International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Design and Synthesis of Digital Watermarking Chip Using Inverse Modified Discrete Cosine Transform (IMDCT) in Hardware Description Language (HDL) Environment

Adesh Kumar, Mani Priya Singh, Renu Gola

***Abstract* – Digital watermarking is the process of embedding data, called a watermark, into a multimedia object such that the watermark can be detected whenever needed for digital rights management (DRM). The object may be an image, audio, video, text, or graphics. Watermarking requires two operations, embedding the watermarks with the information and extraction. Because of copyright protection, watermarking techniques are often evaluated based on their robustness, recoverability, and invisibility. Field programmable gate arrays (FPGAs) are extensively used in rapid prototyping and verification of a conceptual design and also used in electronic systems when the mask production of a custom IC becomes prohibitively expensive due to the small quantity. The research work focuses the watermarking chip design and synthesis using Inverse Modified Discrete cosine transform (IMDCT) with optimized hardware parameters. The work is carried out in Xilinx ISE 14.2 software and functional checked in Modelsim 10.0 a student edition. The results are tested on Sparten-3 FPGA kit and memory utilization is found 156538 kB.**

***Keywords* – Very High Speed Integrated Circuit Hardware Description language, Very Large Scale of Integration, Field Programmable Gate Array, Register Transfer Logic, Inverse Modified Discrete cosine Transform.**

I. INTRODUCTION

Internet based multimedia technologies such as images, video and audio require network security to create, transmit and distribute the data over long distance. There are three basics to protect the data over internet namely, cryptography Steganography [7] [9] [20] and water marking [1] [4]. In cryptography include transmission and reception of secured text and image using encryption and decryption technique. Steganography is the technique to hide and extract the information using a carrier signal [20]. The third one, watermarking is a technique for hiding proprietary information in the perceptual data. Watermarking involves the content authentication, copyright protection [8] detection of duplication and alteration. In the original message watermarks are used to protect the data and at the receiving end these watermarks are extracted. So watermarks are used with the secret information to protect it. Watermarking requires two operations, embedding the watermarks with the information and extraction. Watermark may be an image, plain text data, password, serial number or authentication key. According to the type of document, watermarking techniques can be divided into four categories; they are (i) text watermarking [8] [9] (ii) image watermarking (ii) audio watermarking [9] and (iv) video marketing. Image watermarking can be classified both in spatial domain and frequency domain. Visible watermarks [22] appear visible to a casual viewer on careful inspection. Primary images are embedded with the invisible fragile watermark technique in such a way that modification or manipulation of the image would destroy or alter the watermark. The alteration made to the pixel value is perceptually not noticeable and it is possible to recover with appropriate decoding. Human perception classified watermarking as robust and fragile. In image processing, the watermarking techniques are classified into three types, visible watermark, Invisible fragile watermark [4] [7] and Invisible robust watermark. All watermarking techniques are compatible with hardware, software or both together. There is a close relationship of watermarking and cryptography [11] [21] but watermarking is distinct from encryption. Watermark embedded process and extraction processes are shown in the figure 1 and figure 2 respectively.

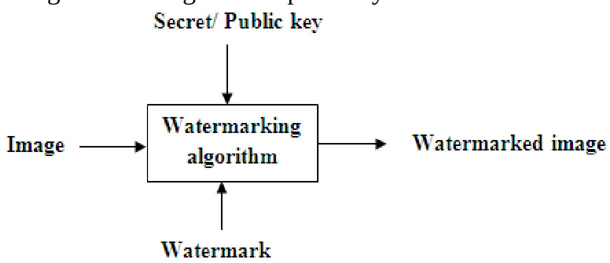

Fig.1. Watermark embedding process [18]

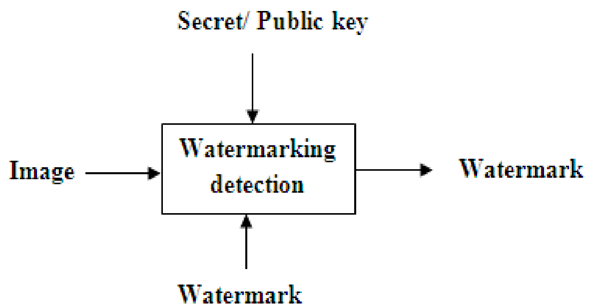

Fig.2. Watermark extraction processes [18]

