International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 23rd February 2018. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-2

Title: Digital Modular Implementation of DSP Systems for Data and Design Hiding Applications.

Volume 07, Issue 02, Page No: 656 – 665.

Paper Authors

***ATHIM S V V S MANIKANTA, P.SATYAVANI.**

* Dept of ECE, Kakinada Institute of Engineering and Technology.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

DIGITAL MODULAR IMPLEMENTATION OF DSP SYSTEMS FOR DATA AND DESIGN HIDING APPLICATIONS

***ATHIM S V V S MANIKANTA, **P.SATYAVANI**
*PG Scholar, Dept of ECE, Kakinada Institute of Engineering and Technology, Korangi, A.P.
**Assistant Professor, Dept of ECE, Kakinada Institute of Engineering and Technology, Korangi, A.P.

ABSTRACT

This thesis presents a novel approach to design confounded circuits for digital signal processing applications using high level transformations, a key based confounding finite-state machine (FSM), and a reconfiguration. The aim is to design Digital Signal Processing circuits which are reutilized by the specific operational methods by the designer. This design aims at the high-level transformations of repeated state graphs which have been utilized for area, speed, power compromises. It is the primary idea to develop a design flow to use high level transformations that not solely meet these tradeoffs however additionally change the architectures each structurally and functionally. Many modes of operations are introduced for obfuscation wherever the outputs are meaningful from an indication process point of view, however are functionally incorrect. Examples of such methods incorporates the next order digital filter primarily based applications that are executed in an exceedingly time multiplexed fashion. Many meaningful modes are make use to reconfigure the filter order for various applications. Still existing modes may correspond with non-meaningful modes. The configure data controls varied modes of the circuit operation. Functional obfuscation is fulfill by the right value key, and configures data. Incorrect input key is unsuccessful to change the reconfiguration and an incorrect configure data generates either a meaningful however nonfunctional or non-understandable mode. Here we have a liability to perform some chance of activating the right mode, which ends up the reduced operations to an obfuscated DSP circuit. The efficiency of proposed implementation is verified with IMAGE SCALLING WITH INTERPOLATION AND DECIMATION design, strong high level obfuscation is proved and analyzed for various key sizes.

RELATED WORK:

Most popular traditional approaches include: (a) FSMwatermarking based on Unused Transitions: the authors in [18] introduced the first IP protection using FSM watermarking. The algorithm is based on extracting the unused transitions in a state transition graph (STG) of the behavioral model. In their solution, extra transitions are added to satisfy the design goals. (b) FSMwatermarking by Property Implanting: the author in [13] tried to manipulate the STG of the finite state machine to implant the watermark as a property. The property was topological in nature and was defined in terms of visited states ($s \rightarrow s \rightarrow \cdots \rightarrow s$). In order to define the topological property, the author added extra states and state transitions in a systematic way to satisfy a specific topological requirement. (c) FSM watermarking by Integration of Two Distinct FSMs: the authors

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

in [6] designed a completely newFSM as a watermark and then the watermark FSM was combined with the original FSM to create an integrated composite FSM.Constructing a new watermark FSM was done by adding new states and transitions. More recently, a FSM watermarking scheme by making the authorship information a non-redundant property of the FSM wasproposed in [3]. In this work, the watermark bits were added into the outputs of the existing and free transitions of STG. Another method was proposed in [11]. In this work, a set of edges were added as a dummy entity. This was done by assigning state encoding values. The new edges created by this method were paired with an unused state input combination, and the output was specified as a don't-care condition. Despite these popular methods which can be effective in protecting IPs of FSMs as demonstrated in these works, these approaches are fundamentally based on expanding the original FSM to an enlarged FSM with new states and/or state transitions.

