ISSN 2321-807X
Volume 12 Number20
Journal of Advances in chemistry

PERFORMANCE ANALYSIS OF WATERMARKING APPROACH FOR VLSI DESIGN INTELLECTUAL PROPERTY PROTECTION

Dr. M. MEENAKUMARI
Associate Professor, Department of ECE, SNS College of Engineering, Coimbatore
mnakumari@gmail.com

ABSTRACT

VLSI technology brought revolution in EDA industry. Fabrication of complicated system on a chip is possible by using reusable module called Intellectual Property **(**IP) core. IP cores that became an integral part of the electronic design industry influenced and had a rather significant and almost incomparable impact with respect to system designing in any chip. IP designs for any organization are imperative; contrary, IP designs that are shared can significantly cause high security risks. The majority of IP's require time as well as effort for purposes of designing and verification, however there still remains the possibility of these being copied or minor modifications to hide proof of ownership. To overcome this problem watermarking technique is recommended for IP Core protection. Watermark insertion in multilevel increases the security of the system. In this paper the ownership information is inserted in state transition outputs of State Transition Graph employing hierarchical representation of Finite state Machine (FSM) and subsequently in the netlist level by embedding watermark in the delay between the states. Watermark insertion at two levels increases the security of the design. Signature generation uses cryptographic algorithm for enhancing the security of the IP core designs. The experimental results show that performance is improved.

Indexing Terms/ Keywords

Intellectual Property, Watermarking, Finite state Machine, Advanced Encryption Standard, Message Digest, Signature generation.

1. INTRODUCTION

The process of sharing IP designs can raise many inherent security threats and risks and additionally conventional IP protection techniques consume a lot of time and sometimes costs make these unaffordable as stated in Cui and Chang [1]. In the year 2010, a German corporate security association show cased a report wherein huge amount was lost because of intellectual property theft Rajat and Swarup [2]. This kind of IP theft effects are twofold as firstly it caused a great revenue loss and simultaneously rewards the inventors or license owners that deliver goods and services on the basis of these, including jobs and work assignments that are associated with the losses. Hence IP design protection in VLSI is an area that is actively being researched in lieu of finding means and methods to safeguard IP.

The time to bring product into market is reduced due to IP core development considerably and resultantly products may be generated within specified duration of time. VLSI IP cores designer require assurance that their design will be protected and redistribution by illegal customer will be prevented. IP designs involve huge investment by companies; contrary though IP design sharing inherently poses high security risks. Watermarking has proven to be quite useful in this regards and a technique that provides protection against unauthorized IP core usage.

2. EXISTING METHODS

Oliveira [4] proposed the watermarking of sequential circuits. The fundamental nature of these approaches is to exploit unused input/output sequence or including new input/output sequences at the FSM representation of the design. This scheme has been proposed to implant watermarks in regular sequential functions by modifying the original function in a structured fashion. Watermarking of sequential parts of the design makes use of two different kinds which is used on adding new input/output sequences at the FSM representation as discussed by Torunoglu and Charbon [6]. The most important merit of both schemes is the capability of identifying the existence of the watermark even at all lower design levels.

Abdel-Hamid et al [7] proposed a method that uses the existing edges of the FSM and finds coinciding edges within the watermark that can be mapped into the original FSM. A new FSM watermarking scheme by making the authorship information a non-redundant property of the FSM was proposed by Cui et al [8]. . Hierarchical state machines are finite state machines whose states themselves can be other form of another state machine .Girault et al [5] introduced a state charts model which is the first techniques for hierarchal representation of FSM (HFSM). A single state x at one level of the

hierarchy is taken as present in one of the several states of y or z at lower level of hierarchy. The author discussed that FSM's can be concurrently combined. Hierarchical FSM can be embedded within a variety of concurrently model. The performance of the system is improved by combining FSM with concurrent models of computation

Abhishek et al [9] presented a methodology based on embedding ownership data as a segment of the IP design's FSM. Watermarking approach additionally added number of states in STG which makes its design complex. Once FSM enters into a watermarked state it will move into next watermarked state irrespective of the input. In the FSM watermarking method proposed by Arunkumar and Shangari [10]the digital watermark bits are seamlessly introduced into the outputs of the existing and free transitions of STG to overcome the vulnerability attack and minimize the design error. The design protection at HDL level was discussed in [3,13]. Jilang Zhang [11,12] discussed IP Protection using PUF. J.Kufel [14] proposed a method for watermarking soft IP .Carson[15] discussed an another method called fingerprinting technique. IP protection by state encoding is proposed by Edward Jung in [16,17].Dong fong [18] discussed a gate level design protection.

