IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

Encrypted Image Transmission over Wireless OFDM Communication Channel

Ensherah A. Naeem[1] and Masoud Alajmi[2]

Department of Electrical Engineering, Faculty of Industrial Education, Suez University, Suez 43518, Egypt[1]

Department of Computer Engineering, College of Computers and Information Technology, Taif University,

Al-Hawiya 21974, KSA[2]

Abstract: This study investigates the performance of Chaotic Baker Map and Double Random Phase Encoding (DRPE) encryption schemes in comparison with wireless communication channel. A comparison is drawn between the discrete Fourier transform (DFT)-orthogonal frequency-division multiplexing (OFDM) system on one hand, and the discrete wavelet transform (DWT)-OFDM system and the discrete cosine transform (DCT)-OFDM system in an additive white Gaussian noise (AWGN) environment on the other. The Haar wavelet and quadrature phase shift keying (QPSK) modulation format are also considered. The study includes detailed mathematical calculations designed to measure the peak signal to noise ratio (PSNR) of two encryption schemes over OFDM system on AWGN channels. The results obtained through these simulations demonstrate clearly that the DFT-OFDM system yields the best performance.

Keywords: AWGN, Chaotic Baker Map, DRPE

I. INTRODUCTION

The wireless communication channel is noisy and open to intruders. Hence, an efficient cryptosystem is therefore required to make the wireless communication channel reliable and secure enough for image transmission. Because of the tight relationship between chaos theory [1-2] and cryptography, chaotic cryptography has been extended to design image encryption schemes. Chaotic systems are sensitive to conditions at the outset, which means small differences in initial conditions can yield widely diverging outcomes during mapping, topological mixing property and ergodicity are the main advantages of these maps.

The OFDM, a type of wireless communication system, is used to transmit encrypted images. This multicarrier modulation technique is widely used for achieving high data rate in wireless communication systems. The OFDM divides the whole channel into several narrow, orthogonal subchannels and then send the data in parallel. Another advantage to ODFM is its ability to ameliorate the detrimental effects of frequency selective fading. Several performance parameters can measure the sharpness of an image after reception, including the Peak Signal to Noise Ratio (PSNR); most often, ODFM is used to evaluate the quality of a reconstructed image.

The remainder of this study is presented below, beginning with a description of the OFDM system model (Section 2), followed by an explanation of the encryption algorithm of the chaotic Baker map (Section 3). Based on this information, we describe the qualities and capabilities of the DRPE (Section 4). Next, we address how noise affects the image that has been received and decrypted (Section 5). Then, simulation results are discussed and analysed (Section 6). Finally, the conclusion outlines the disadvantages of wireless communication channel performance and lays out specific improvements made possible through the use of Chaotic Baker Map and DRPE encryption schemes (Section 7).

II. SYSTEM MODEL (OFDM)

There is a specific protocol of sequential steps used to transmit encrypted images in an OFDM communication. They are detailed here for reference. The process begins by encrypting the image, followed by transforming it into a serial stream of bits. Next the image data must move from being serial to being parallel, so that that image data is ready for the digital modulation step. Depending on which OFDM version will be used [3-6], we next run the IFFT, the IDCT or the IDWT, in order to separate a wideband signal of bandwidth B into two or more L narrowband signals, each having a bandwidth of B/L, so the image data is now in a valid format for digital modulation. The aggregate symbol rate is thus maintained, but each subcarrier undergoes flat fading, or ISI-free communication if the cyclic prefix (CP) employed is greater than the delay spread. Another alternative to the CP approach is to add zeros at the end of each symbol in the so-called zero padding (ZP) approach. The resulting cyclic prefixed- or zero-padded symbols can be transmitted serially through the wideband channel. Upon reception, an operation occurs (. FFT, DCT, or DWT) that discards CP or the padded zeros and demodulates L received symbols, leaving only the L data symbols. The decryption and retrieval process of the transmitted

DOI 10.17148/IJARCCE.2020.9337

image is thus complete. Our comparison study focuses on the FFT (or DCT, or DWT) step and on the guard interval insertion stage [7-8].
Our study was designed to determine (1) which OFDM version is best for transmitting encrypted images, and (2) which guard interval insertion method is best suited for encryption schemes.