III. EXISTING METHOD

As this paper is the first attempt to develop a methodology to obfuscate DSP circuits by utilizing high-leveltransformations, it is hard to compare with other existing obfuscation methods which are general to a wide variety of designs. Therefore, we have introduced two metrics to analyze the security, Most of the hardware obfuscation techniques in this paper can also be applied to DSPcircuits. However, the use of high-level transformations from a security perspective has not been incorporated into any of these prior hardware obfuscation techniques. In addition, other circuit locking techniques only achieve protection at one-level (i.e., encrypt the normal functionality by a key), while our proposed methodology provides a two-level protection (i.e., structural obfuscation and functional obfuscation). The main advantage of the proposed methodology is the generation of meaningful variation modes from a signal processing point of view, since the meaningful modes create ambiguity to the adversary such that it is hard forth adversary to distinguish the desired functionality from other variation modes. Other existing methods, such as [6], [7], are not specific to DSP circuits, which would not be able to ensure meaningful variation modes from signal processing point of view. In addition, meaningful variation modes enable our proposed design methodology to be adaptable to reconfigurable applications. Finally, when considering the metrics of the design performance, our proposed methodology is also superior. While our proposed approach only alters the logic of switches, most of the existing methods are based on explicit FSM modifications (e.g., the technique proposed in [13]), which are not scalable since the construction of the FSM is not practical for even moderate-sized circuits, not to mention that the number of added obfuscation states can be relatively large as compared with the original FSM. In our proposed methodology, area consumption is slightly increased due to the increased cost of the control logic for the obfuscated switches.

PROPOSED DESIGN:

Block Diagram:

The block diagram mainly contains five blocks each block has own importance in

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

implementation. The different blocks are image input block, main control block, line register block, combined filter block and Interpol bilinear block. The operation of each block is described herein the preceded headings. The program execution of each block is also explained with the help of flow charts. Clock and reset signals are given to each block so that they operated synchronously. The image input isn't given by me it's internally generated signal. Whenever reset value is high i.e logic one the output is 000000……whenever reset value is logic 0 and correct key's given to regulate then the correct or desired output get in the output. For the execution of program clock is given as input.

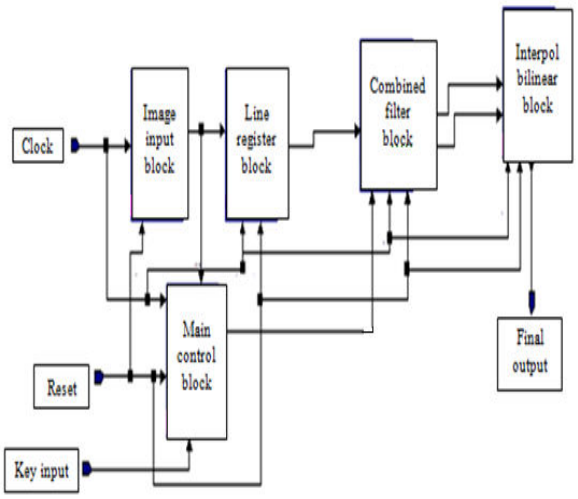


Figure 3.2 Block Diagram.

3.5.1 Image Input Block:

This block is nothing however a counter that generates count values 0 to 255 that is 256 bits of data. This information is organized as 16x16 matrix type that is greyscaled image. For every one bit different colors are assumed. Here is flow chart which explains about how the count values generated and counting value increased.

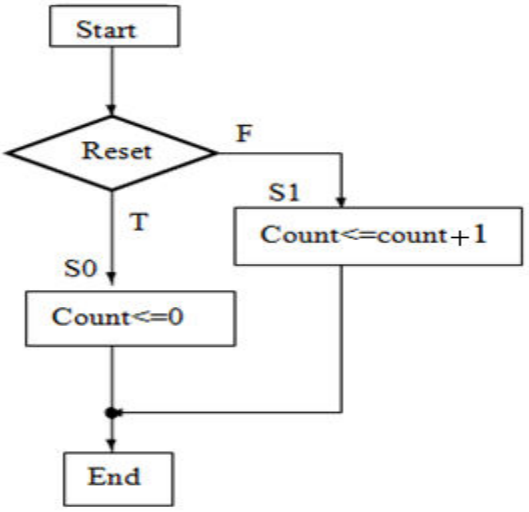


Figure 3.3 Flow chart for image input block

3.5.2 Main Control Block:

This block explains about the states which are changed from one to another when timeout occurs and key values are given. For every timeout condition and different key values transition of states changed. This is given in the finite state machine diagram.