3. Hierarchical Representation of FSM

FSM is a mathematical model of computation used to design both computer program and sequential logic circuits .It is considered as an abstract machine with one of a finite number of states. The machine could be in only one state at a time which is called its current state. When initiated by a triggering event, the machine can change from one state to another which is called a transition.

Basic FSM have a large number of states and transitions which in turn makes the analysis tough. Hierarchical approach solves these problems. A state in Hierarchical FSM may be furthermore refined into another FSM. The outside FSM is called master and the inside FSM is called as slave. The state which does not have self loop is called atomic state. The state with self loop is called hierarchical state. The input sequence for the slave FSM is modeled to be a subset of input combination of its master FSM and also the output sequence for the slave FSM are a subset of the output signals from its master. For example, state S_2 depicted in Fig.1 is refined into another FSM but the state S_1 is not refined. Here a and b are input variables. The output variables are denoted by u and v. The master FSM consist of three states S_1, S_2, S_3.

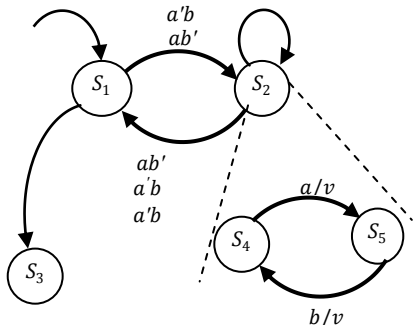

Fig.1. Hierarchical FSM

4. PROPOSED METHODOLOGY

The watermarking is one of the techniques used for protecting the IP core designs. Signature generation uses cryptographic algorithm for enhancing the security of the IP core designs.

4.1 Ordered Gate Level (OGL) Watermarking Approach

The proposed approach focuses on embedding IP designer data into versatile designs depicted in the form of state diagram. Hardware designs are generally formulated in a hierarchical manner wherein the main system model which is defined in one large block is represented in terms of sub blocks illustrated by smaller blocks and so on, until entire illustration of the system is completed. FSMs are nested inside other modules. The response of hierarchical FSM is defined as follows: if the current state is not refined, the hierarchical FSM just acts as a fundamental FSM: If the current state is refined then the corresponding slave FSM responds and then the master FSM reacts. Thus, two transitions are activated and two actions are performed. Slave FSM generally have one entry point and one or more exist points.

4.2 Signature Generation

AES and MD5 encryption algorithms are used for the generation of signature. The string which denotes the IP core developer is encrypted using 128 bit AES algorithm. Then, the encrypted output is given as input to MD5 hash generation block to afford high data integrity. MD5 validates data integrity via the generation of a 128 bit message digest from data

input. The bits generated from MD5 are called as signature. The required 8/16/32/64 bit signature are generated from 128 bits output of MD5 using digital logic box (DLB) as depicted in the Fig.2.

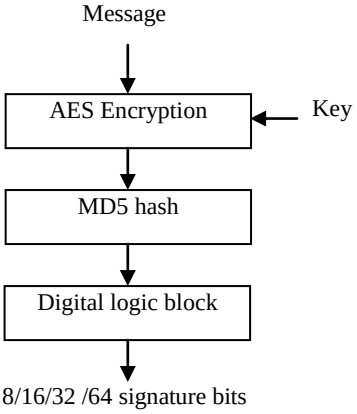

Fig.2.Generation of 8/16/32/64 bit signature bits

4.3 Watermark Insertion

The watermark insertion technique uses the existing and unused transitions in the FSM are used to insert the watermark information. For a completely specified FSM, extra input/output bits can be integrated to embed the data. In complex sequential designs, a number of such small FSMs exists which can be used to watermark the complete design by watermarking the entire or a selected subset of these FSMs. Original transitions can be exploited or additionally generated transitions can be used to hide the watermark. The algorithm of the proposed watermarking approach is given below. Let W denotes the watermarking bit and Y represents the output bits.

