Testing-Based Watermarking Techniques for Intellectual-Property Identification in SOC Design

Yu-Cheng Fan, *Member, IEEE*

***Abstract*—The author proposes a novel testing-based watermarking scheme for intellectual-property (IP) identification in this paper. The principles are established for the development of new watermarking IP-identification procedures that depend on current IP-based design flow. The core concept is embedding a watermark-generating circuit (WGC) and a test circuit into the IP core at the behavior design level. Therefore, this scheme can also successfully survive synthesis, placement, and routing and can identify the IP core at various design levels. This method adopts current main system-on-a-chip (SOC) design-for-test (DFT) strategies. The identity of the IP is proven during the general test process without implementing any extra extraction flow. After the chip has been manufactured and packaged, it is still easy to detect the identification of the IP provider without the need to examine the microphotograph. On real designs, our approaches entail low hardware overhead, tracking costs, and processing-time costs. The proposed method solves the IP-identification problem.**

***Index Terms*—Design-for-test (DFT), intellectual-property (IP) identification, system-on-a-chip (SOC), very large scale integration (VLSI) design, watermarking.**

I. Introduction

ADVANCES in semiconductor processing technology have led to the rapid increases in integrated-circuit (IC) design complexity [1], [2]. The shift toward very deep submicrometer processing technology has encouraged IC designers to design an entire system implemented on a single chip. This new paradigm, called the system-on-a-chip (SOC), has changed design methodologies. In order to reduce time to market and to increase productivity, the reuse of previously designed modules is becoming a common practice. Reuse-based and intellectual-property (IP)-based design methodologies have become a major very large scale integration (VLSI) design flow in IC industries [1].

Design reuse leads to the development of IP-identification techniques. Each IP should have identification that represents the design information, including designer identity, version, ownership rights, and provider. The identification can also provide designer information, IP tracing, ownership proof, and IP management. The ability to prove the identity of virtual components is increasing in importance [2]. After the IP has been integrated into a whole chip and packaged, designers can still check the identity of the IP. According to the current literature [1]–[3], a complete and efficient IP-identification technique should include several main characteristics.

1) Proof of identification: The identification method should provide convincing evidence to prove the identity of the IP circuit.
2) Identification of the IP at any design level: In addition, the identification of the IP should easily be performed at the behavior, gate, and physical levels and not be changed during the IC design flow.
3) Low overhead: The IP-identification method should have low protection cost, including both the procedure cost of identification and the time needed for the identification procedure.
4) Low tracking cost: The identification method should have a low tracking cost that expresses the ability and cost of tracking the identity.

There are several approaches to performing IP identification in the literature. One potential method for claiming ownership is to use watermarks. Watermarking is a technique that is traditionally used to securely identify the authenticity of the source of image, video, or audio media [4]–[9].

Recently, a number of watermarking-based IP-identification techniques have been developed [10]–[15], [25]–[39]. In the literature, several techniques have been proposed for IP identification. Although some researchers have investigated the IP-identification methods at the physical design level, few works have proposed the IP-identification scheme at the behavioral design level. Kahng *et al.* [10] developed the protocols for IP watermarking at the physical design level, using the concept of constraint-based watermarking. This constraint-based IP watermarking [25], [26] is one of the leading approaches for IP watermarking. This method usually encodes a user's digital identification as a set of additional design constraints. Then, the scheme adds the constraints into the original design specification, adopting a tool that retrieves the final optimized design specification [29]. Narayan *et al.* [11] 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 the watermark at the physical design level [10], [12]–[15], design partitioning [27], [28], and combinational logic synthesis [14]. After synthesis, placement, or routing, the layout of the soft IP core will be changed. These techniques are, therefore, insufficient in proving the identity of the soft IP core. Additionally, we must look at the photomicrograph if we want to check the identification. These methods are not

Manuscript received April 3, 2006; revised October 15, 2007. This work was supported by the National Science Council (NSC), Taipei, Taiwan, R.O.C., under Grant NSC 95-2218-E-027-008 and Grant NSC 96-2221-E-027-024.

The author is with the Department of Electronic Engineering, National Taipei University of Technology, Taipei 106, Taiwan, R.O.C. (e-mail: skystarfan@ntu.edu.tw)

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIM.2007.911623

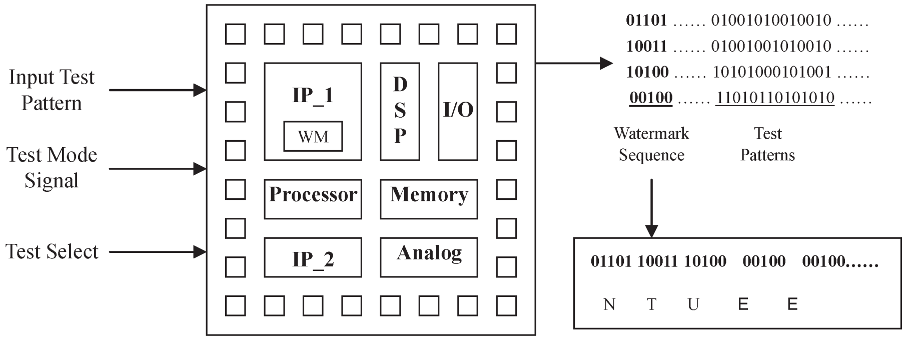


Fig. 1. Prove the identification during test procedure after integrating the IP into SOC.

only complicated but are also inconvenient. It is very difficult to detect the identity of the IP provider once the chip has been packaged.

Oliveira [31] and Torunoglu and Charbon [32] proposed two different techniques to design watermarking circuit. Oliveira [31] adds new input/output sequences to the finite-state-machine (FSM) representation of the design. Torunoglu and Charbon [32] introduced the FSM watermarking approach that extracts the unused transitions in a state transition graph of the behavioral model. When the IP is integrated into a whole chip, the user encounters difficulty in tracking the FSM function. The watermark is hidden in the SOC after the chip has been packaged. The identifications are not easy to prove.

Chapman *et al.* [33], [34] presented a digital-signal-processing (DSP) watermarking scheme. The designer of a high-level digital filter should encode one character as the hidden watermark data in this approach [30]. This design does not have a clear way to track and extract the watermark at lower levels [30]. The watermark must be designed case by case according to the identification of various IPs. It is not convenient.

In this paper, we propose testing-based watermarking techniques for IP-core identification. The core concept is embedding a watermark into a test circuit (TC) at the behavior design level. According to the reusable IP rule released by the Virtual Socket Interface Alliance, a reusable IP must retain the TCs after being integrated into a full SOC [1], [3]. After integrating the IPs into the full SOCs, the only signal in the IP that can be traced is the test signal. If we combine the TC with a WGC, we can easily prove the identity of the IP. After the chip has been packaged, any IP in the chip may be observed and tested (see Fig. 1). In the test mode, the selected IP sends output test patterns and watermark sequences. We can determine the identity of the IP provider according to the watermark sequence.

A set of experiments has been performed to verify the quality of this proposed procedure. We applied our method to five industry IP cores. According to the results, the proposed methods have low hardware costs (no more than 5%), low processing-time (PT) costs, low tracking costs, and high fault coverage (between 90% and 96%). The WGC is invisible at the gate and physical design levels without impairing the normal function.

The proposed method can prove the identity after the IP has been integrated into a whole chip and packaged without the examination of its microphotograph. Moreover, we can also identify the soft IP core at various design levels, even after logic synthesis, placement, and routing. The experimental results demonstrate that the proposed techniques are feasible and efficient.

The rest of this paper is organized as follows. In Section II, we explain the watermark creation, the IP-based design flow with watermarking, and the IP-core cryptography. In Section III, we introduce the concept of the design-for-test (DFT) strategies for IP identification. Section IV describes the experimental results. In Section V, the conclusions of this paper are stated.

II. IP-Based Design Flow With Watermarking

In this section, we develop an IP-identification approach using the testing technique. This method is developed depending on the current IP-based design flow [1]. Our explanation will describe the design process to solve the IP-identification problem. Fig. 2 shows the IP-based design flow with watermarking. The design procedure will be introduced next.

A. Watermark Design

First of all, the watermark, which can intuitively represent one's identity, is generated as a binary sequence and inserted into each IP core. We propose a coding technique for the design of the digital watermark. The watermark is a symbol that stands for the organization's title, a laboratory's mark, or a personal name, and it is comprised of a sequence of bits. For example, we can use the symbol "NTUEE ISLAB" to represent National Taiwan University, Department of Electrical Engineering, and Integrated Systems Laboratory. We describe our symbol according to the coded table [see Fig. 3(a)] that we constructed beforehand. We use 01101 to represent N, 10011 to represent T, 10100 to represent U, 00100 to represent E, and so on [see Fig. 3(b)]. With this method of encoding, just 50 b is needed to describe "NTUEE ISLAB." The digital-watermark sequence is a meaningful symbol, despite its short sequence. We independently insert this type of watermark into each IP core. Then, we design a WGC to generate the watermark bit streams.

