Lucas Algorithm for Medical Images Encryption and Transmission using Orthogonal Frequency Division Multiplexing for Medical Health Information Systems and its VLSI Realization

Gangadhar Ch (✉), Md Habibulla
Prasad V. Potluri Siddhartha Institute of Technology,
Vijayawada, India
gangadharch1111@gmail.com

Abstract—Security of medical images is critical for transmission of medical images and relevant patient information through public health information systems networks. Image encryption is an important tool for protecting medical images by converting them into unrecognisable formats for the transmission and reception of medical images. This paper proposes an algorithm for medical image encryption using Lucas Algorithm, and a discrete wavelet transform based transmission and reception technique, which is known as orthogonal frequency division multiplexing (OFDM). This paper presents an implementation of Lucas Algorithm for image encryption and combines it with Discrete wavelet transform orthogonal frequency division multiplexing using Field Programmable Gate Array.

Keywords—Terms: Lucas transform, cryptography, medical image encryption, image decryption, WOFDM, VLSI

1 Introduction

Security of medical images is critical for transmission of medical images and relevant patient information through public health information systems networks. OFDM uses the orthogonality principle. In orthogonal frequency division multiplexing (OFDM), adjacent subcarriers are orthogonal to each other and there are no guard-bands for signal recovery [1]. Fast Fourier Transform is useful as an OFDM transmitter. FFT-based orthogonal frequency division (OFDM) is complex to transmit high speed data. Wireless communications networks are based on technology of Fourier transform. Fourier decomposition decomposes information into elementary frequencies, but these are sines and cosines. The wavelet basis functions are much more compact than sine functions and cosine functions. The wavelet transform refers to different resolutions, in time and space. Wavelet base functions offer a multifaceted solution to wireless communication systems [2]. High-speed data networks are going to boost future communication tools [3-7]. Wavelet transform based system can give

powerful control over neighbour subcarriers. Remote and private wireless networks can now be more easily accessed [8]. The security of digital medical images is extremely vital as images are distributed through the public network [9-10].

This paper proposes Lucas image encryption algorithm and wavelet transform based Orthogonal Frequency Division Multiplexing (WOFDM) for transmission and reception for protected medical image communication.

2 The Proposed Encryption and Decryption Using Lucas Transform Algorithm

The Lucas Transform is used to scramble the input image marix X to generate the image Y.In Lucas Transform , basically, the Lucas sequence is a recursive sequence and defined by.

$$L_p(j) = \begin{cases} 2 & i < 0 \\ 1 & i = 0 \\ L_p(j-1) + L_p(j-p-1) & i > 0 \end{cases} \quad [1]$$

By applying the equation (1) and (2), we have construct the series and Lucas series containing numbers. and Lucas transform can be easily represented as a 2-by-2 matrix by any four consecutive terms of the numbers, this matrix can be used to scramble an image by using a mask. A generalized and Lucas mask can be described in general way.

$$\begin{bmatrix} x_{new} \\ y_{new} \end{bmatrix} = \begin{bmatrix} L_i & L_{i+1} \\ L_{i+2} & L_{i+3} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \quad [2]$$

Where x,y, xnew ,ynew $\in$ 0,1,2,3,4,… fi,Li are the ith term of the and Lucas series. $\begin{bmatrix} x \\ y \end{bmatrix}$ is the pixel coordinate in origin image and xnew, ynew is the new coordinate for the pixel in the scrambled image. This scanner will scramble an image and generate a new photo.

Encryption method using Lucas and transform at the transmitter is shown in figure1 and described as:

1. The input image will be read as a matrix X. It is necessary to process the image or matrix to squared matrix to get the highest possible quality output.
2. Randomly rotates the individual elements of matrix X by using Lucas and transform on input matrix to get matrix Y.

The encrypted image Y is applied to wavelet transform based Orthogonal Frequency Division Multiplexing (WOFDM) for transmission and received image is decrypted using decryption algorithm.

