Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 3976-3984*

Research Article

A Watermark Approach for Image Transmission: Implementation of Channel Coding Technique with Security

G.Aparna[a], P.Hema Sree[b], D.Nagajyothi[c], M.Kezia Joseph[d], B.Rajendra Naik[e]

[a] [a]Research Scholar, Department of Electronics and Communication Engineering, University College of Engineering, Osmania University-500040, Telangana, India
[b]Associate Professor, ECE Department, CVR Engineering College, Ibrahimpatnam, Telangana
[c]Associate professor, ECE DEPARTMENT,Vardhaman College of EngineeringKacharamShamshabadHyderabadTelangana
[d]Professor, ECE Department, Stanley College of Engineering and Technology for Women, Abids, Nampally, Telangana
[e]HoD, ECE Department, University College of Engineering, Osmania University, Hyderabad, Telangana

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: In this paper an approach for secured digital image transmission with watermark is being proposed. The tremendous growth in technology for various applications demand secured communications across the wireless channels. Secured image transmission is the one of the prominent process in digital communication applications. A watermark is embedded in to the image data that is to be protected from unauthorized users. The cryptographic algorithms chosen for secured transmission led to the need for hardware implementation. In the process of secured image transmission turbo encoder is proposed for error correction. The proposed approach is realized in terms of hardware for the digital logic size, area and power consumption using Xilinx 14.2 software. Synthesizing and implementation of verilog code on the target device xc6slx150-2fgg484 for timing constraints, device utilization and performance details.

Selection and/or Peer-review under responsibility of International Conference on Mechanical, Electronics and Computer Engineering

Keywords: Encryption, Digital Image Water marking, turbo coding, JPEG 2000

1. Introduction

The rapid growth in wireless communications and multimedia applications has given good scope for digital image transmission with security. The implementation of the secured algorithms to ensure secured data transmission need hard ware realization in logic size, area and power consumption point of view. Research on secured transmission is focused as the information that is being transmitted through wireless channel is prone to noise mostly for which reason the data gets corrupted. Hence, turbo coded method suggested in the approach can recover the lost or errant data from the received data. The high bit error rates that are caused due to transmission of data through wireless channel can also be overcome with this approach [1]. One of the best solutions to obtain the lost is to incorporate the system with source channel coding. Turbo channel coding with iterative soft decoding provides the better performance which is nearer to optimal Shannon capacity error criteria. In today's advanced multi-media era, the size of the file (Image file) is expected to be as low as possible while preserving the quality of it. To accomplish this JPEG 2000 image standard proves to be the best in class which is very much useful for faster transmission.

The JPEG 2K-standard is low in complexity which made it ease for hardware implementation through VLSI realization [2]. This image standard is based on discrete wavelet transforms (DWT) in coordination with arithmetic entropy coding [3].

In this paper, a digital image watermarking approach with DWT and turbo coding is proposed. This approach also includes transmission of the watermarked image with high security, in order to transit at faster rate it incorporates JPEG2K standard. Lastly it investigates to implement the entire process through VLSI realization.

This paper is organized as follows; section 1 presents the need and necessity of the work and the objectives that were framed to be implemented in the work. Section-2 presents in details description of the proposed approach. Section 3 presents the proposed watermarking technique with turbo coding concluded with experimental results in section5..

2.Proposed Approach

The proposed digital watermarking method consists of JPEG compression and turbo coding at either side of encoder and decoder. This method is meant for quantized DCT bases which consist of three main process steps namely zigzag scanning coding, run length coding and Huffman coding.

When realized in hardware terms using VLSI, zigzag scanning uses dual Random Access Memory (RAM) for faster processing. On the other hand, run length coding counts the intermediate zero in between the successive non-zero Discrete Cosine Transform (DCT) elements to reduce the data size [4]. In order to reduce the complexity of the Huffman coding a lookup table with the frequency of occurrence of particular code pattern value combinations were employed in decreasing order of probabilities which are connected with inconsistent length codes. The entire process flow is designed and implemented using Low power approaches in Verilog HDL [5].