B. WGC Design

The WGC is composed of several parallel-input–serial-output (PISO) registers and inverter gates (see Fig. 4) [16]. When the test-mode signal is active (test mode $= 1$), the WGC

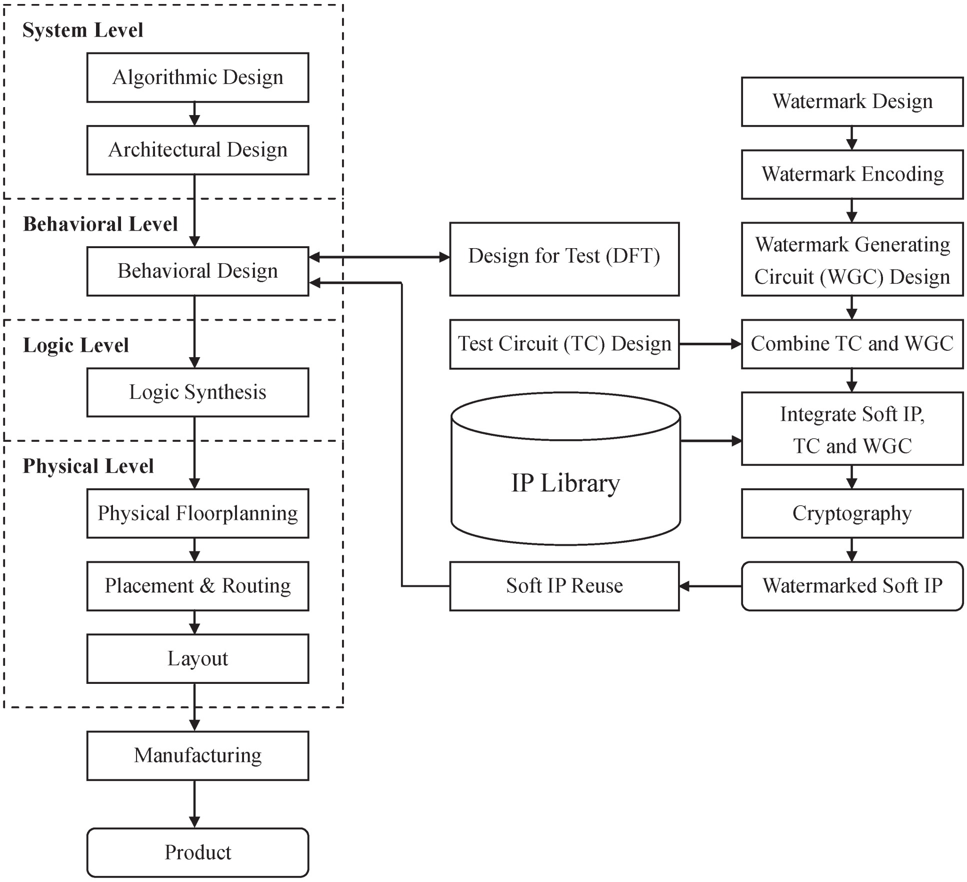


Fig. 2. IP-based design flow and watermarking procedure.

A	00000	H	00111	O	01110	V	10101
B	00001	I	01000	P	01111	W	10110
C	00010	J	01001	Q	10000	X	10111
D	00011	K	01010	R	10001	Y	11000
E	00100	L	01011	S	10010	Z	11001
F	00101	M	01100	T	10011		
G	00110	N	01101	U	10100		

(a)

01101	**10011**	**10100**	**00100**	**00100……**
N	T	U	E	E

(b)

Fig. 3. (a) Coded table. (b) Watermark.

will be turned on. The parallel watermark data are generated by the inverters. If the watermark value is one, the circuit directly generates the value. If the watermark value is zero, there is an inverter that translates the test-mode signal into zero. The watermark data are generated via the test-mode signal and inverters. The PISO translates the parallel watermark data into a sequence. If the soft IP core has several output pins, there will be several sets of WGCs.

C. Test Circuit (TC)

A reusable soft IP core should include the complete TC [1], [3], [17], [18]. The input test pattern will be sent into the IP, and the output test pattern can be observed at the output pins. By comparing the output test pattern and correct signals, the faults can easily be detected.

D. Combining TC With WGC

After the WGC has been designed, we combine the TC with the WGC (see Fig. 4). How the TC is combined with the WGC is very important. We propose five methods for combining the TC with the WGC, and we analyze the characteristics of each method.

1) Headed watermark-sequence method: When the chip is in the test mode, the chip sends out first the watermark sequence. After sending out the entire watermark sequence, the chip sends the output test patterns [Fig. 5(a)]. The watermark sequence is like the header of a bit stream. Therefore, we call this scheme the "headed watermark-sequence method." This method enables the watermark to simply be extracted. The drawback is that the watermark is easy to guess or remove.
2) Periodic watermark-sequence method: When the chip is in the test mode, the chip will alternate between the watermark sequence and the test patterns [Fig. 5(b)]. As the watermark sequence periodically appears, we call

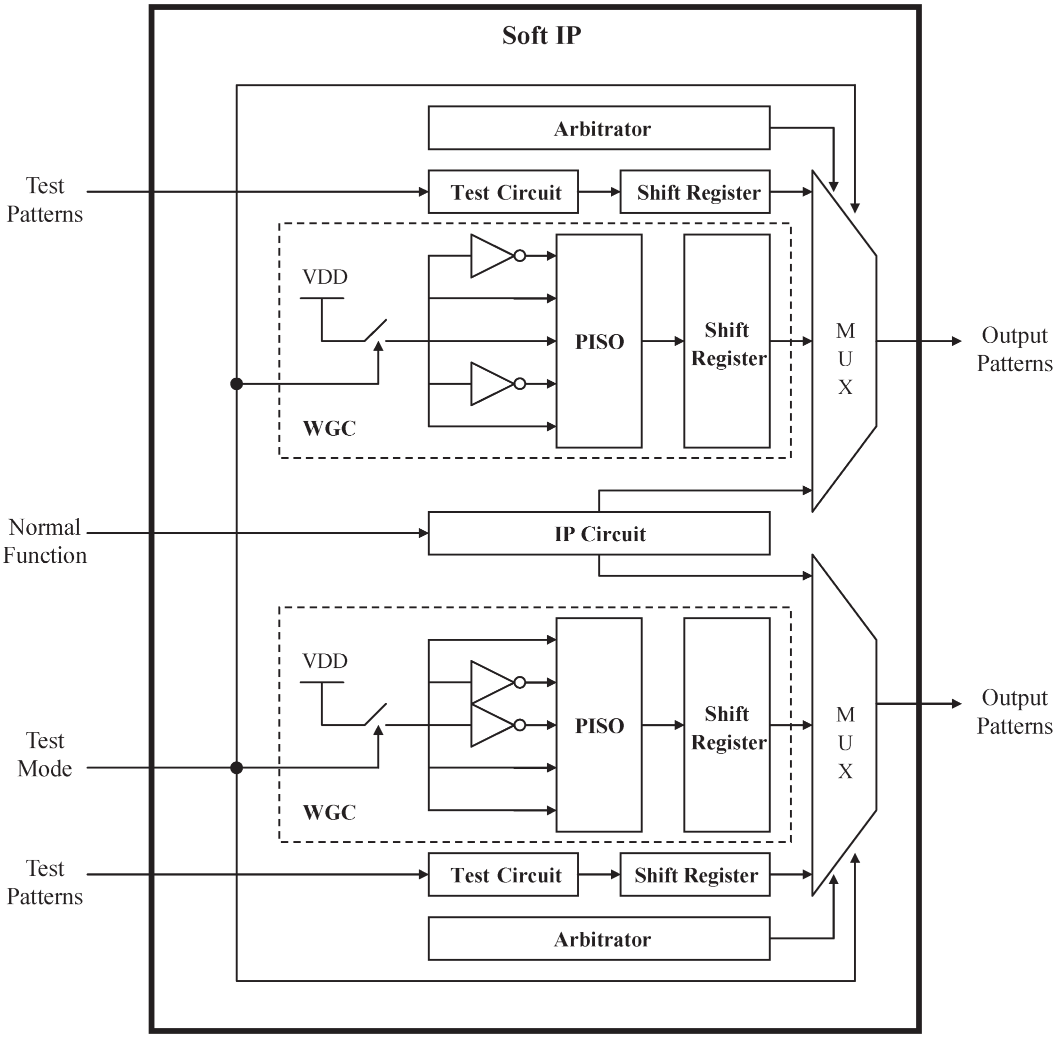


Fig. 4. Architecture of soft IP, watermark generating circuit (WGC) and test circuit.

the proposed scheme the "periodic watermark-sequence method." We can extract the watermark at any time because it periodically appears. However, this scheme has a higher hardware overhead.