III. ENCRYPTION ALGORITHM FOR A CHAOTIC BAKER MAP

Before transmission, the image must be encrypted using a 2-D chaotic map, the Baker Map, to convert a unit square into itself. In the process its operation is divided into two halves which are then stacked on top of each other. (1) and (2) provide a description of the Baker Map, *B* [9,13]:

$$B(x,y) = \left(2x, \frac{y}{2}\right) \qquad \text{when } 0 \le x < \frac{1}{2} \qquad (1)$$

$$B(x,y) = \left(2x-1, \frac{y}{2}+\frac{1}{2}\right) \qquad \text{when } \frac{1}{2} \le x \le 1 \qquad (2)$$

Interestingly, randomization normally does not employ this straightforward function that divides the square into two equal rectangles. The chaotic Baker Map has two versions, in which a transfer operator (U), called the “secret key”, is employed for the division of the map. The “secret key” is a vector that has (k) elements, such that the square is divided into (k) vertical rectangles.

3.1 Generalized Baker map

The Baker Map generalization] occurs in this sequence:

1- Division of an N×N square matrix into k vertical rectangles of height N and with width n_i (value of each element in U where N =n_1+n_2+….n_k).
2- Horizontal stretching of the vertical rectangles according to the value of their height.
3- Stacking the rectangles, the left one on the bottom and the right one on top.

3.2 Discretized Baker map

The purpose of discretizing a Baker Map is to assign one pixel to another objectively. Map denotation begins with B(n_1,n_2,……,n_k), where the sequence of k integers, n_1,n_2,……,n_k, is selected with each integer n_i dividing N, and $N_i = n_1 + ... + n_i$. Then we map pixel (*r*,*s*), with $N_i \le r < N_i + n_i$ and $0 \le s < N$ to [9-13]:

$$B_{(n_1,.....,n_k)}\ (r,s) = \left[\frac{N}{n_i}(r-N_i) + s \bmod \frac{N}{n_i}, \frac{n_i}{N}\left(s - s \bmod \frac{N}{n_i}\right) + N_i\right] \qquad (3)$$

This following factors delineate the formula (3): first comes division of an N×N square matrix k vertical rectangles of height N and with width n_i (value of each element in U where n_1+n_2+….n_k = N). Next comes division of each vertical rectangle N×n_i d into n_i boxes, each box containing N points. In the third and final step, the Baker Map becomes discretized after mapping each of the boxes is mapped to a row of pixels in parallel columns (left one on the bottom and right one on the top).

IV. DOUBLE RANDOM PHASE ENCODING (DRPE)

DRPE is an optical-based method that is commonly used to encode the input image using two random phase masks (PM1 and PM2), located respectively in the input and spatial frequency planes within 4f optical system [14-18].

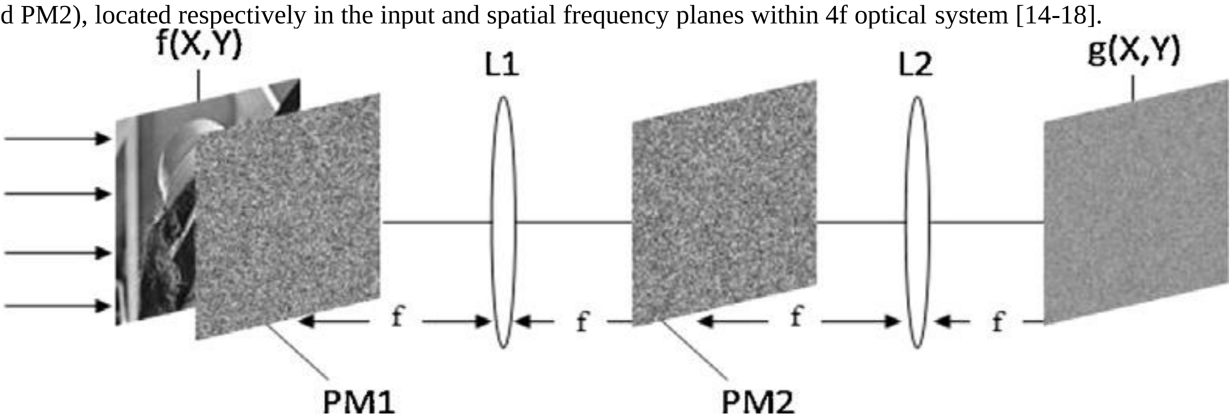

Fig. 1: Double random phase encoding process [14].