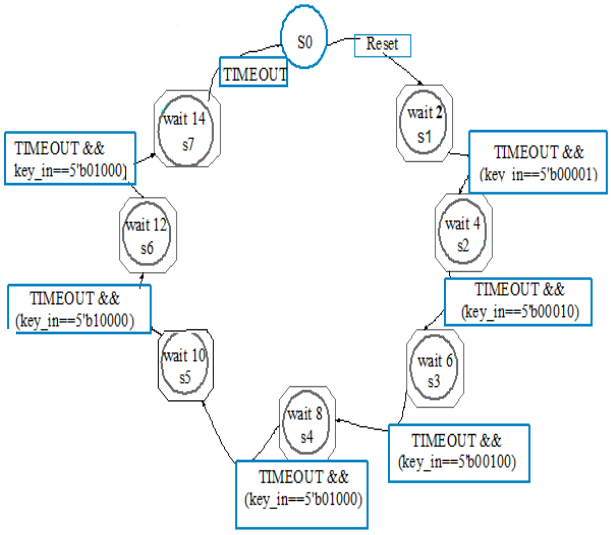
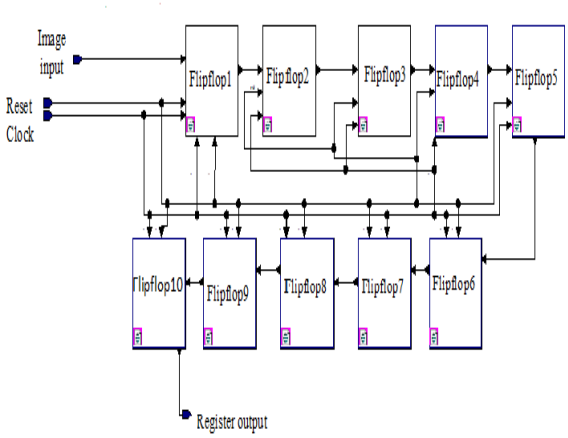


Figure 3.4 Main Control Mechanisms.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

3.5.3 Line Register Block:

In this block shifting and delay of input data takes place. In this registers which are flip flops only used for storing, delaying and shifting operations. The program execution of each flip flop is same and the flow is explained in the flow chart. Shifting of data takes in each flip flop.



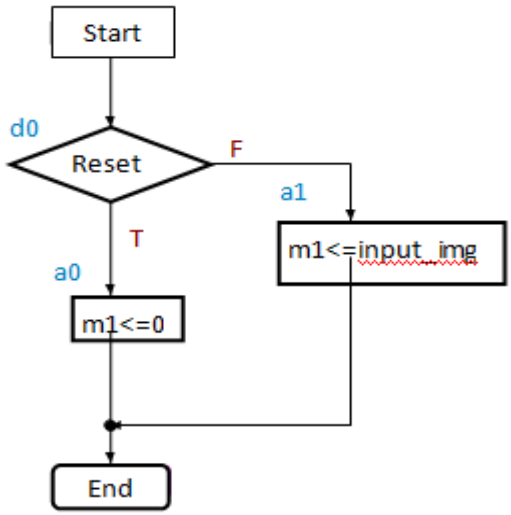
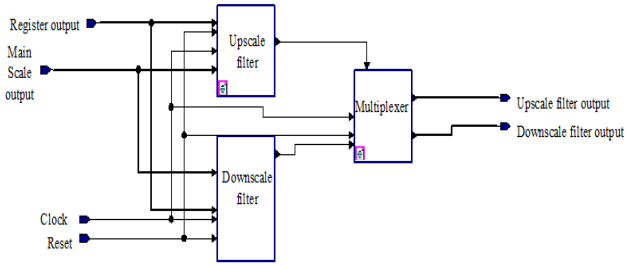


Figure 3.5 Line Register and Flow Chart.

3.5.4 Combined Filter Block:

In this module the data is chooses depends on left or right shifting operations in line register block by using a multiplexer. Based on left shift or right shift the data is upscaling or downscalig is takes place. In this we have two filters one upscale filter and another one is downscale filter. The choose of multiplexer output based on the filter output values which are upscaled or which are downscaled. The flow chart gives the information about execution of program.