3) Cyclic redundancy watermark-sequence method: When the chip is in the test mode, it sends n-bit output test patterns [Fig. 5(c)]. After the output test patterns are sent, the chip then sends 1 b of watermark data, i.e., the chip alternately sends n-bit output test patterns and 1-b watermark data. The watermark sequence and output test patterns thus cyclically appear. The watermark data are similar to the cyclic redundancy check code. Therefore, we call the proposed scheme the "cyclic redundancy watermark-sequence method." We can extract the watermark every n bits of the output test patterns and detect the identity from the watermark sequence. This method is easy to extract the watermark and hard to destroy the identification. However, this scheme also has a higher hardware overhead.
4) 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, 2, the chip sends 1-b output test pattern, 1-b watermark data, 5-b output test patterns, 1-b watermark data, 2-b output test patterns, 1-b watermark data, and so on [Fig. 5(d)]. This method has high security. It is hard to guess and remove. However, this circuit is more complex. We also need to generate a pseudorandom sequence and store it in the memory.
5) Operational watermark-sequence method: This method involves performing EXCLUSIVE-OR (XOR) operations on the watermark sequence and output test patterns to obtain new patterns [Fig. 5(e)]. When the chip is in the test mode, the chip sends the new patterns. We can extract the watermark after the XOR operations on the new patterns and test patterns to get a watermark sequence. This method has high security. It is hard to guess and remove. The drawback of the method is that if some bits are in error, it is impossible to recognize which circuit has failed (WGC or TC).

We can choose one of the aforementioned methods, depending on our requirements. We consider the applications

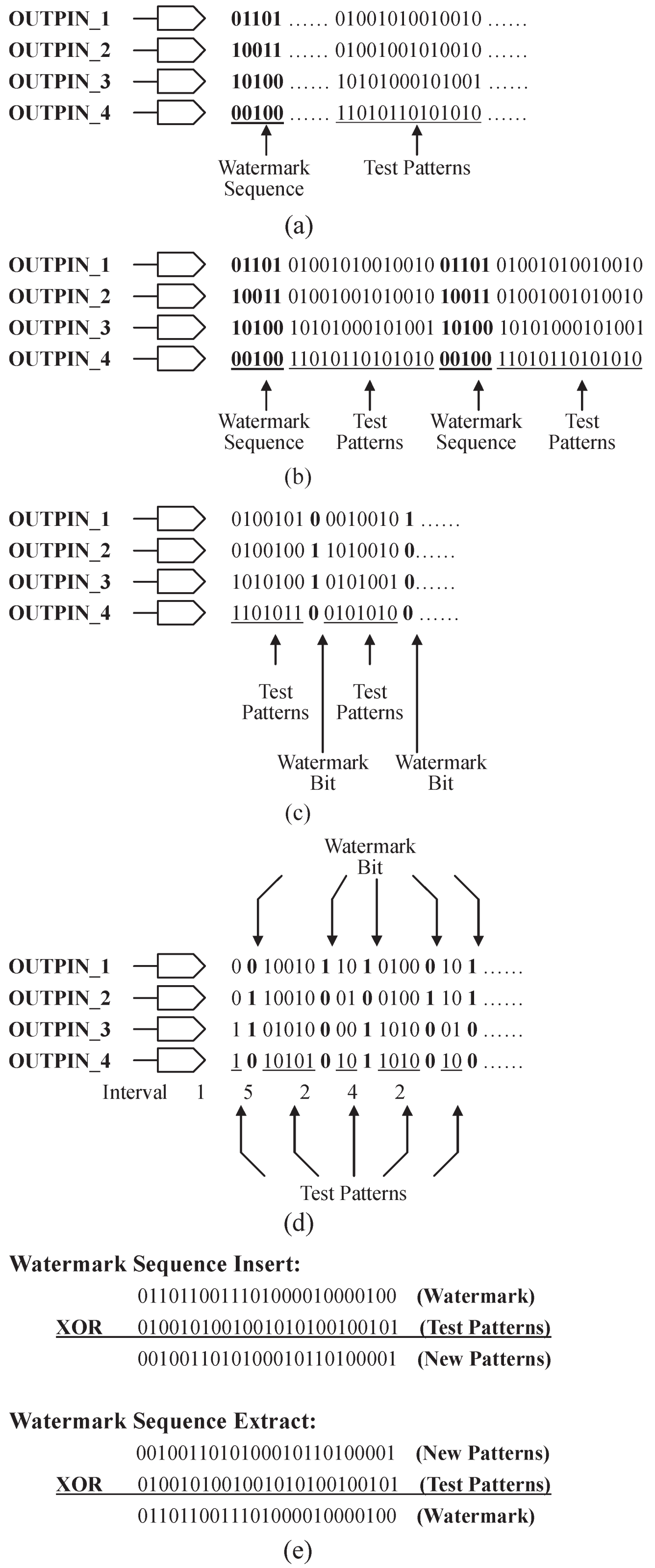
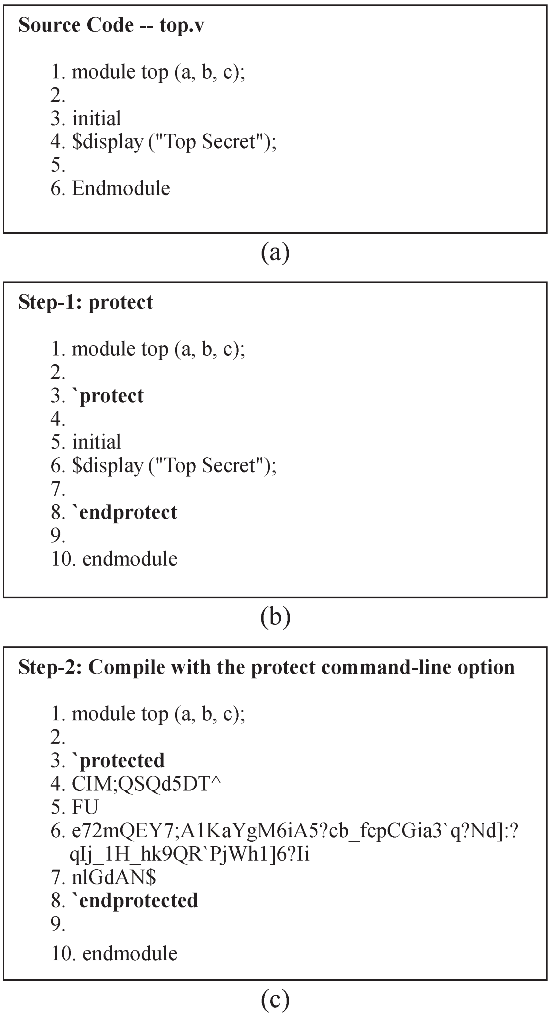

OUTPIN_1 01101 ...... 01001010010010 ......
OUTPIN_2 10011 ...... 01001001010010 ......
OUTPIN_3 10100 ...... 10101000101001 ......
OUTPIN_4 00100 ...... 11010110101010 ......
Watermark Sequence
Test Patterns
(a)
OUTPIN_1 01101 01001010010010 01101 01001010010010
OUTPIN_2 10011 01001001010010 10011 01001001010010
OUTPIN_3 10100 10101000101001 10100 10101000101001
OUTPIN_4 00100 11010110101010 00100 11010110101010
Watermark Sequence
Test Patterns
Watermark Sequence
Test Patterns
(b)
OUTPIN_1 0100101 0 0010010 1 ......
OUTPIN_2 0100100 1 1010010 0......
OUTPIN_3 1010100 1 0101001 0......
OUTPIN_4 1101011 0 0101010 0 ......
Test Patterns
Test Patterns
Watermark Bit
Watermark Bit
(c)
Watermark Bit
OUTPIN_1 0 0 10010 1 10 1 0100 0 10 1 ......
OUTPIN_2 0 1 10010 0 01 0 0100 1 10 1 ......
OUTPIN_3 1 1 01010 0 00 1 1010 0 01 0 ......
OUTPIN_4 1 0 10101 0 10 1 1010 0 10 0 ......
Interval 1 5 2 4 2
Test Patterns
(d)
Watermark Sequence Insert:
0110110011101000010000100 (Watermark)
XOR 0100101001001010100100101 (Test Patterns)
0010011010100010110100001 (New Patterns)
Watermark Sequence Extract:
0010011010100010110100001 (New Patterns)
XOR 0100101001001010100100101 (Test Patterns)
0110110011101000010000100 (Watermark)
(e)

Fig. 5. We propose five methods to combine the test circuit with a watermark-generating 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.

before watermarking the IP. For example, we use the "headed watermark-sequence method" to protect a small IP and use the "random watermark-sequence method" to protect a large IP.



