Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 12, December 2015, pg.215 – 223

FPGA Implementation of OFDM with Steganography

Linto Thomas, R.Jagadish, M.Pradeep

Sasurie Academy of Engineering Coimbatore, India
lintomon@gmail.com, arsjaga@gmail.com, saepradeep@gmail.com

Abstract- Orthogonal Frequency Division Multiplexing (OFDM) is a multi-carrier modulation technique. It provides high bandwidth efficiency because the carriers are orthogonal to each other and multiple carriers share the data among themselves. The main advantage of this transmission technique is its robustness to channel fading in wireless communication environment. Here we design and implement a baseband OFDM transmitter and receiver. The implementation has been carried out in hardware using Field Programmable Gate Array (FPGA). Both the transmitter and the receiver are implemented on a single FPGA board. The designing has been done in Verilog HDL. And also aims to include an encryption technique called steganography, which ensure the secure transmission of data. In this technique the sender simply hides message by keeping it inside some other file, image, text, audio or video. The steganography does not change the message, instead just hides it from people.

Keywords-Orthogonal Frequency Division Multiplexing (OFDM), Field Programmable Gate Array(FPGA), Synthesis process in verilog HDL, Design Flow, Steganography

I. INTRODUCTION

Demand for broadband access is increasing at a quick rate, and at the same time, is not limited to areas that already have an existing high quality infrastructure. For instance, developing countries and rural areas may not have the existing telecom infrastructure or the existing connections, typically over copper, to meet the requirements of Digital Subscriber Line (DSL) technology. Furthermore, it is expected that users will require more bandwidth on the move. While current technologies can meet this bandwidth demand, the useful range is limited. This limitation opens up opportunities for technologies such as Orthogonal Frequency Division Multiplexing. The increased demands in security aspects of transmission, culminated in the

development of many advanced cryptographic techniques. The steganography is the art and the science of the hidden communications. As the cryptography, the steganography has been practiced for many years. In the past, people made it with hidden tattoos, with invisible inks, wooden charts with wax, among many other methods. Currently the same principle applies when sending some message; the sender simply hides such a message by keeping it inside some other file, image, text, audio or video.

II. ORTHOGONAL FREQUENCY DIVISIOM MULTIPLEXING

Orthogonal frequency division multiplexing (OFDM) is a multi-carrier digital modulation technique that has been recognized as an excellent method for high speed bi-directional wireless data communication. OFDM effectively squeezes multiple modulated carriers tightly together, reducing the required bandwidth but keeping the modulated signals orthogonal so they do not interfere with each other.

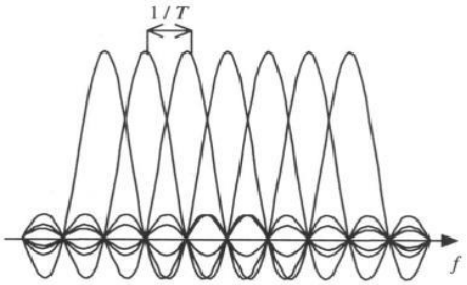


Figure 1 Spectrum Overlap in OFDM

OFDM is similar to FDM but much more spectrally efficient by spacing the sub-channels much closer together (until they are actually overlapping). This is done by finding frequencies that are orthogonal, which means that they are perpendicular in a mathematical sense, allowing the spectrum of each sub-channel to overlap another without interfering with it. Since DFT has heavy computational requirements, therefore, Fast Fourier Transform (FFT) was utilized.

