2004 IEEE Asia-Pacific Conference on Advanced System Integrated Circuits(AP-ASIC2004)/ Aug. 4-5, 2004

DIRECT ACCESS TEST SCHEME FOR IP CORE PROTECTION

Yu-Cheng Fan, Hsueh-Yen Yang and Hen-Wai Tsao

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

In this paper, we propose a novel direct access test scheme for intellectual property (IP) protection. The principles of new watermarking IP protection procedures depend on current IP-based design flow. The core concept is embedding a watermark generator and a test circuit into the IP core at the behavior design level. This method adopts the direct access test scheme. The ownership right is proven during the direct access test process. The watermark does not need to be designed case-by-case according to different IPs. On real designs, our approaches have low hardware overhead, tracking cost, processing time cost, and probability of coincidence. This scheme can protect the soft IP core at various design levels. It is still easy to detect the ownership rights of the IP provider after the chip has been manufactured and packaged. Experimental results have demonstrated that the proposed direct access test scheme-based watermarking approaches are indeed practical. The IP provider will be able to trace a company that has engaged in the unauthorized reselling of copies of the IP.

I. INTRODUCTION

The shift toward very deep sub-micron processing technology has encouraged IC designers to design an entire system implemented on a single chip. This new paradigm of system on a chip (SOC) has changed the design methodologies. In order to reduce time-to-market and increase productivity, reuse-based and intellectual property (IP)-based design methodologies have become a major concern in IC industries [1]. IP-based design however poses significant high security risks. The protection of virtual components is increasing in importance. There are several approaches to performing IP protection. One potential solution for claiming ownership is to use watermarks.

Recently, a number of watermarking-based IP protection techniques have been developed. In the literature [2]-[7], several techniques have been proposed for IP core protection. There are three main watermarking schemes discussed in the open literature: constraint-based watermarking, finite state machine based watermarking, and digital signal processing watermarking.

Kahng el al. [2] proposed constraint-based IP watermarking as one of the leading approaches for IP watermarking. These techniques usually encode a user's digital signature as a set of additional design constraints, add these constraints into the original design specification, and optimize this input specification using a tool that retrieves the final optimized design specification. The main advantage of the approach is its actual low overhead. Nevertheless, the watermark cannot be detected except at the same level of abstraction [3]. Besides, the designer must examine the photomicrograph to check the ownership rights after the chip has been packaged.

Oliveira [4], and Torunoglu et al. [5] introduced two different techniques used for watermarking of sequential parts of a design. Both algorithms are based on adding new input/output sequences to the finite state machine (FSM) representation of the design. The main advantage of both approaches is the ability to detect the presence of the watermark at all lower design levels [3]. Moreover, the user encounters difficulty in tracking the FSM function when the IP is integrated into a whole chip. After the chip has been packaged, the watermark is hidden in the SOC; the ownership rights are not easy to prove.

Chapman et al. [6] proposed a digital signal processing (DSP) watermarking scheme. The algorithm is based on the ability of designers to make minor changes in the decibel (db) requirements of digital filters. This approach depends on a very low data rate, just one character (says, 7 bits), which makes it impractical for use in an industrial environment. The approach does not have a clear way to track and extract the watermark at lower levels [3]. The watermark must be designed case-by-case according to the characteristics of various IPs and hence is not convenient.

In this paper, we propose direct access test scheme (DATS)-based watermarking techniques for IP core protection. According to the IP reusable rule released by the Virtual Socket Interface Alliance (VSIA), a reusable IP must keep the test circuits after being integrated into a full system on a chip (SOC) [1]. After integrating IPs into full SOCs, the only signal in the IP that can be traced is the test signal. If we combine the test circuit with a watermark generator, we can secure the ownership rights of the IP provider easily.

First of all, the watermark, which stands for the designer's rights, is represented by binary data. The watermark generator [7] is designed to generate the watermark data. Then, we combine the test circuit with the watermark generator at the behavior design level. Next, direct access test scheme [8] for IP protection are considered when IPs are integrated into a full SOC. After the chip has been packaged, any IP in the chip may be observed and tested. In test mode, the selected IP

0-7803-8637-X/04/$20.00

sends output test patterns and watermark sequences. We can check the ownership rights of the IP provider according to the watermark sequence. The IP provider is also able to trace a company for reselling unauthorized copies of the IP.

Finally, a set of experiments has been performed to verify the feasibility of this proposed procedure. We try to ascertain the watermark sequence through direct access testing strategy. The experimental results demonstrate that the proposed techniques are feasible and efficient.