Source Code -- top.v

```
module top (a, b, c);

initial
$display ("Top Secret");

Endmodule
```

(a)

Step-1: protect

```
module top (a, b, c);

`protect

initial
$display ("Top Secret");

`endprotect

endmodule
```

(b)

Step-2: Compile with the protect command-line option

```
module top (a, b, c);

`protected
CIM;QSQd5DT^
FU
e72mQEY7;A1KaYgM6iA5?cb_fcpCGia3`q?Nd]:?
  qIj_1H_hk9QR`PjWh1]6?Ii
nlGdAN$
`endprotected

endmodule
```

(c)

Fig. 6. (a) Verilog source core. (b) Protection directive. (c) Compile with the protect command line option.

E. Integrating Soft IP Core, TC, and WGC

After the watermark-sequence method is chosen, the soft IP core will be integrated with the WGC and TC. The architecture of the circuit is shown in Fig. 4. This architecture is composed of the IP circuit, TC, arbitrator, shift registers, multiplexer (MUX), PISO, and inverters. The normal function output, test pattern output, and watermark sequence are connected to the output pins through a 4-to-1 MUX. In the normal mode $(\text{test-mode signal} = 0)$, the IP executes the normal function. In the test mode $(\text{test-mode signal} = 1)$, the "test-mode signal" and "arbitrator" control the WGC and TC. The parallel watermark data are generated when the test-mode signal is active. The PISO translates the parallel watermark data into the serial watermark sequence. At the same time, the test patterns are input into the chip, and the output test pattern is generated by the TC. Then, the arbitrator controls the order of the output signal [19]. The chip sends out the watermark sequence and test pattern according to the different watermark-sequencing methods. The waiting data will be stored in the shift registers. The test-mode signal and arbitrator also control the MUX to send out the watermark sequence and test patterns in order. The designer can identify the IP provider using the watermark sequence.

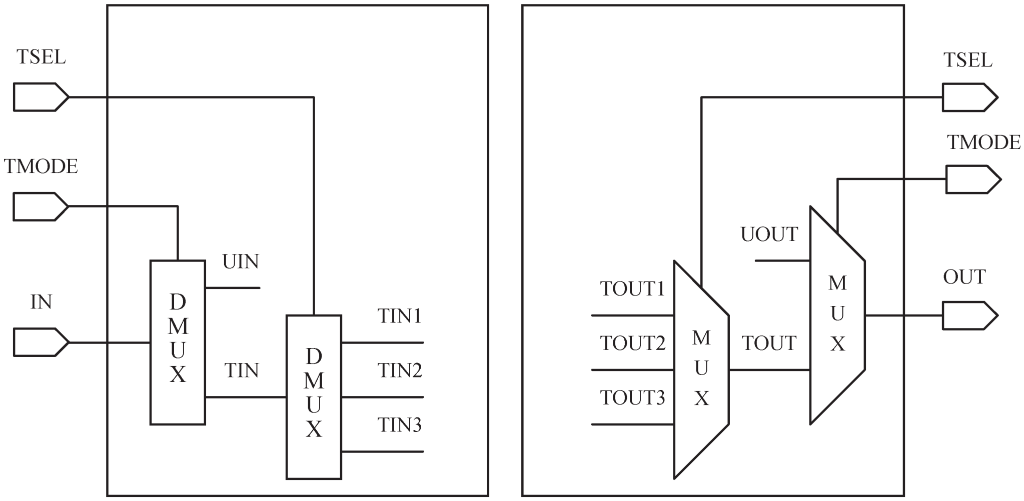


Fig. 7. DATS requires the modification of the I/O ports. (a) Input pin modification. (b) Output pin modification.

F. Cryptography

The soft IP core and WGC are designed using the hardware description language (HDL). In order to prevent illegal modifications, the IP core and WGC will be protected with 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 protects the proprietary HDL source descriptions from being modified.

For example, we adopt the Verilog HDL to design a soft IP core (see Fig. 6(a), [20], and [21]). The directives “protect” and “endprotect” bound a region once it has been compiled into a protected form [see Fig. 6(b)]. After processing, the protected file is created [see Fig. 6(c)]. The masked regions for protection in the original source description become unreadable. After the protection procedure, designers or legal customers can reuse the soft IP core to design a new chip, depending on the IP.

III. DFT Strategies

In order to demonstrate that our method is feasible and efficient, we consider two kinds of SOC DFT strategies for IP identification in this section [17], [18]. We adopt several industrial IP cores and try to get the watermark sequence through different designs for testing strategies. The examples are intended to demonstrate the use of the watermark IP identification and SOC DFT techniques presented throughout the experiments.

A. Direct-Access Test Scheme (DATS)

The DATS is often adopted in the SOC design field [22]. This scheme provides for separate testing of individual block or core cells using proven test vectors. This method makes the IP core’s inputs, outputs, and bidirectional ports accessible outside the chip by mapping them onto the chip’s pins. Using this scheme [22], any embedded core in the chip can independently be isolated, simulated, and tested from the rest of the chip. The 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, as shown in Fig. 7. TMODE and TSEL are the two control pins added to the chip.

In Fig. 8, three main IP cores—VC3301, VC3302, and VC3303—are shown. An input pin, called the TMODE, is distributed to all components, whereas the multiplexing of the I/O pins is done only when necessary. The circuit functions in the normal mode when TMODE $= 0$. The module under test, be it a core or a user-defined logic (UDL), is in the test mode when TMODE $= 1$ and TSEL $= 1$. Meanwhile, all the other modules are inactive for testing (the test control signal “TSEL” equals zero). The selected IP core can thus independently be tested. 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 WGC embedded in the soft IP core. The output test pattern includes the watermark sequence and test sequence and can clearly be observed from the output pins in the test mode. According to the arrangement of the output test pattern, the watermark sequence can easily be extracted. We can then determine the identity from the watermark sequence. The advantage of this approach lies in its simplicity and in testing the core as if it were the only circuit on the IC. It is widely adopted in the SOC design field.

B. Scan-Based Test Scheme (SBTS)

The SBTS is also widely adopted in the SOC design field [17], [18], [23]. This approach is based on using the scan chains of the cores as a test access mechanism (TAM). It assumes that all cores include the scan path and makes a minimal change to the I/O of the tested modules, cores, or UDLs. Such an assumption is realistic since the scan-path design is now widely practiced. In typical cases of soft and firm cores, system designers include the scan path, whereas in hard cores, a scan path is already included. The scan-path chains of all the cores are then used to justify 1) test vectors to an internal component and 2) test responses to the chip’s outputs.

