**Secured OFDM System Using Chaotic Interleaving For Wireless Standards**

**Ankita Shrivastava, Nidhi Singh, Deepak Sharma, Aakash Thakur and Nitesh Garodia**

*Department of Electronics and Communication Engineering*

*Jaypee University of Engineering and Technology*

*Guna (M.P.) 473226, INDIA*

E-mail:- [deepakforu23@rediffmail.com](mailto:deepakforu23@rediffmail.com)

**Abstract:** Multimedia transmission with their security has emerging rapidly and received a lot attention by the researcher working in the communication area in a last decade. In this paper, a new scheme is proposed for transmission of encrypted images based on chaotic interleaving over the Orthogonal Frequency Division Multiplexing (OFDM) a multi carrier modulation system for the wireless standards. In this proposed scheme, from image size the keys are generated with the help of three constants and performing XOR operation between generated keys and selected pixels of image. OFDM system is used for proposed technique due to its use in wireless communication and having capability of high rate data transmission with efficient bandwidth utilization and immunity to the frequency selective fading channels. The simulation results show that proposed schemes reduces the PAPR as compared to conventional schemes and maintains the bit error rate performance and high PSNR of the system especially at low signal to noise ratio. Moreover, our proposed encryption algorithm especially provides better security over advanced encryption standard (AES) and data encryption standard (DES) algorithms with larger key space and smaller encryption decryption time.

**Keywords:** Bit error rate (BER), Chaotic Interleaving,Multicarrier communications, orthogonal frequency division multiplexing (OFDM), Peak to average power (PAPR), Peak to signal noise ratio (PSNR).

1. **Introduction**

The growing demands of multimedia wireless communication require large data rate transmission with high speed and security[1-2]. Multi carrier modulation (MCM) fulfils this requirement very efficiently and provides robustness in fading for multipath channel as well as interference. OFDM is one of the promising multi carrier modulation (MCM) technologies for transmission of data stream over a number of sub-carriers with bandwidth efficiency. It also eliminates inter-symbol interference (ISI) with the help of cyclic preﬁx (CP). The only major disadvantage of OFDM system is envelope fluctuation which leads to high instantaneous peak-to-average power ratio [3]. This important MCM technology, OFDM applied in several applications such as IEEE 802.11a, IEEE 802.16[4], Digital Audio Broadcasting (DAB)[5], Digital Video Broadcasting (DVB)[6], long term evolution (LTE), terrestrial broadcasting, HIPERLAN/2 and 4G mobile communication systems.

Encryption is a process for protecting information from undesirable attacks by converting in the form of non-recognizable format for unknown undesirable users. In OFDM system does not have any inherent security features. Hence, additional encryption/decryption algorithms should be implemented to enable OFDM system data security from hostile attackers. Now all standards have incorporated security feature to ensure that data has been securely transmitted over the channel. Currently various encryption schemes are such as, LTE uses stream ciphers SNOW 3G, ZUC and block cipher AES [7] schemes. GSM uses stream cipher A5 technique [8], etc.

In paper a cyclic prefix OFDM system is implemented with proposed encryption technique to increase the security multimedia specially images. In this scheme chaotic maps are used to build strong interleaves. The proposed interleave is applied to the image prior to modulation. The advantage of the proposed chaotic interleaving scheme is that it increases the key space as the size of data increases by using XOR operation with selected pixel of images and transmitted through OFDM system for wireless standard and raises the security of data.

This paper is organized in four segments. Section II provides an overview of the CP OFDM system along with chaotic interleaving based encryption algorithm along with their mathematical formulation. Section III includes performance parameters, result and their discussion on statistical analysis and describes the superiority by comparing the performance over existing schemes. Last but not least final segment IV, summarizes entire results, concludes remark and suggests the possible scope of scheme in future.

**II. Proposed Scheme**

In this section proposed encryption-OFDM system is described under two phases where first phase discussed the proposed encryption algorithm and second phase focused on the transmission of this encrypted data over CP based OFDM system [9-10].