Decryption method using and Lucas transform at the receiver is shown in figure2 and described as:

The original image X can be generated by the inverse of the Lucas transform described in the equation [3].

$$\begin{bmatrix} x_{new} \\ y_{new} \end{bmatrix} = \text{inverse} \begin{bmatrix} L_i & L_{i+1} \\ L_{i+2} & L_{i+3} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \qquad\qquad [3]$$
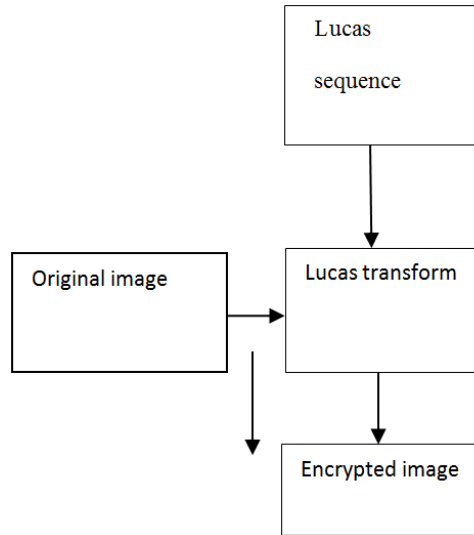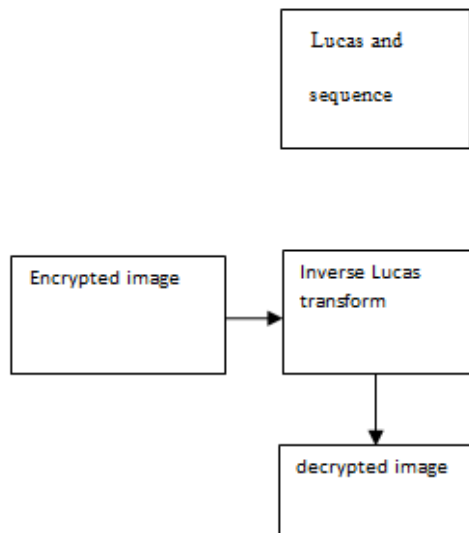
Fig. 1. Encryption Method

Fig. 2. Decryption Method

3 Implementation of Discrete Wavelet Transform (DWT) OFDM System

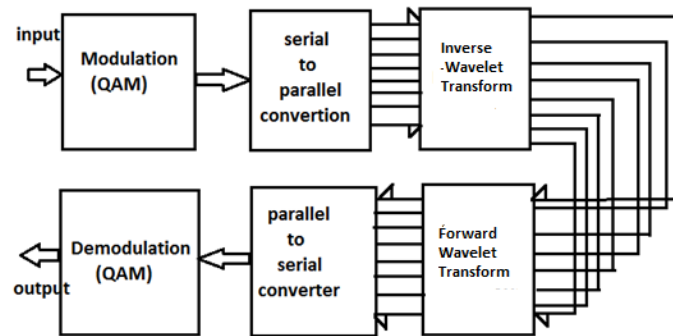The DWT OFDM system was modelled using VHDL and implemented using FPGA is shown in Figure3.

Fig. 3. Shows the setup for a DWT OFDM transmitter and receiver.