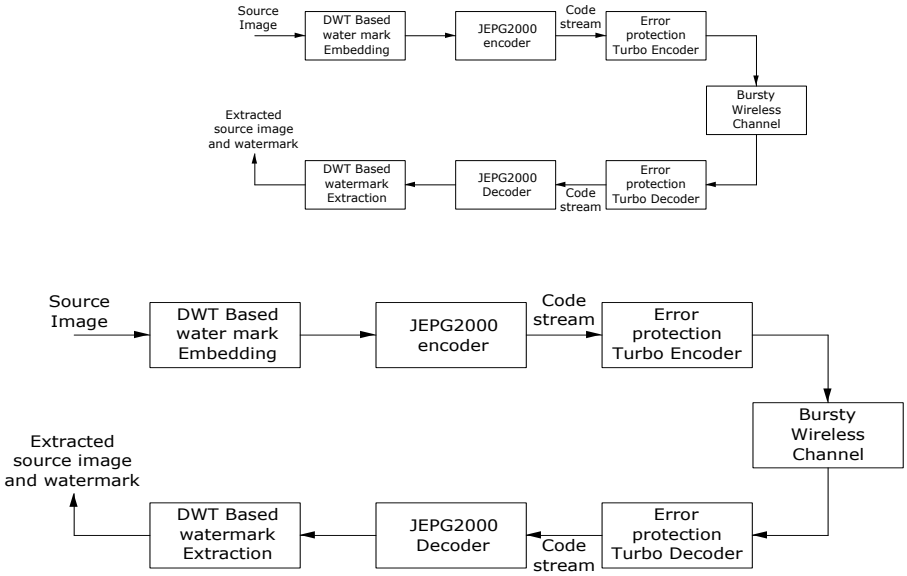

Fig. 1. Schematic block diagram of the proposed approach.

The hardware architecture for the proposed approach is synthesized with RTL compiler which is mapped into 90mm standard cells while the simulation were performed using Model Sim. The layout is designed using IC compiler. Power consumption is restricted to 0.78mW for run length encoder and 0.884mW for run length decoder in the stipulated area.

Below figure 1 shows the block diagram of the proposed approach of image transmission with watermarking. In this process the watermark is embedded into the cover image and then the JPEG-2K standard is performed for efficient compression. Turbo coding is employed as the channel source coding for error free transmission.

3.Digital Water Marking Technique

The proposed digital watermarking consists of four stages namely structuring watermark, embedding watermark, processing watermarked image and extracting the watermark. In the complete process the technique used should embed the watermark without distorting the original input image and while extracting there should not be any loss of information. The watermark should be imperceptible for few applications like secured communications in medical area especially.

The DWT and IDWT process is performed using Haar wavelet transform which can be analyzed using the following equations

$$High(n) = \mathrm{Im}\,age(2n+1) - \mathrm{Im}\,age..... \quad (1)$$

$$Low(n) = \mathrm{Im}\,age(2n) + round\,\frac{High(n)}{2})... \quad (2)$$

$$\mathrm{Im}age(2n) = Low(n) - round(\frac{high(n)}{2})... \quad (3)$$

$$\mathrm{Im}age(2n+1) = High(n) + \mathrm{Im}age(2n)... \quad (4)$$

In numerical analysis and functional analysis DWT is employed as it captures both frequency and location information called as location in time. The main advantage of Haar wavelet is that it helps to analyze the sudden transitions in the signal. The properties of Haar transform of no multiplication requirement and equal lengths of input and output finds wide range of applications for image compression.

The watermarking algorithm is implemented in three steps:

- At first, the secret watermark most significant bits are embedded into the least significant bits of the decomposed cover image low frequency sub band using DWT and bit plane slicing as shown in below figure2.
- The watermarked image is subjected to different attacks to test its robustness and legibility over the transmission.
- At the extraction, the watermark is extracted blindly without the information of original image.

The process of embedding is replicated for both LH and HL components. The inverse transform is applied to the modified coefficients to obtain the watermarked spatial elements forming a watermarked image. In this approach HH and LL sub bands are not utilized as it was realized that they are not so robust and it find cumbersome at the extraction.