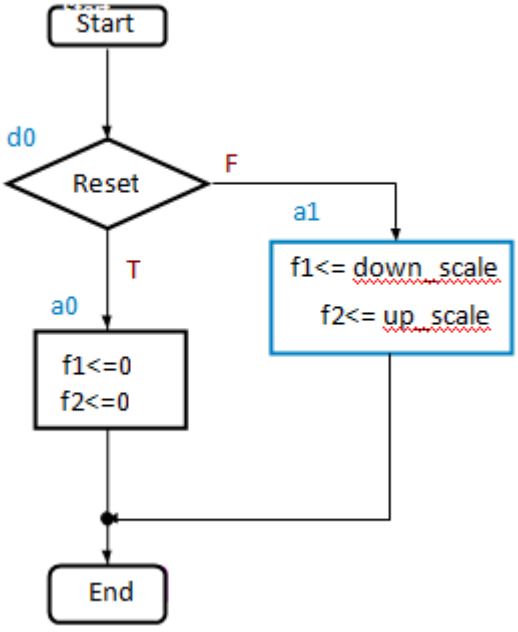


Figure 3.6 Combined Filter and Flow Chart.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Design Flow of the Proposed DSP Circuit Obfuscation Approach:

The DSP hardware prevention methodology is done through confounding by preventing the functionality via high level transformations. This method assist the designer to target the DSP design piracy by dominant the circuit configuration among the generated variation modes F G SR clock reconfigurator reset state M U X . . . pick signal connection one, connection two, connection k counfounding configuration FSM key (switch instances).

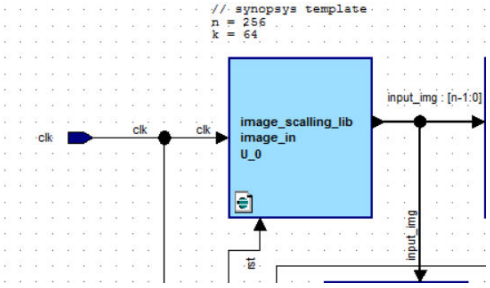


Figure 3.8 Counter design for DSP obfuscation

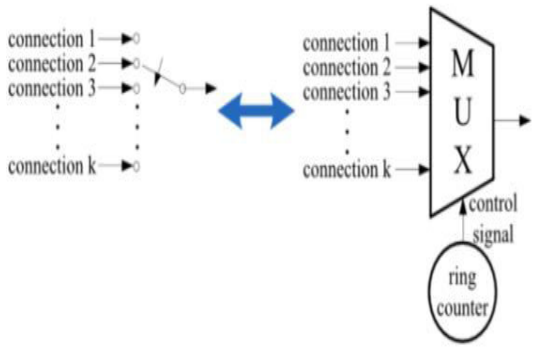


Figure 3.9 Switch design for DSP obfuscation

The detailed design procedure is described below:

Step1: DSP algorithm: - This step creates the DSP algorithm based on DSP application

Step2: High-level transformation choice: - Based on the precise application, applicable high-level transformation ought to be chosen consistent with the performance demand.

Step3: Obfuscation via high-level transformation: - Suitable high level transformations are applied. With obfuscation variation modes, and totally different configurations of the switch instances are designed.

Step4: Secure switch design: - The secure switch is meant for the development of high level transformations.

Step5: Two level FSM generation: - The reconfigurator and therefore the confounded FSM are comprised into the DSP design. The configuration key is generated at this stage.

Step6: Design specification: - This step comprises the HDL and netlist creation and simulation of the DSP system. The proposed design methodologies don't need vital changes to established verification and testing flows. In fact, the confounded DSP circuit with the proper key behaves rather like the first circuit.

Here we tend to use the DSP circuits are to be confounded via high level transformations by suitably designing the switches in an exceedingly secure manner. The switches which are created with high level transformations are periodic with period N to one switchs. These switches will be enforced as multiplexers, whose control signals are obtained from ring counters as shown in Figure 3.10. Thus, the protection of the switch depends upon implementation of the ring counters such the outputs of the ring counters

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

are going to be obfuscated. An FSM is often outlined by a 6-tuple (I, O, S, S0, F,G), where S, S0, F, G may be a finite set of internal states, I and O represent the inputs and outputs of the FSM, severally, F is that the next-state function, G is that the output function, and S0 is that the initial state. However, in distinction to general FSMs, the FSM of a ring counter is input independent, such it endlessly transits to future state depends on the current state. As a result, the control signal of the switches are periodic.

