International Journal of Computer and Communication Technology

Volume 7 | Issue 2 Article 9

April 2016

Copyright Protection for Intellectual Property

P. Nalini
Department of Electronics and Communication Engineering, Nalanda Institute Of Engineering And Technology, Sattenapalli, p.naliny@gmail.com

K. Sam Prasad
Department of Electronics and Communication Engineering, Nalanda Institute Of Engineering And Technology, Sattenapalli, ksamprasad@gmail.com

L. Srinivas
Department of Electronics and Communication Engineering, Nalanda Institute of Engineering and Technology, Sattenapalli, srinivas_lanki@yahoo.com

Follow this and additional works at: https://www.interscience.in/ijcct

Recommended Citation
Nalini, P.; Sam Prasad, K.; and Srinivas, L. (2016) "Copyright Protection for Intellectual Property," *International Journal of Computer and Communication Technology*: Vol. 7 : Iss. 2 , Article 9.
DOI: 10.47893/IJCCT.2016.1350
Available at: https://www.interscience.in/ijcct/vol7/iss2/9

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Computer and Communication Technology by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

Copyright Protection for Intellectual Property

P. Nalini, K. Sam Prasad & L. Srinivas

Department of Electronics and Communication Engineering,
Nalanda Institute Of Engineering And Technology, Sattenapalli
E-mail : p.naliny@gmail.com

Abstract – Intellectual property takes several forms, the most important of which are patents, copyrights, and trade rights. Patents protect inventions. One can patent methods and processes, new varieties of plants, and (more weakly) designs. The VSI alliance proposed the usage of the three approaches for proper protection of IP designs.

The detection approach directly interacts with the VLSI design, and is considered an overhead on the design cycle. IP watermarking and IP fingerprinting are the main approaches used, where the design is watermarked (tagged) then different tracking techniques are used to keep track of the usages of such design. Reuse-Based design methodology has taken hold, the very large scale integration (VLSI) design industry is confronted with the increasing threat of intellectual property (IP) infringement.

Keywords - *Finite state machine (FSM), intellectual property (IP) protection, IP watermarking, sequential design, state transition graph (STG).*

I. INTRODUCTION

Intellectual property takes several forms, the most important of which are patents, copyrights, and trade rights. Patents protect inventions. One can patent methods and processes, new varieties of plants, and (more weakly) designs. But one cannot patent things that are obvious, functionality without mechanism (that is, a system to do X without describing how it gets done), or laws of nature. Patents are about ideas. Even without knowledge of a patented invention, one can go to court to prohibit the independently developed device that uses it. Copyright governs artistic expression, not ideas. It prohibits, for a finite time, the copying of artistic works. In the US, a copyright currently lasts for the life of the author plus 70 years, but national laws vary. Copyright protects against direct copying of a product, not ideas' protection. If one has never having seen a design, creates a similar design, then she/he has not violated the copyright. Trade secrets: provide legal protection for companies that want to keep information from the public. A trade secret law is, in some sense, the opposite of patent law.

Digital piracy generally includes the following cases: 1) Illegal Access: A pirate tries to receive a digital product from a network site without permission; 2) Intentional Tampering: A pirate modifies a digital product in order to extract/insert features for malicious reasons and then proceeds to its retransmission. The authenticity of the original product is lost; and 3) Copyright Violation: A pirate receives a product and resells it without getting the permission to do so from the copyright owner.

II. COMMUNICATING FINITE STATE MACHINES

If we allow overlap of the sets of input and output signals of a finite state machine, in all fairness, we cannot say what will happen without first considering in more detail what a ‘‘signal’’ is. We assume that signals have a finite range of possible values and can change value only at precisely defined moments. The machine executes a two-step algorithm. In the first step, the input signal values are inspected and an arbitrary executable transition rule is selected. In the second step, the machine changes its control state in accordance with that rule and updates its output signals. These two steps are repeated forever. If no transition rule is executable, the machine will continue cycling through its two-step algorithm without changing state, until a change in the input signal values, effected by another finite state machine, makes a transition possible. A signal, then, has a state, much like a finite state machine. It can be interpreted as a variable that can only be evaluated or assigned to at precisely defined moments. The machines must share a common ‘‘clock’’ for their two-step algorithm, but they are not otherwise synchronized. If further synchronization is required, it must be realized with a subtle system of handshaking on the signals connecting the machines.

III. PROPOSED ALGORITHM

To verify the authorship, one needs to run the watermarked FSM with the input sequence, ˆX = {ˆX1, ˆX2, • • • , ˆXN}, applied on state ˆs1. If the operation halts before N transitions, the watermark cannot be detected. Otherwise, an output sequence ˜Y of N × k bits is obtained. The bits indexed by the set B of m random numbers are selected from ˜Y to form an ordered sequence ˜W . The authorship is proved if ˜W perfectly matches or is highly correlated with the watermark W of the IP owner.