Figure 1 Overview of proposed encryption-OFDM system

The encryption algorithm is proposed using chaotic[11-13] interleaving which is based on image size and generates key with the help of two constants and performing XOR operations between generated keys and each pixel of image. Consequently, the resultant image is an encrypted image. The inverse of encryption algorithm is applied to decrypt the image i.e. decryption algorithm is suitably applied to retrieve the original image. The major steps of the proposed encryption algorithm are as follows below. The proposed encryption algorithm is represented in form of flowchart:

Figure 2 Flowchart of proposed encryption technique

Mathematical representation of encryption algorithm:

1. Taking size of input image and store it in n and m variable ( let say n=4 and m=4)

1. n1=n\*m\*8
2. Create zero size matrix

1. To generate a key we need two constant

* bin\_x\_N = 0.300001
* x\_N = 0

1. Define the values of zero size matrix

* x\_N = 1 - 2\* (bin\_x\_N)^2
* if x\_N > 0.0 then bin\_x = 1
* bin\_x\_N = x\_N

1. Again form zero matrix of size for storage of key

1. Define the value for key generated matrix using 128\*1 matrix

* key(ind1)=key(ind1)+bin\_x(ind2\*ind1) \* 2 ^ (ind2-1)

1. Xoring between original image and generated key matrix

The resultant of first phase encrypted image is feed as input to OFDM system and this encrypted image is transformed into a serial stream of bits. Thereafter the data is converted into serial to parallel bit stream to form it valid for digital modulation and hence IFFT is performed on parallel data with CP OFDM. The transmitted data of each parallel sub channel is modulated by using quadrature phase modulation. The IFFT is performed to break a wideband signal of bandwidth into narrowband signal using subcarriers hence on these modulated data are processed by IFFT to generate multicarrier OFDM signal with low complexity, fast processing and making it in realizable form. These resultant symbols are sent in a serial manner through the wideband channel. In order to avoid intersymbol interference cyclic prefix guard interval is inserted. Subsequently, at the receiver the guard interval is discarded and received symbols are demodulated using FFT which provides the data symbols. On these received symbols decryption algorithm is applied and original image is retrieved[14]. In figure 3 block diagram shown below illustrates the proposed scheme processing way out.

Figure 3 CP-OFDM System model

The simulation parameters of OFDM system model are listed in Table 1.

**Table 1: OFDM parameters for wireless standard**

|  |  |
| --- | --- |
| FFT length | 128 |
| No. of carriers (carriers count) | 32 |
| Length of guard interval (guard time) | IFFT\_size/4 |
| Bit per symbol | 2(QPSK) |
| Channel Clipping (dB) | 2 |
| Signal to noise ratio (dB) | 5 |
| Bits per word or word size | 8 |
| Length of one symbol (frame length) | IFFT size + guard time |
| Noise environment | AWGN |

**IV. Simulation result**

In this section, the simulation results are demonstrated on Lena and Cameraman test images at different sizes for encryption algorithm, OFDM system and combining encryption algorithm with CP OFDM system for wireless standard IEEE 802.11 and compared its performance over existing schemes. The superiority of proposed scheme is determined using performance parameter PSNR, MSE, key size and BER. These performance parameters are given by,

(1)

(2)

Where*,* and are the input and output image respectively of size

The bit error rate (BER) expressed as the number of bit errors per unit time. It is a dimensionless quantity and expressed as mathematically,

(3)

In the simulation, Lena image of size 400\*400 is tested on proposed model. Figure (5) shows the simulation result.

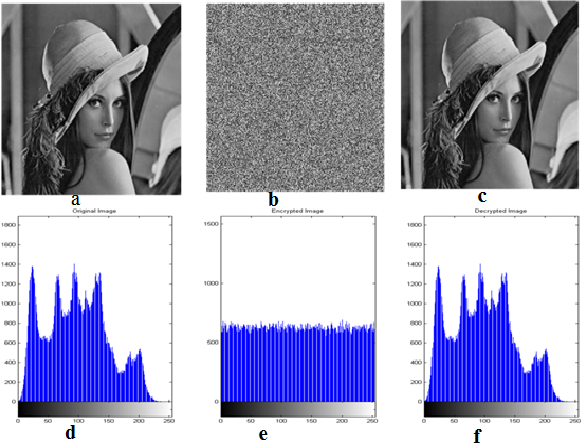


Figure5: Simulation results of proposed encryption algorithm

In figure (5) image (a) is original image, image (b) is the encrypted version of original image and image (c) is the final output image and (d), (e), (f) are the corresponding histograms of original, encrypted and final output image respectively.

