International Journal of Electronics and Electrical Engineering

Volume 2 | Issue 2 Article 12

October 2013

FSM BASED DIGITAL WATERMARKING IN IP SECURITY

SK. MASTANBEE
Dept. Of ECE, SMCE, Guntur, shaikmastanbi80@yahoo.com

G. SUSEELAMMA
Dept. Of ECE, SMCE, Guntur, Suseela.gera@gmail.com

E. ADINARAYANA
Dept. Of ECE, SMCE, Guntur, adinarayana@yahoo.in

Recommended Citation

MASTANBEE, SK.; SUSEELAMMA, G.; and ADINARAYANA, E. (2013) "FSM BASED DIGITAL WATERMARKING IN IP SECURITY," *International Journal of Electronics and Electrical Engineering*: Vol. 2 : Iss. 2 , Article 12.
Available at: https://www.interscience.in/ijeee/vol2/iss2/12

FSM BASED DIGITAL WATERMARKING IN IP SECURITY

SK.MASTANBEE, G.SUSEELAMMA & E.ADINARAYANA

Dept. Of ECE, SMCE, Guntur
shaikmastanbi80@yahoo.com, Suseela.gera@gmail.com, adinarayana@yahoo.in

Abstract: IP providers are in pressing need of a convenient means to track the illegal redistribution of the sold IPs. An active approach to protect a VLSI design against IP infringement is by embedding a signature that can only be uniquely generated by the IP author into the design during the process of its creation. a VLSI IP is developed in several levels of design abstraction with the help of many sophisticated electronic design automation tools. Each level of design abstraction involves solving some NP-complete optimization problems to satisfy a set of design constraints. In this paper, a new dynamic watermarking scheme is proposed. The watermark is embedded in the state transitions of FSM at the behavioral level.

Keywords: *Sequential Design, Finite state machine (FSM), intellectual property (IP) protection, IP watermarking.*

1. INTRODUCTION

Watermarking techniques were widely used throughout history, for copyright protection as well as data hiding. IP watermarking was introduced as a candidate to protect this sensitive copyright information. IP blocks are delivered in three main flavors depending on price, applications, and contracts between companies. The Virtual Socket Interface (VSI) architecture describes such levels as:

Soft IPs**:** are delivered in the form of synthesizable hardware design language (HDL) code. They have the advantage of being more flexible and the disadvantage of not being as predictable in terms of performance (i.e., timing, area, power). Soft IPs typically have increased intellectual property risks because RTL (register transfer level) source code is required by the integrator.

Firm IPs**:** are optimized in structure and topology for performance and area through floor planning/placement, possibly using a generic technology library. Firm IPs offer a compromise between soft and hard. Firm IPs include a combination of synthesizable RTL, reference technology library, detailed floor-plan, and a full or partial netlist. Firm IPs do not include routing. Risks are equivalent to those of soft IPs if RTL is included and are less if it is not.

Hard IPs**:** are optimized for power, size, or performance and mapped to a specific technology. Examples include netlists that are fully placed, and routed, or optimized custom physical layout. They have the advantage of being much more predictable, but consequently are less flexible and portable due to process dependencies. Hard IPs require, at a minimum, a high level behavioral model, a test list, full physical and timing models along with the final layout. The ability to protect hard IPs is much better because of copyright facilities and there is no requirement for an RTL code.

The VSI Alliance IP protection development working group [5] identifies three main approaches to secure IPs. First, a *deterrent* approach, where the owner uses legal means trying to stop attempts for illegal distribution, i.e., using patents, copyrights and trade secrets. Second, a *protection* approach, where the owner tries to prevent the unauthorized usage of the IP physically by license agreements and encryption. Protection techniques mostly based on model encryption [4], or distributed environment [9], fall short in securing designs or track them in case they are stolen or reused without permission. For such reasons, a third *detection* approach was introduced, where the owner detects and traces both legal and illegal usages of the designs as in watermarking or fingerprinting. This tracking should be strong enough to be considered as evidence in front of a court if needed. The VSI alliance proposed the usage of the three approaches for proper protection of IP designs

2. IP WATERMARKING EVALUATION CRITERIA

a. *Relying On The Secrecy Of The Algorithm***:** According to one of the oldest defined security rules, defined by Kerckhoffs [20] in 1883, any encryption or security technique should not rely on the secrecy of the algorithm, but to the mathematical complexity of such algorithm, "*The system must not require secrecy and can be stolen by the enemy without causing trouble*".