III. FIELD PROGRAMMABLE GATE ARRAY

By modern standards, a logic circuit with 20000 gates is common. In order to implement large circuits, it is convenient to use a type of chip that has a large logic capacity. A field programmable gate arrays (FPGA) is a programmable logic device that support implementation of relatively large logic circuits. FPGA is different from other logic technologies like CPLD and SPLD because FPGA does not contain AND or OR planes. Instead, FPGA consists of logic blocks for implementing required functions. An FPGA contains 3 main types of resources: logic blocks, I/O blocks for connecting to the pins of the package, and interconnection wires and switches. The logic blocks are arranged in a two-dimensional array, and the interconnection wires are organized as horizontal and vertical routing channels between rows and columns of logic blocks. The routing channels contain wires and programmable switches that allow the logic blocks to be interconnected in many ways. FPGA can be used to implement logic circuits of more than a few hundred thousand equivalent gates in size. Equivalent gates is a way to quantify a circuit's size by assuming that the circuit is to be built using only simple logic gate and then estimating how many of these gates are needed.

IV. VERILOG HDL

Verilog HDL is one of the two most common Hardware Description Languages (HDL) used by integrated circuit (IC) designers. The other one is VHDL.HDL allows the design to be simulated earlier in the design cycle in order to correct errors or experiment with different architectures. Designs described in HDL are technology-independent, easy to design and debug, and are usually more readable than schematics, particularly for large circuits. Verilog can be used to describe designs at four levels of abstraction:

- Algorithmic level (much like c code with if, case and loop statements).
- Register transfer level (RTL uses registers connected by Boolean equations).
- Gate level (interconnected AND, NOR etc.).
- Switch level (the switches are MOS transistors inside gates).

The language also defines constructs that can be used to control the input and output of simulation. More recently Verilog is used as an input for synthesis programs which will generate a gate-level description (a netlist) for the circuit. Some Verilog constructs are not synthesizable. Also the way the code is written will greatly affect the size and speed of the synthesized circuit.

A . Synthesis Process in Verilog HDL

Synthesis is to construct a gate-level net list from a model of a circuit described in Verilog. The synthesis process is described in diagram below

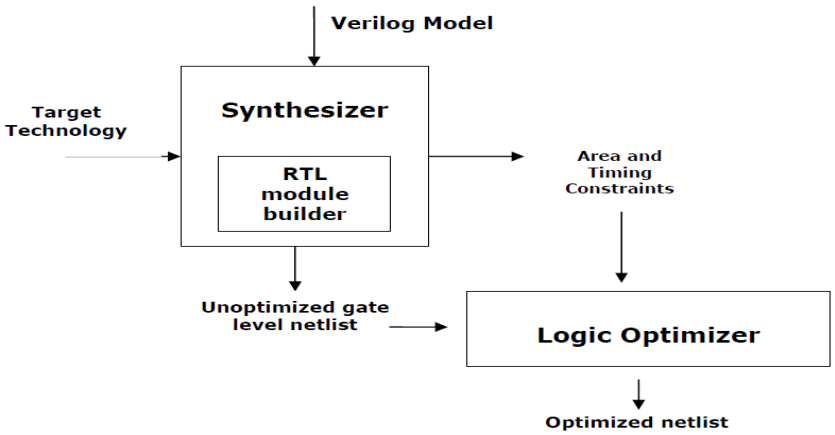


Fig 2 Synthesis process in Verilog HDL

A synthesis program may generate an RTL net list, which consists of register-transfer level blocks such as flip-flops, arithmetic-logic-units and multiplexers interconnected by wires. All these are performed by RTL module builder. This builder is to build or acquire from a library predefined components, each of the required RTL blocks in the user specified target technology. The above synthesis process may produce an optimized gate level net list. A logic optimizer can use the produced net list and the constraint specified to produce an optimized gate level net list. This net list can be programmed directly into a FPGA chip.