Step 1: Initiate any randomly chosen state S_i, $S_i \in S_A$ where S_i is current state and S_A is atomic state

Step 2: If the single transition output matches with watermarking bits is found i.e.,

W=Y

The next state is S_j

Step 3: If the output of more than one transition matching with watermarking bits are found, then a transition from S_i to the next state with maximum number of free input combinations, will be chosen as t_i which is the transition from source state S_i, to destination state S_j

Step 4: If the signature sequence is not equivalent to any of the outputs i.e $W \neq Y$, then the inputs of S_i will be checked to detect if there is any free input that can be exploited to add an extra transition. Choose next state S_i from the set of next state with the highest number of free input combinations. A new input/output pair, $X_i/O(t_i)$,is added for the transition t_i. Else, a new edge directed from S_i to S_{i+1}labeled with $X_i/O(t_i)$,will be generated in STG(M) for t_i and $O(t_i) = Y_i$

Step 5: If the state S_i is a hierarchical state, the entry point of the slave FSM is the newly reached state. The input and output bits fpr slave FSM are subset of input and output bits of hierarchical FSM which is determined in the following manner.

$\mathrm{m} = \text{number of inputs in original FSM}$

$\mathrm{n} = \text{number of outputs in original FSM}$

(i) For even number of input and even number of output bits, the subset of input consist of m/2 bits and subset of output consists of n/2 output bits.

(ii) For even number of input and odd number of output bits, subset of input consist of $m/2$ inputs bits and subset of output consisting of $\frac{n-1}{2}$ and $\frac{n+1}{2}$ bits.

(iii) For odd number of input and odd number of output bits, subset of input consist of $\frac{m-1}{2}$ and $\frac{m+1}{2}$ bits whereas the subset of output consisting of $\frac{n-1}{2}$ and $\frac{n+1}{2}$ bits.

(iv) For odd number of input and even number of output bits, subset of input consist of $\frac{m-1}{2}$ and $\frac{m+1}{2}$ bits whereas the subset of output consisting of $\frac{n}{2}$ bits.

Step 6: Compare the outputs transition of the newly reached slave state S_s to the generated watermark signature and check if they coincide i.e. W=Y. If the output transition t_i is equal to Watermark bits, then t_i will be considered part of the watermark sequence. The next state S_j will be determined based on the transition used. In this scenario, the newly reached state is either an exit point or just another state in the slave FSM.

Step 7: If they reached state is not an exit point of the slave HFSM, the master state will be made to reside in the same state through the self loop transition. Only a part of the output transition, the slave part, will be considered in the watermark insertion.

Step 8: If reached state is an exit point of the slave HFSM, the master state will be considered as an atomic state.

Step 9: The algorithm will loop until all the signature bits are embedded.

After the FSM is watermarked by above mentioned algorithm, the next level insertion continues. Watermark bit generated by Fig [2] are grouped by three bits and its decimal equivalent is calculated. Watermark insertion process at netlist level utilizes net time delays in the synthesized result. The large number of nets in the design provides sufficient room to embed long watermarks. In this method Non-critical nets are identified, and its delay T_d is compared with the watermark bit T_w.The threshold value of delay T_h is determined by the following formula

$$T_h = \left\lfloor \frac{T_{min} + T_{max}}{2} \right\rfloor \quad (1)$$

Where $T_{min} = 0$ and $T_{max} = 9$

Case 1: $if\ |T_d - T_w| \leq T_h$

If the absolute value of the difference between the delay's last digit and the watermark bit is less than the threshold, T_h then replace the delay's last digit with the watermark bit.

Case 2: $if\ |T_w - T_d| > T_h$

If the value of delay's last digit is greater than the watermark bit then replace the delay's last digit with delay's last digit minus watermark bit.

5. RESULTS AND DISCUSSION

The benchmark circuit is taken in .kiss2 format. In .kiss2 format i represent number of inputs, o represents number of outputs p represents number of product terms and s represents number of states. The sequential benchmark circuits are taken from IWLS'93 benchmark suite; MCNC and open cores are used. The circuits are analyzed for three different sizes of watermarks. The original benchmark circuits are shown in Table 1. Totally, 11 benchmark circuits are considered for the analysis. The proposed method is simulated using Modelsim SE 5.7g.