The process of how the DRPE modulates the input image (f(x,y)), in a random phase mask (θ(x,y)), attained through (4) is illustrated in Fig. 1.

$$\theta(x,y) = \exp\,[i2\pi\theta_0(x,y)] \quad (4)$$

Fourier transform of the modulated image is attained after passing the first lens. Then, the second random phase mask can modulate the resulting image as shown in (5):

$$\varphi(x,y) = \exp\,[i2\pi\varphi_0(u,v)] \quad (5)$$

The only two phase functions inserted in the input plane and Fourier plane, respectively, are represented in (4-5) θ_0(x,y), and φ_0(x,y); their values are randomly distributed over interval [0,2π]. The inverse Fourier transform occurs through the second lens and results in the encoded image (g(x,y)) as shown in (6).

$$g(x,y) = FT^{-1}\{FT\{f(x,y).\theta(x,y)\}.\varphi(u,v)\} \quad (6)$$

We preformed this process (7) to reconstruct the input image ($f(x,y)$).

$$f(x,y) = FT^{-1}\{FT\{g(x,y).\exp\,[-i2\pi\varphi_0(u,v)]\}\,.\exp\,[-i2\pi\theta_0(x,y)]\} \quad (7)$$

The decryption procedure is the same as encryption, only in reversed order. Note that in order to retrieve the original image, DRPE needs to utilize the random phase masks, also called "private keys".

The preponderance of research to date centers on ways to produce more secure encryption systems, focusing in particular on how to generate phase mask [17-18] and how to insert phase masks efficiently in a cover image [19- 20]. Transmitting large phase masks (the same size as the input image) requires not only huge cover image but reduces DRPE's security considerably. To avoid this problem, researchers have proposed a number of different methods. The first attempt suggested a cascaded iterative Fourier transform (CIFT) algorithm [21] where two phase masks are concurrently produced from the input image via an iterative method. This method does not require encoded image transmission: instead, the two encoding keys are inserted into the host image. Then the receiver extracts the two keys from the host image, allowing the input image to be reconstructed. The second method generates two masks using an affine transformation operation that passes through a pseudo-random pattern that was produced from a source image. The character of each individual mask correlates to the distinct parameters of the affine transformation and the iteration numbers that determine the degree of randomness. The implementation of affine transformation involves reflection, translation, rotation, shearing and scaling operations. Rather than jeopardizing security by sending the encryption mask, a secure channel is used to send a source image and 18 parameters indicated by the affine transforms [22].

V. THE DIFFERENT TRANSFORM TYPES

OFDM is performed on the different transforms such as the FFT, the DCT, and the DWT

5.1 The Fast Fourier transform (FFT)

An FFT is a faster, more efficient computational algorithm technique to compute the DFT [23] and its inverse. Let X_0, ..., X_{N-1}be complex numbers. The DFT can be expressed as in (8) [24]:

$$X_k = \sum_{n=0}^{N-1} x_n\, e^{-\frac{2\pi i}{N}nk} \qquad k = 0, \dots\dots\dots\dots, \qquad N-1 \quad (8)$$

The function that implements the transform is Y = fft(x) and the one implements the inverse transform y = ifft(X) for vectors of length N by (9) [24]:

$$X(k) = \sum_{j=1}^{N} x(j)w_N^{(j-1)(k-1)}$$

$$x(j) = (1/N)\sum_{k=1}^{N} X(k)w_N^{-(j-1)(k-1)} \quad (9)$$

5.2 The DCT

The DCT and its inverse of N × N image are expressed as (10-11) [24-25]:

$$C(u,v) = \frac{2}{N}\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (10)$$

$$f(x,y) = \frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha(u)\alpha(v)C(u,v)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (11)$$

f (x, y) characterizes the pixel intensity at the image domain (x,y) while C(u,v) represents the DCT coefficient at the transform domain (u,v). α(u)and α(v) are shown in (12).