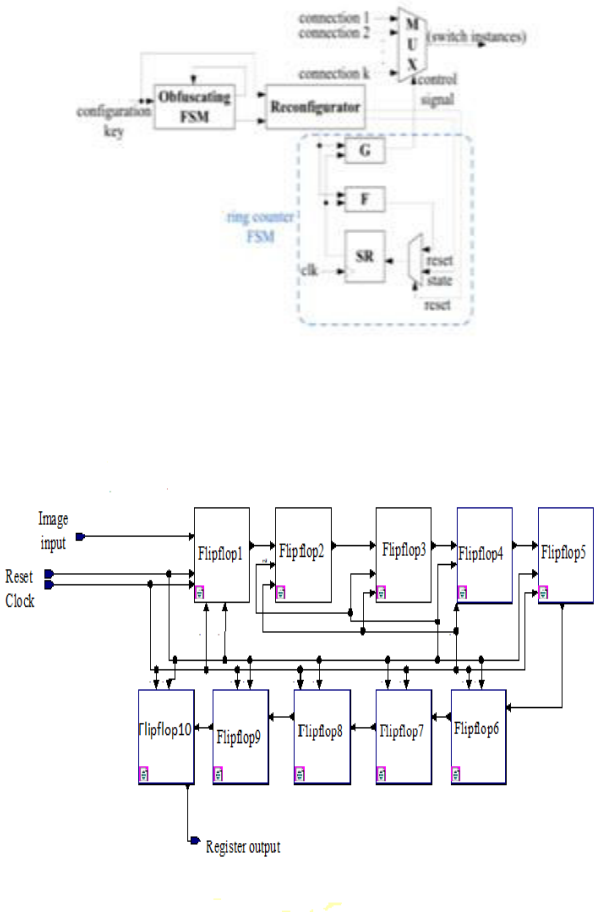


Figure 3.10 Representing design blocks for Reconfiguration for Obfuscation.

Our scaling methodology needs low computational quality and solely one line memory buffer, thus it's appropriate for low price VLSI implementation. Figure 3.2 shows diagram of the each stage VLSI design for our scaling methodology. The design contains seven main blocks: counter module (CM), register bank (RB), Interpolator and decimator and therefore the controller. Every of them is represented concisely within the following subsections.

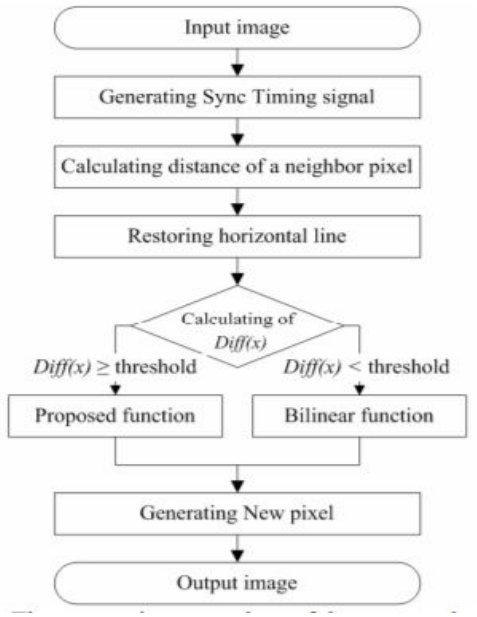


Figure 3.11 Algorithm and Flow Chart for Proposed Design.

1. **Counter Module:** This module is mainly utilized for sequence and generate image pattern for the specified application.
2. **Register Bank**: Here the purpose of the register bank is to provide the different shifting and storing of the image data in different levels.
3. **Interpolation:** Interpolation is a technique of constructing new data points in the well known data points.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

4. **Decimation:** Decimation by a number factor, M, will be explained as a 2-step method, with identical implementation that's additional economical.

a. Decrease high frequency signal components with a digital low pass filter.

b. Down sample the filtered signal by M, that is, keep only every M sample, remaining values are deleted.