An original image is embedded with the information carrying the watermark. The watermarked image is stored and transmitted and then decoded by the receiver [11]. Cryptography helps to resemble the image so that it cannot be understood. A digital watermark could be used either source based or destination based. From the application point of view, source based watermarks are used for authentication or ownership identification [3]. In this a unique watermark [3] [6] is identifying that the owner is introduced to all the parallel copies of a particular image being distributed and it also used to identify weather a received image has been tampered with. If the each distributed copy is getting a unique watermark, it could be a destination based watermark and it could be used to determine the buyer in case of illegal reselling. In real time, watermarking will solve the issues of source authentication [21]. In the real time stream exchange, the parties involved to check the authenticity of the data received with the help of watermark extraction bits available in the embedded stream [4] [6] . This watermark can be used into the video stream at source, channel or at the receiver side. In the proposed system a simple video streaming authentication system is using watermarking at the source principle rather than at video delivery or at channel. The system is applicable for both unicast and multicasting application.

A video server sends out a networked visual program of high quality to its user in multicast application scenario like VoD [12] as shown in figure 3. In this video stream is embedded with N watermarks and send over the internet. The video serve is exhausted by authenticating all the outgoing video streams. So the same content is watermarked at the server side their recipient specific information for video finger printing and traitor tracing and respective attacks are taken care. There are N recipients to extract the watermarked output. Each recipient can receive the embedded video stream having their own information as a watermark. Due to the insecure nature [14] of the network or channel, there is the possibility of malicious attacks [4] in the contents. So, it becomes very difficult for the receiver to get the original content without any authentication mechanism between the users involved in exchanging the streams.

Digital watermarking [15] [16] can be computer aided information used in carrier signal to hide the information. Digital watermarks [15] may be used to verify the integrity or authenticity of the carrier signal or to show the identity of its owners. It is prominently used to copyright material and for illegal authentication. Digital watermarks are only perceptible under certain conditions like traditional watermarks i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it gets perceivable, it is of no use. Traditional Watermarks [16] may be applied to visible media like images or video, whereas in digital watermarking, the signal may be audio, pictures, video, texts.

Tools Utilized: Design and implementation of IMDCT for watermarking chip includes the following software development tools: Project navigator application ISE 14.2 of Xilinx Company, is a tool to design the IC and to view their RTL (Register Transfer Logic) schematic. Model SimEE 10.1b students edition of Mentor Graphics Company is used for simulation and debugging the functionality. The hardware chip implementation is done using VHDL programming language.

The paper is organized as follows: Section I presents the introduction and the tools utilized. Section II discusses the mathematical model of DCT. Section III presents the mathematical model of IMDCT. Section IV describes the Methodology & Tools and Section V describes the Result and FPGA Synthesis. Section VI presents the Device utilization and timing summary and Conclusions is presented in Section VII.

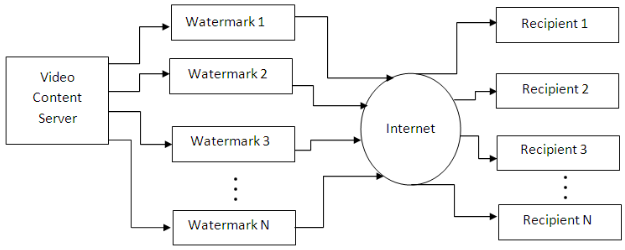

Fig.3. Watermarking by video content server over internet

II. Mathematical Model of Discrete Cosine Transform

Formally, the discrete cosine transform [2] is a linear, invertible function $F : \mathbb{R}^N \rightarrow \mathbb{R}^N$ (where R denotes the set of real numbers), or equivalently an invertible $N \times N$ square matrix. There are several variants of the DCT [2] [15][16]with slightly modified definitions. The N real numbers $x_0, \ldots, x_{N-1}$ are transformed into the N real numbers $X_0, \ldots, X_{N-1}$ according to one of the formulas of DCT -1, DCT II, DCT-III, DCT-IV and multidimensional DCT.

