Watermarking Based IP Core Protection

Yu-Cheng Fan and Hen-Wai Tsao

Integrated System Lab
Department of Electrical Engineering and Graduate Institute of Electronics Engineering
National Taiwan University, Taipei, Taiwan, 10617, R.O.C.
E-mail : d9921004@ee.ntu.edu.tw

ABSTRACT

This paper presents a watermarking technique for intellectual property (IP) core protection. We propose a method for embedding a watermark into IP core. In this work, we establish principles for development of new watermarking-based IP protection procedures. This technique is applicable to IP-based design. The proposed technique successfully survives synthesis, placement and routing. After the chip has been packaged, it's still easy to detect the ownership rights of the IP provider.

1. INTRODUCTION

The advance of semiconductor processing technology has led to a rapid increase in IC design complexity. IP-based design has become a major concern in IC industries [1]. Design reuse has led to the development of intellectual property protection techniques. The protection of virtual components becomes more and more important. One potential solution for claiming the ownership is to use watermarks. Watermarking is a technique traditionally used to securely identify the authenticity of the source of image, video or audio. Recently, a number of watermarking-based IP protection techniques have been proposed. In the literature, several techniques have been developed for IP core protection. Although some researchers have investigated into the physical design level, few researches have been done on behavioral design level. In [2], Andrew developed the protocols for IP protection at the physical design level, using the concept of constraint-based watermarking. In [3], Naveen Narayan proposed a method for embedding a watermark by modifying the number of vias or bends used to route the nets in a design. All of these techniques embed watermark at the physical design level [4][5][6][7]. After synthesis, placement and routing, layout of the soft IP Core will be changed. These techniques are therefore not enough to protect the ownership rights of the soft IP Core. Besides, we must look at the photomicrograph if we want to check the ownership rights. These methods are not only complicated but also inconvenient. It's very difficult to detect the ownership rights of the IP provider after the chip has been packaged.

In order to solve these problems, we propose a method for embedding a watermark into soft IP core. The watermark is embedded into the test circuit. The generality of soft IPs will keep the test circuits after integrating IPs into full SOCs[8]. The designer provides the test vectors (input and output vectors) to detect the packaged-chip[9]. After integrating IPs into full SOCs, the only signal in IP that we can trace is the test signal. If we combine test circuit with watermark generating circuit, we can secure ownership rights of the IP provider easily. It's also easy to detect the ownership rights of the IP provider. After the chip has been packaged, any IP in the chip may be observed and tested. In test mode, the appointed IP sends output test patterns and watermark sequence. We can get ownership rights of the IP provider according to watermark sequence. The IP provider is able to trace a company for unauthorized resold copies of the IP. Because the watermark generating circuit has been designed on behavioral level, the proposed embedding technique can survive the synthesis, placement and routing.

The paper is organized as follows. IP-based design flow with watermark is described in Section 2. Section 3 describes experimental results and discussions. In Section 4, the conclusion of this paper is stated. The references are shown in Section 6.

2. IP BASED DESIGN FLOW WITH WATERMARK

We propose a new watermarking technique to solve the copy detection problem. Figure 1 describes the IP-based design flow with watermark. We use the digital watermarks with visually recognizable patterns. The owner of the IP tries to design a uniquely identifying watermark that may be a personal seal, an organization logo, or designer's signature. First of all, the watermark is generated as a binary pattern and then permuted to disperse the spatial relationship according to some pseudorandom order. We design a watermark generating circuit to generate the watermark bit-streams.