b. *Level of reliability* **:** This is a very important measure, which can be divided into two main aspects: (1) *robustness*, which measures the strength of the hidden mark against attacks, and the percentage of undetected watermarked design that might appear; and (2) *false positive*, which occurs whenever the detector could find a mark in a non watermarked design. Both measures are related to attack analysis and will be discussed in details in the next subsection.

c.*Affecting design functionality***:** Testing and verification of hardware systems is an extremely complicated task. Watermarking techniques should prove their soundness against such a criteria, preferably by proving it mathematically.

d. *Preventing intruder from re-embedding another watermark***:** As a passive technique, one of the main challenges of watermarking schemes is the authenticity of the watermark. Scheme designers need to find techniques to protect their designs from intruders who may try to embed another watermark in the design at least to destroy watermark authenticity in front of a court.

e. *Embedding enough data to identify ownership***:** The watermarking scheme should add enough data to identify the owner of the design. This data should be concrete enough to be considered as an evidence in front of a court. Nevertheless, the data size should be small enough to neither impose a high overhead on the design size nor to affect the design performance. The amount of data embedded is one of the measures used to differentiate between different IP watermarking techniques.

f. *Implementation overhead:* Watermarking a design is a complementary process to increase its competitiveness but affecting the design performance or having a high overhead in the insertion process would be considered a real drawback. For IP watermarking, we will consider the area, power and delay overheads compared to the original design without watermarking.

g. *Detection and tracking***:** Watermark insertion is only half the process, tracking and detection is the second important aspect in any watermarking technique. Tracking and detecting the watermark or its traces after possible attacks is essential.

This will be considered as one of the main aspects for judging watermarking techniques *Asymmetry*.

IP Watermarking: State-of-the-Art:

Many IP watermarking or fingerprinting techniques can be found in the open literature. IP watermarking techniques can be classified into two main classes: (1) *dynamic watermarking*, where the watermark cannot be detected except by running the watermarked IP to detect the generated signal, such as digital signal processing (DSP) or finite state machine (FSM) watermarking; and (2) *static watermarking*, where the watermark is considered a property of the design, and can only be detected by different static techniques, such as route and placement watermarking

3. WATERMARKING FINITE STATE MACHINES

A FSM watermarking scheme was proposed by inserting redundant transitions into the original STG after the unspecified transitions in the STG are searched and associated with the user-defined input/output sequence. The weakness of this scheme is the monotonous use of only the unspecified transitions with the specified outputs of STG for watermark insertion. The embedding capacity is limited by the number of free input combinations. For FSMs with limited unspecified transitions, the probability of coincidence is high.

FSM WM Based on Unused Transitions:

The algorithm is mainly based on extracting the unused transitions in a state transition graph (STG) of the behavioral model. These unused transitions are inserted in the STG and associated with a new defined input/output sequence, which will act as the watermark. In case the FSM is completely specified (CSFSM), new input/output pairs are added to expand the FSM. The minimum number of transitions needed (*n*min) is then calculated, and compared to the maximum number of free transitions (*n*max) to satisfy the probability (*Pu*) that a non-watermarked design would carry this watermark by coincidence. If this probability cannot be satisfied, input/output pairs should be added to satisfy the watermark requirements. The input/output sequence is calculated, such that the input sequence is random to the set of unused transition inputs. On the other hand, the output, which is the hidden information, is encrypted using a key (*K*). Extra transitions are added such that the output of the given input sequence generates the encrypted hidden data, i.e., one should have both the key and the input sequence to be able to read the watermark. Figure 3 shows an example of the watermarking process, where Figure 3(a) shows the original design, Figure 3(b) describes the watermarked design, and Figure 3(c) shows another watermarked solution after augmenting the inputs to add more transitions. The approach works at a high level of the design flow, which provides extra strength, and does not depend on the secrecy of the algorithm as a way of securing the design. The algorithm can be detected at mostly all lower design levels, sometimes even after design manufacturing. The authors, however, used the probability of coincidence as the only measure for robustness, which only covered the false-positives case. To evaluate the approach using the proposed evaluation criteria, we had used the values generated by the authors in [42] to calculate both the masking probability (*Pum*) and the removal probability (*Pu r*) for the IWLS93 [25] benchmark set shown in Table 1. Considering all transitions have equal occurrence probabilities, the masking probability (*Pum*) can be calculated as “*the probability that any attack would delete at least one transition in order to cover the watermark without affecting any of the original design transitions*”. Hence, P_u^m was calculated as follows:

$$P_m^u = \frac{n_{\min}}{n + n_{\min}}$$

Static Watermarking Techniques: Constraint-Based IP Watermarking

Constraint-based IP watermarking approach is a generic algorithm that can be used at different levels of the design flow. The approach is based on the usage of available tools used mainly to solve NP-hard problems. The algorithm adds extra constraints to such solution, yielding to the new watermarked design. The approach is based on a generic optimizer and constraint-satisfaction (SAT) problems [7]. The watermarking tool proposed is mainly composed of the following parts (Figure 4):

The watermark is presented to the constraint generator. In the generator, the watermark is first encrypted, then transferred through a hash function (to shorten its length). Finally, it is converted to a set of extra constraints, through the well-formed grammar, forming a new set of constraints which is added to the available ones. Both the design and the set of constraints are fed to the black-box optimizer resulting in a watermarked solution. The watermark is then a set of extra constraints that will limit the set of possible solutions to a smaller set. The watermark becomes stronger as the "*watermark subset*" is smaller. Kahng el al. [7] illustrated this approach using a simple satisfiability (SAT) problem [3]. Many problems in hardware design are modeled as a classical NP complete constraint satisfaction problem. For instance, let SAT (U,C) be a finite set of variables U and a collection $C = \{c1, c2, . . . , cn\}$ of clauses over U. The SAT problem relies on finding the set of all satisfying assignment ("truth assignment") of C that satisfies all the clauses in U. Adding extra constraints to such problem direct the solution to identify uniquely the watermarked solution. The proposed scheme is the dominant approach for hardware IP watermarking designs, and although we classify it as a static approach yet some of its applications can be dynamic. Due to the generic nature of the approach, it was applied to different levels of the IP design flow. At the system level, for instance, it was used to watermark memory graph coloring problems [1], as well as graph partitioning problems [4] and linear programming problems [6]. At lower design levels, the approach was used even more heavily with routing placement, and floor planning [9].

4. EXPERIMENTAL RESULTS

The result in 5.1 has the input1 and input 2 as said in the statement mentioned .the corresponding output shows that both given inputs are equal i.e 1. The result has the input1 and input 2 as said in the statement mentioned .the corresponding output shows that both given inputs are not equal i.e 0

In fig 5.b S stands for state . In SXXinput signal name the first x stands for initiating state and the other x stands for terminating state. Some state transition have don't care 'x' as input.

The outputs are the encoded watermark in the output of the each FSM state. In the above result the resultant watermarked outputs are stated in which each state in the finite state machine if involves in the watermarking then output exist if not the sate output is null(XX as in simulation waveform).

The above simulation result are the signals used for watermarking the FSM. During the watermarking state the inputs of all the corresponding states are selected as in the above simulation result when state s1 is selected corresponding inputs are mentioned with signal names inputstate. Signal yout represent the compatibility of each input to the watermark. .done are signals to avoid the state to be twice watermarked

5. CONCLUSION

A new robust dynamic watermarking scheme by embedding the authorship information on the transitions of STG at the behavioral synthesis level. The proposed method offers a high degree of tamper resistance and provides an easy and noninvasive copy detection. The FSM watermark is highly resilient to all conceivable watermark removal attacks. The redundancy in the FSM has been effectively utilized to minimize the embedding overhead. By increasing the length of input code sequence for watermark retrieval and allowing the output compatible transitions to be revisited to embed different watermark bits, the watermarks are more randomly dispersed and better concealed in the existing transitions of FSM.

Similar to other FSM watermarking schemes , this method is not applicable to some ultrahigh speed designs that do not have a FSM. Fortunately, regular sequential functions are omnipresent in industrial designs, making FSM watermarking a key research focus for dynamic watermarking.

The methodology proposed in this thesis is a new technique that offers a realistic secure and robust watermarking for IP designs. Furthermore, it presents a first step towards combining both concurrency and watermarking techniques. Based on our previous work in this domain, we believe that the proceeding future work can be completed and expanded.