DCT-I

$$X_k = \frac{1}{2}(x_0 + (-1)^k x_{N-1}) + \sum_{n=1}^{N-2} x_n \cos\left[\frac{\pi}{N-1} nk\right]$$

where $k = 0, \ldots, N-1$

DCT-II

$$X_k = \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N}\left(n + \frac{1}{2}\right)k\right]$$

where $k = 0, \ldots, N-1$

DCT-III

$$X_k = \frac{1}{2}x_0 + \sum_{n=1}^{N-1} x_n \cos\left[\frac{\pi}{N} n \left(k + \frac{1}{2}\right)\right]$$

where $k = 0, \ldots, N-1$

DCT-IV

$$X_k = \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N}\left(n + \frac{1}{2}\right)\left(k + \frac{1}{2}\right)\right]$$

where $k = 0, \ldots, N-1$

Multidimensional DCT

$$X_{k1,k2} = \sum_{n_1=0}^{N_1-1}\left(\sum_{n_2=0}^{N_2-1} \cos\left[\frac{\pi}{N_2}\left(n_2 + \frac{1}{2}\right)k_2\right] x_{n_1,n_2}\right)\cos\left[\frac{\pi}{N_1}\left(n_1 + \frac{1}{2}\right)k_1\right]$$

$$X_{k1,k2} = \sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1} x_{n_1 n_2} \cos\left[\frac{\pi}{N_1}\left(n_1 + \frac{1}{2}\right)k_1\right]\cos\left[\frac{\pi}{N_2}\left(n_2 + \frac{1}{2}\right)k_2\right]$$

III. Mathematical Model of IMDCT

The drawback of DCT-I to DCT-IV is that these applicable for 1 D DCT [2] and having slower speed. Multidimensional DCTs can be used for 2D DCT design

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

but it also has slower speed. Chip design for 2D digital watermarking can faster using IMDCT [5] transformation. It accepts 18 discrete values. 18-point IMDCT (block size 36) for implementation is given by the following equation.

$$\widehat{x_m} = \frac{2}{N}\sum_{k=0}^{\left(\frac{N}{2}\right)-1} X_k.\cos\left[\frac{\pi}{2N}(2k+1)\ \left(2m+1+\frac{N}{2}\right)\right],$$
$$with\ m = 0,1,2,\ldots\ldots\ldots,N-1$$

Generally, it is a lapped transform, the recovered data sequence $\{\widehat{x_m}\}$ does not correspond to the original data sequence $\{x_m\}$. To obtain the correct $\{x_m\}$ the outputs of consecutive transforms have to be combined. It can be seen that N/2 (non redundant) input values result in N output values (of course the MDCT [5] reads N input values and results in N/2 output values). Since it is not completely clear whether Equation1 should be called an N-point IMDCT [5] or an N/2-point IMDCT, in the following we shall identify these transforms given the number of inputs. Considering an18-point IMDCT that delivers 36 output values, thus length *N* will be 36. Figure 4 shows how 36 discrete values are obtained in which 18 values are for DCT-II and 18 values are for DST-II, combining or shuffling the discrete values provides 36 values discrete output.

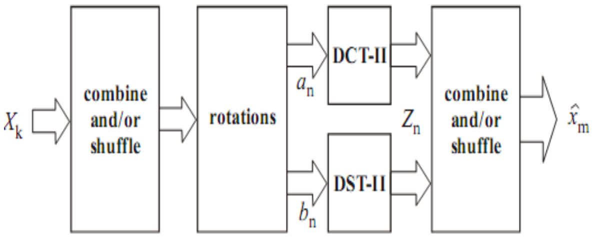

Fig.4. Basic set up of IMDCT [5]

Considering a case for N =36, we start from an 18 values input sequence: $\{X_0, X_1, \cdots, X_{17}\}$. The output of rotational block is given by

$$a_n = X_n\cos\left[\frac{\pi}{2N}(2n+1)\right] + X_{N/2-1-n}\sin\left[\frac{\pi}{2N}(2n+1)\right]$$

$$b_n = X_n\sin\left[\frac{\pi}{2N}(2n+1)\right] - X_{\frac{N}{2}-1-n}\cos\left[\frac{\pi}{2N}(2n+1)\right]$$

$$Here\ n = 0,1,2,\ldots..\frac{N}{4}-1$$

The left most' combine and shuffle'-block is thus nothing more than a reverse ordering of the second half of the input data.

IV. Methodology and Tools

Project navigator Application Version 6.1i or ISE 13.0 of Xilinx Company: Xilinx has been a semiconductor industry leader at the forefront of technology, market and business achievement. It is a tool to design the IC and to view their RTL (Register Transfer Logic) schematic .It is a tool to test the code on FPGA environment and all parameters detail is required to implement the Chip.

Model SimEE 10.0 D of Mentor Graphics Company: Mentor Graphics was the first to combine single kernel simulator (SKS) technology with a unified debug environment for Verilog, VHDL, and System C. The combination of industry-leading, native SKS performance with the best integrated debug and analysis environment make ModelSim the simulator of choice for both ASIC and FPGA design. The best standards and platform support in the industry make it easy to adopt in the majority of process and tool flows.