DOI 10.17148/IJARCCE.2020.9337

$$\alpha(u) = \alpha(v) = \begin{cases} \frac{1}{\sqrt{2}}, & u = v = 0 \\ 1, & otherwise \end{cases} \qquad (12)$$

5.3 The DWT

Conversely, the DWT is performed using multi-level filter banks [26-27]. The mathematical formulation of a single level decomposition of a 1-D signal *x(k)* represented as shown in (13) and (14):

$$y_{high}(k) = \sum_n x(k)g(2k-n) \qquad (13)$$

$$y_{low}(k) = \sum_n x(k)h(2k-n) \qquad (14)$$

where $y_{high}(k)$ and $y_{low}(k)$ represent the outputs, respectively, of the high-pass and low-pass filters after sub-sampling by 2. The DWT is done on images row by row and then column by column. The image is divided into four bands after wavelet decomposition; a low-frequency band LL, and three high-frequency bands LH, HL, and HH.

VI. SIMULATION EXPERIMENT

In this section, we conduct simulation experiments to determine how efficient several different version OFDM will be transmission of encrypted images. In the experiment, we compare the OFDM versions with attention to how each one varies according to the number of subchannels.

We use an AWGN channel with the following settings: energy to noise per bit, Eb/N_0 = 3 dB, modulation level = 2, guard interval length, and GIL =32 bits. The simulation parameters are recoded in Table 1. The results are presented in Tables 2-4. Given the results, the FFT-ODFM emerges as the most effective channel for transmission.

Table 1: Simulation Experiment Parameters [28]

Transmitted data type	(Lena.bmp) image		
Channel type	AWGN channel	Fading channel	
Transform type	FFT transform	DCT transform	DWT transform
Encryption type	Baker Map	DRPE	
Modulation type	QPSK modulation		
Number of sub-channel (Nc)	128 subchannel		
Energy to noise per bit (Eb/N0)	3 dB		
Guard interval length (GIL)	32 bits		
Modulation level	2		
Symbol rate	250,000 symbols/second		
Bit rate	Symbol rate Nc modulation level		

Table 2 shows the PSNR values at various guard interval lengths, including (1) FFT-OFDM, (2) DCT-OFDM, and (3) DWT (Haar) -OFDM with QPSK modulation when AWGN channel is present.

Table 2: PSNR values and lengths

Scheme	**Channel**	**Peak Signal to Noise Ratio (PSNR)**						
		GIL : 2bits	**4bits**	**8bits**	**16bits**	**32bits**	**64bits**	**128bits**
Baker	FFT	-42.5845	-42.6027	-42.5965	-42.6191	-42.6032	-42.6171	-42.7057
	DCT	14.9239	14.8036	14.8508	14.7883	14.6019	14.3959	15.942
	DWT	14.9218	14.728	14.4478	14.0727	13.0797	11.5749	15 .8274
DRPE	FFT	16.5035	16.3473	16.2637	15.9509	15.5427	14.7311	13.5129
	DCT	16.4487	16.3792	16.2476	15.9958	15.5265	14.6716	13.5268
	DWT	16.4271	16.3314	16.2139	15.9325	15.5367	14.6384	13.483

DOI 10.17148/IJARCCE.2020.9337

Table 3 provides PSNR values at various numbers of subcarrier for (1) FFT-OFDM, (2) DCT-OFDM and (3) DWT (Haar) -OFDM with QPSK modulation when AWGN channel is present.