The two-level inverse wavelet packet data transform structure and wavelet packet data transform structure are shown in fig.4a and fig.4b.
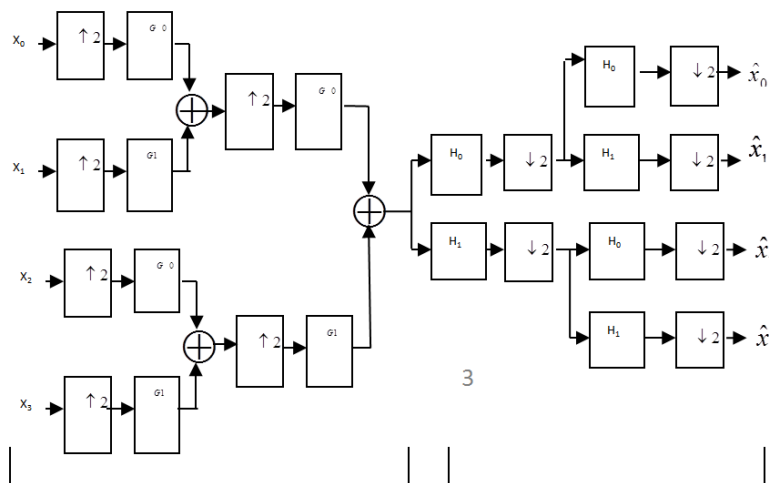

Fig. 4. (a) Two level inverse wavelet packet transform structure
(b) Two level wavelet packet transform structure

Discrete wavelet transform can be used as a reversible and lossless transform. Below are the equations for forward and inverse wavelets transform filters.

3.1   Forward discrete wavelet transform

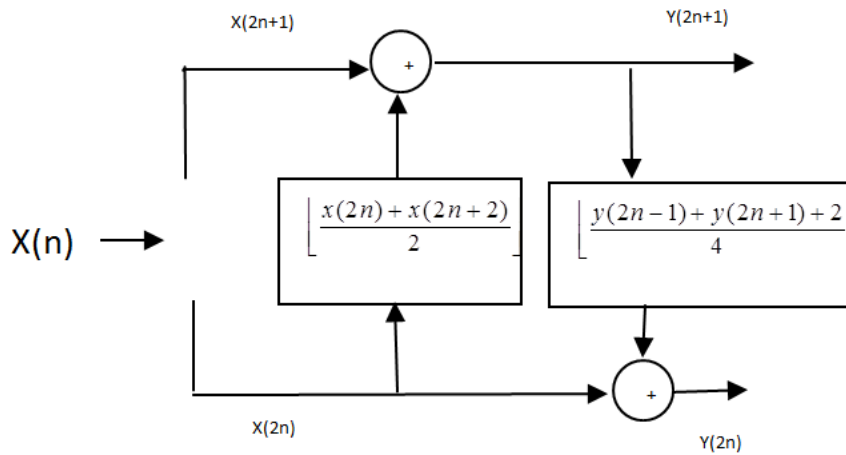$$y(2n+1) = x(2n+1) - \left\lfloor \frac{x(2n) + x(2n+2)}{2} \right\rfloor \qquad (4)$$

$$y(2n) = x(2n) + \left\lfloor \frac{y(2n-1) + y(2n+1) + 2}{4} \right\rfloor \qquad (5)$$

3.2   Inverse discrete wavelet transform

$$x(2n) = y(2n) - \left\lfloor \frac{y(2n-1) + y(2n+1) + 2}{4} \right\rfloor \qquad (6)$$

$$x(2n+1) = y(2n+1) + \left\lfloor \frac{x(2n) + x(2n+2)}{2} \right\rfloor \qquad (7)$$

VLSI Architecture of Wavelet Transform is Illustrated in the fig.5 and fig.6

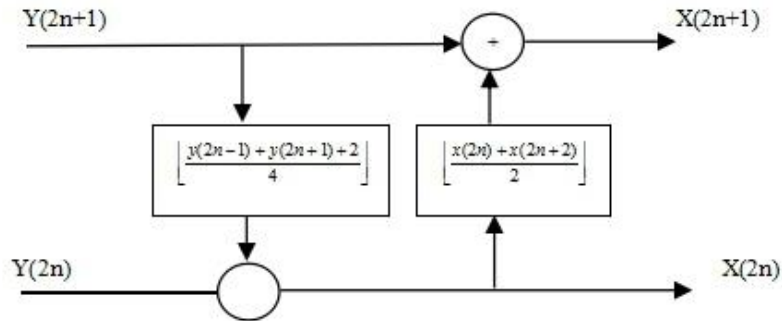**Fig. 5.** Architecture of Discrete wavelet transform

Fig. 6. Architecture of Inverse Discrete wavelet transform

4 Result Analysis

We designed our Lucas and transform encryption, decryption and DWT OFDM using VHDL and executed logic simulation with the use of XILINXISE and ModelSim.