Simulation and Design Steps: The diagram shown in the figure 5 explains basic steps for simulating a design in ModelSim.

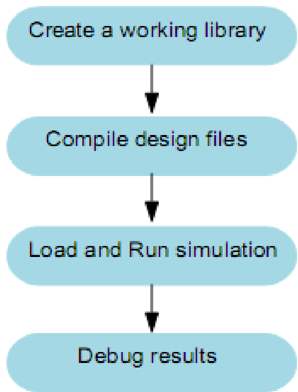

Fig.5. Chip Design Process Flow [13] [15]

Creating the Working Library: In ModelSim [15], all designs are compiled into a library. Typically start a new simulation in ModelSim by creating a working library called "work," which is the default library name used by the compiler as the default destination for compiled design units.

Compiling Design: After creating the working library [15], design is being compiled into it. The ModelSim library format is compatible across all supported platforms.

Loading and Running the Simulator with the Design: With the design compiled, simulator is loaded with design by invoking the simulator on a top-level module (Verilog) or a configuration or entity/architecture pair (VHDL). Assuming the design loads successfully, the simulation time is set to zero, simulation can be done by entering a run command.

V. Results & FPGA Synthesis

The snapshot shown in figure 6 is taken from the modelsim 10.1 software. It shows the functional output and figure 7 shows the internal schematic of Register Transfer Logic (RTL) view extracted from Xilinx ISE. *CLK and Reset* are the inputs. *X* is the input of sample and y is the sample output.

Step input 1: *reset =1, clk* is applied for synchronization and then run. Force the discrete values *of X [0:17][32:0]. The value [0:17][32:0]* signifies that X is an array of 18 discrete values of 32 bits.

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Step input 2: reset =0, clk is applied for synchronization,

In the modelsim waveform shown in figure *X [0:17][32:0]*represents the sample input of the image and *Y[0:17][32:0]*represents the sample output of image. *p_state, n_state* are the intermediate signals which shows the state transition during each discrete values, *done* is a control signal which represents the status of each state after every

The Spartan 3E [23] [24] starter kit provides easy way to test the various programs in the FPGA itself, by dumping the 'bit' file of the designed program in Xilinx software into the FPGA and then observing the output .The Spartan 3E FPGA board comes built in with many peripherals that help in the proper working of the board and also in interfacing the various signals to the board itself. Some of the peripherals included in the Spartan 3E FPGA board include: 2-line, 16-character LCD screen used for display the output, PS/2 mouse [23] or keyboard port can be connected to the FPGA, VGA display port [24] used to display various encoded images via a screen. The image encoding would be done by the FPGA via the aid of the program and then the encoded image would be displayed on the screen. Two 9-pin RS-232 [23] ports help in the transmission of serial data to and from the FPGA board, 50 MHz clock oscillator is the system clock which helps in giving the clock signal to the various events taking place within the FPGA and the various programs that require clock for their working, A Digital clock manager [23] [24] can also be used to reduce the frequency of the system clock so that it is useful for various other purposes which need smaller clock frequency [10].

On-board USB-based FPGA [24] download and debug interface is also in the Sparten-3E kit in which the programmable file is dumped into the FPGA via the USB based download cable. Hence it is very much helpful in the testing of the programs whether they are working correctly or not, eight discrete LEDs can be interfaced to glow when a particular output becomes high. Hence the LEDs can be interfaced to show the output of a single bit. Figure 8 shows the view and peripherals of Sparten 3 FPGA.

Four slide switches and four push-button switches are used to give the inputs to the FPGA board. They can also act as the reset switches for the various program Kit also has four-output, SPI-based on board Digital-to-Analog Converter (DAC) on board which is to be interfaced to give the analog output to the digital data values. Two-input, SPI-based [23] Analog-to-Digital Converter (ADC) with programmable gain preamplifier converts the real world analog signals into digital values.

