Fibonacci Multichaos Algorithm for Medical Image Encryption for Transmission Through Wavelet Transform Based OFDM System and Its VLSI Realization

https://doi.org/10.3991/ijoe.v18i06.30281

Ch.Gangadhar(✉), Md. Habibulla, T.Mahalakshmi, D.Praveena, Ch.SriLakshmi, K.Phani Rama Krishna
PVP Siddhartha Institute of Technology, Vijayawada, India
gangadharch1111@gmail.com

Abstract—At every stage of the digital media transfer, storage, and retrieval process, sensitive images are rendered indecipherable through the use of image encryption. Germany's hospitals have relied on image encryption for years to keep patient data from being accessed by the IT personnel, stolen or left recorded into the network system that could be compromised remotely. In order to encrypt a file manually, the process is extremely time- and effort-consuming. Automating this process while retaining high security is desirable. In this research, we present an approach for encrypting medical images that combines scientific computing with cryptography. This algorithm uses the Fibonacci Multi Chaos Algorithm to encrypt medical images, making them more secure. Distinct wavelet transform orthogonal frequency division multiplexing is used to convey picture data in this work, which is a reliable and secure method.

Keywords—Fibonacci transform, chaos, cryptography, VLSI, WOFDM

1 Introduction

Multiplexing OFDM, or Orthogonal Frequency Division Multiplexing, is an acronym that stands for Orthogonal Frequency Division. It's impossible for two subcarriers to interfere with one another because they're orthogonal, there aren't any "guard bands" for signal recovery. are no "guard-bands" for signal recovery [1]. Wireless networks are built on the Fourier transform in order to keep up with high-speed requirements, which allows you to divide information into elementary frequencies. In order to make our representations more accurate, we use wavelet bases instead of analogized sines and cosines, which may not be as effective for representing signals [2]. Even if wireless communication is becoming increasingly vital in our daily lives, we also know that the current techniques of data transfer are inefficient [3]. Different frequency components are scaled down using the wavelet transform, an operation in mathematics [4].

Image processing and speech analysis are two areas where this process can be used. Analysis of time-series data using wavelets is an alternative to the Fourier transform

method. A wavelet transform can decompose a time series into different frequencies without losing much information at low frequencies or high frequencies [6]. It is also worth noting that wavelets have been used in a wide range of applications from image compression to video coding.

Our new wavelet technology has been proven to be a better solution for transmitting data wirelessly than traditional approaches. This means faster downloads and lower bandwidth usage on your cell phone bill. Control of neighbouring subcarriers can be achieved using a wavelet transform-based system [9]. Wireless networks in remote and private locations can now be accessed more easily [10]. It provides an efficient coding scheme, which is especially designed for the applications of video transmission [11-12]. Wavelets have found a wide range of applications in signal processing such as image compression, speech recognition, seismic analysis etc... More recently they have become popular tools in machine learning algorithms due to their ability to capture both local and global information from signals or images [13-14]. For both individuals and businesses, digital images can be a valuable asset. However, the high monetary value of images on the internet poses a serious threat to their safety [15-17].

This paper's Fibonacci chaos image encryption algorithm and wavelet transform-based Orthogonal Frequency Division Multiplexing can be used to secure the transmission and reception of protected images (WOFDM).

2 The proposed image crypto algorithms using Fibonacci multichaos algorithm

Creating subchaoses in a chaotic system, which can be defined as a single-dimensional state-ergodic properties and initial value sensitivity are all included in this logistical mapping. A chaotic system has strange attractors and sensitive dependence on initial conditions. The three chaotic matrices X0, X1 and X2 can be used to measure chaotic sequences because of different initial values. The function described by:

$$s(j+1) = \mu s(j)(1 - s(j)) \tag{1}$$

where $\mu = 3.9,3.7\ and\ 3.5.$ are used.

Let the three chaotic sequence matrices S_0, S_1, and S_2. then encrypted matrix:

$$E = S0\ xor\ S1\ xor\ S2\ xor\ g \tag{2}$$

Let g indicate an image matrix of size OxP pixels and g(x, y) , $0 \le x \le O - 1,0 \le y \le P - 1$,be gray level of g at location (x, y).The encrypted image matrix denoted by E. In order to scramble the marix E, the Fibonacci Transform is used.