The overall performance of watermarking approach is analyzed by standard cell approach. The design is synthesized to the gate level using a 180 nm, 1.2 Volts, standard-cell CMOS technology using Cadence Encounter RTL Compiler. Cadence delivers innovative technologies from RTL to GDSII, while providing optimal performance, capacity, and quality of silicon for complex design closure, low power, mixed signal, advanced node, and signoff analysis. The RTL code is simulated through cadence nc-verilog simulator and functionally verified. Power consumed by proposed approach is shown in Fig 3. Fig.4 shows the time slack of proposed approach. It is clearly observed from the figure that power consumption by proposed method is very less and execution takes only less time.

Table 1. Details of original benchmark circuit

Bench mark Circuits	No of inputs (i)	No of outputs (o)	No of product terms (p)	No of states (s)
bbara	4	2	60	10
dk15	3	5	32	4
dk17	2	3	32	8
ex4	6	9	21	14
s27	4	1	34	6
s386	7	7	64	13
ex1	9	19	138	20
bbtas	2	2	24	6
lion	2	1	11	4
s1	8	6	107	20
s208	11	2	153	18

Table 2.Performance of the proposed method for different watermarks

Bench mark Circuits	No of cells occupied			Cell area (nm^2)		
	16 bits	32 bits	64 bits	16 bits	32 bits	64 bits
bbara	75	76	84	1324	1400	2252
dk15	60	69	97	1227	1341	2417
dk17	138	135	127	2588	2501	2438
ex4	75	94	115	1796	1989	2289
s27	36	37	36	699	699	699
s386	124	141	147	2458	2628	2714
ex1	296	312	316	5362	5375	5462
bbtas	59	65	76	1205	1263	1477
lion	19	19	20	372	376	378
s1	141	143	143	2795	2835	2835
s208	157	167	167	3112	3310	3310

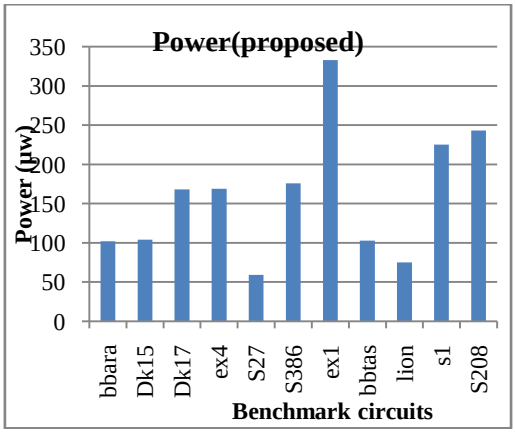

Fig.3. Power consumed by proposed approach for 64 bit watermark

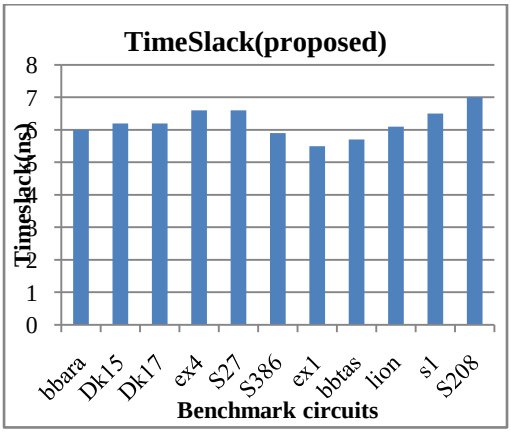

Fig.4. Time slack by proposed approach for 64 bit watermark

6. CONCLUSION

The proposed approach using watermark at two levels provides a high degree of protection and offers simple and not tending to spread undesirably copy detection and FSM is extremely flexible to all imaginable watermark removal attacks. The redundancy in the FSM has been efficiently used to reduce the embedding overhead. From the results it is observed that the proposed approach provides a robust solution for IP protection. The results sustain the objective of minimizing the impact of watermark insertion on the circuit performance and the area overhead.

REFERENCES

1. Cui, A, Chang CH and Tahar S. 2008. IP Watermarking Using Incremental Technology Mapping at Logic Synthesis Level. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol.27, no. 9, 1565-1570.
2. Rajat, SC and Swarup, B. 2011. Security Against Hardware Trojan Attacks Using Key-Based Design Obfuscation. Journal of Electronic Testing, vol.27, no.6, 767-785.
3. Encarnacion, C, Antonio, G, Luis, P and Antonio, L. 2007. IPP @ HDL: Efficient Intellectual Property Protection Scheme for IP Cores. IEEE Transaction on Very Large Scale Integration Systems, vol.15, no.5, 578-591.
4. Oliveira, AL. 1999. Robust techniques for watermarking sequential circuit designs. In Proceedings of the 36th annual ACM/IEEE Design Automation Conference, 837-842.
5. Girault, A, Lee, B and Lee EA. 1999. Hierarchical Finite State Machines with Multiple Concurrency Models. IEEE Transactions On Computer-Aided Design Of Integrated Circuits And Systems, vol. 18, no. 6, 742-760.