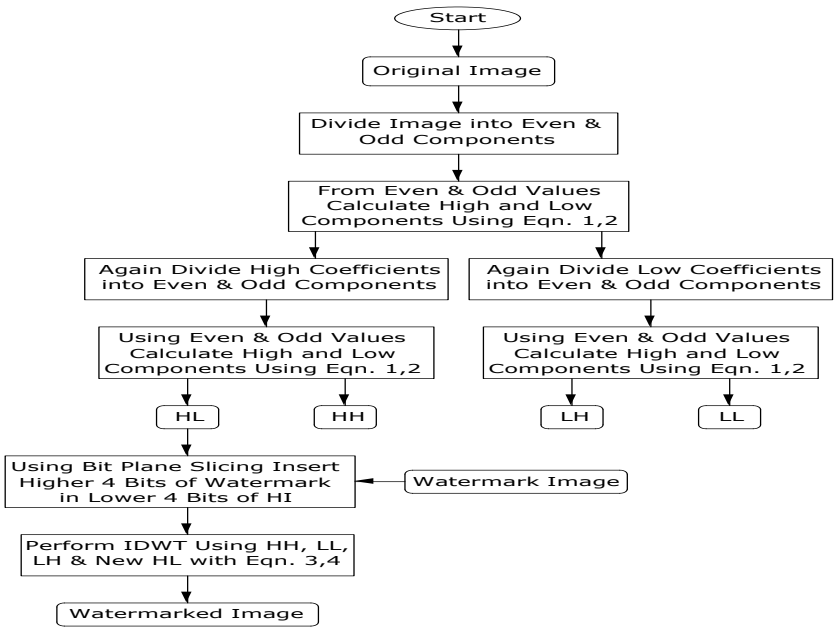

Fig. 2. flow diagram of watermarked image, Original Watermark, Extracted Watermark.

4.Turbo Coding

The encoder used in this approach represented in Figure 3 consists of four states convolutional encoder and an interleaver. A coder rate of 1/3 turbo coding with parallel concatenation is considered however the encoder is comprised of two ½ code rate convolutional encoders. The encoder receives un-coded data bits which processed as set of parity bits at the output. The convolutional encoder receives an interleaved sequence of these information bits. The decoding is performed using the BCJR algorithm. The main intension of the decoding algorithm is to iterate among two SISO (Soft Input / Soft Output). The decoder shown in Figure 4 receives a real value as the input signal and then outputs data information as an approximation of expressing in terms of the transmitted bits probability. In the entire design the choice of interleaver is very crucial which is meant to minimize the correlation of neighboring bits at the input of the convolutional encoder.

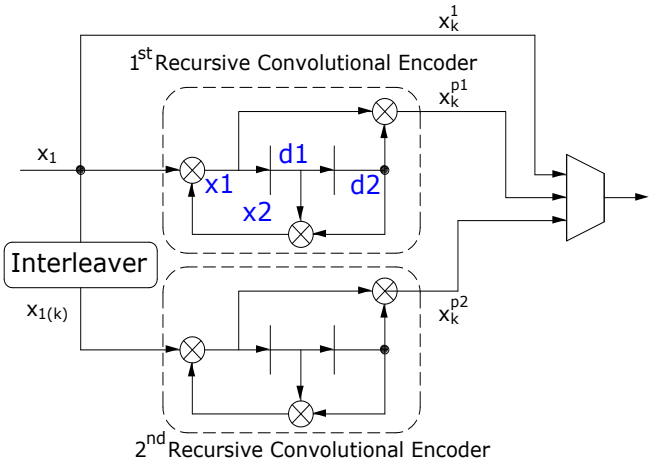

Fig. 3. The architecture of the Turbo Encoder.

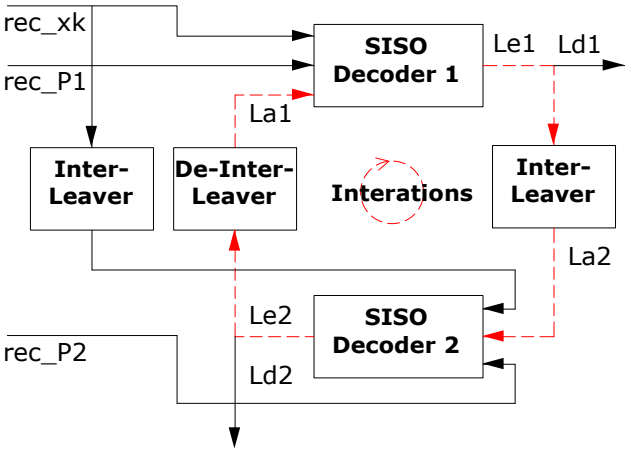

Fig. 4.The architecture of the Turbo Decoder

5.Results

The hardware implementation of the approach is shown in the results below in the tabular form Table 1 and Table 2 in FPGA device utilization summary of the encoder and decoder implemented on the target device. The synthesis report gives the structure of the encoder and decoder and their RTL respectively.