Table 3: PSNR values at various numbers of subcarrier

Scheme	**Channel**	**Peak Signal to Noise Ratio (PSNR)**					
		Nc: 64	**128**	**256**	**512**	**1024**	**2048**
Baker	FFT	-42.6212	-42.6178	-42.6115	-42.5971	-42.6059	-42.5799
	DCT	14.2573	14.5478	14.7094	15.0221	14.8259	20.3305
	DWT	11.6373	13.0798	13.9942	14.6327	14.6587	21.1349
DRPE	FFT	14.7152	15.4827	15.9685	16.2547	16.4077	16.4735
	DCT	14.6538	15.5189	16.0163	16.2772	16.3969	16.4644
	DWT	14.6583	15.5076	15.959	16.2584	16.4099	16.4249

Table 4 outlines the PSNR values at different energy to noise per bit for (1) FFT-OFDM, (2) DCT-OFDM and (3) DWT (Haar) -OFDM with QPSK modulation when AWGN channel is present.

Table 4: The PSNR values at different energy to noise per bit

Scheme	**Channel**	**Peak Signal to Noise Ratio (PSNR)**					
		Eb/N$_0$: 0dB	**5dB**	**10dB**	**15dB**	**20dB**	**25dB**
Baker	FFT	-42.7994	-42.536	-42.5143	-42.5142	-42.5142	-42.5142
	DCT	9.533	20.1734	56.4593	inf	inf	inf
	DWT	8.6962	17.5322	44.5046	inf	inf	inf
DRPE	FFT	-42.6114	17.4526	18.9152	18.9192	18.9674	18.9192
	DCT	14.6484	17.51	18.9066	18.9192	18.9674	18.9192
	DWT	13.0158	17.4803	18.9095	18.9192	18.9674	18.9192

The performance These results clearly demonstrate that the DRPE encryption algorithm performed better than the Baker Map for DCT-OFDM and DWT-OFDM systems. In FFT-OFDM system, on the other hand the Baker Map was proved to be the optimal choice for image encryption. In addition, the DRPE encryption algorithm provides lower PSNR values than the Baker Map does for DCT-OFDM and DWT-OFDM systems.

VII. CONCLUSION

This study compared and contrasted how FFT-OFDM, DCT-OFDM and DWT-OFDM perform when used to transmit an encrypted image over AWGN and fading channel. We also investigated in detail the effect of different modulation parameters on the quality of reconstructed images. Our findings indicate that FFT-OFDM is clearly superior to Baker Map for the transmission of encrypted images, but DCT-OFDM and DWT-OFDM are better suited to DRPE for the transmission of encrypted images.

REFERENCES

[1]. F. Dachselt and W. Schwarz, "Chaos and Cryptography," IEEE transactions on circuits and systems , vol. 48, NO. 12, DECEMBER 2001.
[2]. M. Asiml and V. Jeotil, "On Image Encryption: Comparison between AES and a Novel Chaotic Encryption Scheme," IEEE ICSCN 2007, MIT Campus, Anna University, Chennai, India, pp.65-69. Feb. 22-24, 2007.
[3]. P. Tan, N. C. Beaulieu, "A Comparison of DCT-Based OFDM and DFT-Based OFDM in Frequency Offset and Fading Channels," Beaulieu, *Fellow, IEEE,* IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 54, NO. 11, NOVEMBER 2006.
[4]. F. Gao, T. Cui, A. Nallanathan, and C. Tellambura, "Maximum Likelihood Based Estimation of Frequency and Phase Offset in DCT OFDM Systems under Non-Circular Transmissions: Algorithms, Analysis and Comparisons," IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 56, NO. 9, SEPTEMBER 2008.

DOI 10.17148/IJARCCE.2020.9337

[5]. P. Tan, N. C. Beaulieu, "Precise Bit Error Probability Analysis of DCT OFDM in The Presence of Carrier Frequency Offset on AWGN Channels," IEEE GLOBECOM 2005.

[6]. P. Tan, N. C. Beaulieu, "An Improved DCT-Based OFDM Data Transmission Scheme," IEEE 16th International Symposium on Personal, Indoor and Mobil Radio Communication, 2005.

[7]. H. Schulze and C. Luders, "Theory and Application of OFDM and CDMA Wideband Wireless Communications," John Wiley & Sons. Ltd, pp.145-264, 2005.