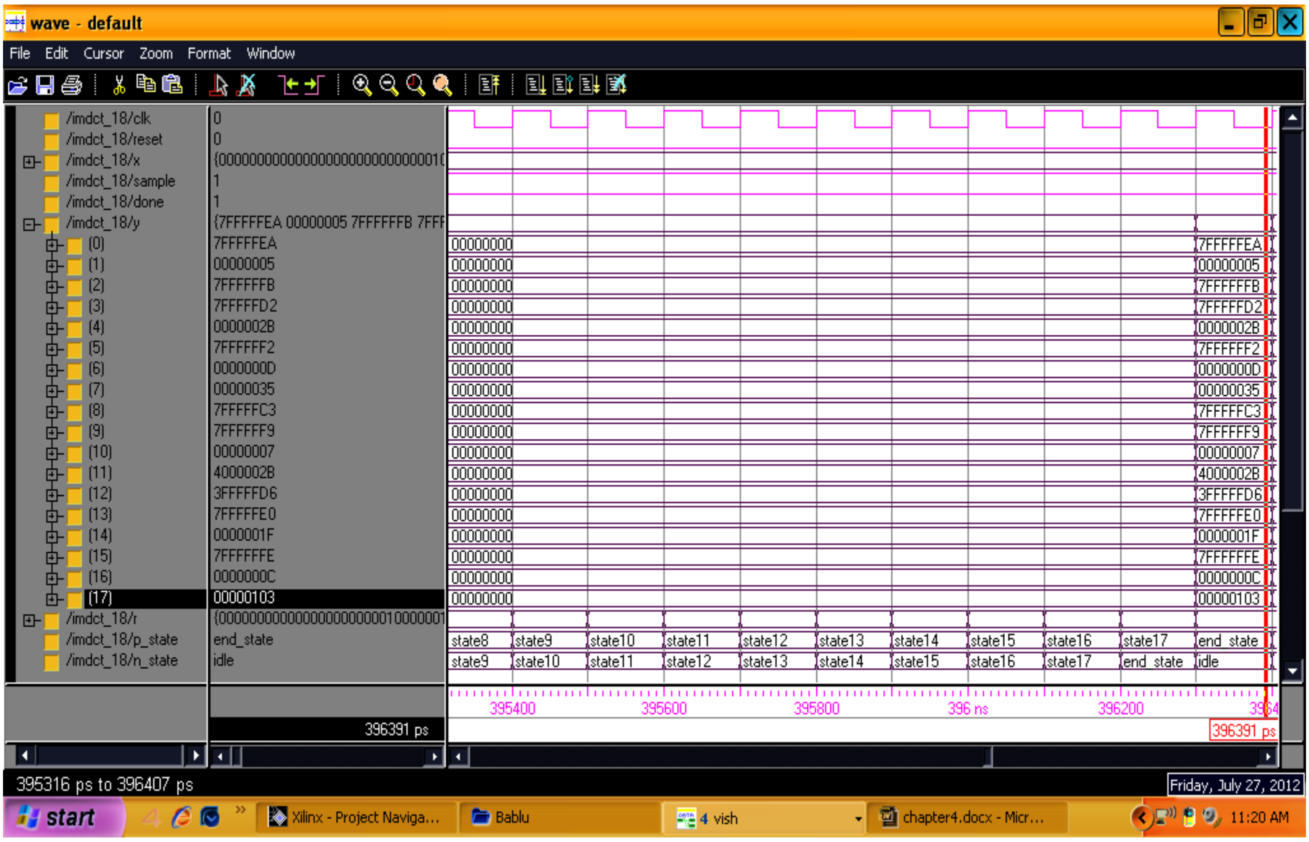

Fig.6. Modelsim waveform with watermarked samples using IMDCT

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

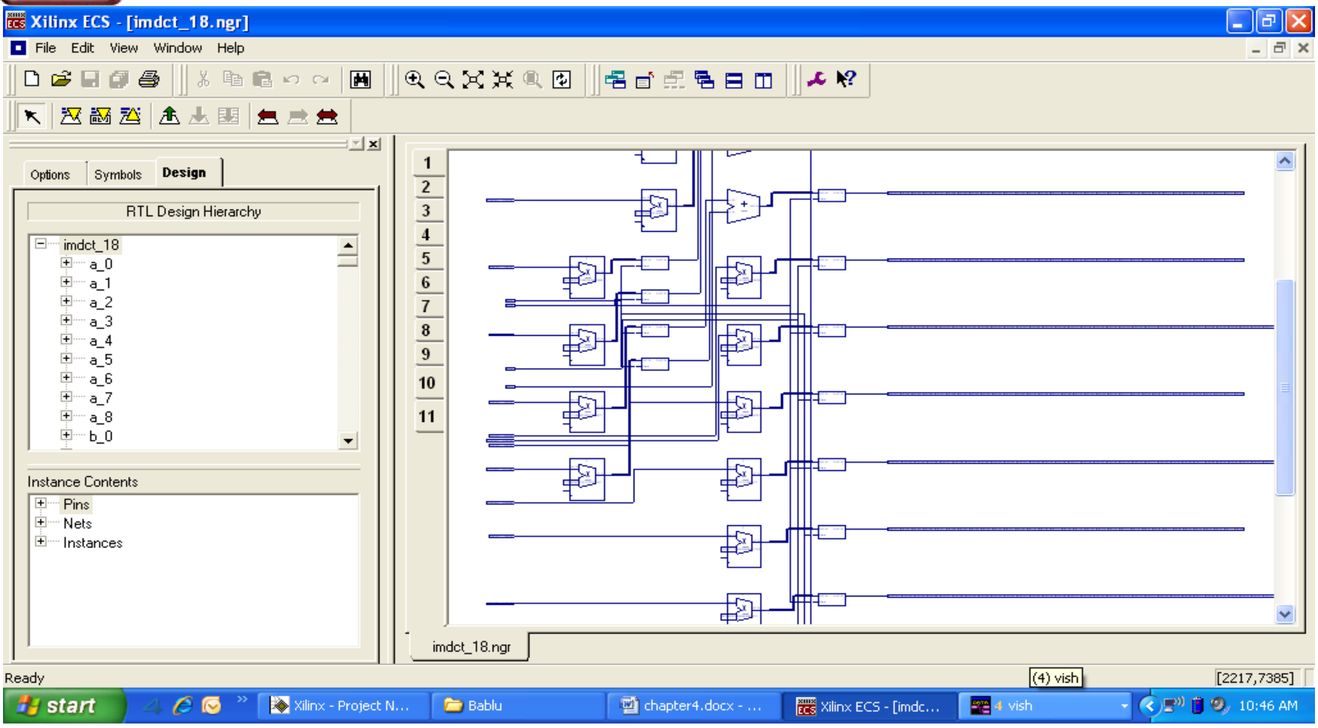

Fig.7. Register transfer logic (RTL) schematic of IMDCT

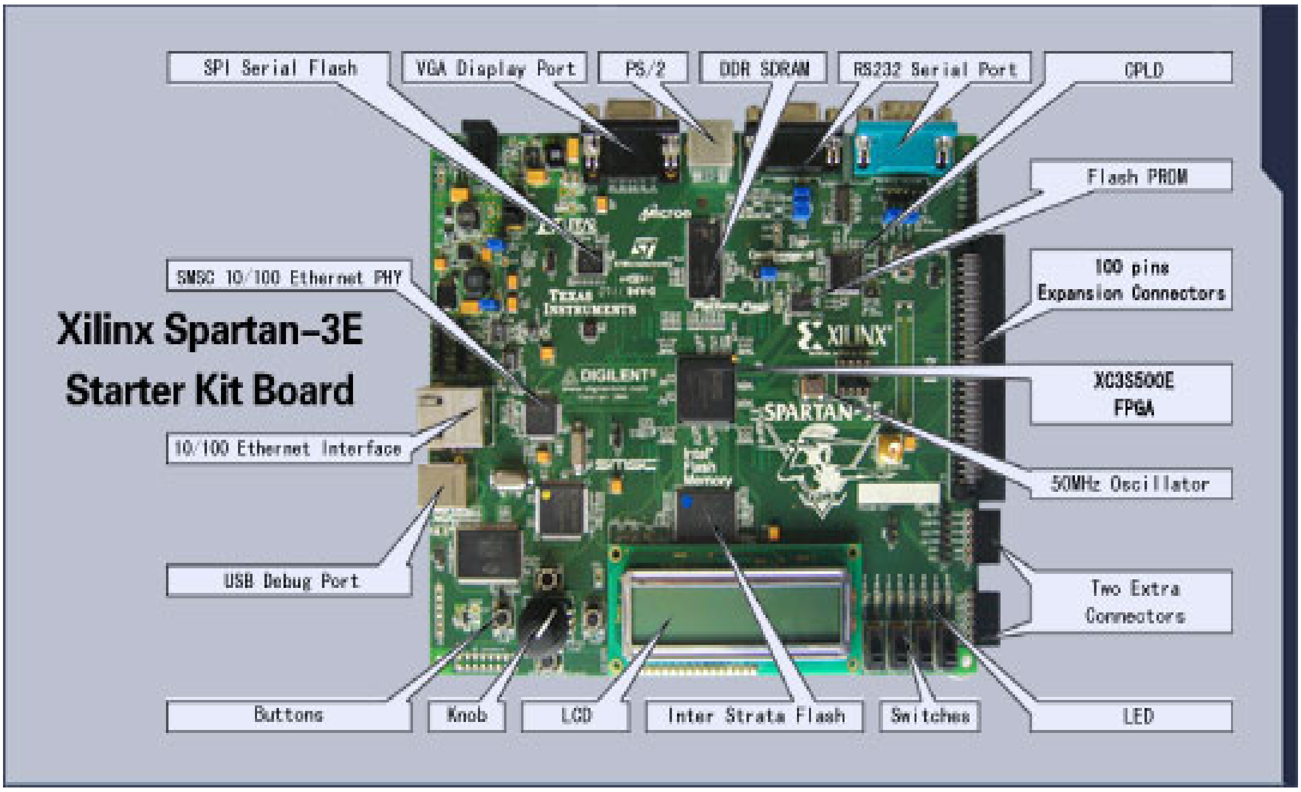

Fig.8. Sparten 3E FPGA View [23]

VI. Device Utilization and Timing Summary

Device utilization report is the report of used device hardware in the implementation of the chip. Device includes the detailed summary of number of slices, number of flip flops, number of LUTs, number of bounded IOBs , number of GCLks, total memory utilization etc. Timing report shows the value of minimum and maximum time to reach the output after clock pulse and before clock pulse is applied. It also lists the value of minimum period and maximum frequency supported by the FPGA device. Table 1 shows the detail of device utilization for IMDCT Module.

Timing Summary
Selected Device: 3s200pq208-4
Speed Grade: -4
Minimum period: 2.223ns (Maximum Frequency: 449.843MHz)
Minimum input arrival time before clock: 19.322ns
Maximum output required time after clock: 6.379ns

Table 1: Device utilization in IMDCT structure