Slice Logic Utilization	Used	Available	Utilization
Number of Slice Registers	1,526	184,304	1%
Number used as Flip Flops	1,526		
Number used as Latches	0		
Number used as Latch-thrus	0		
Number used as AND/OR logics	0		
Number of Slice LUTs	1,033	92,152	1%
Number used as logic	881	92,152	1%
Number using O6 output only	460		
Number using O5 output only	54		
Number using O5 and O6	367		
Number used as ROM	0		
Number used as Memory	4	21,680	1%

Number used as Dual Port RAM	0		
Number used as Single Port RAM	0		
Number used as Shift Register	4		
Number using O6 output only	4		
Number using O5 output only	0		
Number using O5 and O6	0		
Number used exclusively as route-thrus	148		
Number with same-slice register load	142		
Number with same-slice carry load	6		
Number with other load	0		
Number of occupied Slices	427	23,038	1%
Nummber of MUXCYs used	204	46,076	1%
Number of LUT Flip Flop pairs used	1,451		
Number with an unused Flip Flop	217	1,451	14%
Number with an unused LUT	418	1,451	28%
Number of fully used LUT-FF pairs	816	1,451	56%
Number of unique control sets	69		
Number of slice register sites lost to control set restrictions	198	184,304	1%
Number of bonded IOBs	207	338	61%
Number of RAMB16BWERs	0	268	0%
Number of RAMB8BWERs	10	536	1%
Number of BUFIO2/BUFIO2_2CLKs	0	32	0%
Number of BUFIO2FB/BUFIO2FB_2CLKs	0	32	0%
Number of BUFG/BUFGMUXs	1	16	6%
Number used as BUFGs	1		
Number used as BUFGMUX	0		
Number of DCM/DCM_CLKGENs	0	12	0%
Number of ILOGIC2/ISERDES2s	0	586	0%
Number of IODELAY2/IODRP2/IODRP2_MCBs	0	586	0%
Number of OLOGIC2/OSERDES2s	0	586	0%
Number of BSCANs	0	4	0%
Number of BUFHs	0	384	0%
Number of BUFPLLs	0	8	0%
Number of BUFPLL_MCBs	0	4	0%
Number of DSP48A1s	0	180	0%
Number of ICAPs	0	1	0%
Number of MCBs	0	4	0%
Number of PCILOGICSEs	0	2	0%
Number of PLL_ADVs	0	6	0%
Number of PMVs	0	1	0%
Number of STARTUPs	0	1	0%
Number of SUSPEND_SYNCs	0	1	0%
Average Fanout of Non-Clock Nets	3.26		

Table 2. FPGA Device Utilization summary

Slice Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	1,198	184,304	1%
Number used as Flip Flops	1,198		
Number used as Latches	0		
Number used as Latch-thrus	0		
Number used as AND/OR logics	0		
Number of Slice LUTs	968	92,152	1%
Number used as logic	827	92,152	1%
Number using O6 output only	572		
Number using O5 output only	63		
Number using O5 and O6	192		
Number used as ROM	0		

Number used as Memory	0	21,680	0%
Number used exclusively as route-thrus	141		
Number with same-slice register load	132		
Number with same-slice carry load	9		
Number with other load	0		
Number of occupied Slices	403	23,038	1%
Number of MUXCYs used	168	46,076	1%
Number of LUT Flip Flop pairs used	1,233		
Number with an unused Flip Flop	272	1,233	22%
Number with an unused LUT	265	1,233	21%
Number of fully used LUT-FF pairs	696	1,233	56%
Number of unique control sets	69		
Number of slice register sites lost to control set restrictions	186	184,304	1%
Number of bondedIOBs	86	338	25%
Number of RAMB16BWERs	0	268	0%
Number of RAMB8BWERs	10	536	1%
Number of BUFIO2/BUFIO2_2CLKs	0	32	0%
Number of BUFIO2FB/BUFIO2FB_2CLKs	0	32	0%
Number of BUFG/BUFGMUXs	2	16	12%
Number used as BUFGs	2		
Number used as BUFGMUX	0		
Number of DCM/DCM_CLKGENs	0	12	0%
Number of ILOGIC2/ISERDES2s	0	586	0%
Number of IODELAY2/IODRP2/IODRP2_MCBs	0	586	0%
Number of OLOGIC2/OSERDES2s	0	586	0%
Number of BSCANs	0	4	0%
Number of BUFHs	0	384	0%
Number of BUFPLLs	0	8	0%
Number of BUFPLL_MCBs	0	4	0%
Number of DSP48A1s	0	180	0%
Number of ICAPs	0	1	0%
Number of MCBs	0	4	0%
Number of PCILOGICSEs	0	2	0%
Number of PLL_ADVs	0	6	0%
Number of PMVs	0	1	0%
Number of STARTUPs	0	1	0%
Number of SUSPEND_SYNCs	0	1	0%
Average Fanout of Non-Clock Nets	3.38		