6. Torunoglu, I and Charbon, E. 2000. Watermarking-based copyright protection of sequential functions. IEEE Journal of Solid-State Circuits, vol.35, no.3,434-440.
7. Abdel-Hamid, AT, Tahar, S and Aboulhamid, EM. 2005. A public-key watermarking technique for IP designs. Design, Automation and Test in Europe, Proceedings, vol.1, 330- 335.
8. Cui, A, Chang, CH, Tahar, S and Abdel-Hamidm, AT.2011. A Robust FSM Watermarking Scheme for IP Protection of Sequential Circuit Design. IEEE Transactions on Computer-aided Design of Integrated Circuits and Systems, vol. 30, no. 5,.678-690
9. Abhishek, B, Debapriya, BR, Deep, B, Archan, S, Aniket, S, Tirtha, SD and Sarkar, SK 2011. FPGA Implementation of IP Protection through Visual Information Hiding. International Journal of Engineering Science and Technology (IJEST), vol. 3,no. 5,.4191-4199.
10. Arunkumar, P and Shangari, B. 2012. A New FSM Watermarking Method to Making Authorship Proof for Intellectual Property of Sequential Circuit Design Using STG. International Journal of Modern Engineering Research (IJMER), vol.2, no.6, 4159-4161.
11. Jiliang Zhang, Yaping Lin, Yongqiang Lyu, and Gang Qu. 2015.A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-Per-Device Licensing. IEEE Transactions on Information Forensics and Security, Vol. 10, No. 6, 1137-1150.
12. Jiliang Zhang, Qiang Wu, Yi-Peng Ding.2016.Techniques for Design and Implementation of an FPGA-Specific Physical Unclonable Function. Journal of Computer Science and Technology, Vol 31, No 1 . pp 124-136
13. E. Castillo, D. P. Morales, A. García, L. Parrilla, E. Todorovich, and U. Meyer-Baese.2015. Design Time Optimization for Hardware Watermarking Protection of HDL Designs.The Scientific World Journal. Article ID 752969.
14. J.Kufel,Sequence-Aware Watermark Design for Soft IP Embedded Processors.2015. IEEE Transactions on Very Large scale Integration. Volume 24 Issue 1 276-289.
15. Carson Dunbar and Gang Qu. 2015. Satisfiability Don't Care condition based circuit fingerprinting techniques. The 20th Asia and South Pacific Design Automation Conference 19-22 Jan. 2015 .815 – 820.
16. Edward Jung and Seonho Choi. 2015. Identification of IP Control Units by State Encoding. IEEE Computer Society Annual Symposium on VLSI 8-10 July 2015. 216 – 220.
17. Edward jung, Cedric marchand Lilian Bossuet.2015. Identification of embedded control units by state encoding and power consumption analysis. Proceedings of the 30th Annual ACM Symposium on Applied Computing.1957-1959.
18. Dongfang Li , Wenchao Liu , Xuecheng Zou and Zhenglin Liu.2015. Hardware IP Protection through Gate-Level Obfuscation. 14th International Conference on Computer-Aided Design and Computer Graphics (CAD/Graphics) 26-28 Aug. 2015 .186 – 193.

Dr.M.Meenakumari completed her B.E degree in Electronics & communication engineering from Madurai Kamaraj University, Madurai in 1989 and M.E Degree in Applied Electronics from Anna University,Chennai in 2004. She received her Ph.D. in Information and Communication Engineering from Anna University,Chennai in the year 2015. Currently she is working as Associate Professor at SNS college of Engineering, Coimbatore, Tamilnadu, India. Her research interests include,VLSI Design,Digital system design and IP core protection of VLSI circuits.She has more than 21 years of Teaching Experience.She has published 14 papers in reputed journals and 12 papers in conferences.She has received fund from ISRO for organizing seminar.