Medical Covid virus image is shown in figure.7 and Encrypted image is shown in figure 8. Encrypted image is transmitted through discrete wavelet transform based OFDM and received image is shown in figure9. CTSCAN image is shown in figure.10 and Encrypted image is shown in figure 11. Encrypted image is transmitted through discrete wavelet transform based OFDM and received and decrypted CTSCAN image is shown in figure12.
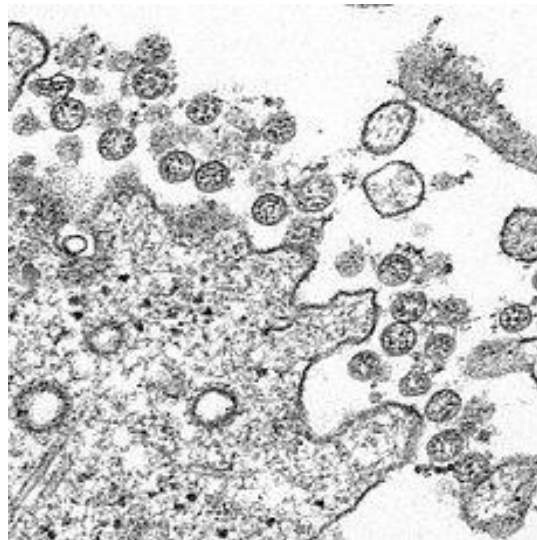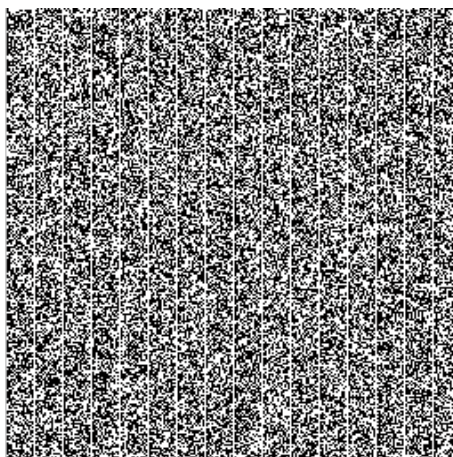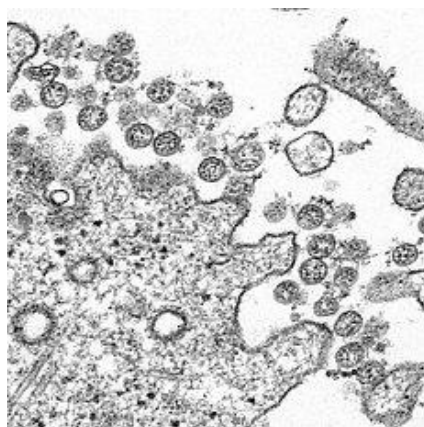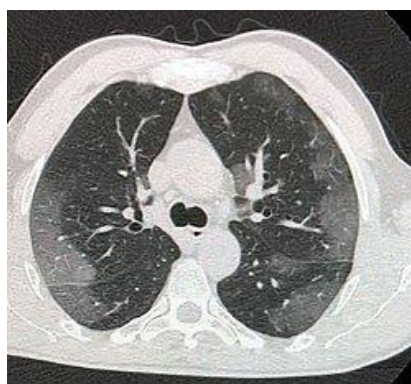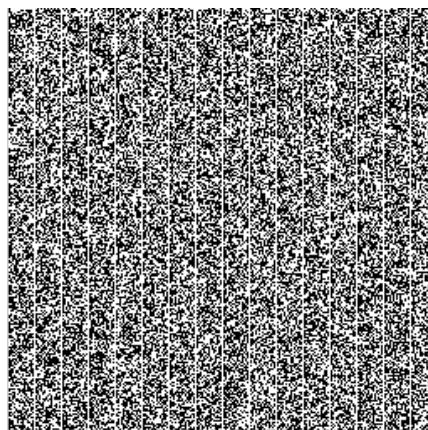