Although the ownership can be authenticated directly by running the watermarked FSM with ˆX, it does not permit the IP authorship to be field authenticated by the IP buyers after the watermarked FSM has been implemented into an integrated circuit and packaged. Since only the test signals can be traced after the chip is packaged, the authorship of the watermarked FSM can be verified off chip by making it a part of the test kernel.

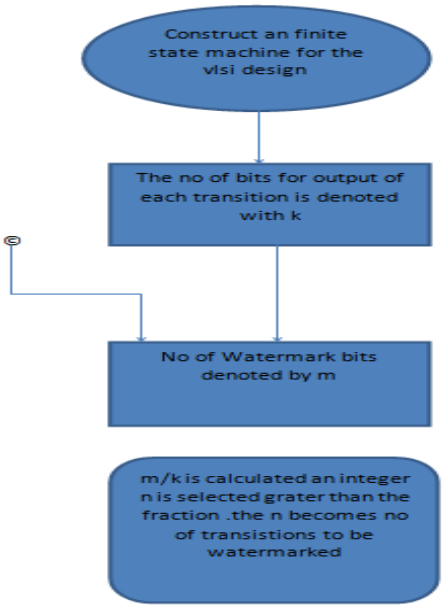


Fig. 1 Algorithm part-1

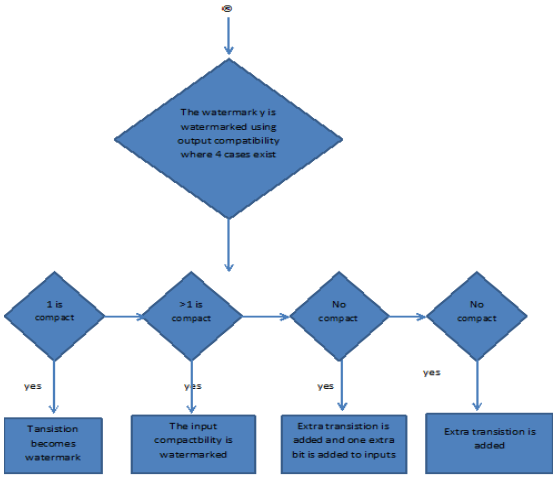


Fig. 2 Algorithm part-2

A sequence of test vectors can be applied serially through the scan-in, Sin pin to bring ˆM to the designated state ˆs1 in the test mode, followed by N designated test vectors that incorporate ˆX. The output responses ˜Y can then be collected serially from a scan-out Sout pin externally to verify the authenticity of ˆM . This convenient way of watermark verification can be performed by the end users provided that scan design is also incorporated in the watermarked IP chip. Since the scan chain is used as a medium to aid authorship verification of the IP encapsulated in the test kernel. The aggressor needs additional effort to also successfully tamper or redesign the test structure to provide the fault coverage of the pirated IP. Failure to detect the scan chain signature alerts malicious tampering or removal of the test structure in attempt to misappropriate the protected IP.

The watermark W is inserted into STG(M) by modifying some of its edges without changing the operational behavior of M to find a sequence of N consecutive transitions, t i = _ˆsi, ˆsi+1, ˆXi, ˆYi_, i = 1, 2, . . . , N, such that each watermark bit, wl ∈ W,