The rest of the paper is organized as follows. In Section II, we explain direct access testing strategies for IP protection. In Section III describes the experimental results. In Section IV, the conclusion of this paper is stated.

II. DIRECT ACCESS TESTING STRATEGIES FOR IP PROTECTION

In this section, we develop a novel direct access testing strategies (DATS) for IP core protection. This method is developed depending on current IP-based design flow [1]. Our explanation will abstract the design process to solve the copy detection problem. Figure 1 describes the IP-based design flow with watermarking.

First of all, the watermark that can represent one's identity intuitively is generated as a binary sequence. Then, we design a watermark generator to generate the watermark bit-streams. The watermark generator is composed of several parallel input serial output registers (PISO) and inverter gates [7]. When the test mode signal is active (Test Mode=1), the watermark generator will be turned on. The parallel watermark data is generated by the inverters. If the watermark value is one, the circuit generates the value directly. If the watermark value is zero, there is an inverter that translates the test mode signal into zero. Watermark data is generated via the test mode signal and inverters. The PISO translates the parallel watermark data into a sequence. If the soft IP has several output pins, there will be several sets of watermark generator. Then, we combine test circuit with watermark generator (see Fig. 2). When the chip is in test mode, the chip will send out watermark sequence and test patterns alternately. According to the watermark sequence, we can verify ownership rights of the IP provider [9].

The soft IP will be integrated with the watermark generator (WG) and test circuit (TC). The architecture of the circuit is shown in Figure 2. The normal function output, test pattern output and watermark sequence are connected to the output pins through a 4-to-1 MUX. In normal mode (Test Mode signal = 0), the IP executes the normal function. In test mode (Test Mode signal = 1), the "test mode signal" and "arbitrator" control the watermark generator and test circuit. 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 are input into the chip and the output test pattern is generated by test circuit. Then, the arbitrator controls the order of the output signal. The chip sends out the watermark sequence and test pattern according to the watermark sequencing methods. The waiting data will be stored in shift registers. The test mode signal and arbitrator also control the multiplexer to send out the watermark sequence and test patterns in order. The soft IP core and watermark generator are designed using hardware

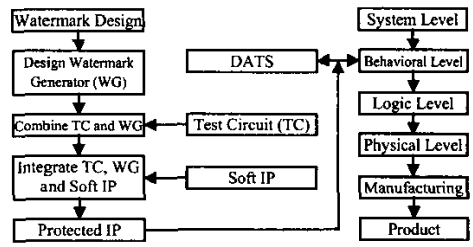

Fig. 1. DATS-based watermarking procedure.

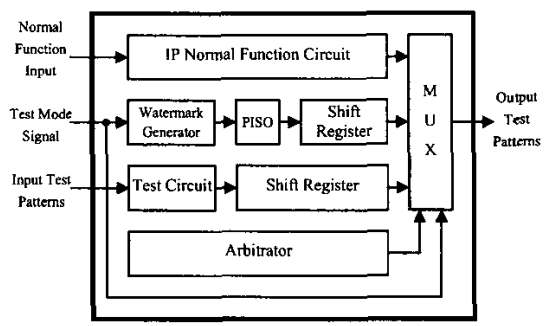

Fig. 2. Architecture of soft IP, watermark generator (WG) and test circuit.

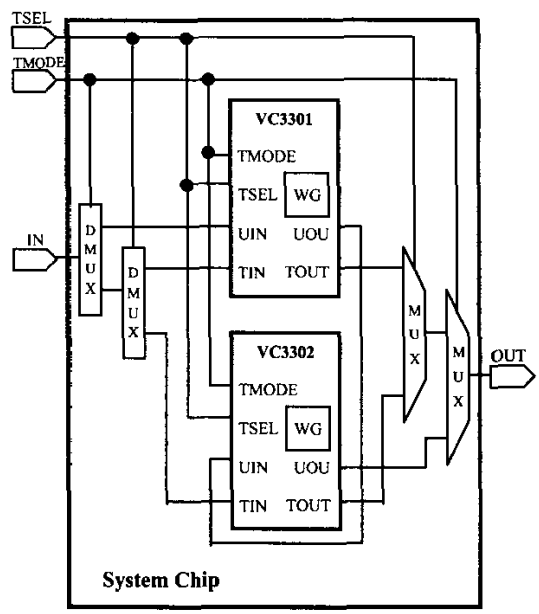

Fig. 3. DATS architecture.

description language (HDL). In order to prevent illegal copying and modification, the IP core and watermark generator will be protect by encoding techniques. We adopt a cryptographic encoding scheme to encode a source description. After the cryptographic encoding, the masked regions in a source description will be processed into an intermediate form. This scheme may appear anywhere in the source description. The masked regions for protection in the original source description become unreadable. This allows proprietary HDL source descriptions to be protected from being accessed or modified.