V. BLOCK DIAGRAM AND DESCRIPTION

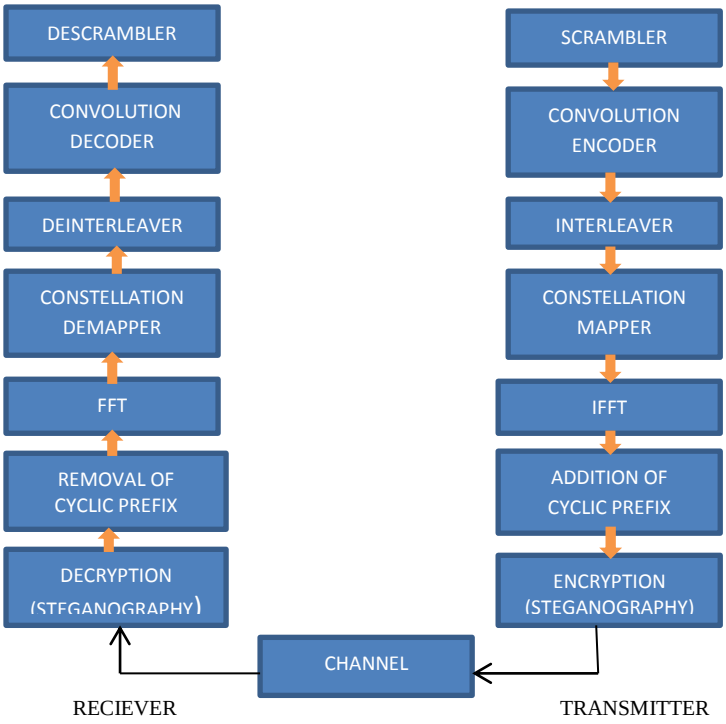


Fig 3 Block Diagram representation of the System

A. Transmitter Section

Transmitter section consists of Scrambler, Convolution Encoder, Interleaver, Constellation Mapper, IFFT, Addition of Cyclic Prefix and Encryption which is nothing but the Steganography

1) *Scrambler:* A scrambler (often referred to as a randomizer) is a device that manipulates a data stream before transmitting. Data bits are given to the transmitter as inputs. These bits pass through a scrambler that randomizes the bit sequence. The purpose of scrambling is to eliminate the dependence of a signal's power spectrum upon the actual transmitted data and making it more disperse to meet maximum power spectral density requirements, because if the power is concentrated in a narrow frequency band, it can interfere with adjacent channels .

1.1) *Algorithm*

Step1: Initialize random 8bit value in the shift register

Step 2: XOR the fourth and the seventh bit. Let the Output be Y

Step 3: XOR the serial input bi along with Y and it's the bitwise output of the scrambler

Step 4: Right shift the register along with the scrambler output

Step 5: Continue steps 2,3,4

2) *Convolution Encoder:* Convolutional coding is part of the Forward Error Correction (FEC) done in communication systems. The purpose of forward error correction (FEC) is to improve the capacity of a channel by adding some carefully designed redundant information to the data being transmitted through the channel. The process of adding this redundant information is known as channel coding. Convolutional codes operate on serial data, one or a few bits at a time. There are a variety of useful Convolutional, and a variety of algorithms for decoding the received coded information sequences to recover the original data.

2.1) Algorithm

Step 1: Consider this system as a FSM with initial state 00
Step 2: From the 8 bit output of Scrambler take each bit serially. Bits will be 1 and 0
Step 3: If previous state is 00 and input is 0 next state is 00
Step 4: Else if previous state is 00 and input is 1 next state is 01
Step 5: Else if previous state is 01 and input is 0 next state is 10
Step 6: Else if previous state is 01 and input is 1 next state is 11
Step 7: Else if previous state is 10 and input is 0 next state is 00
Step 8: Else if previous state is 10 and input is 1 next state is 01
Step 9: Else if previous state is 11 and input is 0 next state is 10
Step 10: Else if previous state is 11 and input is 1 next state is 11
Step 11: Output of Encoder is a 16 bit value

3) *Interleaver:* Deep fades in the spectrum may cause groups of subcarriers to be less reliable than others, thereby causing bit errors to occur in bursts rather than being randomly scattered. Interleaving is applied to randomize the occurrence of bit errors prior to decoding. At the transmitter, the coded bits are permuted in a certain way, which makes sure that adjacent bits are separated by several bits after interleaving. According to the standard, all data bits must be interleaved by a block interleaver with a block size corresponding to the number of bits in a single OFDM symbol. Interleaving is the reordering of data that is to be transmitted so that consecutive bytes of data are distributed over a larger sequence of data to reduce the effect of burst errors. The use of interleaving greatly increases the ability of error protection codes to correct for burst errors. Many of the error protection coding processes can correct for small numbers of errors, but cannot correct for errors that occur in groups There are two types of interleaver commonly referred as block and convolutional interleaver. In a block interleaver, the input data is written along the row of a memory configured as a matrix, and then read out along the columns. A variation in a block interleaver is a pseudo random block interleaver, in which data is written in memory in a sequential order and read in a psuedo random order. Here we are using block interleaver.