The Xilinx ISE (Integrated Software Environment) is used to perform synthesis. The synthesis report of encoder and decoder, the simulation output, the power report of the encoder and decoder, the timing report of the encoder and decoder, the delay report of encoder and decoder and the area report of the encoder and decoder, the RTL view of encoder and decoder are shown in the various figure 5,6,7,8 below.

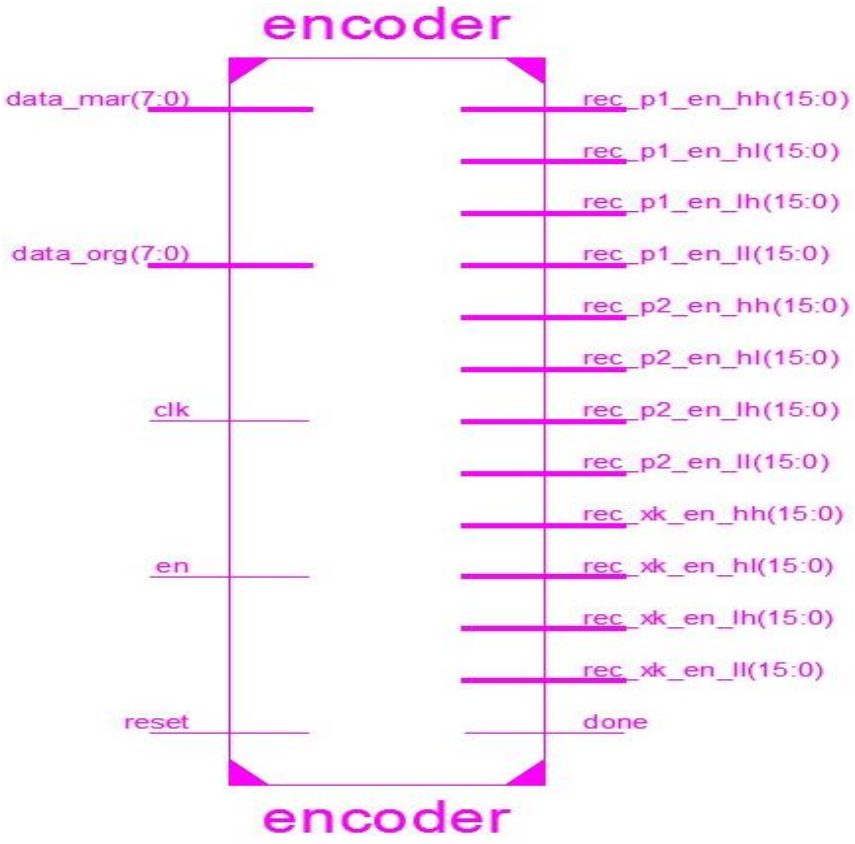

Figure 5 Encoder

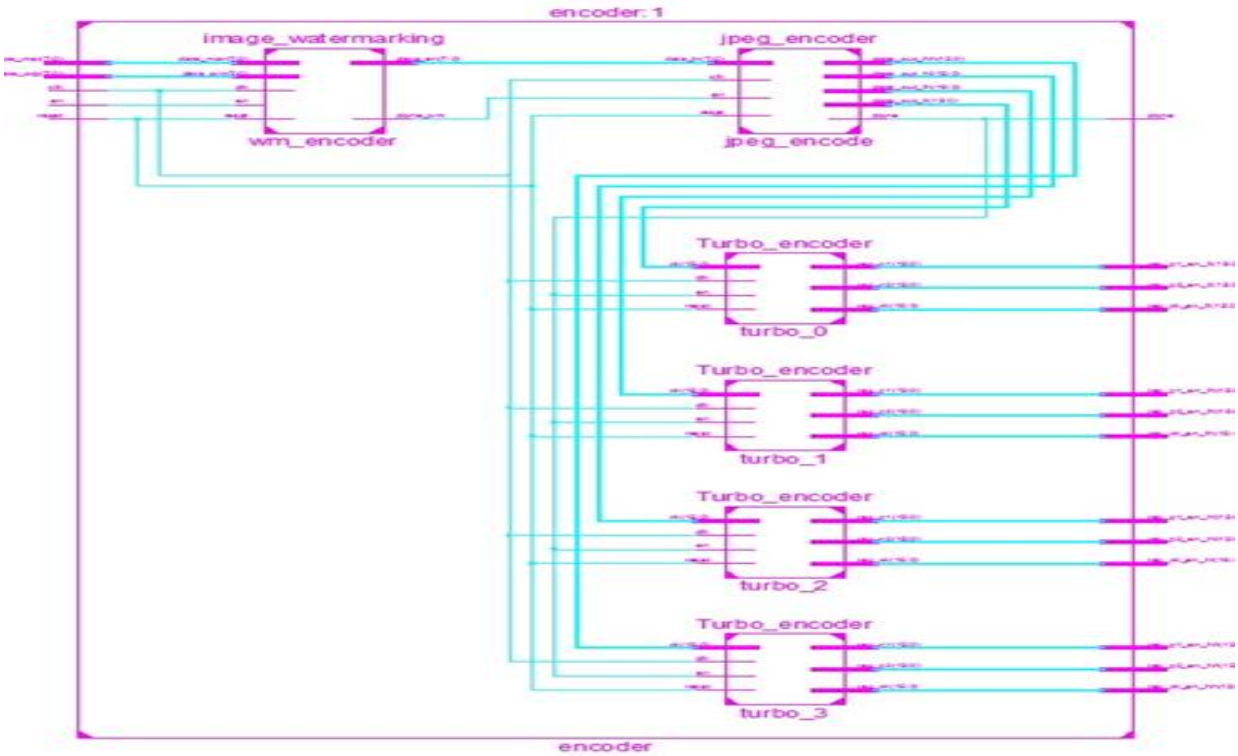

Fig.6 .RTL view of Encoder

Numerical Values of few parameters observed from the results. FPGA used for implementing is Xilinx Spartan6 XC6slx150-2fgg484.