After the watermark generating circuit has been designed, we combine test circuit with watermark generating circuit. When the chip is in test mode, the chip will send out watermark sequence and test patterns. According to the watermark sequence, we can get ownership rights of the IP provider. How to combine test circuit with watermark generating circuit is very important. We propose five methods to combine test circuit with watermark generating circuit and analyze the advantage and the disadvantage of each method:

a) Headed Watermark Sequence Method: When the chip is in test mode, the chip sends out watermark sequence first. After sending out all watermark sequence, the chip sends output test patterns. (Fig. 2(a)) The watermark sequence is like the header

0-7803-7761-3/03/$17.00 ©2003 IEEE

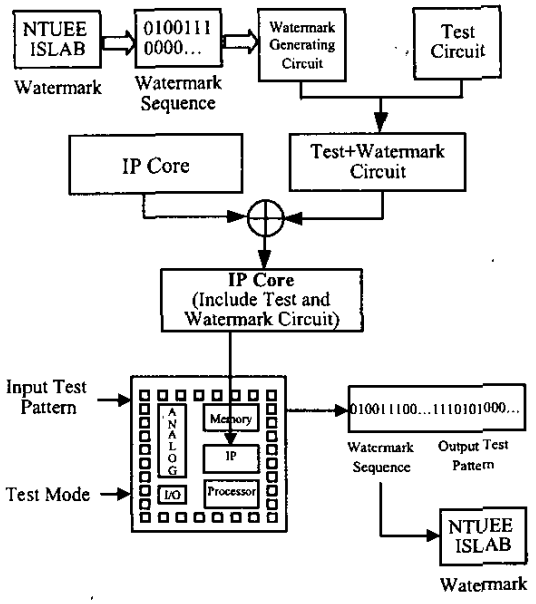


Figure 1. "Watermarking Based IP Core Protection" Design Flow

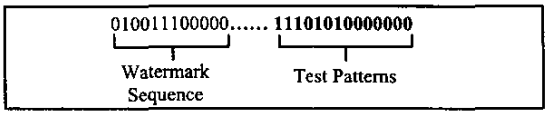
of a bit-stream. Therefore, we call this scheme "Headed Watermark Sequence Method." This method extracts the watermark simply. The drawback of the method is that the watermark is easy to detect or remove.

b) Periodic Watermark Sequence Method: When the chip is in test mode, the chip will send out watermark sequence and test pattern alternately. (Fig. 2(b)) The watermark sequence appears periodically. Therefore, we call the proposed this scheme "Periodic Watermark Sequence." We can extract the watermark at any time. It is also easy to detect because the watermark appears periodically.

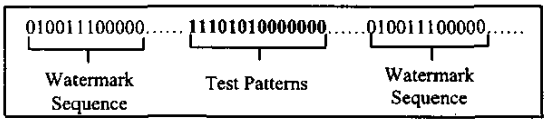
c) Cyclic Redundancy Watermark Sequence Method: When the chip is in test mode, the chip sends n-bit output test patterns. (Fig. 2(c)) After the output test patterns are sent, the chip sends one bit watermark data. The chip sends n-bit output test patterns and one bit watermark data alternately. The watermark sequence and output test patterns appear cyclically. The watermark data is like the redundancy bit near the test pattern every n bits. Therefore, we call the proposed this scheme "Cyclic Redundancy Watermark Sequence Method." We can extract the watermark every n bits output test patterns and detect the ownership rights from the watermark sequence. It is easy to extract the watermark and hard to destroy ownership rights.

d) Random Watermark Sequence Method: We try to generate a pseudorandom sequence and store it in the memory first. According to the random order, the chip sends watermark data. For example, if the random sequence is 1、5、2、4、7, the chip sends one bit output test pattern, one bit watermark data, five bits output test patterns, one bit watermark data, two bits output test patterns, one bit watermark data , and so on. (Fig. 2(d)) This method has high security. It is hard to be detected and removed. The drawback of the method is that high hardware complexity.

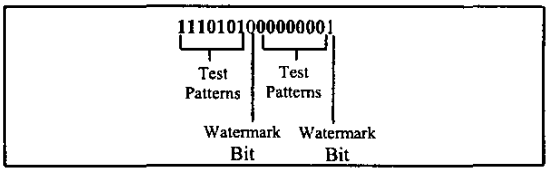
e) Operational Watermark Sequence Method: To perform exclusive-or (XOR) operation on the watermark sequence and output test patterns to obtain new patterns. (Fig. 2(e)) When the chip is in test mode, the chip sends the new patterns. We can extract the watermark after exclusive-or (XOR) operation on the new patterns and test patterns to get a watermark sequence. This method has high security. It is hard to be detected and removed. The drawback of the method is that if some bits are in error, we could not recognize which circuit is fail (watermark generating circuit or test circuit).