3.1) Algorithm

Step 1: Consider an empty matrix of size 4*4.
Step 2: Input the convolution Encoder output in a Row wise order to the Matrix
Step 3: Take the values from the matrix in a Coloumn wise order and it's the output of interleaver

4) *Constellation Mapper:* The Constellation Mapper basically maps the incoming (interleaved) bits onto different sub-carriers. Different modulation techniques can be employed (such as QPSK, BPSK, QAM etc.) for different sub-carriers. Constellation Mapper maps the incoming bits onto separate sub carriers. In the proposed design there are 64 sub-carriers and each of them is modulated using QPSK, therefore the function of Constellation Mapper would be to map every two bits

on a single carrier, because in QPSK two bits make up one symbol.Figure shows the constellation diagram of QPSK. Mapping of bits on constellation points is done in accordance with gray code so that adjacent constellation points may have just one bit different.

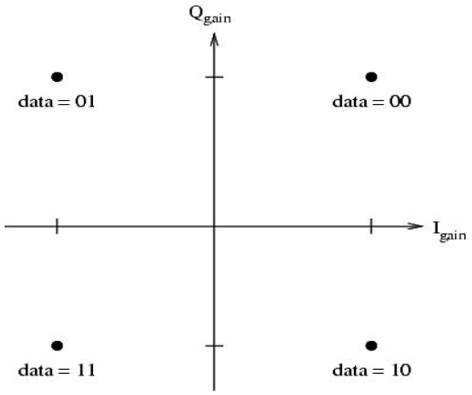


Figure 4 QPSK constellation diagram

4.1) Algorithm

Step 1: Input of QPSK is Taken as each consecutive 2 bits from the output of Interleaver.
Step 2: If the input is 00 map the data to a carrier having 64 sub carriers 0,2,4,6,8,.....126
Step 3: If the input is 01 map the data to a carrier having 64 sub carriers 30,32,34....156
Step 4: If the input is 10 map the data to a carrier having 64 sub carriers60,62,64….186
Step 5: If the input is 11 map the data to a carrier having 64 sub carriers 90,92,94…216
Step 6: Each of the carriers are phase shifted 90 degrees .

5) *IFFT:* This is the most important block in the OFDM communication system. In 1971 Discrete Fourier Transform (DFT) was used in baseband modulation/demodulation in order to achieve orthogonality. Since DFT has heavy computational requirements, therefore, Fast Fourier Transform (FFT) was utilized. For an N point discrete Fourier Transform the required number of computations is N(N-1), but that for FFT/IFFT is Nlog (N), which is much lesser than DFT.The FFT/IFFT operates on finite sequences. Waveforms which are analog in nature must be sampled at discrete points before the FFT/IFFT algorithm can be applied. It is IFFT that basically gives OFDM its orthogonally. The IFFT transform a spectrum (amplitude and phase of each component) into a time domain signal. It converts a number of complex data points into the same number of points in time domain. The FFT/IFFT operates on finite sequences. Waveforms which are analog in nature must be sampled at discrete points before the FFT/IFFT algorithm can be applied. The Discrete Fourier Transform (DFT) operates on sample time domain signal which is periodic. The equation for DFT is:

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-j2\pi k / N}$$

X(k) represents the DFT frequency output at the k-the spectral point where k ranges from 0 to N-1. The quantity N represents the number of sample points in the DFT data frame. The quantity x(n) represents the nth time sample, where n also ranges from 0 to N-1. In general equation, x(n) can be real or complex.The corresponding inverse discrete Fourier transform (IDFT) of the sequence X(k) gives a sequence x(n) defined only on the interval from 0 to N-1 as follows

$$x(n) = \frac{1}{N} \sum_{k=0}^{N-1} X(k) e^{j2\pi k / N}$$

The DFT equation can be re-written into:

$$X(k) = \sum_{n=0}^{N-1} x(n) W_N^{nk}$$

The quantity can be defined as:

$$W_N^{nk} = e^{-j2\pi k / N}$$

This quantity is called Twiddle Factor. It is the sine and cosine basis function written in polar form Examination of the first equation reveals that the computation of each point of DFT requires the following: (N-1) complex multiplication, (N-1) complex addition (first term in sum involves ej0 = 1). Thus, to compute N points in DFT require N(N-1) complex multiplication and N(N-1) complex addition. As N increases, the number of multiplications and additions required is significant because the multiplication function requires a relatively large amount of processing time when even using computer. Thus we are using fast fourier transform using radix 2 algorithm. When the number of data points N in the FFT/IFFT is a power of 4 (i.e., N = 4v), we can, of course, always use a radix-2 algorithm for the computation. In the decimation-in-frequency algorithm, the outputs or the frequency domain points are regrouped or subdivided In the decimation-in-frequency IFFT algorithm, the outputs are decimated; therefore, inputs to the IFFT are given in the actual order. In this way we get the output in a rearranged order.

6) *Cyclic Prefix Adder:* Cyclic prefix is basically a replica of a fractional portion of the end of an OFDM symbol that is placed at the beginning of the symbol. It completely removes inter-symbol interference that can occur due to Multipath. Cyclic prefix (CP) is a copy of last part of OFDM symbol. CP is placed in front of the symbol. The reason behind the use of CP is multipath transmission. Cyclic prefix is effective only if its duration is greater than the delay spread. Multipath transmission causes what we call as delay spread. At receiver, signals from direct path and multipath (the copy versions) are received in superposition method. Thus, the received signal suffers degradation or termed as fading. OFDM can minimize the delay spread since it is a parallel transmission such that it has longer symbol duration. However, to solve delay spread completely, guard interval (GI) is used. For OFDM, GI is known as cyclic prefix (CP) as proposed by Peled and Ruiz. The architecture of cyclic prefix adder simply consists of an address ROM that stores addresses, a RAM to store incoming data in sequential order and a counter that provides read addresses to the RAM.

6.1) Algorithm

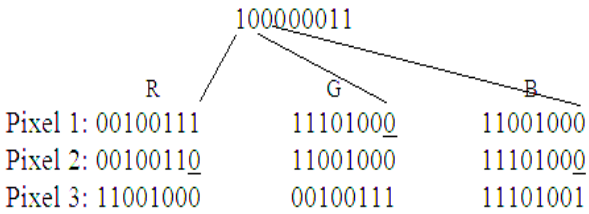
Step 1: Take consecutive 13 bits from IFFT output as input of cyclic prefix adder
Step 2: Copy the last 12 bits of the input
Step 3: Paste it in front of the input
Step 4: Thus a 25 bit Output is formed

7) *Steganography:* In this technique the sender simply hides his message by keeping it inside some other file, image, text, audio or video Here we are using an image to hide the data bits. For this different techniques can be used.in the proposed design we are using the least significant bit insertion technique. This technique is the most popular and simple technique. It takes an image, and reconstructs the original image by hiding the data bits in the pixel codes. Least significant bits of the pixel codes are replaced by the data bits. The Example given below shows the description for steganography.