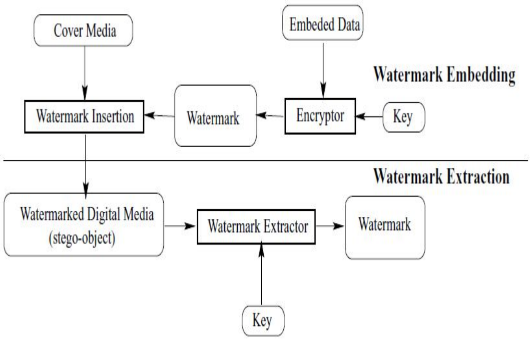

Figure 1 Watermarking scheme

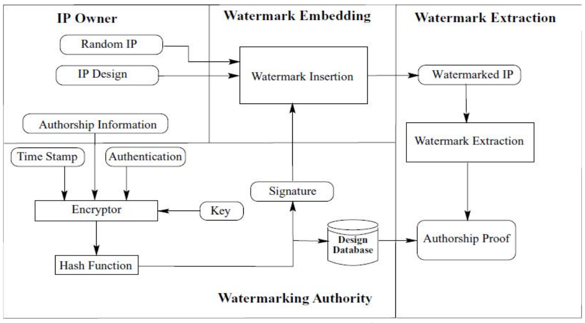

Figure 2 IP Watermarking

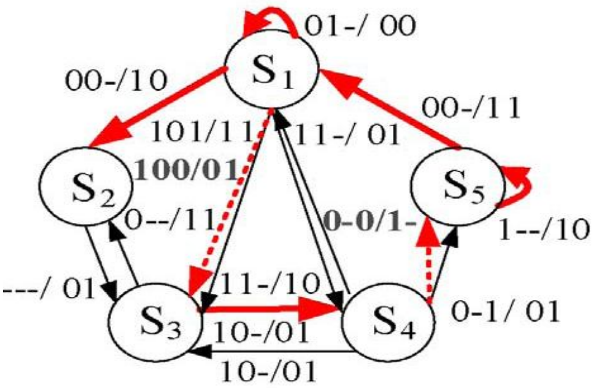

Figure 3 Watermarked STG By proposed method

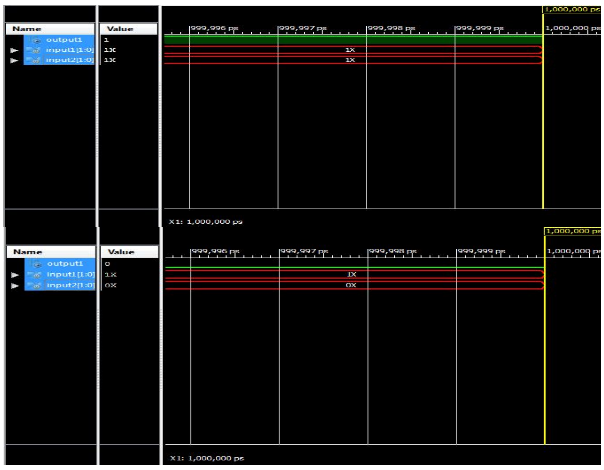

Figure 4 a. Simulation Results of compatibility mode

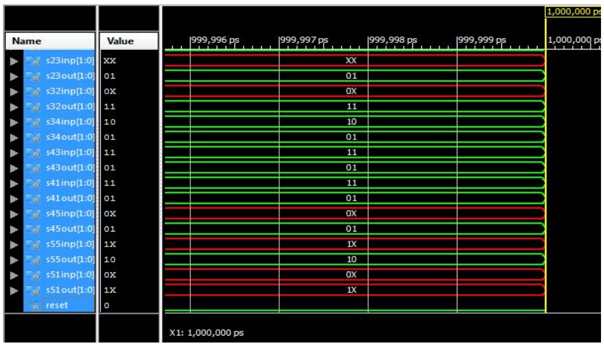

Figure 5 b. Inputs to the proposed module

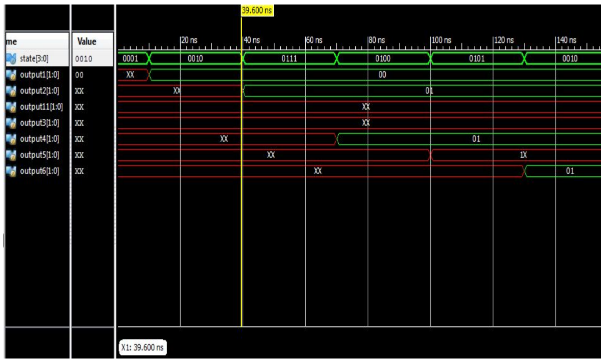

Figure 6 c. watermarked FSM transition output

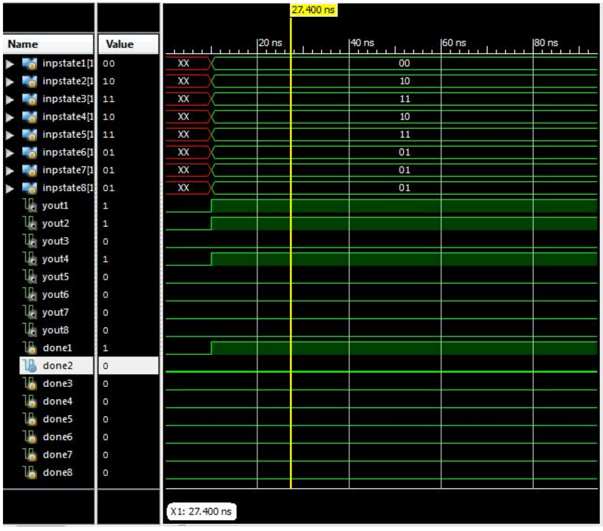

Figure 7 d. Results obtained during processing of watermarking

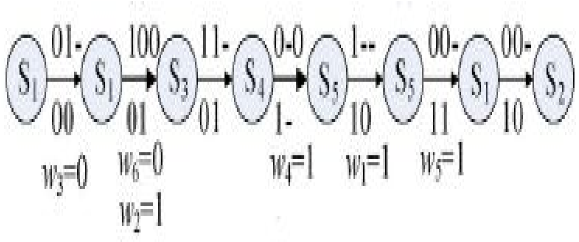

Figure 8 Excitation of watermarked STG

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their comments which were very helpful in improving the quality and presentation of this paper.

REFERENCES:

[1] D. Kirovski, Y. Y. Hwang, M. Potkonjak, and J. Cong, “Protecting Combinational logic synthesis solutions,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 25, no. 12, pp. 2687–2696, Dec.2006.

[2] A. T. Abdel-Hamid, S. Tahar, and E. M. Aboulhamid, “A survey on IP watermarking techniques,” in *Design Automation for Embedded Systems*, vol. 10. Berlin, Germany: Springer-Verlag, Jul. 2005, pp. 1–17..

[3] A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, “Constraintbased watermarking techniques for design IP protection,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 20, no. 10, pp. 1236– 1252, Oct. 2001.

[4] A. Cui and C. H. Chang, “Watermarking for IP protection through template substitution at logic synthesis level,” in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2007, pp. 3687–3690.