[8]. E. Lawrey, "The Suitability of OFDM as A Modulation Technique for Wireless Telecommunications, With A CDMA Comparison," Thesis submitted by Eric Lawrey for the Degree of Bachelor of Engineering with Honours in Computer Systems Engineering at James Cook University, ppt 29-70, in October 1997.

[9]. Jiri Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic Map," Center for Intelligent Systems & Department of Systems Science and Industrial Engineering SUNY Binghamton Binghamton, NY 13902 6000.

[10]. J. Daemen, V. Rijmen, "The Rijndael Block Cipher," AES Proposal: Rijndael, Document version 2, Date: 03/09/99.

[11]. M. Yang , N. Bourbakis, S. Li, "Data-Image-Video Encryption," IEEE POTENTIALS, 2004.

[12]. F. Han, X. Yu, S. Han, "Improved baker map for image encryption," 1st International symposium on systems and control in aerospace and astronautics (ISSCAA), pp. 1273–1276, 19-21 January 2006.

[13]. S. Lian, J. Sun, Z. Wang, "Security analysis of a chaos-based image encryption algorithm," Physica A: Statistical and Theoretical Physics, vol. 351(2-4), pp. 645-661.

[14]. J. L. Horner and B. Javidi, Opt. Eng., vol. 38, Special Issue on Optical Security, 1999.

[15]. B. Javidi, Optical and Digital Techniques for Information Security. New York: Springer, 2005.

[16]. P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett., vol. 20, pp. 767–769, 1995.

[17]. H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, The fractional Fourier transform with Applications in Optics and Signal Processing. (John Wiley & Sons, Chichester, 2001).

[18]. M. Nakazawa, T. Hirooka, F. Futami, and S. Watanabe, “Ideal distortion-free transmission using optical Fourier transformation and Fourier transform-limited optical pulses,” IEEE Photonics Technology Letters, vol. 16, no. 4, pp. 1059–1061, 2004.

[19]. Castro, J. M., I. B. Djordjevic, and D. F. Geraghty, "Novel super structure gratings for optical encryption," J. Lightwave Technol., Vol. 24, 1875-1885, 2006.

[20]. Singh, M., A. Kumar, and K. Singh, "Encryption and decryption using a phase mask set consisting of a random phase mask and sinusoidal phase grating in the Fourier plane," ICOP 2009- International Conference on Optics and Photonics, CSIO, Chandigarh, India, Oct. 30-Nov. 1, 2009.

[21]. Liu S, Yu S, Zhu B: Optical image encryption by cascaded fractional Fourier transforms with random phase filtering. Optics Communications 187 (2001) 57-63.

[22]. Unnikrishnan G, Joseph J, Singh K: Optical encryption by double-random phase encoding in the fractional Fourier domain. Optics Letter 25 (2000) 887-889.

[23]. G. D. Mandyam, "Interspread Sinusoidal Transforms For OFDM Systems," Nokia research center, 2004 IEEE.

[24]. Tan P., & Beaulieu, N. C. (2006). A comparison of DCT-based OFDM and DFT-based OFDM in frequency offset and fading channels. IEEE Transactions on Communications, 54(11), 2113–2125.

[25]. G. D. Mandyam, "On the Discrete Cosine Transform and OFDM Systems," Nokia research center, IEEE 2003.

[26]. Abdullah, K., & Hussain, Z. M. (2007). Performance of Fourier-based and wavelet-based OFDM for DVB-T systems. In Proceedings of the 2007 Australasian telecommunication networks and applications conference, Christchurch, New Zealand.

[27]. Vats, V. B., Garg, K. K., & Abad, A. (2008). Performance analysis of DFT-OFDM, DCT-OFDM, and DWT-OFDM systems in AWGN. In Proceedings of the IEEE fourth international conference on wireless and mobile communications.

[28]. Hilmey, M., S. Elhalafwy, and M. Zein Eldin. “Efficient transmission of chaotic and AES encrypted images with OFDM over an AWGN channel.” In 2009 International Conference on Computer Engineering & Systems, pp. 353-358. IEEE, 2009.

DOI 10.17148/IJARCCE.2020.9337