Down sampling alone roots high frequency signal elements to be misinterpreted by later users of the information that may be a kind of distortion known as aliasing. The primary step, is to suppress aliasing to a suitable level. During this application, the filter is termed an anti aliasing filter, and its design is mentioned below. Conjointly see undersampling for data concerning downsampling bandpass functions and signals. When the anti-aliasing filter is an IIR design, it depends on feedback from output to input, before the downsampling step. With FIR filtering, it's an easy meet to calculate solely each M^{th} output. The calculation performed by a decimating FIR filter for the ordinal output sample could be a real.

$$y(n) = \sum_{k=0}^{k-1} x[nM - k].h[k]$$

RESULT ANALYSIS

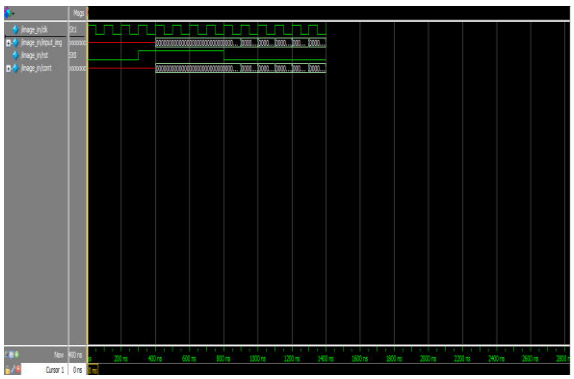
Introduction:

This chapter gives the information about the output waveforms of each and every block and additionally the Xilinx results which gives the knowledge about how the area and power dissipation values of chip are dropped to a small value.

Output Waveforms:

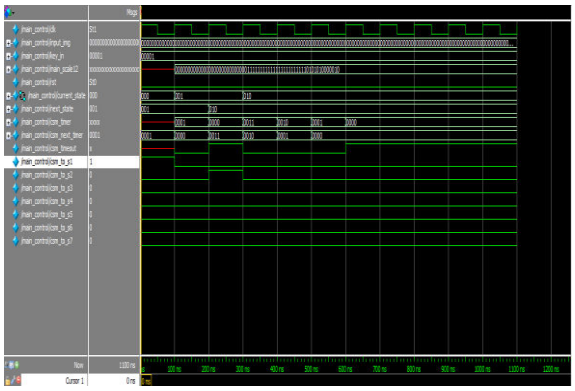
Image input block output:

This waveform output is exported from modelsim. For every clock cycle the output of image input block are changed whenever the reset value is zero. If reset value is one the output of block is not changed the value is like 000000……



Main control block output:

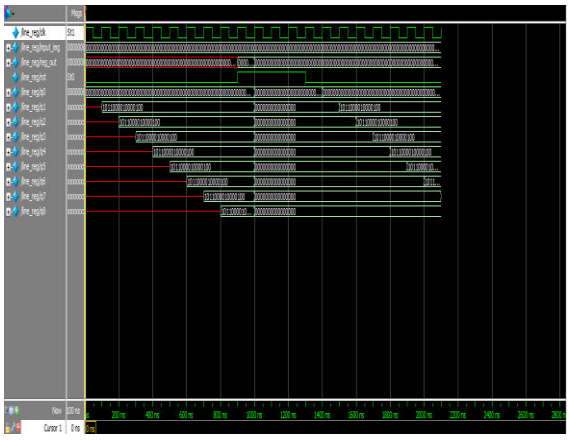
In main control block output the states are changed. In this design block the key value 00001 is given then the state is altered from s0 to s1.If the key values are not given the transition of states not happen.



Line registers block output:

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

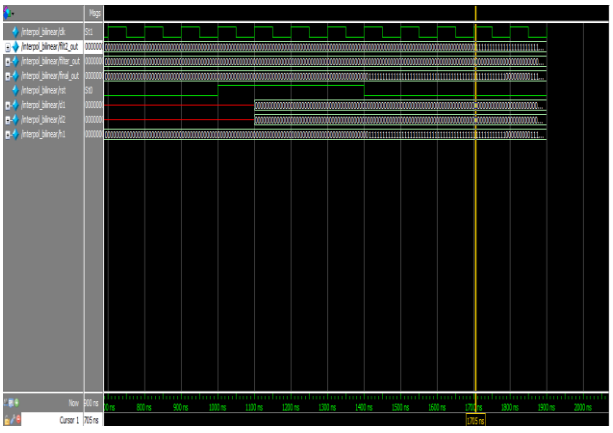
In line register block shifting of information bits takes place that is determined within the waveforms that takes only the reset value is zero. If reset value is one the shifting of bits not happen in waveforms.