Then Lena image is transmitted using OFDM without chaotic interleaving with different bit energy to noise ratio(SNR) in the presence of additive white Gaussian noise (AWGN). QPSK is used for baseband modulation.128 subcarriers are used in OFDM and a guard interval length = 1/4 of the symbol duration is implemented. The simulation results are shown in Figure (6).

Figure 6 Received Image through only

OFDM

Figure 6 shows simulation result of experiment with different SNR value. Figure (a) is at

Eb/No=5dB, PSNR= 58.99, figure (b) is at Eb/No=10dB, PSNR= 67.72, figure (c) is at

Eb/No=15dB, PSNR= 68.65.

Next we have compared the encryption and decrypted time of proposed algorithmfordifferent size of Lena image. From table it can be concluded that as image size is increasing encryption and decryption time is also increasing.

Table 2: Analysis Encryption and Decryption Times (sec) of proposed algorithm with

Different image size

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TEST DATA=LENA** | **IMAGE SIZE** | **ENCRYPTED TIME** | **DECRYPTED TIME** | **MSE** | **PSNR** |
| **DATA 1** | 200\*200 | 0.287030 | 0.020428 | 0.297025 | 53.40 |
| **DATA 2** | 250\*250 | 0.149467 | 0.031040 | 0.190096 | 55.34 |
| **DATA 3** | 300\*300 | 0.185822 | 0.056403 | 0.132011 | 56.92 |
| **DATA 4** | 400\*400 | 0.195845 | 0.089081 | 0.074256 | 59.42 |
| **DATA 5** | 500\*500 | 0.268797 | 0.164309 | 0.047524 | 61.36 |
| **DATA 6** | 600\*600 | 0.426025 | 0.278919 | 0.033003 | 62.94 |
| **DATA 7** | 700\*700 | 0.522826 | 0.420782 | 0.024247 | 64.28 |

Next, we have compared the proposed encryption algorithm with existing algorithm [15] on various parameters.

Table 3: Comparison of Proposed Encryption Algorithms (Lena.jpg)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **DES ALGORITHM** | **AES ALGORITHM** | **PROPOSED ALGORITHM** |
| **IMAGE SIZE** | 128\*128 | 128\*128 | 128\*128 |
| **KEY SIZE** | 2^56 | 2^128 | 16384\*1 |
| **ENCRYPTION TIME(SEC)** | 215.9359 | 99.871 | 0.139393 |
| **DECRYPTION TIME (SEC)** | 183.5455 | 84.9404 | 0.007583 |
| **MSE** | 8185.4343 | 8149.8396 | 0.2755159 |
| **PSNR** | 7.6057 | 7.5523 | 48.82 |
| **AVERAGE ENCRYPTION TIME** | 0.54238 | 0.9192 | 0.244850 |

From above table we can conclude that proposed algorithm is better in terms of MSE, PSNR as compared with existing algorithm. In the above table average encryption time is calculated for 13 test data.

In next experiment, comparison of only OFDM system for image transmission with existing system in terms of PSNR for Lena and Cameraman image is done. From the results in table it can be concluded that for lower values of SNR our OFDM system is much better and for higher values of SNR system is giving constant values.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **SCHEME**  **IMAGE** | **EXISTING SYSTEM**  **Eldokany et.al.(2015)[16]** | | **EXISTING SYSTEM**  **E.M. El-Bakary et.al.[17]** | | **PROPOSED SYSTEM** | |
| **SNR** | **PSNR** | **SNR** | **PSNR** | **SNR** | **PSNR** |
| **CAMERAMAN** | 5 | 23.78 | - | - | 5 | 54.54 |
| 10 | 48.05 | - | - | 10 | 58.66 |
| 15 | >60 | - | - | 15 | 59.22 |
| **LENA** | - | - | 2 | 31.7 | 2 | 50.33 |
| - | - | 4 | 35.9 | 4 | 51.97 |

Table 4: Comparison of only OFDM system with Existing OFDM system [16-17]

In next experiment, Lena image of image size 500\*500 is transmitted using OFDM with chaotic interleaving with a bit energy to noise ratio Eb/N0 = 5 dB in the presence of additive white Gaussian noise (AWGN). QPSK is used for baseband modulation. 128 subcarriers are used in OFDM and a guard interval length = 1/4 of the symbol duration is implemented. Simulation results of the experiment are shown in Figure (7).