On the image matrix E, the Fibonacci Transform is then applied, scrambling the image and producing the image E2.

The Fibonacci sequence is a recursive one and is defined by the Fibonacci Transform.

$$F_p(i)=\begin{cases}0 & i<0\\ 1 & i=0\\ F_p(i-1)+F_p(i-p-1) & i>0\end{cases} \tag{3}$$

The Fibonacci sequence has been constructed using the equation (1). Using any four consecutive terms of the Fibonacci numbers, a 2-by-2 matrix can be created that can be used to scramble an image. This mask can be described in general as a Fibonacci mask.

$$\begin{bmatrix}x_{new}\\ y_{new}\end{bmatrix}=\begin{bmatrix} f_i & f_{i+1}\\ f_{i+2} & f_{i+3}\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix} \tag{4}$$

Where x,y, x_{new} ,y_{new} ∈ 0,1,2,3,4,… fi is the ith term of the Fibonacci series. $\begin{bmatrix}x\\ y\end{bmatrix}$ Is the original image's pixel coordinate and xnew,ynew is the scrambled image's pixel coordinate. Image scrambling is possible with this scanner.

a) Fibonacci transform-based encryption at the transmitter:

- As an image, the matrix E will be read. To ensure the best possible quality, the image or matrix must be processed into a squared matrix.
- Using a Fibonacci input matrix, E2 is generated by randomly rotating the individual elements of E.

Wavelet transform based Orthogonal Frequency Division Multiplexing (WOFDM) is used to transmit the encrypted image E2 and the received image is decrypted using the decryption algorithm, as described below.

b) Fibonacci transform based receiver:

The image E can be generated by the inverse of the Fibonacci transform described in [5].

$$\begin{bmatrix}x_{new}\\ y_{new}\end{bmatrix}=\text{inverse}\begin{bmatrix} f_i & f_{i+1}\\ f_{i+2} & f_{i+3}\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix} \tag{5}$$

c) Decryption method using chaos at the receiver:

The three chaotic sequence matrices S_0, S_1, and S_2 are generated using equation (1):

$$gconstructed = S0\ xor\ S1\ xor\ S2\ xor\ E$$

3 Implementation of Discrete Wavelet Transform (DWT) OFDM system

Structures for the two-level inverse wavelet packet data transform and the wavelet packet data transform are shown in Figure 1a and Figure 1b.

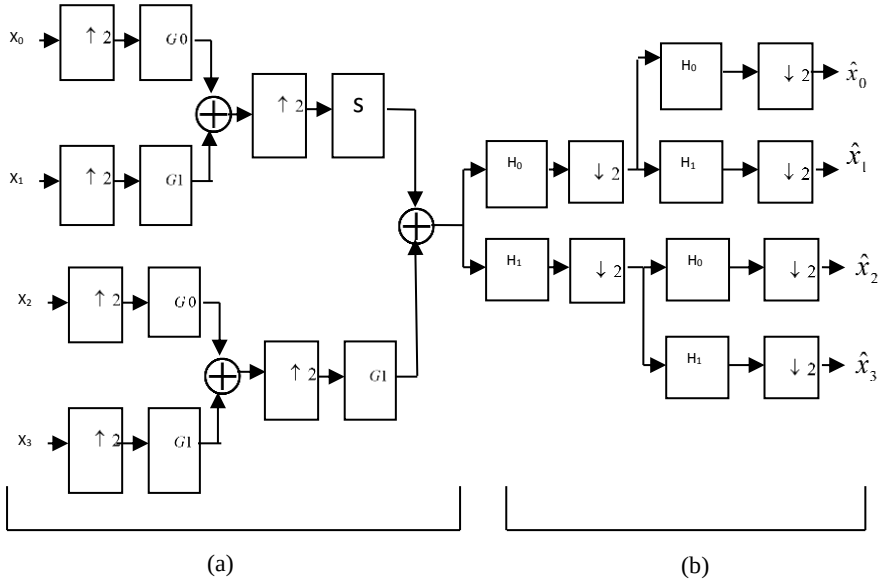

Fig. 1. (a) Two level inverse wavelet packet transform structure (b) Two level wavelet packet transform structure

Following are descriptions of highpass and lowpass wavelet packet transform filters, both in the forward and inverse directions.

