Design and Simulation of Intellectual Properties Protection using Clipping Filter Algorithm with Random Placement

Surya Michrandi
School of Electrical Engineering
Telkom University
michrandi@telkomuniversity.ac.id

Fairuz Azmi
School of Electrical Engineering
Telkom University
worldliner@telkomuniversity.ac.id

Hanjara Cahya Adhyatma
School of Electrical Engineering
Telkom University
adhyatma.han@google.com

Abstract—System on a Chip (SoC) is an embedded system module that has functionality in a silicon chip board that can also be called Veri Large Scale Integration (VLSI). The owner of the SoC design owns the copyright on the design of the system that has been created. Fabless manufacturing is a way of printing hardware modules that Integrated Circuit (IC) designers are Outsourching from outside the printing factory. Fabless manufacturing from IC design has gap design theft When the design will be printed or when the project requires mutiple module With various functions from various designers. Therefore every module is VLSI Of this chip designer requires proof of ownership of the designer or Production companies. In this study plans to make the verification of ownership design with 2 specific key verification that is Polygate as the main key that will activate the second key, and the second key will be active which process using digital filter algorithm.

Index Terms—VLSI, Intellectual Property Protection, Digital Signal Processing, Polygate Watermark.

1 Introduction

Providing a series of watermarks as a safeguard to a printed VLSI blueprint that indicates ownership of the designer or module manufacturer will protect against cheating others who will steal the design. So the possibility of theft or plagiarism that causes losses to the company or designer because of its design is stolen or plagiarism reduced. [1]

2 Related Works

Broadly speaking the technique of Intellectual Property Protection (IPP) watermarking can be classified into 2 classes namely Dynamic Watermarking and Static Watermarking. Dynamic Watermarking is a watermark that can not be detected except by running a watermarked IP to detect the resulting signal, such as digital signal processing (DSP), or finite state mechine (FSM) watermarking. Static Watermarking is a watermark that refers to the properties of a design, and can only be detected in different static ways, such as paths and watermarking placements.[2] One of the other safeguards is to convert the simulated file from a file. The RTL source code that enables is not easy to be reverse-engineered by third parties, so the model can not be changed and reused with other purposes by third parties and irresponsible users. However, this way only protects from the softwere side that protects the IP from being misused by third party users.[3] For IP security used in project sharing and reusable projects can be used with the security of Digital Signal Processing cell that allows integration in the system. In this research will perform a combination of polymorph gate IP protection with digital filter algorithm. Using a combination of these two techniques will provide additional security to IP protection that is likely to over write a smaller watermark. Therefore in this study proposed a combination of existing methods to improve security capabilities in an existing VLSI module. Combine polygate as a combination key to enable the digital filter module to be used as a watermark.

3 Watermarking

Providing a series of watermarks as a safeguard to a printed VLSI blueprint that indicates ownership of the designer or module manufacturer will protect against cheating others who will steal the design. So the likelihood of theft or plagiarism is reduced which causes losses to the company or the designer because of his design is stolen or in plagiarism.

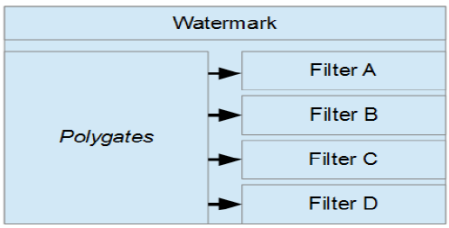

Fig. 1. Simulation results for the network.

The design will be designed with a combination of Low Pass Filter, High Pass Filter, Band Pass Filter, and Band Reject Filter. This combination will be determined and enabled by polygate as a key to activating a combination

of digital filters. After the digital filter is active then the data combination will pass through a combination of filters enabled from the polygate combination.[8], [9] Then the result data combination of these processes will form a special pattern that becomes the watermark data of the designer that characterizes the identity of the designer. Once given the watermark then the module will be tested again its performance. If there is a decrease in performance it should be re-improved the algorithm and then re-tested its performance until obtained the best performance.