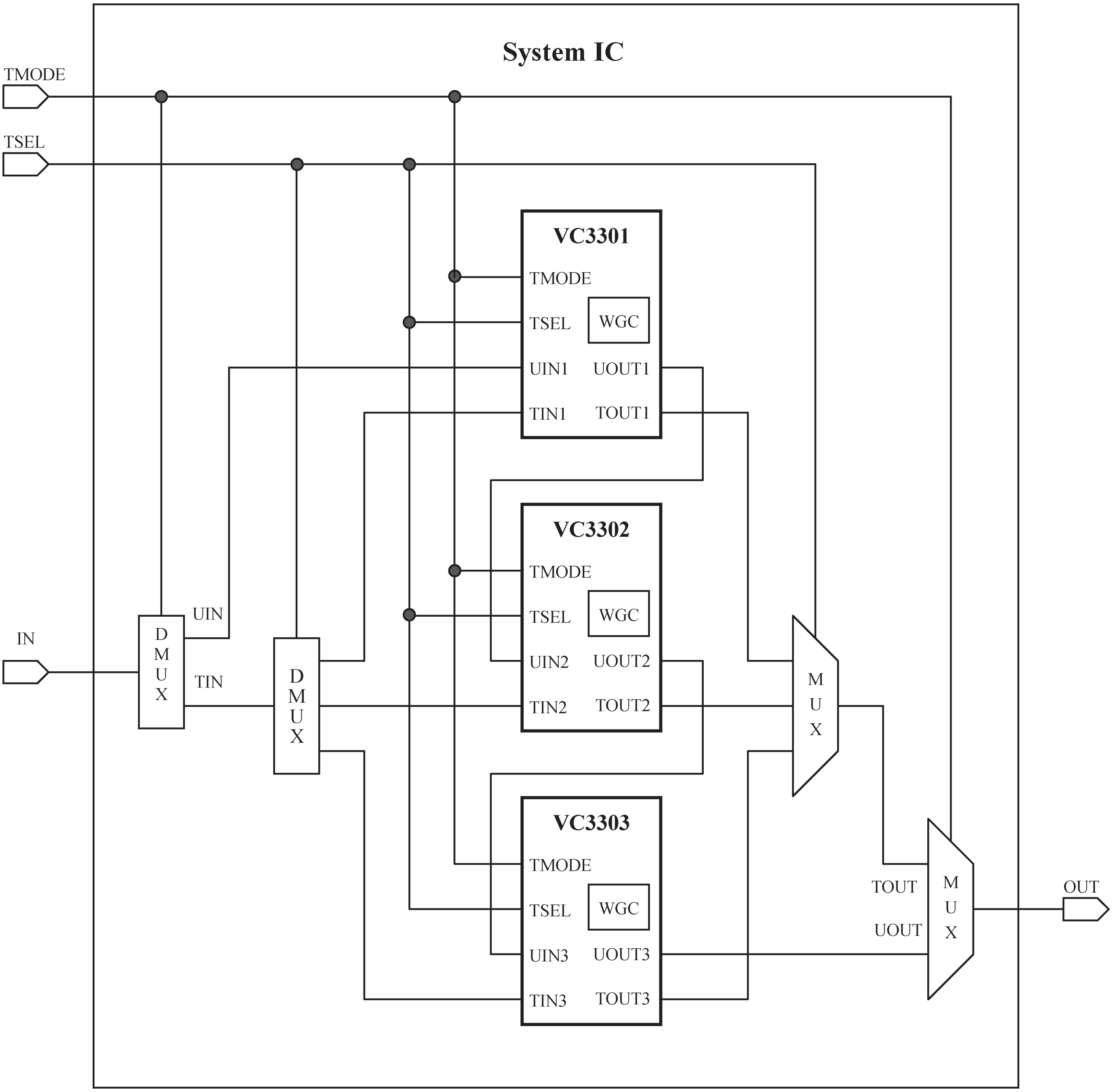


Fig. 8. DATS implementation example.

The scan chains of the various modules of the system are used to regulate the test data traffic in and out of the chip. For this, each module can be made transparent by representing it with its scan chain only, as shown in Fig. 9. We call this representation the transparent model of the module. The models are transparent in the sense that the test data can be propagated through them without information loss [24]. After the determination of the scan paths for all cores, the S-graph for all UDL logic is formed and merged with them. This will result in different scan chains through the chip, which need to be connected in a judicious manner to allow the application of the test patterns and the observation of the responses from any component on the chip.

The scan chains of the individual cores can be connected in a daisy chain [23]. The schemes are shown in Fig. 9. A bypass flip-flop is placed across each chain. The output of the scan chain and the bypass flip-flop are multiplexed to allow for whether the core is working in the bypass or scan mode. This arrangement gives various alternatives in testing the cores. It is possible to test only one core and bypass the others at any time. The individual IP cores of the chip can independently be tested through the scan-chain circuit during silicon debugging and diagnosis. The same test method can be reused to test other IP cores on the chip. This method can concurrently test all the cores and, as soon as one core runs out of patterns, can put it in the bypass mode [23].

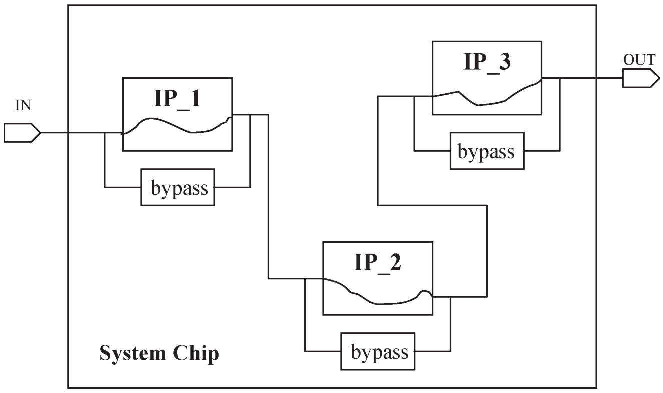


Fig. 9. Scan path as test access mechanism (Daisychain).

In Fig. 10, three main IP cores—VC3301, VC3302, and VC3303—are shown. The selected IP core can independently be tested. Whenever TMODE = 0, the circuit functions in the normal mode. When TMODE = 1 and TSEL = 1, the module is put in the test mode. Meanwhile, all the other modules are inactive for testing, and their TSEL = 0. The test pattern is sent into a selected IP core and transfers the output test data. The WGC is triggered at the same time. When the test-mode signal is active, the selected IP is under test and sends the output test pattern, which includes the watermark and test sequences. The test pattern output of the soft IP core can be propagated to a primary output of the chip through the transparent images of the cores. The output test pattern can be observed from the output pins in the test mode. According to the arrangement of the output test pattern, the watermark sequence can easily be extracted.

IV. Experimental Results

In this section, a series of experiments has been conducted to evaluate the effectiveness of the testing-based watermarking techniques for IP identification. In order to verify the properties of the proposed method, we applied our method to five industry IP cores. The aspects of the test IP cores are given in Table I. The IP cores were designed using Verilog HDL and were verified beforehand. In this section, we analyze the watermark hardware overhead, PT, fault coverage, imperceptibility, tracking techniques, and tracking cost.

A. Hardware Overhead

The proposed watermarking methods were applied to the industry IP cores. The results for the hardware overhead are summarized in Table II. We designed five kinds of WGC that separately generate 30–60-b watermark sequences. The table reports gate count and hardware overhead for each WGC. For example, we designed a 60-b watermark sequence using the proposed method. The headed watermark-sequence method requires 204–223 gates. The periodic watermark-sequence method requires 344–357 gates. The cyclic redundancy watermark-sequence method requires 304–332 gates. The random watermark-sequence method requires 310–334 gates. The operational watermark-sequence method requires 238–258 gates. We increase the area by no more than 5% to add a WGC. Our proposed methods thus entail low hardware costs.

We reused the IP cores to design new chips. The DFT was considered in these chips. We adopted the DATS and SBTS to test these new chips. The results for the hardware overhead are summarized in Table III. In chip_1, the DATS needs 2734 gates, and the SBTS needs 3851 gates. These two types of DFT schemes increase the area by no more than 5%. The DFT schemes also entail low hardware overhead.

B. Processing Time (PT)

The watermarking characteristics are summarized in Table IV. We analyze the characteristics of the WGC that generates the 60-b watermark sequence. We report the quality measures for each test of soft IP cores. These measures are PT (in minutes:seconds) required for the synthesis tool, number of test patterns, and fault coverage. The synthesis PT 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 identification circuit increases by 14–27 s to synthesize the circuit. Our proposed methods entail low PT costs.

C. Fault Coverage and Testing Overhead

The numbers of test patterns and fault coverage are summarized in Table IV. We generate a suitable number of test patterns to test the IPs. The fault coverage of each IP is between 90% and 96%.

The testing characteristics are summarized in Table IV. We analyze the characteristics of test-vector-bit overhead and test-time overhead. We report the quality measures for each test of soft IP cores. The testing PT for each test IP core is measured using the testing tool. The CPU times are for a 448-MHz UltraAX-MP. The test vector adds the extra bit overhead by no more than 1.5%. The test time also adds the extra PT by no more than 1.5%. Although the technique adds cost but no value in part test time for the production IC test, the watermark test is more useful in examining the chips in the field for patent violations. It is worth designing a testing-based watermarking sequence in the test pattern.

D. Watermarking in Various Design Levels

We try to use different synthesis constraints to transfer the HDL core into the logic gates. For example, "area-optimization constraints" and "timing-optimization constraints" are separately adopted. The watermark function is not changed after logic synthesis because we embed the watermark into the TC at the behavioral design level. After placement and routing, we can still detect the identity, according to the watermark sequence, without error. According to the results, the proposed method can identify the soft IP core at the behavioral, gate, and physical design levels.