In order to prove that our method is feasible, we adopt several industrial IP cores and try to get the watermark sequence through direct access testing strategies. The examples are intended to demonstrate the use of watermark IP protection and direct access test scheme presented throughout the experiments.

The direct access test scheme is often adopted in the SOC design field [10]. DATS provides for separate testing of individual block or core cells using proven test vectors. This method makes the IP core's inputs, outputs, and the bi-directional ports accessible outside the chip by mapping them onto the chip's pins. Using this scheme [10], any embedded core in the chip can be isolated, simulated, and tested independently of the rest of the chip. Test vectors can then be generated to check the interconnections between the various virtual components of the chip. The scheme requires the I/O ports that are not primary I/Os of the chip to be modified [10]. TMODE and TSEL are two control pins added to the chip.

In Fig. 3, two main IP cores, VC3301 and VC3302, are shown. An input pin, TMODE, is distributed to all components, while the multiplexing of the I/O pins is done only when necessary. The circuit functions in normal mode when TMODE = 0. The module under test, be it a core or a UDL, is in test mode when TMODE = 1 and TSEL =1. Meanwhile, all the other modules are inactive in testing and their TSEL = 0. The selected IP core can thus be tested independently. When the test mode signal is active, the selected IP is under test and sends the output test pattern. The test mode signal also triggers the watermark generator embedded in the soft IP core. The output test pattern includes the watermark sequence and test sequence and can be observed clearly from the output pins in test mode. According to the arrangement of the output test pattern, the watermark sequence can be easily extracted. We can then identify the ownership rights from the watermark sequence. The advantage of this approach lies in its simplicity and in testing the core as if it is the only circuit on the IC. It is adopted widely in the SOC design field.

III. EXPERIMENTAL RESULTS

In this section, a series of experiments has been conducted to evaluate the effectiveness of the direct access testing strategies for IP core protection. In order to verify the properties of the proposed method, we applied our method to three industry IP cores. The IP cores were designed using Verilog hardware description language and verified beforehand.

1) Hardware Overhead: The proposed watermarking methods were applied to the industry IP cores. Results for the hardware overhead are summarized in Table Ⅰ. The table reports gate count and hardware overhead for each watermark generator (WG). For example, we designed 60-bit watermark sequence using the proposed method. The watermark generator requires 344~348 gates. We just increase the area no more than five percent to add a watermark generator. Our proposed methods thus have low hardware cost.

We reused the IP cores to design new chips. We adopted the direct access test scheme (DATS) to test these new chips. Results for the hardware overhead are summarized in Table Ⅱ. In chip_1, the direct access test scheme needs 2734 gates. This scheme increases the area no more than five percent. The approach has also low hardware overhead.

2) Processing Time (PT): The watermarking characteristics are summarized in Table Ⅲ. We analyze the characteristics of the watermark generator that generates the 60-bit watermark sequence. We report four quality measures for each test of soft IP cores. These measures are: processing time in (mm:ss) required for the synthesis tool, number of test patterns, fault coverage and probability of coincidence. The synthesis processing time for each test IP core is measured using the Synopsys tool. The CPU times are for a 448-MHz UltraAX-MP. The IP that adds the extra watermark protection circuit just increases the time less. Our proposed methods have low processing time cost.

3) Fault Coverage (FC): The number of test patterns (NTP) and fault coverage are summarized in Table Ⅲ. We generate a suitable number of test patterns to test the IPs. The fault coverage of each IP is between 93% and 96%.

4) Probability of coincidence: In the literature [2], a watermark's capability to prove the authorship is expressed as a parameter Pc. Essentially, Pc is the probability of a non-watermarked solution carrying our watermark by coincidence. Designers wish this probability to be convincingly low so as to have a strong proof of authorship. We can compute Pc according to the number of test patterns and watermark sequences. Computing Pc is typically straightforward. Let x be the number of the watermark sequence. Let p be the repeated times of watermark sequence. The probability of coincidence is given by [11]

$$Pc = 1/(2^{x \cdot p}).$$

According to the above results, Pc. is sufficiently small. Because this probability is convincingly low, the proposed methods provide strong proof of authorship. It is also difficult to guess from the output test pattern.