3.1 Polymorph

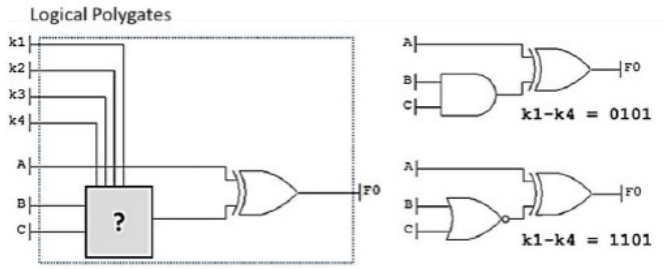

Fig. 2. Simulation results for the network.

Polymorph gate is gate that will change the property of gate such while the key selector key is change. Example is from AND function will active while key is 0101 and it will change to NOR function while key change to 1101.

3.2 Watermark Flow

Filter is 3 bit data filter that will clip maximal value or minimal value that has set before. So the data that will go through system is accepted data from clipping filter. In this illustration showed how IC is watermarked with

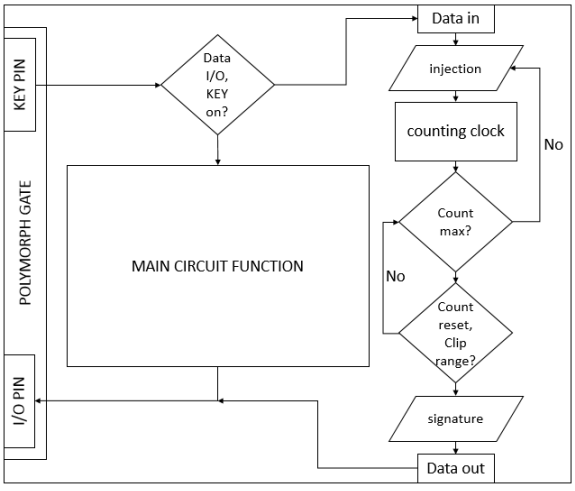

Fig. 3. Simulation results for the network.

given technique. With polymorph gate as bridge between watermark and main circuit function and key pin as gate to access between main function and watermark. To access watermark, developer will activated combined code to given key pin in the printed IC, and after the key activated it will open bridge in the polymorph to watermark circuit. After watermark circuit is opened, developer will inject secret encoded data to circuit and it will decode the given data as signature on the output pin. Data injected as bit stream so it need time to inject and waiting for de-coded output stream.

To extract signature from injected data it will counting how many data will be slice and clip it until given tolerate count. After that data will be checked if the data is inside tolerated range, if yes data will be transferred to polymorph I/O as extracted signature data.

3.3 Data I/O

Data in data out is example how filter is going in and let the verification data through system generated and will procced so data will change to specific bit array. By injected long bit stream data to IC with purpose to deceive the attacker. And the output is just specific short bit stream data. The purpose given long input and short output is to avoid watermarks is detected by forced data injection. And here is example with streaming bit data with clipping on the 5/1 injection data. With 20 data stream and 4 data output as zero is ignored. Inputted data will be procced with given algorithm before to extract signature data.

TABLE 1
Data time verification 20 to 4 clock

Time	in 0	in 1	in 2
0	1	1	1
1	1	0	1
2	1	1	0
3	0	1	0
4	0	1	1
5	1	0	0
6	0	1	0
7	0	0	0
8	1	1	1
9	1	0	0
10	0	1	0
11	0	0	1
12	0	1	0
13	1	0	1
14	0	1	1
15	1	0	0
16	0	1	0
17	1	1	1
18	0	1	1
19	0	0	0

Time	out 0	out 1	out 2
0	0	0	0
1	0	1	0
2	0	0	0
3	0	0	1
4	0	1	1

3.4 Layouting

Gate for layout use CMOS technology. The protection use simple basic CMOS gate for mixed implemented for hard removal from reverse engineering, there are:

3.5 Layout Verification

For simple see through layout with just verification without mixed gate placement, here is total gate if the gate collected as one cell:

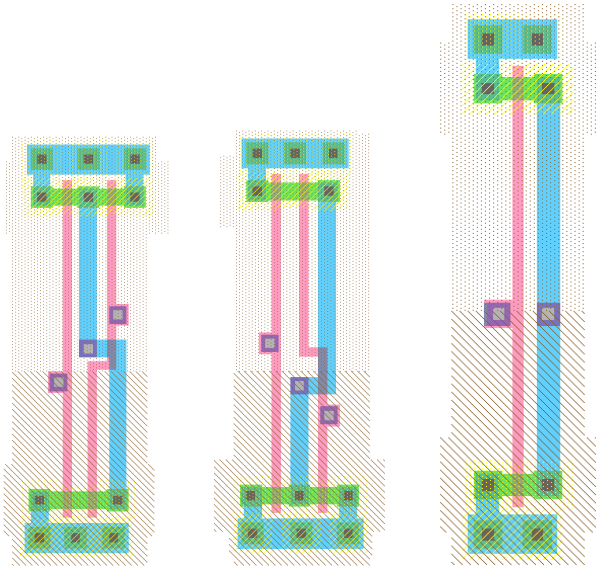

Fig. 4. Simulation results for the network.

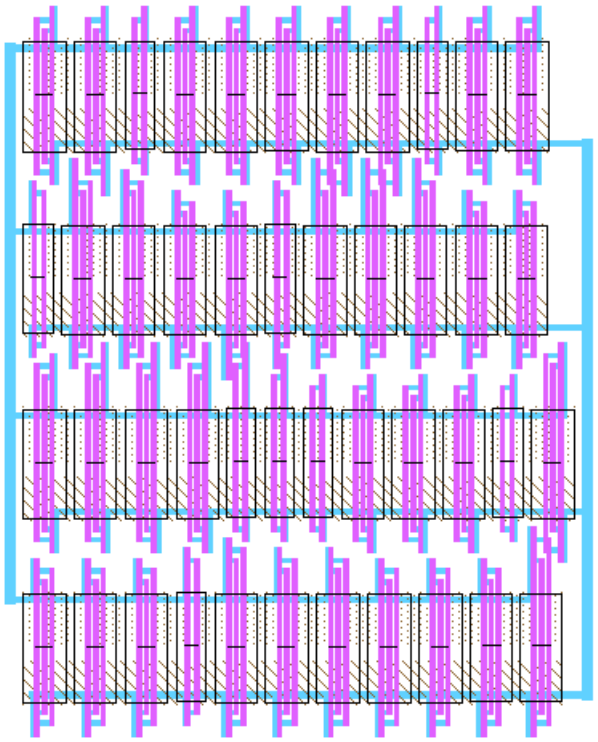

Fig. 5. Simulation results for the network.

3.6 Mixed Random Gate Placement

In general technique when engineer will manufacturing IC is make hierarchy of cells so it will easy to routing and tracing circuit problem. But if the watermark circuit is manufactured with that technique it will easy to expose watermark circuit inside the IC. So it will lead to hard removal and reverse engineered the IC. To prevent that happening the watermark cell will generate without hierarchy and placed with random routing algorithm. So it will not be so obvious that watermarks circuit is implemented within the main IC core circuit. Mixed Random Gate Placement is randomize

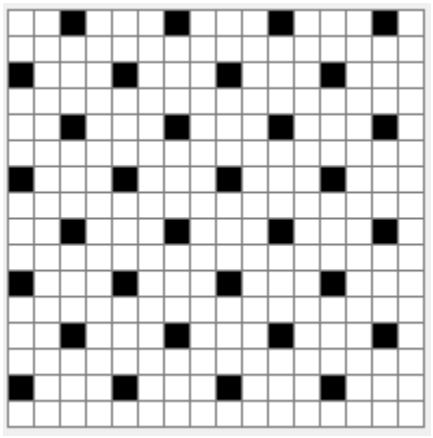

Fig. 6. Simulation results for the network.