Example LSB: To insert an A : 100000011 in the 3Pixels RGB:

	R	G	B
Pixel 1:	00100111	11101001	11001000
Pixel 2:	00100111	11001000	11101001
Pixel 3:	11001000	00100111	11101001

The underlined bits are modified bits, the others are equal



Also a secret key steganographic algorithm is described, that given a message aims to hide it into a cover such that even if an attacker detects the existence of the message, the attacker will not be able to recover it without the secret key that is known only to sender and receiver. In this design a memory block stores the values of the pixels of the image which is in the form of say 65×65 matrix. From this large matrix another matrix of smaller size is selected to hide the data. The least significant two bits of each pixel value is replaced by the data bits. Size of the matrix selected for hiding the data is 100×64.Here each input symbol to the steganography is of size 25 bits.1024 such symbols have to be hide inside the image. The image with the hide data is transmitted.

B. Receiver Section

1) *Desteganography:* In the transmitter section the encryption technique steganography is implemented on the data before transmission, in order to secure the data from the outsiders.in steganography data kept hided inside an image and this image is transmitted. That is all the pixel value of the image including the modified pixel values in which data was hided is transmitted. Each pixel value is 8bits.at the receiver these pixel values of these image is received and in desteganography the data is recovered from these pixel values using the secret key. So it is the decryption process and data is recovered from the image.

1.1 Algorithm

Step 1: Receive the image by grouping every 8 bits of serially received data.
Step 2: Select every final 2 bits of the grouped data.
Step 3: Arrange the data to get the actual information

2) *Removal of cyclic prefix* : The cyclic prefix was added at the transmitting end in order to avoid inter symbolic interferences, therefore during reception it must be eliminated for any further processing of the recovered signal. This is done by removing the first 12 bits of the symbols obtained from the desteganography.

2.1 Algorithm

Step 1: take consecutive 25 bits from Desteganography output as input of Cyclic Prefix remover.
Step 2: Remove the first 12 bits of the input.
Step 3: Thus a 13 bit output is formed.

3) *FFT:* Details on FFT/IFFT algorithm and hardware implementation were given above. In order to implement FFT in Hardware algorithm is same. In the proposed design pipelined architecture has been chosen in order to make the FFT design area efficient. Additionally fixed point FFT implementations has been carried out to avoid any overflows resulting from the complex multiplications in the FFT design we are using 8 point radix2 fixed FFT. In the decimation in time FFT algorithm, inputs to the FFT are given in the bit reversal order.in this way we get the output actual order.

3.1 Algorithm

Step 1: Take input to this block as 13 bits.
Step 2: Compute FFT
Step 3: Output of each computation is 8 bit

4) *Constellation Demapper :* The function of the constellation de-mapper is to map the qpsk symbols (complex numbers) coming from the output of FFT to the data points shown in the constellation diagram shown in figure 4. Basically it is the inverse procedure of what was done in the constellation mapper at the transmitter. Therefore basically incoming constellation points are mapped on to the data points.

4.1 Algorithm

Step 1: Input of De-QPSK is taken as each consecutive 64 subcarriers from the output of FFT.
Step 2: If the sub carriers are 0,2,4…126.Then output is 00
Step 3: If the sub carriers are 30,32,34…156.Then output is 01
Step 4: If the sub carriers are 60,62,64.…186.Then output is 10
Step 5: If the sub carriers are 90,92,94.…216.Then output is 11
Step 6: Thus a 16 bit output is formed

5) *Deinterleaver :* In the transmitter section interleaving was defined as a process in which bits, within a block of 16 bits, are re-arranged in order to avoid burst errors. DE-Interleaving performs the inverse task. It re arranges the interleaved bits into their original order. Recall the row-column method of interleaving discussed in the previous section.de interleaving is done the same way, the difference being that interleaver takes the input data in column wise and output row wise

5.1 Algorithm

Step 1: Consider an empty Matrix of size 4*4
Step 2: Input the convolution encoder output in a column wise order to the matrix
Step 3: Take the values from the matrix in a row wise order and it's the output of deinterleaver
Step 4: Bits are rearranged by these process.