$$g = \frac{1}{4\sqrt{2}}[1+\sqrt{3},\ 3+\sqrt{3},\ 3-\sqrt{3}, 1-\sqrt{3}\ ] \tag{6}$$

$$h = \frac{1}{4\sqrt{2}}[1-\sqrt{3},\ -3+\sqrt{3},\ 3+\sqrt{3},\ -1-\sqrt{3}\ ] \tag{7}$$

$$g_{inverse} = \frac{1}{4\sqrt{2}}[3-\sqrt{3},\ 3+\sqrt{3},1+\sqrt{3},1-\sqrt{3}\ ] \tag{8}$$

$$h_{inverse} = \frac{1}{4\sqrt{2}}[1-\sqrt{3},\ -1-\sqrt{3},3+\sqrt{3},-3-\sqrt{3}\ ] \tag{9}$$

In the case of a reversible transformation, the discrete wavelet transform can be used without loss.

4 Result analysis

Our Fibonacci transform encryption, decryption, and DWT OFDM were designed using VHDL and XILINX FPGA and Mentor Graphics Model Simulation tools. Figure 2 shows the CTSCAN (Lungs Image) data, while Figure 3 shows the encrypted image. Figure 4 shows the decrypted image after the encrypted image was transmitted through OFDM using a discrete wavelet transform.

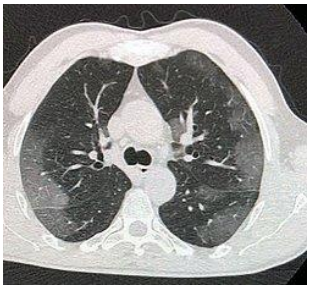

Fig. 2. CTSCAN original image

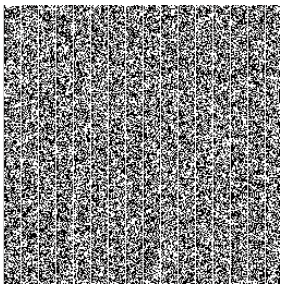

Fig. 3. CTSCAN encrypted image

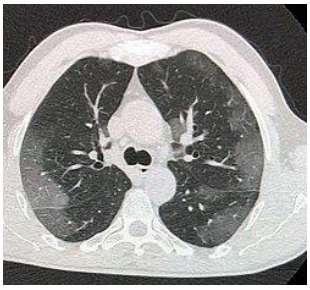

Fig. 4. Received CTSCAN image

Table 1 summarises the resources needed to implement the Fibonacci transform encryption and discrete wavelet transform based OFDM on an FPGA using Xilinx ISE.

Table 1. FPGA (Field Programmable Array) (Kintex) summary of usage

SNO.	Use of Slice Logics	
1	Slice LUTs: the total number.	72945 out of 712000

Summary of Timing: Maximum frequency of clock=47MHZ

5 Conclusion

Fibonacci chaos and discrete wavelet transform based OFDM transmitter and receiver are proposed and implemented in this paper using FPGA.The efficiency of VLSI architecture for the proposed algorithm is demonstrated by implementation of CTSCAN (Lungs Image) image using XILINX FPGA and Mentor Graphics Model Simulation tools.

6 References

[1] L. Hanzo and Keller T, "Adaptive Multicarrier Modulation: A Convenient Framework for Time-Frequency Processing in Wireless Communications." Proceedings of the IEEE 88.5 (2000) 609 – 639. https://doi.org/10.1109/JPROC.2000.849156

[2] T. Nguyen and W. H. Chang, "An OFDM-specified lossless FFT architecture," IEEE Trans. Circuits Syst II: Express Briefs, vol. 53, no. 6, pp. 1235-1243, June 2006. https://doi.org/10.1109/TCSI.2006.875167

[3] B. Kelley, "Software Defined Radio for Broadband OFDM Protocols," Proc. IEEE Intern. Conf. Systems, Man, Cybernetics, San Antoniou, TX, Oct. 2009, pp. 2309-2314. https://doi.org/10.1109/ICSMC.2009.5345986

[4] Jacques Palicot, Rémi Gribonval, and Chafii Marwa, "Wavelet modulation: An alternative modulation with low energy consumption", Comptes Rendus Physique, vol. 18, no. 2, pp. 156-167, Jan. 2017. https://doi.org/10.1016/j.crhy.2016.11.010

[5] Lee Daniel TL and Akio Yamamoto, "Wavelet analysis: theory and applications", Hewlett Packard jouma145, vol. 44, no. 44, 1994.