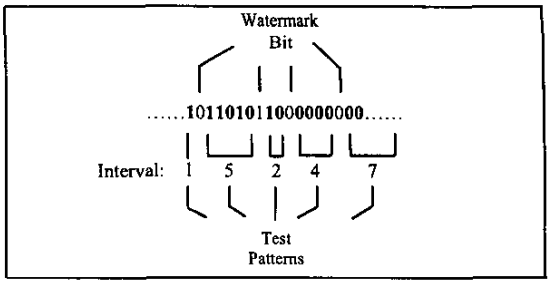
(a) Headed Watermark Sequence Method



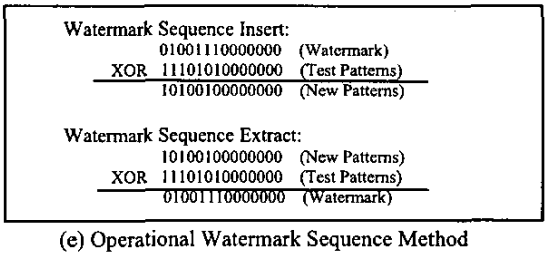
(b) Periodic Watermark Sequence Method



(c) Cyclic Redundancy Watermark Sequence Method



(d) Random Watermark Sequence Method



(e) Operational Watermark Sequence Method

Figure 2. We propose five methods to combine test circuit with watermark generating circuit

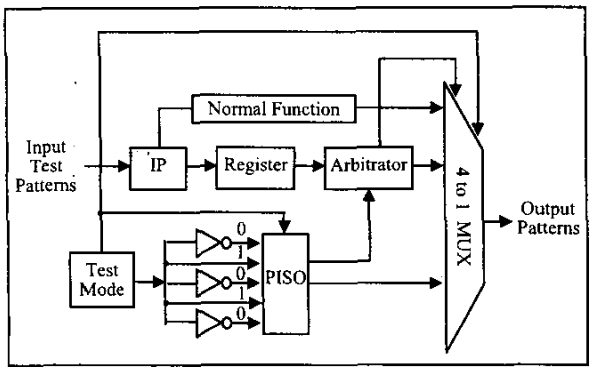


Figure 3. Architecture of the watermark generating circuit (Headed watermark sequence method)

We can choose one of the above methods depending on our requirement. For example, we use the "Headed Watermark Sequence Method." We design the watermark generating circuit and combine the test circuit with watermark generating circuit. The architecture of the circuit is shown in Figure 3. When someone uses this chip in test mode, the "test mode signal" control the watermark generating circuit and test circuit. The watermark generating circuit is composed of PISO (parallel in serial out register) and several inverter gates. The parallel watermark data is generated when the test mode signal is active. The PISO translates the parallel watermark data into the serial watermark sequence. At the same time, test patterns input into the chip. In this method, the chip sends out watermark sequence first and sends out test pattern later. According to the watermark information, the IP provider is able to rearrange the watermark sequence using the predefined pseudorandom order. The IP provider is able to trace a dishonest company for unauthorized resold copies of the IP. We don't need to look at the photomicrograph if we want to check the ownership rights. This method is easier than conventional methods.

3. EXPERIMENTAL RESULTS AND DISCUSSIONS

We have performed a set of experiments to evaluate the effectiveness of the "watermarking based IP core protection". In order to verify the property of the architecture proposed, we present five IPs to validate this approach in this section.