6) *Convolution Decoder :* In the transmitter section convolution coding is done as a part of the forward error correction(FEC).Convolution encoder used to code the data. Thus in the transmission section 16 bit coded data is produces corresponding to the 8 bit data. Convolution decoder performs the reverse task. The 16bit coded data is decoded to the 8bit actual data. Following figure shows the input output parameters of the convolution encoder

6.1 Algorithm

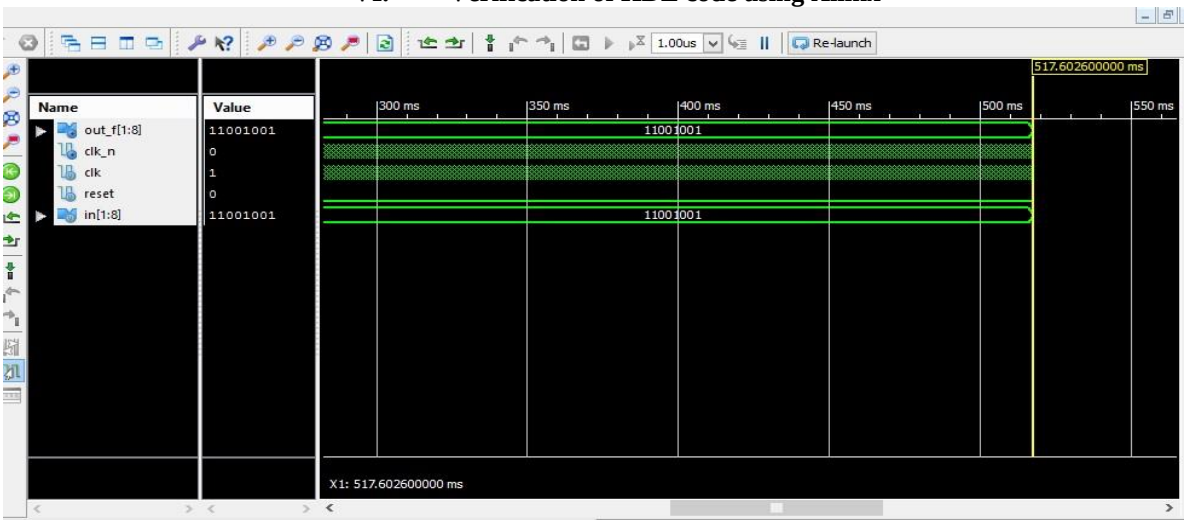
Step 1: Consider this system as a FSM with initial state 00
Step 2: From the 2 bit output of deinterleaver take each bit serially. Bits will be 1 and 0
Step 3: If previous state is 00 and next state is 00 then output is 0
Step 4: Else if previous state is 00 and next state is 01 then output is 1
Step 5: Else if previous state is 01 and next state is 10 then output is 0
Step 6: Else if previous state is 01 and next state is 11 then output is 1
Step 7: Else if previous state is 10 and next state is 00 then output is 0
Step 8: Else if previous state is 10 and next state is 01 then output is 1
Step 9: Else if previous state is 11 and next state is 10 then output is 0
Step 10: Else if previous state is 11 and next state is 11 then output is 1
Step 11: Output of Decoder is a 8 bit value

7) *Descrambler :* This block simply descrambles the scrambled data. A bit is latched at the positive edge of the clock

7.1 Algorithm

Step 1: Initialise random 8bit value in a shift register.
Step 2: XOR the fourth and seventh bit. Let the output be Y
Step 3: XOR the serial input bit from decoder along with Y and it's the OFDM output
Step 4: Right shift the register along with the serial input from decoder output
Step 5: Continue steps 2,3,4 thus we get entire OFDM Output

VI. Verification of HDL code using Xilinx



The proposed system has been verified using Xilinx simulator using Verilog codes. We provided an input data of "11001001"and we received the same data at the output. And also we checked for many other inputs of 8 bits which all showing a positive results. Therefore we can conclude the system is working proper manner.