[6] R. L. Allen et al., Laplacian and orthogonal wavelet pyramid decomposition in coarse to fine registration, IEEE Trans. Signal Proc.41, 12, 3.536-3540, 1993. https://doi.org/10.1109/78.258092

[7] R. L. Allen et al., Laplacian and orthogonal wavelet pyramid decomposition in coarse to fine registration, IEEE Trans. Signal Proc.41, 12, 3.536-3540, 1993. https://doi.org/10.1109/78.258092

[8] Kon Max Wong, Jiangfeng Wu and Tim N. Davidson "Wavelet Packet Division Multiplexing and Wavelet Packet Design Under Timing Error Effects," IEEE Transactions on Signal Processing, Vol. 45, No. 12, December 1997. https://doi.org/10.1109/78.650245

[9] R. A. Haddad and A. N. Akansu, Multiresolution Signal Decomposition, Academic Press, Boston, 1992.

[10] S. G. Mallat, Multifrequency channel decompositions of images and wavelet models, Trans. IEEE Acous. Speech Sig. Proc.ASSP-37, 12, 2091-2110, 1989. https://doi.org/10.1109/29.45554

[11] B. Furht and D. Socek. Multimedia security: encryption techniques. In IEC Comprehensive Report on Information Security, International Engineering Consortium, Chicago, IL, pages 335.349, 2004. https://doi.org/10.1201/9781420038262-3

[12] S. J. Li and X. Zheng, "On the security of an image encryption method," Proc. IEEE International Conference on Image Processing (ICIP 2002), vol.2, pp.925-928, 2002.
[13] N. Masuda .and K. Aihara, "Cryptosystems with discretized chaotic maps," IEEE Trans. on Circuits and Systems - I: Fundamental Theory and Applications, 2002, vol. 49, no. 1, page(s): 28-40. https://doi.org/10.1109/81.974872
[14] Y. Chen, A. Leung, "Bifurcation and Chaos in Engineering", Springer, 1998. https://doi.org/10.1007/978-1-4471-1575-5
[15] Rafeek Mamdouh Tawfiq Yanni, Nashaat El-Khameesy El-Ghitany, Khaled Amer, Alaa Riad, Hazem El-Bakry "A New Model for Image Segmentation Based on Deep Learning", International Journal of Online and Biomedical Engineering, pp. 28-47.2021-07-02. https://doi.org/10.3991/ijoe.v17i07.21241
[16] Rafeek Mamdouh Tawfiq Yanni, Hazem M. El-Bakry, Alaa Riad, Nashaat El-Khamisy "Internet of Things For Surgery Process Using Raspberry Pi" International Journal of Online and Biomedical Engineering, pp. 96-115,2020-09-18. https://doi.org/10.3991/ijoe.v16i10.15553
[17] Mohammed Ateeq Alanezi "A Novel Methodology for Providing Security in Electronic Health Record Using Fuzzy based Multi Agent System" International Journal of Online and Biomedical Engineering, pp. 93-102 .2021-11-15. https://doi.org/10.3991/ijoe.v17i11.25347

7 Authors

Ch.Gangadhar, Md. Habibulla, T.Mahalakshmi, D.Praveena, Ch.SriLakshmi and K.Phani Rama Krishna work at Prasad V. Potluri Siddhartha Institute of Technology in Vijayawada of Andhra Pradesh in India (Corresponding author email Id: gangadharch1111@gmail.com).

Article submitted 2022-02-17. Resubmitted 2022-03-25. Final acceptance 2022-03-31. Final version published as submitted by the authors.

Imprint

iJOE – International Journal of Online and Biomedial Engineering
http://www.i-joe.org

Indexing
International Journal of Online Engineering is indexed in Clarivate Analytics ESCI, IET INSPEC, Elsevier Scopus, DBLP, DOAJ, Ulrich, Microsoft Academic Search, and EBSCO.

Publication Frequency
Monthly

ISSN
2626-8493

Publisher
International Association of Online Engineering (IAOE)
Kirchengasse 10/200
A-1070 WIEN
Austria