Verifications components with main IP cell component. So it will placed wherever inside IP cell. Here is figure that tell how verifications components gate placed inside main IP cell:

The dark dot representation of NAND, NOR and INVERTER from verification components. So for hard removal watermark it will change entire design and it will harder to detect watermark from random placement.

4 Analysis

In this section, analysis is focution on how watermark actualy didn't create error to original design so watermark will be usefull to protect original design from thiefing.

4.1 Watermark softwere simulation

This is simulation from data given before. Data from device to read and inject data is translated as alphabetic character from 3 bits data stream. It is show long data stream with short data output as signature.

4.2 Power Consumption Orogonal Design

Power consumption is the most important thing in the electronic design, adding more component mean more power is needded to drive the device. Here data from experiment with original design in power consumption needed to drive the device:

4.3 Power Consumption Watermark

Power consumption is the most important thing in the electronic design, adding more component mean more power is needded to drive the device. Here data from experiment with original design in power consumption needed to drive the device:

4.4 Comparison

On the Table 2 are comparison about all parameter that tested on

TABLE 2
Input Array

H	111
F	101
G	110
C	010
D	011
E	100
C	010
A	000
H	111
E	100
C	010
B	001
C	010
F	101
D	011
E	100
C	010
H	111
D	011
INPUT	HFGCDECAHECBCFDECHD
OUTPUT	CABE

TABLE 3
Original Power

Supply Source	Supply Voltage	Total Current (mA)	Quiescent Current (mA)
Vccint	1.2	2.01	2.01
Vccaux	2.5	3.00	3.00
Vcco25	2.5	0.20	0.20

TABLE 4
Watermark Power

Supply Source	Supply Voltage	Total Current (mA)	Quiescent Current (mA)
Vccint	1.2	2.89	2.01
Vccaux	2.5	3.00	3.00
Vcco25	2.5	0.20	0.20

5 Conclusion

From the experiment testing for performance analysis with given parameter. The percentage change is still within reasonable limits. So that in its application still can be applied.

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.
[2] R. Chapman and T. S. Durrani, IP Protection of DSP Algorithms for System on Chip Implementation, vol. 48, no. 3, pp. 854861, 2000.
[3] Watermarking Techniques for Electronic Circuit Design, no. 1, pp. 117.
[4] Q. Liu, W. Ji, Q. Chen, and T. Mak, IP Protection of Mesh NoCs Using Square Spiral Routing, vol. 24, no. 4, pp. 15601573, 2016.
[5] A. Cui, C. Chang, S. Member, S. Tahar, and S. Member, A Robust FSM Watermarking Scheme for IP Protection of Sequential Circuit Design, vol. 30, no. 5, pp. 678690, 2011.
[6] T. Nie, Performance Evaluation for IP Protection Watermarking Techniques.
[7] J. Zhang, Y. Lin, Y. Lyu, G. Qu, and S. Member, A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-Per-Device Licensing, vol. 10, no. 6, pp. 11371150, 2015.
[8] J. Zhang, Y. Lin, Q. Wu, and W. Che, Watermarking FPGA Bitfile for Intellectual Property Protection, pp. 764771.
[9] A. B. Kahng et al., Watermarking Techniques for Intellectual Property Protection.
[10] V. G. Moshnyaga and H. Nita, STG-based Detection of Power Virus Inputs in FSM.

TABLE 5
Comparison

No.	Parameter	Before	After	Delta
1.	Gates	5234	5324	1.72
2.	Layout	Lamda	lamda	
3.	Power	A	A	
4.	Functional	Normal	Normal	zero