3.1 Results

To verify the feasibility of the architecture proposed, we present some results of experiments. Watermarking results for the synthesis experiments are summarized in Table I . We report synthesis results for each IP. These results provide the hardware cost overhead. We design five kinds of watermark generating circuits that can generate 20 bits watermark sequence separately. The Headed Watermark Sequence Method needs 207~223 gates. The Periodic Watermark Sequence Method needs 349~371 gates. The Cyclic Redundancy Watermark Sequence Method needs 297~314 gates. The Random Watermark Sequence Method needs 509~533 gates. The Operational Watermark Sequence Method needs 625~641 gates. We just increase area no more than five percent to add watermark-generating circuit. Our proposed methods are low hardware cost.

Table II summarizes the results of synthesis, placement and routing. Because we embed the watermark into the test circuit at the front-end, the watermark function is not changed after synthesis. No matter what kind of constraint is used, we still can extract the watermark sequence correctly. After placement and routing, we can still detect ownership rights according to the watermark sequence.

Table III summarizes the results of gates tampering and P&R tampering. Because the watermark generating circuit is hidden in the whole chip, it cannot render visible artifact in Synopsys schematic view. If attacks want to modify the watermark generating circuit from synthesis circuit or chip layout, they destroy the normal IP function at the same time. We attempt to temper synthesis circuit and layout. The normal function of the IP has distortion simultaneously. We still can extract the greater part of watermark sequence even though the IP is destroyed.

The experimental results demonstrate that our proposed embedding technique can indeed survive the tampering, synthesis, placement and routing.

3.2 Discussions

From the experimental results, the design does achieve the goal. Our proposed methods are low hardware cost. It is also easy to implement. Because the watermark generating circuit has been done on behavioral design level, the proposed embedding technique can survive the tampering, synthesis, placement and routing. The watermark is embedded into the test circuit. The generality of soft IPs will keep the test circuits after integrating IPs into full SOCs. We can trace test signal and verify ownership rights after integrating IPs into full SOCs. It's also easy to detect the ownership rights of the IP provider after the chip have been packaged.

4.CONCLUSIONS

We have developed, for the first time, an intellectual property (IP) core protection method that embeds watermark into test circuit. We establish principles for development of new watermarking-based IP protection procedures in this paper. On real designs, we show proofs of authorship with the watermark sequence. After the chip have been packaged, it's still easy to detect the ownership rights of the IP provider. The experimental results show the proposed embedding technique can survive the tampering, synthesis, placement and routing. We don't need to look at the photomicrograph if we want to check the ownership rights. This method is easier than conventional methods. This is a very convenient and feasible scheme.

5.ACKNOWLEDGMENT

The authors gratefully acknowledge NSC Chip Implementation Center (CIC), for supplying the technology models used in the circuit simulations. The authors wish to thank the anonymous reviewers for useful comments.

Table I Watermarking results for the synthesis experiments.

IP	Watermark Case	Gate Count	Increase Gates
IP_1	Original Circuit	15236	-----
	Headed W.S.M.	211	1.38 %
	Periodic W.S.M.	349	2.29 %
	Cyclic W.S.M.	297	1.95 %
	Random W.S.M.	509	3.34 %
	Operational W.S.M.	625	4.10 %
IP_2	Original Circuit	25965	-----
	Headed W.S.M.	207	0.80 %
	Periodic W.S.M.	355	1.37 %
	Cyclic W.S.M.	302	1.16 %
	Random W.S.M.	515	1.98 %
	Operational W.S.M.	640	2.46 %
IP_3	Original Circuit	32571	-----
	Headed W.S.M.	218	0.67 %
	Periodic W.S.M.	361	1.10 %
	Cyclic W.S.M.	309	0.95 %
	Random W.S.M.	519	1.59 %
	Operational W.S.M.	637	1.96 %
IP_4	Original Circuit	39870	-----
	Headed W.S.M.	221	1.55 %
	Periodic W.S.M.	352	0.88 %
	Cyclic W.S.M.	308	0.76 %
	Random W.S.M.	524	1.31 %
	Operational W.S.M.	626	1.57 %
IP_5	Original Circuit	43012	-----
	Headed W.S.M.	223	0.52 %
	Periodic W.S.M.	371	0.86 %
	Cyclic W.S.M.	314	0.73 %
	Random W.S.M.	533	1.23 %
	Operational W.S.M.	641	1.49 %