VII. CONCLUSION

There is some debate as to whether multicarrier or single carrier modulation is better for ISI channels with delay spreads on the order of symbol time. It is claimed in that for some mobile radio applications single carrier with equalisation has roughly the same performance as multicarrier modulation with channel coding, frequency domain interleaving, and weighted maximum likelihood decoding. But there are other problems with multicarrier modulation that impair its performance, most significantly frequency offset and timing jitter, which degrade the orthogonality of the sub channels. In addition the peak to average power ratio of multicarrier is significantly higher than this of single carrier system, which is a serious problem when nonlinear amplifiers are used.Trade offs between Multi carrier and single carrier block transmission system with respect to these impairments are discussed. Despite these challenges multicarrier technique are common in high data rate wireless systems with moderate to large delay speed as they have significant advantages over time domain equalization. In particular the number of taps required for an equalizer with good performance in a high data rate systems is typically large. Thus these equalizers are highly complex. Weights for a large number of equalizer taps in rapidly varying channel. For these reasons, most emerging high rate wireless systems use either multi carrier modulation or spread spectrum to eliminate ISI.OFDM has several interesting properties that suits its use over wireless channels and hence many wireless standards have started to use OFDM for modulation

multiple access.as discussed in our Paper, the simulation results for system was observed. After that the Verilog emulation OFDM systems has been observed using FPGA programme, then we could implement this system on Xilinx Spartan. Steganography transmits secret thorough apparently innocuous covers in an effort to conceal the existence of the secret. Digital image steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking steganography to circumvent such policies and pass messages covertly. In the near future the most important use of steganographic technique will probably be lying in the field of digital watermarking. The possible use of steganography technique is as following: Hiding data on the network in case of a breach, peer to peer private communications, posting secret communications on the web.

REFERENCES

[1] An Evaluation of Software Defined Radio – An Overview, QinetiQ Ltd., 2006.
[2] Alan C. Brooks, Stephen J. Hoelzer, Design and Simulation of Orthogonal Frequency Division Multiplexing (OFDM) Signaling, Final Report, May 15, 2001.
[3] Clause 17, IEEE Std 802.11a, Part 11:Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifications, High-Speed Physical Layer in the 5 GHz Band. 2007.
[4] Subclause 8.3 and appendix B.1.2, IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems, 2009.
[5] Michael F Finneran, WiFi vs WiMAX: A comparison of Technologies, Markets and Business Plans, June 1,
[6] J. Fridich, and R. Du, "Secure SteganographicsMethods for Palette Images", In Information Hiding, 3rdInternational Workshop, Springer 1999,pp. 47-60.
[7] Dulce R. Herrera-Moro, Raúl Rodríguez-Colín, ClaudiaFeregrino-Uribe, "Adaptive Steganography based ontextures" Electronics, Communications and Computers,2007 CONIELECOMP '07 17th international ConferencePage(s): 34 - 34 .
[8] Mehdi Kharrazi, Husrev T. Sencar and Nasir "ImageSteganography: concepts and practice." Memon. PolytechnicUniversity. Broklyn, NY. USA. April 22,2004www.ims.nus.edu.sg/preprints/2004-25.pdf.
[9] Neil F. Johnson, Sushil Jajodia, "ExploringSteganography: Seeing the Unseen ".Journal Title: IEEEComputer. Date: 1998. Volume: 31. Issue: 2. p. 26 – 34.
[10] Farouk, H.A. Saeb, M. " Hybrid Hiding EncryptionAlgorithm (MHHEA) for Data Communication Securitybase on Hybrid Hiding Encryption Algorithm (HHEA) "Comput. Dept., Arab Acad. for Sci., Technol. &Maritime Transp., Alexandria, Egypt; Design,Automation and Test in Europe, 2005. 7-11 March 2005.
[11] Farouk, H. Saeb, M. " Design and implementation ofa secret key steganographic micro-architecture employing FPGA " Dept. of Comput., Arab Acad. for Sci. Technol.& Maritime Transport, Alexandria, Egypt; Design,Automation and Test in Europe Conference and Exhibition, 2004. 16-20 Feb. 2004 Volume: 3, Onpage(s): 212- 217 Vol.3.128