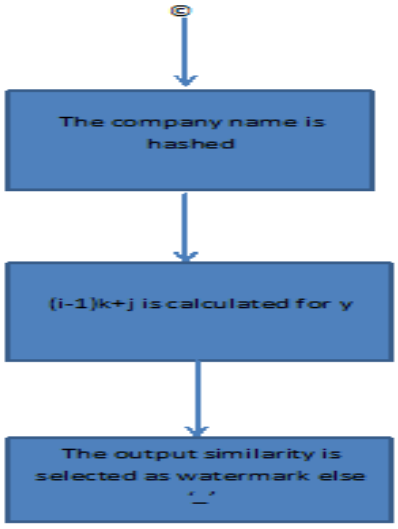


Fig. 3 Algorithm part-3

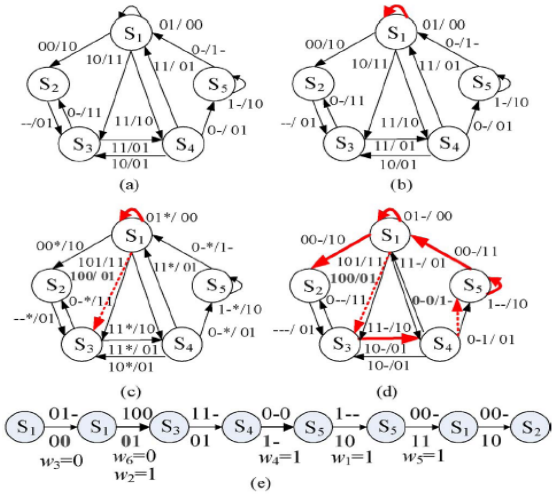


Fig. 4 Example for the Implementation

IV. IP PROTECTION CREDIBILITY

The credibility of the authorship proof can be evaluated by the probability that an unintended watermark is detected in a design [3]. Suppose that an arbitrary input sequence exits to excite N' (N'= N) consecutive transitions through the reachable states of a FSM with k output variables. The output sequence of length N (each output alphabet has k binary bits) will be one of 2k×N possible solutions. The odds that the output sequence contains the identical watermark. A longer watermark has a lower probability of coincidence. As m increases, more new transitions may have to be added. The beauty of our method is the input sequence length, N can increase to mitigate the overhead increment without compromising the authorship credibility. The false positive rate, which is the probability that the watermark is detected in the output sequence under a different random input sequence, can be estimated statistically.

Credibility Analysis:

The following conceivable attacks on watermarking of sequential circuit designs are analyzed with Alice as the IP owner and Bob as the attacker, who attempts to tamper an illegally acquired copy of Alice's watermarked IP.

1) Combinational Logic Re-Synthesis: Bob may use various logic optimization tools [2], [3] to re-synthesize the combinational logic of watermarked FSM. Such combinational logic re-synthesis operation maintains the inputs/outputs behaviors of flip-flops in the design and has no effect on the STG structure. Therefore, the watermark embedded on the STG is robust against attack by combinational logic re-synthesis.

2) Circuit Retiming: Bob may apply retiming transformation [2], [4] to move the latches across the combinational logic blocks of Alice's watermarked FSM without changing the design functionality. Retiming can change the STG structure. Such transformation can be divided into three cases for analysis: 1) splitting one state into two one-step equivalent states; 2) merging two one-step equivalent states into one state; and 3) switching between two states that are one-step equivalent. Two states si and sj are said to be one-step equivalent if and only if the two states have the same outputs and the same next state under the same input excitation. The consequence of splitting, merging or switching transformation on the outputs retrieved in the watermark detection process can be analyzed by the STG before and after retiming. As an example, let states s31 and s32 be two generic onestep equivalent states and the transitions (s1, s31, xt , yt) and (s31, s5, xt+1, yt+1) are traversed in the watermarking process as shown in Fig. 8. Upon retiming, states s31 and s32 are merged into state s3. When the sequence ˆX is applied onto the retimed FSM, transitions (s1, s3, xt , yt) and (s3, s5, xt+1, yt+1) are traversed, the same outputs as Alice's watermarked FSM are generated from these two steps. Similarly, splitting or switching operations on the watermarked FSM will not prevent the detection of Alice's watermark. Alice's watermark will not be

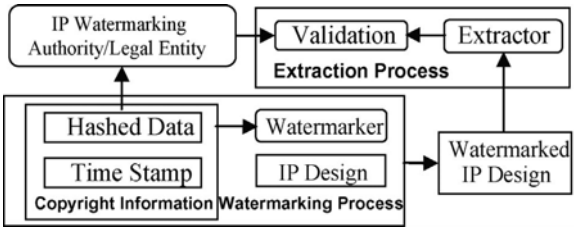
removed as a state can only be substituted by the state with the same behaviors in retiming transformation.

3) State Recoding (or Assignment): Bob may recode the states of Alice's watermarked FSM to remove her watermark. State assignment changes the mnemonic representations of states in Q. It has no effect on the functional specification of FSM [25].

As the watermark is embedded in the state transitions rather than the states, Alice's watermark will survive the state recoding attack.

4) Combinational and Sequential Redundancy Removal: When a redundant fault is identified in a sequential circuit, the part of logic can be deleted to simulate the effect of fault. Bob can remove the combinational logic that is not necessary for the correct circuit behavior.

This attack has a similar effect as the combinational resynthesis attack as far as the sequential behavior is concerned. So it will not affect the embedded watermark.