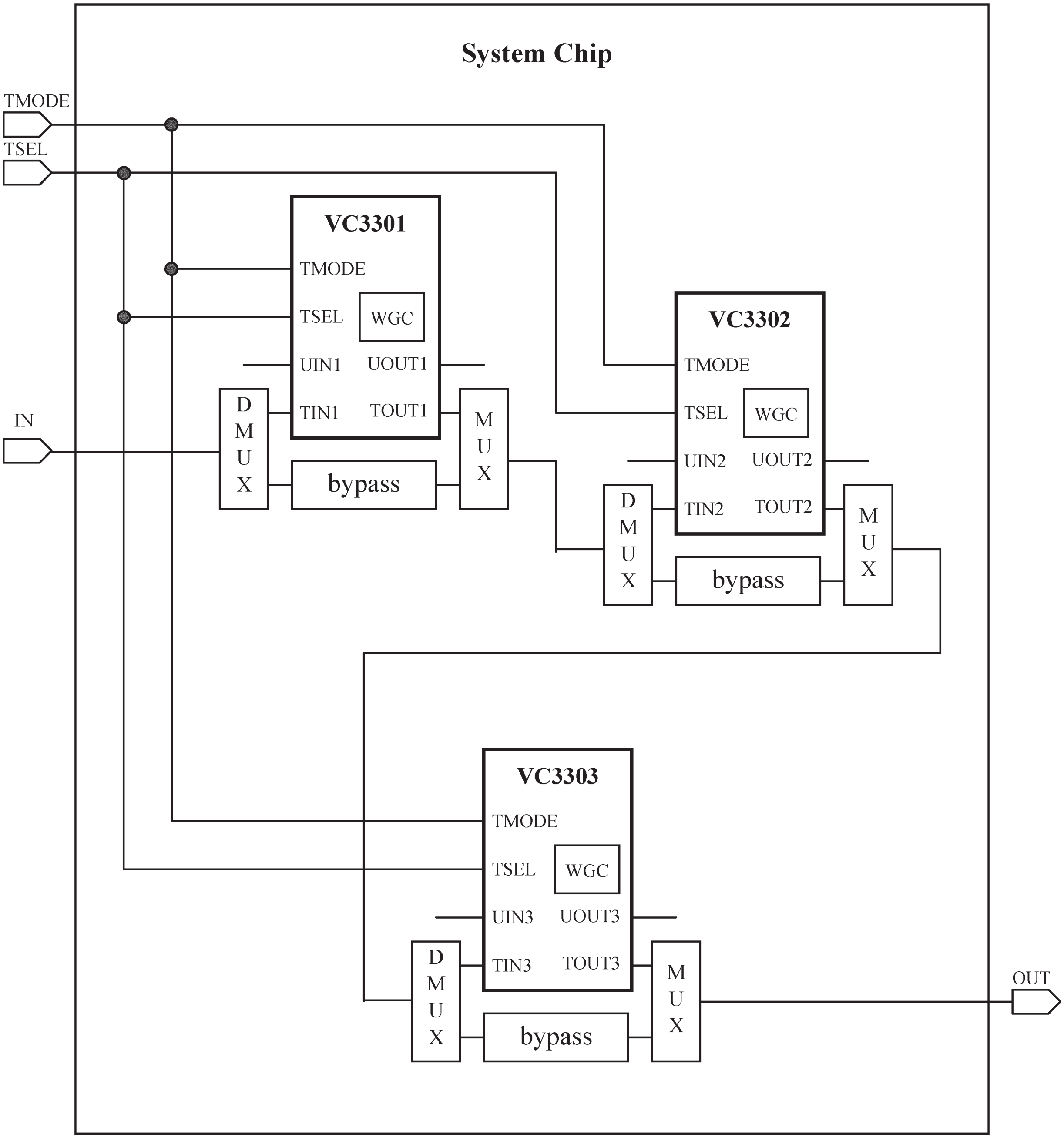


Fig. 10. SBTS implementation example.

TABLE I
NUMBER OF GATES IN THE FIVE IP CORES

IP Name	VC3301	VC3302	VC3303	VC3304	VC3305
Number of Gates	10257	19541	27053	36961	49862

E. Imperceptibility

We observe the IP circuit with the watermark identification circuit at the gate and physical design levels. Fig. 11(a) shows the schematic view without the watermark identification circuit, whereas Fig. 11(b) shows the schematic view with the watermark identification circuit. Fig. 12(a) shows the nonwatermarked layout of VC3301, whereas Fig. 12(b) shows the watermarked layout of the same design. We observe that it is practically impossible to notice any structural change in the watermarked solution. The WGC is invisible at the gate and physical design levels without impairing the normal function.

F. Identification Proof After Chips Have Been Packaged

After the chip has been packaged, we use it in the test mode only and show the proof of identification without examining

TABLE II
WATERMARKING HARDWARE OVERHEAD

IP Name	Watermark Method	30bits W.M.		40bits W.M.		50bits W.M.		60bits W.M.	
		Number of Gates	Area Overhead	Number of Gates	Area Overhead	Number of Gates	Area Overhead	Number of Gates	Area Overhead
VC3301	Original Circuit	10257	-----	10257	-----	10257	-----	10257	-----
	Headed W.S.M.	129	1.26 %	157	1.53 %	178	1.74 %	204	1.99 %
	Periodic W.S.M.	268	2.61 %	284	2.77 %	317	3.09 %	346	3.37 %
	Cyclic W.S.M.	235	2.29 %	253	2.47 %	281	2.74 %	304	2.96 %
	Random W.S.M.	233	2.27 %	262	2.55 %	289	2.82 %	312	3.04 %
	Operational W.S.M.	154	1.50 %	189	1.84 %	208	2.03 %	238	2.32 %
VC3302	Original Circuit	19541	-----	19541	-----	19541	-----	19541	-----
	Headed W.S.M.	131	0.67 %	157	0.80 %	187	0.96 %	212	1.08 %
	Periodic W.S.M.	264	1.35 %	293	1.50 %	319	1.63 %	344	1.76 %
	Cyclic W.S.M.	236	1.21 %	265	1.36 %	288	1.47 %	311	1.59 %
	Random W.S.M.	248	1.27 %	264	1.35 %	293	1.50 %	310	1.59 %
	Operational W.S.M.	169	0.86 %	181	0.93 %	214	1.10 %	239	1.22 %
VC3303	Original Circuit	27053	-----	27053	-----	27053	-----	27053	-----
	Headed W.S.M.	132	0.49 %	161	0.60 %	187	0.69 %	219	0.81 %
	Periodic W.S.M.	273	1.01 %	298	1.10 %	322	1.19 %	348	1.29 %
	Cyclic W.S.M.	246	0.91 %	269	0.99 %	294	1.09 %	311	1.15 %
	Random W.S.M.	244	0.91 %	276	1.02 %	298	1.10 %	320	1.18 %
	Operational W.S.M.	171	0.63 %	199	0.74 %	221	0.82 %	247	0.91 %
VC3304	Original Circuit	36961	-----	36961	-----	36961	-----	36961	-----
	Headed W.S.M.	141	0.38 %	166	0.45 %	196	0.53 %	223	0.60 %
	Periodic W.S.M.	279	0.75 %	294	0.80 %	322	0.87 %	347	0.94 %
	Cyclic W.S.M.	246	0.67 %	275	0.74 %	295	0.80 %	325	0.88 %
	Random W.S.M.	252	0.68 %	279	0.75 %	306	0.83 %	334	0.90 %
	Operational W.S.M.	174	0.47 %	193	0.52 %	231	0.62 %	258	0.70 %
VC3305	Original Circuit	49862	-----	49862	-----	49862	-----	49862	-----
	Headed W.S.M.	145	0.29 %	172	0.34 %	197	0.40 %	223	0.45 %
	Periodic W.S.M.	274	0.55 %	307	0.62 %	334	0.67 %	357	0.72 %
	Cyclic W.S.M.	252	0.51 %	273	0.55 %	309	0.62 %	332	0.67 %
	Random W.S.M.	254	0.51 %	281	0.56 %	314	0.63 %	333	0.67 %
	Operational W.S.M.	179	0.36 %	209	0.42 %	232	0.47 %	258	0.52 %

W.S.M.: Watermark Sequence Method

W.M.: Watermark

TABLE III
DESIGN FOR TEST SCHEME HARDWARE OVERHEAD

Chip Name	DFT Scheme	Number of Gates	Area Overhead
Chip_1	Original Circuit	156654	-----
	DATS	2734	1.75%
	SBTS	3851	2.46%
Chip_2	Original Circuit	231658	-----
	DATS	4569	1.97%
	SBTS	7373	3.18%
Chip_3	Original Circuit	372685	-----
	DATS	7521	2.02%
	SBTS	11982	3.22%

DATS: Direct Access Test Scheme DFT: Design for Test

SBTS: Scan Based Test Scheme

its microphotograph. When the test-mode signal is active, the selected IP core can thus independently be tested. The test-mode signal triggers the WGC embedded in the soft IP core. The selected IP is under test and sends the output test pattern that includes the watermark and test sequences and can clearly be observed from the output pins in the test mode. The watermark sequence can easily be extracted according to the arrangement of the output test pattern. Moreover, we prove the identity during the general test procedure; we do not implement any extra extraction flow. The proposed scheme is low in tracking costs.