Device part	Utilization
Number of Slices	904 out of 1920 47.08%
Number of Flip Flops	627 out of 3840 16.32%
Number of 4 input LUTs	440 out of 3840 11.45%
Number of bonded IOBs	133 out of 141 94.32%
Number of MULT18X18s	2 out of 6 33.33%
Number of GCLKs	1 out of 8 12%

VII. Conclusion

Digital watermarks provide an efficient cost effective means of a digital image which may be used for copyright protection. Such chip can be used in any existing JPEG encoder to watermark images right at the source end. The disadvantage of the watermarking algorithms implemented is that the processing needs to be performed pixel by pixel. Discrete cosines transform (DCT) had been used in the previous techniques to extract the watermarks so far. In the research, IMDCT is used to extract the watermarks in the image, because of its faster speed in comparison to DCT. Design summary result shows numbers of Slices are 47.08 %, Number of Flip Flops 16.32 %, Number of 4 input luts 11.45 %, number of bounder IOBs 94. 32 % Number of MULT18X18s is 33.3 %, Number of GCLKs used is 12 %. Total memory utilization for the chip development is 156538 kB. The chip synthesis is done on Sparten-3E FPGA. The proposed scheme of watermarking can embedded multiple watermarks in color images.

References

[1] A. M. Eskiciogluand E. J. Delp, "An Overview of Multimedia Content Protection in Consumer Electronics Devices," Elsevier Signal Processing: Image Communication, vol.1 6, pp.681–699, 2001.

[2] D.W. Trainor J.P. Heron and R.F. Woods, White paper on "IMPLEMENTATION OF THE 2D DCT USING A XILINX XC6264 FPGA", , Department of Electrical Integrated Silicon Systems Ltd and Electronic Engineering Chlorine Gdn's The Queen's University of Belfast N. Ireland(Page 9)

[3] D. Kundur and K. Karthik, "Digital Finger printing and Encryption Principles for Digital Rights Management," IEEE Signal Processing, vol.52, 2004.

[4] F. Mintzer, G.Braudaway, and M.Yeung, "Effective and Ineffective Digital Watermarks,"in IEEE International Conference on Image Processing (ICIP-97), 1997, vol.3, pp.9–12.

[5] Huibert J. Lincklaen Arriëns "Implementation of an 18-point IMDCT on FPGA, *HJLA*, *June-2005*", page (1-9)[6] H. Berghel, "Watermarking Cyber space," Communications of the ACM, vol.40, no.11, pp.19–24, November1997.

[7] I.J.Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol.6, no.12, pp.1673–1687, Dec1997.