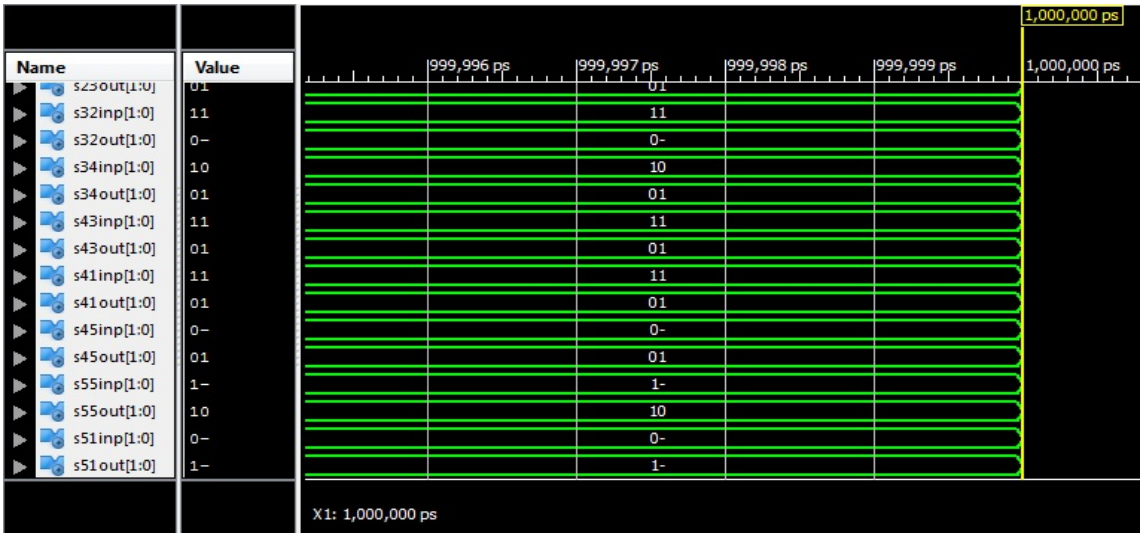


Fig. 5 Watermarking with third party keeping a time-stamped signature.

V. RESULTS AND CONCLUSION

The Experimental Out put are shown in Fig. 6. Our experimental results show that the watermarking incurs acceptably low performance overhead sand possesses very low possibility of coincidence and false positive rate .Similar to other FSM watermarking schemes [2]–[4], 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 [3], making FSM water marking a key research focus for dynamic watermarking.

One recommendation to overcome such limitation is to augment it with combinational watermarking scheme [5] applied simultaneously or on different levels of design abstraction to realize hierarchical watermarking [9], [10]. The watermarked FSM can be fortified by a scan chain watermarking [7] to enable the authorship to be easily verified even after the protected IP has been packaged.

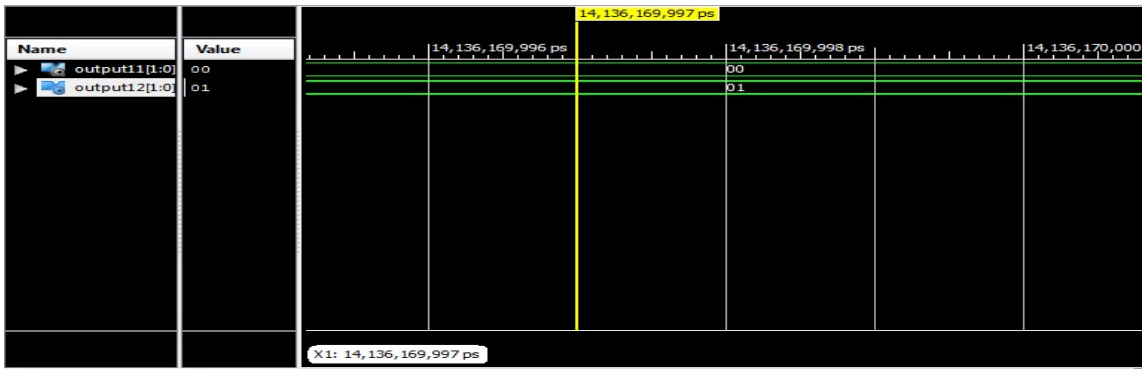


Fig.6 Simulation Results

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, "Stegosignature 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, AlternativesVSI 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.

AUTHORS PROFILE:

P. Nalini

P. Nalini is Pursuing M.Tech (Embedded systems) in Nalanda Institute of Engg. & Tech. She is Interested in Embedded Systems.

K. Sam Prasad

K. Sam Prasad is an Asst. Professor in Electronics & Communication Department in Nalanda Institute Of Engg. & Tech. He has 2 years Experience. He Got his M.Tech From Narasaraopeta Engg. College in 2010.

L.Srinivas

L.Srinivas is an assistant professor and Head of the ECE department in nalanda institute of engineering and technology. He got his M.Tech from Narasaraopet Engineering College in 2010.His Area of interest is communication field

◈◈◈