G. *Proposed Scheme Compared With Other Approaches*

Table V compares several famous IP watermarking techniques. There are four main watermarking schemes discussed

TABLE IV
WATERMARKING CHARACTERISTICS

IP Name	Watermark Method	60 Bits Watermark				
		P. T.	N. T. P.	TVBO	TTO	F. C.
VC3301	Original Circuit	30:31	3981	1.5%	1.5%	95.2%
	Headed W.S.M.	30:45				
	Periodic W.S.M.	31:19				
	Cyclic W.S.M.	31:01				
	Random W.S.M.	31:01				
	Operational	30:51				
VC3302	Original Circuit	66:04	6168	0.97%	0.97%	93.6%
	Headed W.S.M.	66:23				
	Periodic W.S.M.	67:17				
	Cyclic W.S.M.	67:09				
	Random W.S.M.	67:13				
	Operational	66:40				
VC3303	Original Circuit	93:56	7701	0.78%	0.78%	93.1%
	Headed W.S.M.	94:18				
	Periodic W.S.M.	94:43				
	Cyclic W.S.M.	94:31				
	Random W.S.M.	94:40				
	Operational	94:23				
VC3304	Original Circuit	138:20	10965	0.54%	0.54%	91.5%
	Headed W.S.M.	139:01				
	Periodic W.S.M.	139:29				
	Cyclic W.S.M.	139:02				
	Random W.S.M.	139:49				
	Operational	138:56				
VC3305	Original Circuit	161:13	12484	4.8%	4.8%	90.2%
	Headed W.S.M.	161:50				
	Periodic W.S.M.	163:37				
	Cyclic W.S.M.	163:01				
	Random W.S.M.	162:43				
	Operational	161:40				

W.S.M: Watermark Sequence Method

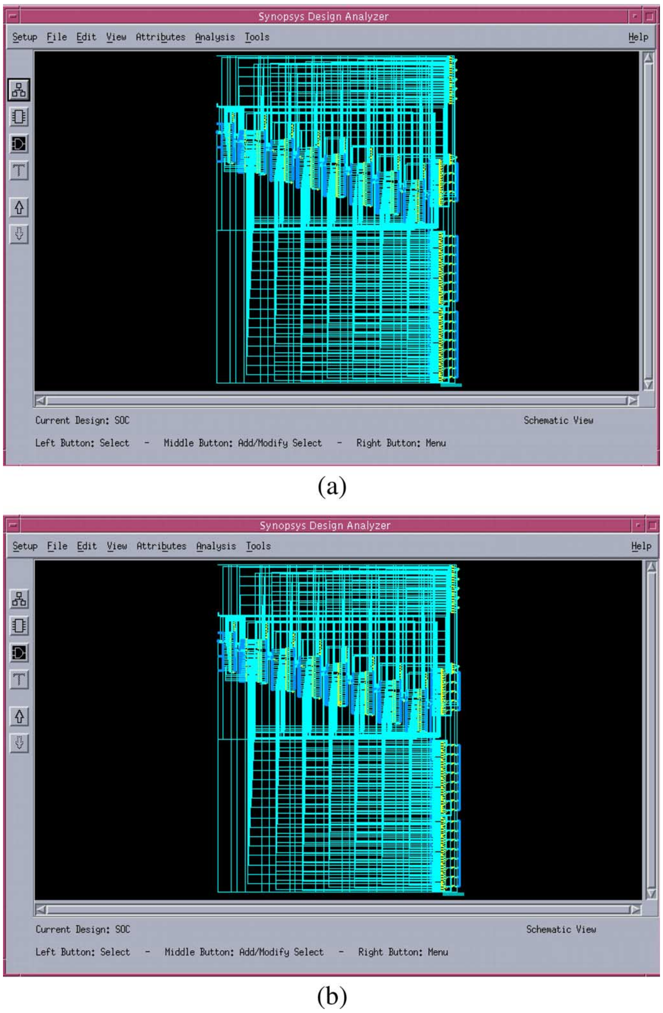
PT: Processing Time

NTP: Number of Test Pattern

FC: Fault Coverage

TVBO: Test Vector Bit Overhead

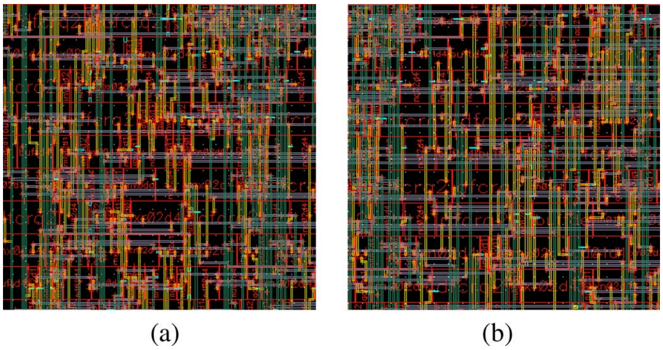
TTO: Test Time Overhead


Synopsys Design Analyzer
Setup File Edit View Attributes Analysis Tools
Help
Current Design: SOC
Schematic View
Left Button: Select - Middle Button: Add/Modify Select - Right Button: Menu
Synopsys Design Analyzer
Setup File Edit View Attributes Analysis Tools
Help
Current Design: SOC
Schematic View
Left Button: Select - Middle Button: Add/Modify Select - Right Button: Menu

(a)

(b)

Fig. 11. (a) Schematic view without watermark identification circuit. (b) Schematic view with watermark identification circuit.



(a)

(b)

Fig. 12. (a) Non-watermarked layout of VC3301. (b) Watermarked layout of the same design.

in the table: the proposed testing-based watermarking, the constraint-based watermarking, the FSM-based watermarking, and the DSP watermarking.

Kirovski and Potkonjak [12], [29], Kahng *et al.* [10], [25], [26], [28], and Narayan *et al.* [11] proposed the constraint-based IP watermarking. The main advantage of this approach is its actual low overhead. Nevertheless, the watermark cannot be detected or tracked, except at the same level of abstraction. Furthermore, the designer must examine the photomicrograph to check the identification after the chip has been packaged.

Oliveira [31] and Torunoglu and Charbon [32] add new sequences to the 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. However, the user encounters difficulty in tracking the FSM function when the IP is integrated into a whole chip. The watermark is hidden in the SOC after the chip has been packaged. The identification is not easy to prove.

Chapman *et al.* [33], [34] proposed a DSP watermarking scheme that depends on a very low data rate. However, the

TABLE V
PROPOSED SCHEME COMPARES WITH OTHER APPROACHES

Type	Scheme	Design Case by Case	Behavioral Design Level	Gate Design Level	Physical Design Level	Packaged	Design Case by Case
Testing Based WM	Proposed Scheme	No	Identify	Identify	Identify	Identify	No
Constraint Based WM	Kirovski [12, 29]	No	None	Identify	Identify	None	No
	Kahng [10, 25, 26, 28]	No	None	None	Identify	None	No
	Narayan [11]	No	None	None	Identify	None	No
FSM Based WM	Oliveira [31]	No	None	Identify	Identify	None	No
	Torunoglu [32]	No	None	Identify	Identify	None	No
DSP Based WM	Chapman [33][34]	Yes	Identify	Identify	Identify	None	Yes

WM: Watermark

approach does not have a clear way to track and extract the watermark at lower levels. The watermark must be designed case by case according to the characteristics of various IPs. It is not convenient.

The proposed method has low overhead. The scheme can detect or track at the behavioral, gate, and physical design levels and packaged chip without examining the photomicrograph. The method does not need to be designed case by case. It is very convenient.

V. CONCLUSION

In this paper, a new testing-based watermarking scheme for IP identification is presented. The ownership rights are proven according to the output test pattern and watermark sequence during the general test procedure without implementing any extra extraction flow. The watermark is a general-purpose design methodology that does not need to be designed case by case according to various IPs. 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 IP watermarking approaches entail low hardware overhead (area increase by no more than 5%), low tracking costs, and low PT costs (time increases by no more than 1 min) and provide a strong proof of identity. The watermark function is not changed after logic synthesis, placement, and routing because the watermark is embedded into the TC at the behavioral design level. The approaches have the ability to detect the presence of the watermark and to identify the soft IP core at various design levels. It is still easy to detect the identity of the IP designer after the chips have been packaged, and there is no need to examine the microphotograph. The experimental results have demonstrated that the proposed method is really a feasible and practical scheme for IP identification. Although the proposed method achieves the goal of IP watermarking, a digital rights management (DRM) platform for SOC/VLSI IP is not currently performed. However, a complete DRM platform is a very important issue for the future. Until now, there has been no paper that has discussed this problem. The complete DRM platform for SOC/VLSI IP is worth researching.