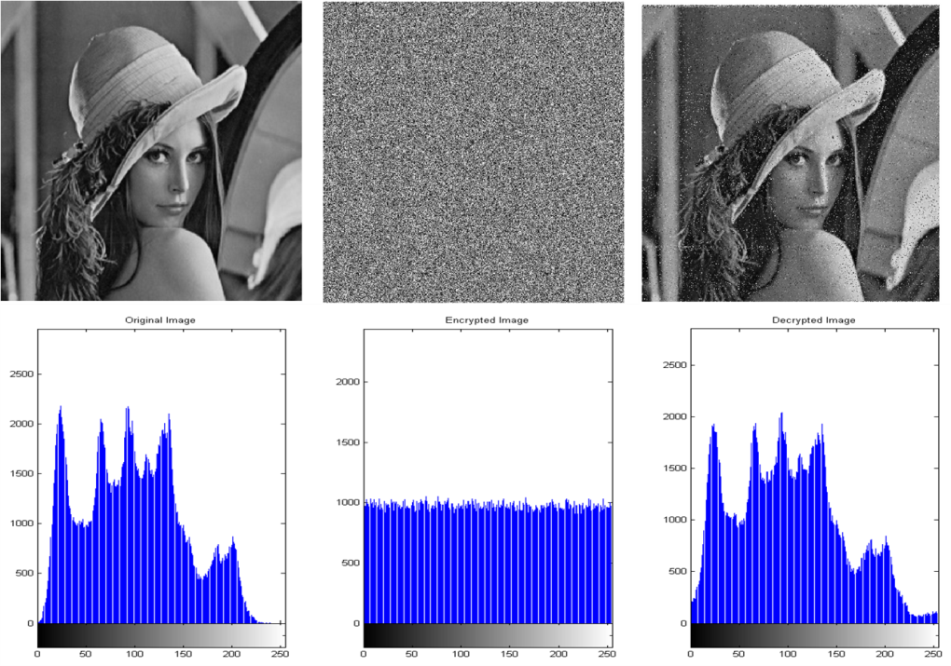


Fig 7: Simulation results of proposed encryption algorithm with OFDM System

In next experiment, Lena image of different sizes is transmitted using OFDM with chaotic interleaving with a bit energy to noise ratio Eb/N0 = 5 dB in the presence of additive white Gaussian noise (AWGN) and QPSK and compared on the basis of PAPR (peak average power ratio), BER (bit error rate), transmitted and received OFDM time. Hence, from table 5 we can conclude that as size of image is increasing transmitted and received OFDM time is increasing but PAPR, BER is reducing with very small variation.

Table 6: Analysis of proposed Encryption algorithm with CP-OFDM system (lena.jpg)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TEST IMAGE LENA** | **IMAGE SIZE** | **ENCRYPTED TIME (in sec)** | **DECRYPTED TIME(in sec)** | **MSE** | **PSNR**  **(db)** | **BER**  **(%)** | **PAPR**  **(db)** | **OFDM**  **Tx** | **OFDM**  **Rx** |
| **DATA 1** | 200\*200 | 0.0189 | 0.018619 | 0.6969 | 49.69 | 13.48 | 12.92 | 1.22 | 0.44 |
| **DATA 2** | 250\*250 | 0.0323 | 0.033345 | 0.6970 | 49.69 | 10.69 | 13.32 | 1.92 | 0.59 |
| **DATA 3** | 300\*300 | 0.0462 | 0.044969 | 0.6953 | 49.70 | 8.90 | 13.52 | 2.24 | 0.70 |
| **DATA 4** | 400\*400 | 0.0936 | 0.101008 | 0.6968 | 49.69 | 8.64 | 13.70 | 4.25 | 1.18 |
| **DATA 5** | 500\*500 | 0.1673 | 0.161061 | 0.6982 | 49.69 | 8.44 | 13.60 | 7.17 | 2.08 |
| **DATA 6** | 600\*600 | 0.2670 | 0.260265 | 0.6990 | 49.68 | 7.82 | 13.84 | 11.77 | 3.14 |
| **DATA 7** | 700\*700 | 0.4116 | 0.405281 | 0.6998 | 49.68 | 8.18 | 14.19 | 19.51 | 4.82 |

