khan, M.A., M. Asim, V. Jeoti and R.S. Manzoor, 2007. On secure OFDM system: Chaos based constellation scrambling. Proceedings of the International Conference on Intelligent and Advanced Systems, November 25-28, 2007, Kuala Lumpur, Malaysia, pp: 484-488.

Liu, H., H. Zhong, T. Zhang and Z. Gong, 2006. A quasi-newton acceleration EM algorithm for OFDM systems channel estimation. Inf. Technol. J., 5: 749-752.

Monisha, B., M. Ramkumar, M.V. Priya, A.J. Philomina, D. Parthiban, S. Suganya and N.R. Raajan, 2012. Design and implementation of orthogonal based haar wavelet division multiplexing for 3GPP networks. Proceedings of the International Conference on Computer Communication and Informatics, January 10-12, 2012, Coimbatore, India, pp: 1-6.

Philomina, A.J., D. Parthiban, B. Monisha, M.V. Priya, S. Suganya, M.R. Kumar and N.R. Raajan, 2012. Channel estimation of WCDMA with synchronized OFDM system for MIMO communication. Proceedings of the International Conference on Computer Communication and Informatics, January 10-12, 2012, Coimbatore, India, pp: 1-6.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012. Regulated OFDM-role of ECC and ANN: A review. J. Applied Sci., 12: 301-314.

Raajan, N.R., B. Monisha, M.R. Kumar, A.J. Philomina, M.V. Priya, D. Parthiban and S. Suganya, 2011. Design and implementation of orthogonal wavelet division multiplexing (OHWDM) with minimum bit error rate. Proceedings of the 3rd International Conference on Trendz in Information Sciences and Computing, December 8-9, 2011, Chennai, India, pp: 122-127.

Raajan, N.R., B. Monisha, K. Vinoth, R. Niranjan and D.D. Padmanabhan, 2012a. CORDIC based modified OFDM for pipelined data process. Proc. Eng., 38: 3300-3307.

Raajan, N.R., B. Monisha, N. Rangarajan and R. Vishnupriya, 2012b. Secured OHWDM using fractals. Proc. Eng., 38: 724-729.

Tahir, M., S.P. Jarot and M.U. Siddiqi, 2010. Wireless physical layer security using encryption and channel pre-compensation. Proceedings of the International Conference on Computer Applications and Industrial Electronics, December 5-8, 2010, Kuala Lumpur, Malaysia, pp: 304-309.

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure communication: A review. Res. J. Inf. Technol., 4: 31-46.

Zhang, L., X. Xin, B. Liu and Y. Wang, 2011. Secure OFDM-PON based on chaos scrambling. IEEE Photonics Technol. Lett., 23: 998-1000.

Zhou, J. and O.C. Au, 2011. On the security of chaotic convolutional coder. IEEE Trans. Circ. Syst. I: Regul. Papers, 58: 595-606.