ACKNOWLEDGMENT

The author would like to thank the Chip Implementation Center (CIC) for supplying the technology models used in the system simulations. He would also like to thank the AU Optronics Corporation (AUO) for supplying the technology and financing for the system design.

REFERENCES

[1] H. Chang, *Surviving the SOC Revolution: A Guide to Platform-Based Design*. Norwell, MA: Kluwer, 1999.

[2] G. Martin and H. Chang, *Winning the SoC Revolution: Experiences in Real Design*. Norwell, MA: Kluwer, 2003.

[3] *Architecture Document Version 1.0*, 1997, Virtual Socket Interface Alliance.

[4] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Mateo, CA: Morgan Kaufmann, 2002.

[5] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[6] Y. P. Wang, M. J. Chen, and P. Y. Cheng, "Robust image watermark with wavelet transform and spread spectrum techniques," in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Nov. 2000, vol. 2, pp. 1846–1850.

[7] Q. Sun and S. F. Chang, "Semi-fragile image authentication using generic wavelet domain features and ECC," in *Proc. Int. Conf. Image Process.*, Sep. 2002, vol. 2, pp. 901–904.

[8] Y. L. Ho and H. C. Wang, "An audio watermarking algorithm based on significant component modulation," in *Proc. IEEE Int. Conf. Consum. Electron.*, Jun. 2003, pp. 212–213.

[9] T. H. Tsai and C. Y. Wu, "An implementation of configurable digital watermarking system in MPEG video encoder," in *Proc. IEEE Int. Conf. Consum. Electron.*, Jun. 2003, pp. 216–217.

[10] A. B. Kahng, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Robust IP watermarking methodologies for physical design," in *Proc. IEEE Des. Autom. Conf.*, Jun. 1998, pp. 782–787.

[11] N. Narayan, R. D. Newbould, J. D. Carothers, J. J. Rodriguez, and W. T. Holman, "IP protection for VLSI designs via watermarking of routes," in *Proc. IEEE Int. Conf. ASIC/SOC*, Sep. 2001, pp. 406–410.

[12] D. Kirovski and M. Potkonjak, "Localized watermarking: Methodology and application to template mapping," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Jun. 2000, vol. 6, pp. 3235–3238.

[13] A. E. Caldwell, H. J. Choi, A. B. Kahng, S. Mantik, M. Potkonjak, G. Qu, and J. L. Wong, "Effective iterative techniques for fingerprinting design IP," in *Proc. Des. Autom. Conf.*, Jun. 1999, pp. 843–848.

[14] J. Lach, W. H. Mangione-Smith, and M. Potkonjak, "Fingerprinting digital circuits on programmable hardware," in *Proc. Int. Workshop Inf. Hiding*, 1998, pp. 16–31.

[15] E. Charbon, "Hierarchical watermarking in IC design," in *Proc. IEEE Custom Integr. Circuits Conf.*, May 1998, pp. 295–298.

[16] Y. C. Fan and H. W. Tsao, "Watermarking for intellectual property protection," *Electron. Lett.*, vol. 39, no. 18, pp. 1316–1318, Sep. 2003.

[17] A. Crouch, *Design for Test for Digital IC's and Embedded Core Systems*. Englewood Cliffs, NJ: Prentice-Hall, 1999.

[18] M. L. Bushnell and V. D. Agrawal, *Essentials of Electronic Testing for Digital, Memory, and Mixed-Signal VLSI Circuits*. Norwell, MA: Kluwer, 2000.

[19] Y. C. Fan and H. W. Tsao, "Watermarking based IP core protection," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2003, pp. 181–184.

[20] *Verilog Hardware Description Language Reference Manual*, Open Verilog Int., Los Gatos, CA, 1991.

[21] *HDL Compiler for Verilog Reference Manual*, Synopsys, Mountain View, CA, 2000.

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

[23] J. Aerts and E. J. Marinissen, "Scan chain design for test time reduction in core-based ICs," in *Proc. Int. Test Conf.*, Oct. 1998, pp. 448–457.

[24] B. T. Murray and J. P. Hayes, "Testing ICs: Getting to the core of the problem," *Computer*, vol. 29, no. 11, pp. 32–38, Nov. 1996.

[25] A. B. Kahng *et al.*, "Constraint-based watermarking techniques for design IP protection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 20, no. 10, pp. 1236–1252, Oct. 2001.

[26] A. B. Kahng, D. Kirovski, S. Mantik, M. Potkonjak, and J. L. Wong, "Copy detection for intellectual property protection of VLSI designs," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Des.*, 1999, pp. 600–604.

[27] G. Wolfe, J. L. Wong, and M. Potkonjak, "Watermarking graph partitioning solutions," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 21, no. 10, pp. 1196–1204, Oct. 2002.

[28] A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Watermarking techniques for intellectual property protection," in *Proc. IEEE Des. Autom. Conf.*, 1998, pp. 776–781.

[29] D. Kirovski and M. Potkonjak, "Local watermarks: Methodology and application to behavioral synthesis," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 22, no. 9, pp. 1277–1283, Sep. 2003.

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

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

[32] I. Torunoglu and E. Charbon, "Watermarking-based copyright protection of sequential functions," in *Proc. IEEE Custom Integr. Circuits Conf.*, 1999, pp. 35–38.

[33] R. Chapman and T. S. Durrani, "IP protection of DSP algorithms for system on chip implementation," *IEEE Trans. Signal Process.*, vol. 48, no. 3, pp. 854–861, Mar. 2000.

[34] R. Chapman, T. S. Durrani, and A. P. Tarbert, "Watermarking DSP algorithms for system on chip implementation," in *Proc. IEEE Int. Conf. Electron., Circuits Syst.*, 1999, pp. 377–380.

[35] H. W. Tsao and Y. C. Fan, "Method and device for IC identification," R.O.C. Patent I226 001, Jan. 1, 2005.

[36] H. W. Tsao and Y. C. Fan, "Method and device for IC identification," U.S. Patent 6 883 151, Apr. 19, 2005.

[37] Y. C. Fan, H. Y. Yang, and H. W. Tsao, "Direct access test scheme for IP core protection," in *Proc. IEEE AP-ASIC Conf.*, Aug. 2004, pp. 262–265.

[38] Y. C. Fan and H. W. Tsao, "Boundary scan test scheme for IP core identification via watermarking," *IEICE Trans. Inf. Syst.*, vol. E88-D, no. 7, pp. 1397–1400, Jul. 2005.

[39] Y. C. Fan, A. Chiang, D. C. Sung, T. C. Chi, J. C. Jiang, Y. T. Hsieh, and J. H. Shen, "Testing based SoC/VLSI IP identification and protection platform," in *Proc. IEEE IMTC*, May 1–3, 2007, pp. 1–4.

Yu-Cheng Fan (S'00–M'05) was born in Hsinchu, Taiwan, R.O.C., in 1975. He received the B.S. and M.S. degrees in electrical engineering from National Cheng Kung University, Tainan, Taiwan, in 1997 and 1999, respectively, and the Ph.D. degree in electrical engineering from National Taiwan University, Taipei, Taiwan, in 2005.

From 1999 to 2000, he was an IC Design Engineer with the Computer and Communications Research Laboratory, Industrial Technology Research Institute, Hsinchu. From 2000 to 2005, he was with the Integrated System Laboratory, National Taiwan University. Since 2006, he has been with the Department of Electronic Engineering, National Taipei University of Technology, Taipei, where he is currently an Assistant Professor. His research interests are consumer electronics, digital watermarking, image and video coding system, digital television broadcasting, and very large scale integration/system-on-a-chip design.

Dr. Fan received the 13th Long-Term (Acer) Paper Awards in 1999. In 2002, he received the Honors of the First Electronics Innovative Design Award at National Taiwan University. In 2003, he received the Best Paper Award (Best Poster) at the 2003 IEEE International Conference on Consumer Electronics. In 2005, he received the IEEE Award for his outstanding leadership and service to the IEEE National Taiwan University (NTU) Student Branch. He received the Best Paper Award at the 2005 IEEE International Conference on Information Technology: Research and Education. He received the Honors of the Second Taiwan Information Storage Association Ph.D. Dissertation Award in 2005 and the Honors of the 19th Long-Term (Acer) Paper Awards in the same year. He was elected Chairman of the IEEE NTU Student Branch in 2003. He is a scholastic honor member of Phi Tau Phi.