Combined filter block output:

In the combined filter block the upscaling and downscaling operations of the image takes place. The upscaled and downscaled waveforms values of image are observed here.

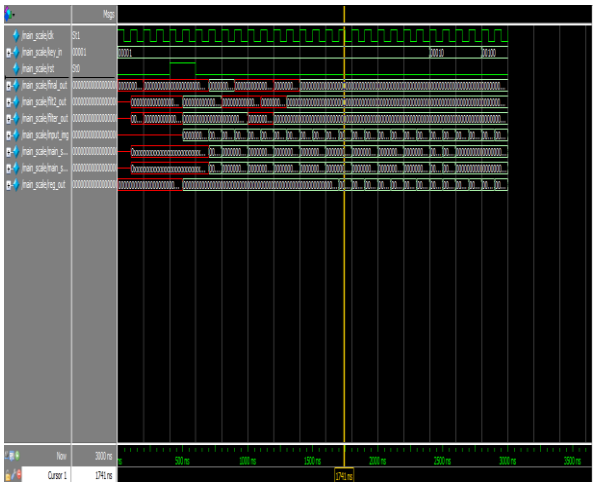
Interpol bilinear block output:



The output of Interpol bilinear block is shown in the waveform. The output image scaled values of the 2 filters are compared once comparison the larger value filter output is come into view as output.

Final output:

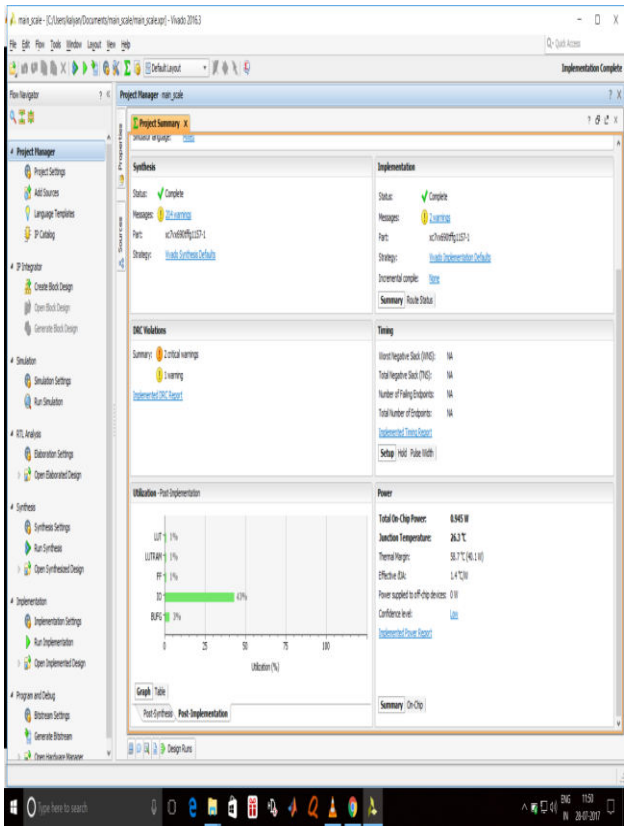
The final output waveform values are observed here whenever the key values are changed the final output values are changed. In waveform the key values 00001, 01000 are given, the output observed with both key values are different in nature.