**V. Conclusion**

In this paper, we have implemented and concluded the performance of FFT-OFDM for the transmission of chaotic interleaving encrypted images over AWGN using QPSK modulation. From all the results, we can conclude that for smaller values of SNR proposed OFDM system is 52.03% better than existing OFDM system for cameraman image and 37 % for lena image and for higher value of SNR it reduce upto 3% for cameraman image . The PSNR value keeps on increasing for proposed encryption algorithm if we keep on increasing the size of image and correspondingly MSE value keeps on decreasing. Comparing proposed algorithm with existing algorithm, proposed encryption algorithm is better since it take less encryption and decryption time. Also the PSNR values are better than existing AES and DES encryption algorithm. It also reveals that as data size increases MSE and BER reduces and PSNR is increasing gradually.

**References**

[1] J. G. Andrews, A.Ghosh and R. Muhamed, “Fundamentals of WiMAX”, Pearson Education, Inc. 2007.

[2] W. Webb, “Wireless Communications”: The Future, John Wiley & Sons Ltd, 2007.

[3] Litsyn S. “Peak power control in Multi-Carrier Communications”, 1st Edition, Cambridge, pp. 209-252 (2007).

[4] “Air Interface for Fixed Broadband Wireless Access Systems” IEEE Standard 802.16, Part 16, 2004.

[5] European Telecommunnication Standard, Radio broadcasting system: digital audio broadcasting

to mobile, portable, and ﬁxed receivers, ETS 300 401, 1996.

[6] European Telecommunication Standard, Radio broadcasting system: Digital broadcasting system

Television, sound, and data services Framing structure, channel coding, and modulation digital

Terrestrial television, ETS 300 744,1996.

[7] 3GPP System Architecture Evolution (SAE): Security Architecture 3rd Generation Partnership Project,Technical Specification Group Services and Systems Aspects.3GPP TS 33.401 v11.0.1.Release June 11, 2011.

[8] L.Chen and G. Gong. In “Communication system security”, Boca Raton, USA: CRC Press, 2012.

[9] G. D. Mandyam,“ On The Discrete Cosine Transform And OFDM Systems”, Nokia research center, IEEE 2003.

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

[11] Suryadi MT, Eva Nurpeti, Dhian Widya,“Performance of Chaos-Based Encryption Algorithm for Digital Image”,TELKOMNIKA, Vol.12, No.3, September 2014.

[12] Huan Zhang, Ruhua Cai ,“Image Encryption Algorithm Based on Bit-Plane Scrambling and Multiple Chaotic Systems Combination”, IEEE 978-1-4244-6837-9/10/ 2010.

[13] Abhishek Misra Ashutosh Gupta Damodar Rai,”Analysing the Parameters of Chaos Based Image Encryption Schemes” World Applied Programming, Vol (1), No (5), December 2011.

[14] M. Hilmey, S. Elhalafwy, and M. Zein Eldin,”Efficient Transmission of Chaotic and AES Encrypted Images with OFDM over an AWGN Channel” IEEE 978-1-4244-5844-8/09/2009

[15] Mitali, Vijay Kumar and Arvind Sharma, ”A Survey on Various Cryptography Techniques” International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),

Volume 3, Issue 4, July-August 2014.

[16] Ibrahim Eldokany1, El- Sayed M. El-Rabaie1,”Efﬁcient Transmission of Encrypted Images with OFDM in Presence of Carrier Frequency Offset” Springer Science+Business Media New York 2015.

[17] E.M. El- Bakary, O Zahran, S. A. El- Dolil, and F. E. Abd El-Samie “Chaotic Maps: A Tool to Enhance the Performance of OFDM Systems”, International Journal of Communication Networks and Information Security (IJCNIS),Vol. 1, No. 2, August 2009.

**Author’s Biography**

**Deepak Sharma** earned his M. Tech. (Microwave Engineering) honors from Madhav Institute of Technology and Science (MITS), Gwalior (M.P.) in 2006. Currently working as an Assistant Professor in Jaypee University of Engineering and Technology (JUET), Guna Before joining JUET, he worked as a Lecturer in the Department of Electronics at MITS, Gwalior (M.P.). Presently, he is pursuing his Ph.D. degree from Jaypee University of Engineering and Technology, Guna.

His Research areas include Antenna Theory, Radar System, Signal processing, Image processing and Integral Transforms.