Fig. 7. Medical Covid virus image
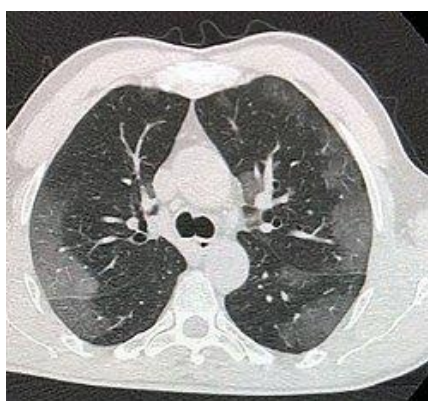
Fig. 8. Medical Covid virus encrypted image

Fig. 9. Received Medical Covid virus image

Fig. 10.CTSCAN Original image

Fig. 11.TSCAN Encrypted image

Fig. 12. Received CTSCAN image

Resource summary used to implement the Lucas and transform encryption and discrete wavelet transform based OFDM using FPGA using Xilinx ISE are shown in table1.

Table 1. FPGA Device(Kintex) utilization summary

SNO.	Slice Logic Utilization	
1	Number of Slice LUTs	73142 out of 712000

Timing Summary:Maximum frequency of clock=46MHZ

5 Conclusion

In this paper, Lucas algorithm based medical image encryption and discrete wavelet transform based OFDM transmitter and receiver is proposed and implemented using

FPGA. The effectiveness of the VLSI architecture designed for the proposed algorithm is demonstrated through the implementation on medical images using XILINXISE and ModelSim.

6   Refrences

[1] W. H. Chang and T. Nguyen, "An OFDM-specified lossless FFT architecture," IEEE

[2] Trans. Circuits Syst II: Express Briefs, vol. 53, no. 6, pp. 1235-1243, June 2006.

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

[4] M. Grangetto, E. Magli, G. Olmo, IEEE Transactions on Multimedia Vol8 (2006) pp905

[5] 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

[6] 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

[7] S. Li, G. Chen, and X. Zheng. Chaos-based encryption for digital images and videos, in B. Furht andD. Kirovski (Eds.), Multimedia Security Handbook,Vol. 4 of Internet and Communications Series, Ch. 3,CRC Press, December 2004. https://doi.org/10.1201/9781420038 262.ch4

[8] D. Socek, S.Li, S. S. Magliveras, and B. Furht, "Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption,"Proc. IEEE First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005, Sep. 2005. https://doi.org/10.1109/securecomm.2005.39

[9] Hatem Elaydi, Personal Health Care System Using IOT, International Journal of Online and Biomedical Engineering (iJOE),Vol 15,No.7. 2019. https://doi.org/10.3991/ijoe.v15i07.102 65

[10] Nohman Khan, Muhammad Imran Qureshi. A Systematic Literature Review on Online Medical Services in Malaysia, International Journal of Online and Biomedical Engineering (iJOE), Vol 16, No.6. 2020.

[11] Mohammad M. Abdellatif, Walaa Mohamed,Telemedicine: An IoT Based Remote Healthcare System, International Journal of Online and Biomedical Engineering (iJOE), Vol 16, No.6. 2020. https://doi.org/10.3991/ijoe.v16i06.13651

7   Authors

Gangadhar Ch and **Md Habibulla** work at Prasad V. Potluri Siddhartha Institute of Technology in Vijayawada of Andhra Pradesh in India. gangadharch1111@gmail.c om, ganga_ch@yahoo.com