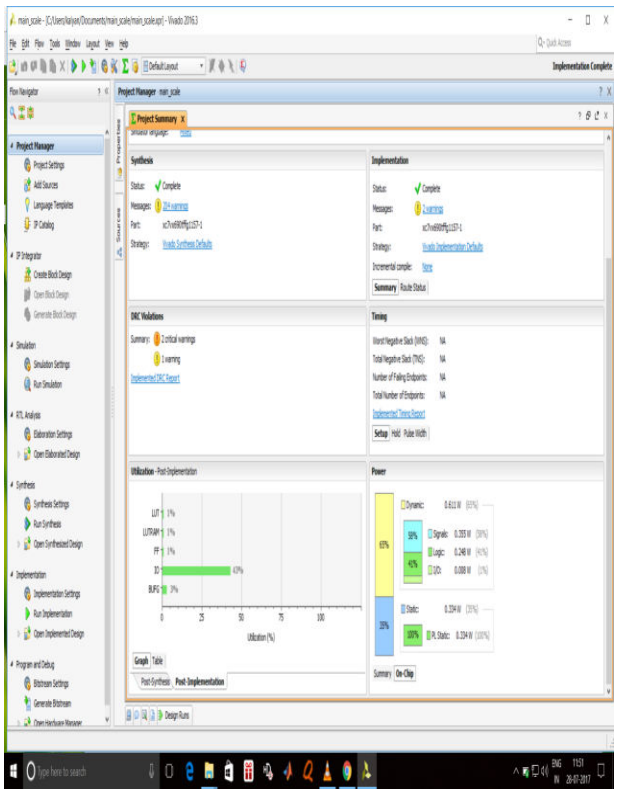


Xilinx Results:

The Xilinx results give the information about how the power consumption is bring to a small value and area of chip is also bring to small value. The static and dynamic power dissipation values are observed. The static power ingestion is concerning 35% and dynamic power ingestion is concerning 65%. Within the dynamic power ingestion much power is dissipated in signals subsequently logics than in input output section. The on chip power is 0.945w, the junction temperature is 26.3^0C which is observed in Xilinx result image. The utilization of power is more in IO blocks.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org





CONCLUSION:

The output resulted waveform of each block is exported and placed here. In this whenever the reset value is high we get the output as 00000…. And reset value is zero we get scaling output. The area of chip and power dissipation values are reduced which are observed in the Xilinx results.

CONCLUSION AND FUTURE SCOPE

This thesis confers an occasional overhead answer to implement DSP circuits which are obfuscated structurally and functionally by utilizing high level transformations techniques. It's shown that confirming the equivalence of DSP circuits by using high level transformations are tougher if some switches may be designed in such a way that they're inconvenient to trace, a configurable switch design is included within the projected design scheme to improve the protection. An entire design flow is given within the proposed confounding methodology, the variation modes and therefore further confounded circuits might even be designed which consistently supported the high level transformations. Obfuscated and reconfigure FSM modes of which reduce the area of performance speed improved to 341.53MHZ.

This work provides awareness in the foremost generalized design which will be praxis built for different image process applications too. Though, the major fundamental point performances on the image are mentioned, the thought could carried forward for filtering applications also. The key summons during this work is to settle on a correct FPGA for prototyping, since the memory buffer wants

huge memory, the crucial aspect is to settle on an FPGA which has enough RAM, FIRST IN FIRST OUT resources.

REFERENCES

[1]. J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Brand and IPprotection with physical unclonable functions," in Proc. IEEE Int. Symp. Circuits Syst., May 2008, pp. 3186–3189.

[2]. G. E. Suh and S. Devadas, "Physical unclonable functions for deviceauthentication and secret key generation," in Proc. 44th Annu. DesignAutom. Conf., Jun. 2007, pp. 9–14.

[3]. A. L. Oliveira, "Techniques for the creation of digital watermarks insequential circuit designs," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 20, no. 9, pp. 1101–1117, Sep. 2001.

[4]. D. Kirovski, Y.-Y. Hwang, M. Potkonjak, and J. Cong, "Intellectualproperty protection by watermarking combinational logic synthesis solutions," in Proc. Int. Conf. Comput.-Aided Design, Nov. 1998,pp. 194–198.

[5]. A. B. Kahng et al., "Watermarking techniques for intellectual propertyprotection," in Proc. 35th Annu. Design Autom. Conf., Jun. 1998, pp. 776–781.

[6]. F. Koushanfar and Y. Alkabani, "Provably secure obfuscation of diverse watermarks for sequential circuits," in Proc. Int. Symp. Hardw.-OrientedSecurity Trust, Jun. 2010, pp. 42–47.

[7]. J. A. Roy, F. Koushanfar, and I. L. Markov, "EPIC: Ending piracy ofintegrated circuits," in Proc. Conf. Design, Autom. Test Eur., Mar. 2008, pp. 1069–1074.

[8]. W. P. Griffin, A. Raghunathan, and K. Roy, "CLIP: Circuit level ICprotection through direct injection of process variations," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 20, no. 5, pp. 791–803,May 2012.