W.S.M: Watermark Sequence Method

Table II Watermarking results for synthesis, placement and routing. (Unit: number of bit error)

IP	Watermark Case	Area Optimization	Timing Optimization	P&R
IP_1	Headed W.S.M.	0	0	0
	Periodic W.S.M.	0	0	0
	Cyclic W.S.M.	0	0	0
	Random W.S.M.	0	0	0
	Operational W.S.M.	0	0	0

Table III Watermarking results for gates tampering and P&R tampering. (Unit: number of bit error)

IP	Watermark Case	Analysis	Gates Tampering (5%)	P&R Tampering(5%)
IP_1	Headed W.S.M.	Bit Error	3	2
		IP Function	Distortion	Distortion
	Periodic W.S.M.	Bit Error	5	6
		IP Function	Distortion	Distortion
	Cyclic W.S.M.	Bit Error	3	3
		IP Function	Distortion	Distortion
	Random W.S.M.	Bit Error	2	2
		IP Function	Distortion	Distortion
	Operational W.S.M.	Bit Error	4	3
		IP Function	Distortion	Distortion

6.REFERENCES

[1] Henry Chang, *Surviving the SOC Revolution – A Guide to Platform-Based Design,* Kluwer Academic Publishers, 1999.

[2] Andrew B. Kahng; Mantik, S.; Markov, I.L.; Potkonjak, M.; Tucker, P.; Huijuan Wang; Wolfe, G. "Robust IP Watermarking Methodologies for Physical Design," *Design Automation Conference*, 1998. Proceedings, 1998, pages: 782 -787

[3] Narayan,N.; Newbould, R.D.; Carothers, J.D.; Rodriguez, J.J.; Holman, W.T., "IP Protection for VLSI Designs Via Watermarking of Routes," *ASIC/SOC Conference*, 2001. Proceedings. 14th Annual IEEE International, 2001, pages: 406 -410

[4] Newbould, R.D.; Irby, D.L.; Carothers, J.D.; Rodriguez, J.J.; Holman, W., "Watermarking ICs for IP protection," *Electronics Letters*, Volume: 38 Issue: 6, 14, March 2002, pages: 272 -274

[5] Caldwell, A.E.; Hyun-Jin Choi; Kahng, A.B.; Mantik, S.; Potkonjak, M.; Gang Qu; Wong, J.L. "Effective iterative techniques for fingerprinting design IP," *Design Automation Conference*, 1999. Proceedings. 36th, 1999, pages: 843 -848

[6] Kahng, A.B.; Lach, J.; Mangione-Smith, W.H.; Mantik, S.; Markov, I.L.; Potkonjak, M.; Tucker, P.; Wang, H.; Wolfe, G. "Watermarking techniques for intellectual property protection, "*Design Automation Conference*, 1998. Proceedings, 1998, pages: 776 –781

[7] Charbon, E., "Hierarchical watermarking in IC design", *Custom Integrated Circuits Conference*, 1998. Proceedings of the IEEE 1998 , 1998, pages: 295 –298

[8] Samiha Mourad, Yervant Zorian, *Principles of testing electronic systems*, New York: John Wiley & Sons, 2000

[9] M. L. Bushnell and V. D. Agrawal, *Essentials of Electronics Testing*, Kluwer Academic Publishers, 2000.

[10] A. B. Kahng, J. Lach, W. H. Manione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Turker, H. Wang, and G. Wolf, "Constraint-based watermarking techniques for design IP protection," *IEEE Trans. on Computer-Aided Design of Intergrated Circuits and Systems,* vol. 20, no. 10, pp. 1236–1252, Oct. 2001.