[8] Kesavan Gopal, Dr. M. Madhavi Latha, "Watermarking of Digital Video Stream for Source Authentication" IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010 pp(1-6)

[9] M.Swanson, M.Kobayashi, and A.Tewfik, "Multimedia Data Embedding and Watermarking Technologies," Proceedings of the IEEE, vol.86, no.6, pp.1064–1087, June1998.

[10] M. Morris Mano Digital Design, Second Edition by Pearson Education.

[11] N. M. Kosaraju, M. Varanasi, and S.P. Mohanty, "A High Performance VLSI Architecture for Advanced Encryption Standard (AES) Algorithm, "in Proceedings of 19th IEEE International Conference on VLSI Design, 2006,pp .481–484.

[12] N. Memonand P.W. Wong, "Protecting Digital Media Content," Communications of the ACM, vol. 41, no.7, pp.35–43, July 1998.

[13] Priyanka Saini, Adesh Kumar, Neha Singh " FPGA Implementation of 2D and 3D image enhancement chip in HDL Environment " International journal of Computer Applications (IJCA) Volume 62, Jan 2013

[14] S.Craver, N.Memon, B.L.Yeo, and M.M.Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications,"IEEE Journal on Selected Areas in Communications, vol.16, no.4, pp.573–586, May1998.

[15] S. P. Mohanty, K.R. Ramakrishnan, and M. S. Kankanhalli, "A DCT Domain Visible Watermarking Technique for Images," in Proceedings of the IEEE International Conference on Multimedia and Expo, 2000, pp.1029–1032.

[16] S. P. Mohanty, K. R. Ramakrishnan, and M.S.Kankanhalli, "An Adaptive DCT Domain Visible Watermarking Technique for Protection of Publicly Available Images," in Proceedings of the International Conference on Multimedia Processing and Systems, 2000, pp.195–198.

[17] Semiconductor Complex Limited, Internet PDF: Data sheets of XC 95 series CPLD [Online].

[18] S Jayaraman, S Esakkirajan, T VeeraKumar Book "Digital Image Processing" Tata Mc Graw Hill Education Pvt Limited New Delhi, Chapter 12 Wavelet based image processing page (660-666).

[19] S. Emmanueland M.S. Kankanhalli, "A Digital Rights Management Scheme for Broadcast Video," ACM- Springer Verlag Multimedia Systems Journal, vol.8, no.6, pp.444–458, June 2003.

[20] S. Katzen beisser and F.A.P. Petitcolas, Information Hiding techniques for steganography and digital watermarking, Artech House, Inc.,MA, USA, 2000.

[21] S.P.Mohanty, "Digital Watamerking of Images," M.S. thesis, Department of Electrical Engineering, Indian Institute of Science, Bangalore, India,1999.

[22] W. N. Lie and L. C. Chang, "Robust and High-Quality Time-Domain Audio Watermarking Based on Low-Frequency Amplitude Modification," IEEE Transaction on Multimedia, vol. 8, no. 1, pp. 46-59, February, 2006.

[23] http://www.xilinx.com/support/documentation/data_sheets /ds312.pdf

[24] http://www.xilinx.com/support/documentation/data_sheets /ds099.pdf

[25] http://mosfet.isu.edu/classes/ee_cs_499_verilog_hdl/ userguides/modelsimuser.pdf

Author's Profile

Adesh Kumar

is B.Tech in Electronics & Communication Engineering from Veera College of Engineering, Bijnor (UPTU, Lucknow) India in 2006. M.Tech in Embedded Systems Technology from SRM University, Chennai in 2008. Currently he is working as an Assistant Professor with the department of Electrical, Electronics and Instrumentation Engineering in "University of Petroleum & Energy Studies" , Dehradun India. He has also worked as Senior Engineer in TATA ELXSI LIMITED Bangalore and faculty member in ICFAI University, Dehradun. His are of interest are VLSI Design, Microprocessors and Embedded System. He has published 20 research papers in international journal and conferences.

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Many Priya Singh
is B.Tech in Computer Science & Engineering from Veera College of Engineering, Bijnor (UPTU, Lucknow) India in 2011. Currently she is M.Tech scholar in Computer Science & Engineering in SRM University, NCR Campus Modinagar Ghaziabad India. Her area of interest is cryptography and digital image processing.

Renu Gola
is M.Tech. in Computer Science & Engineering from Banasthali University, Rajasthan India in 2010. Now she is working with the department of Computer Science & Engineering, SRM University NCR campus India. Her Area of interest are operating system and Digital Image Processing.