5) Watermarking in various design levels: We try to use different synthesis constraints to transfer the HDL core into logic gates. For example, "area optimization constraints" and "timing optimization constraints" are adopted separately. The watermark function is not

changed after logic synthesis because we embed the watermark into the test circuit at the behavioral design level. After placement and routing, we can still detect ownership rights according to the watermark sequence without error. According to the results, the proposed method can protect the soft IP core at the behavioral design level, gate design level and physical design level.

6) Authorship proof after chips have been packaged: After the chip has been packaged, we just use it in the test mode and show proof of authorship without examining its microphotograph. Moreover, we prove the ownership rights during the general test procedure; we do not implement extra extraction flow. The proposed scheme is low in tracking cost.

Table I HARDWARE OVERHEAD

IP Name	Circuit	60bits watermark	
		Gates	Overhead
VC3301	Original Circuit	10257	-----
	WG	346	3.37 %
VC3302	Original Circuit	19541	-----
	WG	344	1.76 %
VC3303	Original Circuit	27053	-----
	WG	348	1.29 %

Table II DATS HARDWARE OVERHEAD

Chip	Circuit	Gates	Overhead
Chip_1	Original Circuit	156654	-----
	DATS Circuit	2734	1.75%
Chip_2	Original Circuit	231658	-----
	DATS Circuit	4569	1.97%

Table III WATERMARKING CHARACTERISTICS

IP Name	Circuit	60 Bits Watermark			
		P T	NTP	FC	Pc
VC3301	Original Circuit	30:31	3981	95.2%	-----
	Add WG	30:45			8.7e-19
VC3302	Original Circuit	66:04	6168	93.6%	-----
	Add WG	66:23			8.7e-19
VC3303	Original Circuit	93:56	7701	93.1%	-----
	Add WG	94:18			8.7e-19

IV. CONCLUSIONS

In this paper, a new direct access test scheme for IP core protection is presented. The ownership rights are proven according to the output test pattern and watermark sequence during the test procedure without implementing extra any extraction flow. A series of experiments has been conducted on several industry IP cores to evaluate the effectiveness of the proposed method. According to the results, our approaches have low hardware overhead (area increase by no more than five percent), low tracking cost, low processing time cost and have a strong proof of authorship because the probability of coincidence is convincingly low (Pc value is smaller than 2.8e-167). The watermark function is not changed after logic synthesis, placement and routing because we embed the watermark into the test circuit at the behavioral design level. It is still easy to detect the ownership rights of the IP designer after the chips have been packaged and there is no need to examining the microphotograph. Experimental results have demonstrated the proposed method is really a practical scheme for IP core protection.

REFERENCES

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

[2] A. B. Kahng, *et al.*, "Constraint-based watermarking techniques for design IP protection," *IEEE Trans. Computer-Aided Design Integrated Circuits Systems*, vol. 20, pp. 776–781, 1236–1252, Oct. 2001.

[3] A. T. Abdel-Hamid, S. Tahar, and E. M. Aboulhamid, "IP watermarking techniques: survey and comparison," in *Proc. IEEE Int. Workshop on System-on-Chip for Real-Time Applications*, pp. 60–65, 2003.

[4] A. L. Oliveira, "Techniques for the creation of digital watermarks in sequential circuit designs," *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems*, vol. 20, pp. 1101–1117, Sept. 2001.

[5] I. Torunoglu, E. Charbon, "Watermarking-based copyright protection of sequential functions," in Proc. IEEE Custom Integrated Circuits Conference, pp. 35–38, 1999.

[6] R. Chapman, T. S. Durrani, "IP protection of DSP algorithms for system on chip implementation," *IEEE Trans. on Signal Processing*, vol. 48, pp. 854–861, March 2000.

[7] Y. C. Fan, and H. W. Tsao, "Watermarking for intellectual property protection," *Electronics Letters*, vol. 39, pp. 1316–1318, Sept. 2003.

[8] M. L. Bushnell, and V. D. Agrawal, *Essentials of Electronic Testing for Digital, Memory, and Mixed-Signal VLSI Circuits*, Kluwer Academic Publishers, 2000.

[9] Y. C. Fan, and H. W. Tsao, "Watermarking based IP core protection," in *Proc. IEEE International Symposium on Circuits and Systems*, pp. 181–184, May 2003.

[10]V. Immaneni, and S. Raman, "Direct access test scheme-design of block and core cells for embedded ASICs," in *Proc. Int. Test Conference*, pp. 488–492, 1990.

[11]P. G. Hoel, S. C. Port, and C. J. Stone, *Introduction to Probability Theory*, Houghton Mifflin Company.