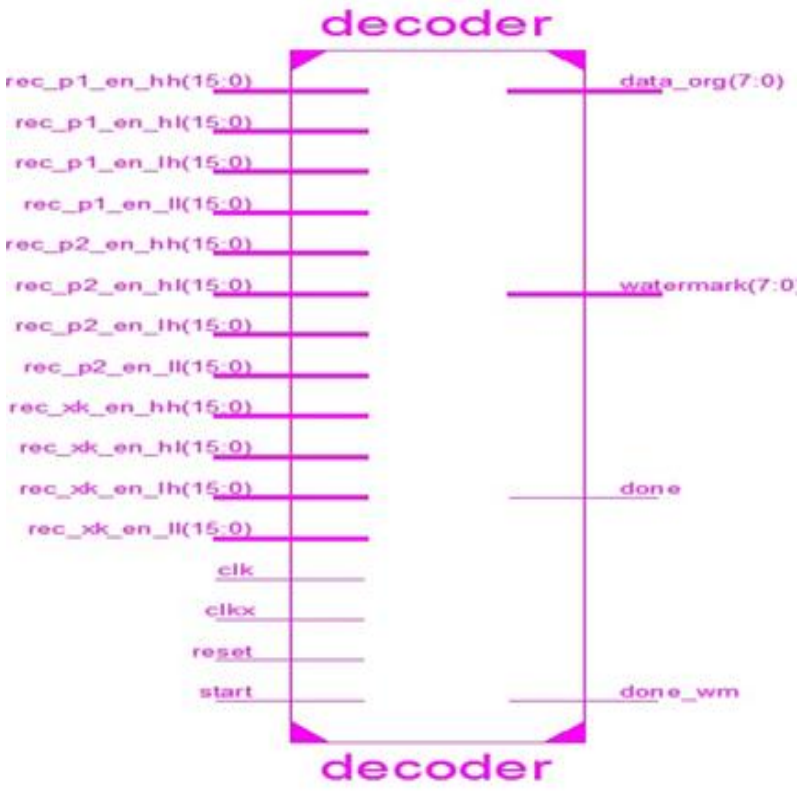

Figure 7 decoder

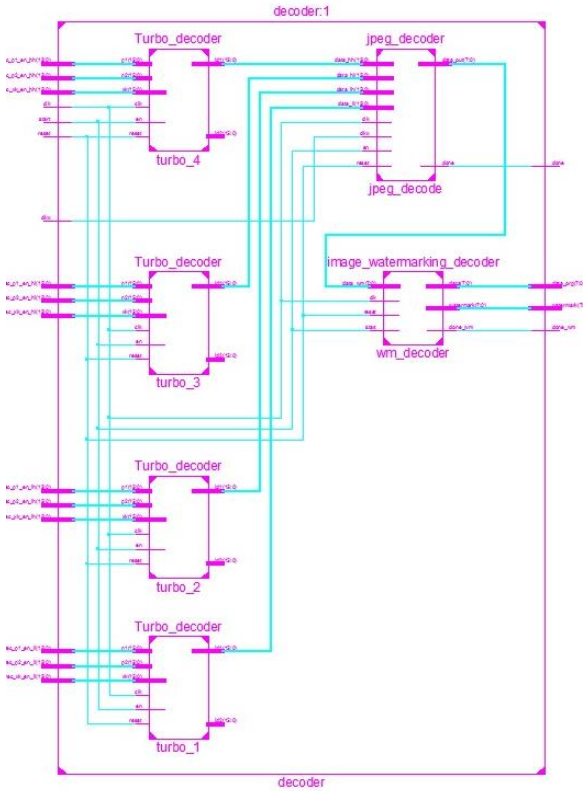

Fig. 8. RTL view of Decoder

6.Conclusions

In this paper an approach for image transmission with security based on Haar Wavelet, JPEG compression and turbo decoder is realized. Results illustrate the hardware realization of the secured transmission approach. From the results it is accomplished that the proposed watermarked approach is efficient and robust as well for digital image transmission with security over wireless channels

References

Rao, K. D. (2010, October). New approach for digital image watermarking and transmission over bursty wireless channels. In IEEE 10th INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING PROCEEDINGS (pp. 1829-1832). IEEE.

Antonini, M., Barlaud, M., Mathieu, P., & Daubechies, I. (1992). Image coding using wavelet transform. IEEE Transactions on image processing, 1(2), 205-220.

Gonzalez, R. C., Woods, R. E., & Eddins, S. L. (2004). Digital image processing using MATLAB. Pearson Education India.

Christopoulos, C., Skodras, A., & Ebrahimi, T. (2000). The JPEG2000 still image coding system: an overview. IEEE transactions on consumer electronics, 46(4), 1103-1127.

Palnitkar, S. (2003). Verilog HDL: a guide to digital design and synthesis (Vol. 1). Prentice Hall Professional.

I. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia". IEEE Transaction on Image processing,Vol 6, issue 12, pp1673-1687, 1997.

Jiri Fridrich ." A New Steganographyic Method for Palette-Based Images". Center for Intelligent Systems, SUNYBinghamton, Binghamton, NY 13902-6000. U.S Government, a grant number F30602-98-c-0009.

M.Kutter, E. Jordan, and E. Bossen ; "Digital signature of Color images using amplitude modulation", J. Electron Imaging, vol. 7, (2), pp.326-332, 1998.

E.T. Lin, E.J. Delp. "A review of data hiding in images", Proceedings of the conference on image process image quality image capture systems, PICS'99'. 25-28, April 1999, savannah, Georgia, pp. 274-278

BENDER, W. GRUHL, D. MORIMOTO N, and A. LU, "Techniques for data Hiding", IBM, syst. J., 35, (3&4) pp.313-336, 1996.

S. K. Moon and R.S. Kawitkar, "Data Security using Data Hiding", IEEE International conference on computational intelligence and multimedia applications, vol. 4, pp. 247-251, Dec. 2007.

KO-Chin Chang, Chien-Ping Chang, Ping S.Huang, and Te-mingTu.:"A novel image steganographic method using Tri-way pixel value Differencing".Journal of multimedia, Vol.3, No.2, June-2008.

K.Suresh Babu, K. B. Raja , Kiran Kumar k , Manjula Devi T H, Venugopal K R ,L.M Patnaik. "Authentication of secret information in image steganography;"TENCON-2008, IEEE Region 10 Conference. pp. 1-6, Nov 2008.