[5] A. Cui and C. H. Chang, “Stego-signature at logic synthesis level for digital design IP protection,” in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2006, pp. 4611–4614.

[6] A. Cui, C. H. Chang, and S. Tahar, “IP watermarking using incremental technology mapping at logic synthesis level,” *IEEE Trans. Comput.- Aided Design Integr. Circuits Syst.*, vol. 27, no. 9, pp. 1565–1570, Sep. 2008.

[7] Intellectual Property Protection Development Working Group, *Intellectual Property Protection: Schemes, Alternatives*VSI Alliance, Aug. 2001, white paper, version 1.1.

[8] I. Hong and M. Potkonjak, “Techniques for intellectual property protection of DSP designs,” in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, vol. 5. May 1998, pp. 3133–3136.

[9] A. Rashid, J. Asher, W. H. Mangione-Smith, and M. Potkonjak, “Hierarchical watermarking for protection of DSP filter cores,” in *Proc. IEEE Custom Integr. Circuits Conf.*, May 1999, pp. 39–42.

[10] A. 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.

Authors Profile:

SK. Mastanbee is Pursuing her Master Degree from SMCE college, Guntur. Interested In the Filed of Electronics and Current progress in Digital Electronics

G.Suseelamma Completed her Master Degree and working as Assistant Professor in ECE Department of SMEC, GUNTUR with 5 years of Teaching Experience .

E. ADINARAYANA is The HOD, Dept of ECE,SMEC. He is working towards Ph.D in electronics & communications engineering from Jawaharlal Nehru Technological University Hyderabad. His current research focus on Signal Processing & wireless Communications.

◈◈◈