IMPROVING THE PROTECTION OF FPGA BASED SEQUENTIAL IP CORE DESIGNS USING HIERARCHICAL WATERMARKING TECHNIQUE

[1]M.MEENAKUMARI, [2]G.ATHISHA

[1]Assistant Professor (SG), Department of Electronics and Communication Engineering SNS College of Engineering, Coimbatore

[2]Professor, Department of Electronics and Communication Engineering, PSNA College of Engg & Technology, Dindigul

E-mail: [1]mnakumari@gmail.com, [2]gathisha@yahoo.com

ABSTRACT

In recent years, Intellectual Property (IP) cores in Very Large Scale Integration (VLSI) have become an active research area as it provides a new-fangled revolution in the Electronic Design Automation industry. An IP core is a previously designed and demonstrated component that can be integrated into design. Owing to the development of IP cores, time consumption becomes less and the product can be arrived in specified time. Designer of VLSI IP cores needs assurance that the design will not be illegally redistributed by consumers. IP core vendors are facing a major challenge to avoid revenue loss due to IP piracy. Watermarking is a well-known technique to protect an unauthorized use of IP core. Finite State Machine (FSM) is one of the representations of sequential digital designs. In this paper, a new dynamic hierarchical watermarking scheme is proposed. The watermark is embedded in the state transitions of FSM at the behavioural level. A watermark is embedded into FSM by hierarchically splitting original FSM into smaller FSMs. Experimental results on benchmark circuits shows that this hierarchical watermarking approach is an efficient method for protecting sequential IP cores.

Keywords: *Reuse, Intellectual Property, IP Core, FSM, Hierarchical Watermarking*

1. INTRODUCTION

Protection of Intellectual property cores plays an important role in several industries mainly due to recent attacks and threats to the original data. Sharing IP blocks faces high security risks. According to [1], a System-On-Chip (SoC) is defined as a complex IC that integrates the major functional elements of a complete end-product into a single chip. SRAM based FPGA technology is the most important issue in recent years because it can be reconfigured every time when FPGA is powered up. SRAM based FPGAs provides a significant solution for implementation of valuable designs as they can be reprogrammed. FPGA design could be easily stolen in seconds and it poses heavy revenue loss. Due to higher usage of FPGAs, there is a need to protect the core designs that run on FPGA as the data inside the FPGA is more susceptible to attackers until it is protected. Fig.1 shows techniques available in FPGA based VLSI design IP protection.

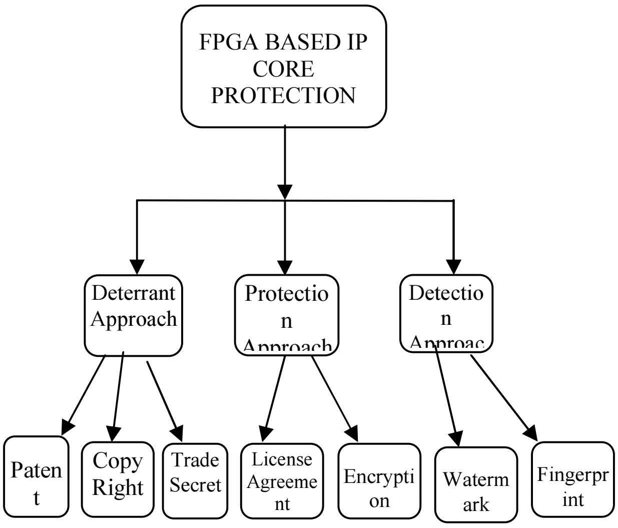

Figure 1: Types of IP Cores

Piracy problems can be categorized in to three classes i) Illegal Access- where the attacker obtains a product without authorization. ii) Tampering, where the attacker modifies a product in order to remove/ include features for malicious motives and then proceeds to its retransmission and iii) Copyright Violation, in which the attacker receives a product and resells it without getting the permission from the copyright owner. A third-party company may obtain an unlicensed copy of the protected IP core and use it in one of their products. Digital watermarking solves the issue of copying digital information. Fingerprinting technology assures the rights of both IP provider and IP users. Thus, four legally-defined categories of intellectual property are Patents, trademarks, copyrights, Trade secrets.

A.T. Abdel Hamid [2] discusses various attacks against IP core watermarking. FPGA based IP core protection survey is discussed in [3]. According to [4], the SoC design flow has three main IP cores as shown in Fig 2.

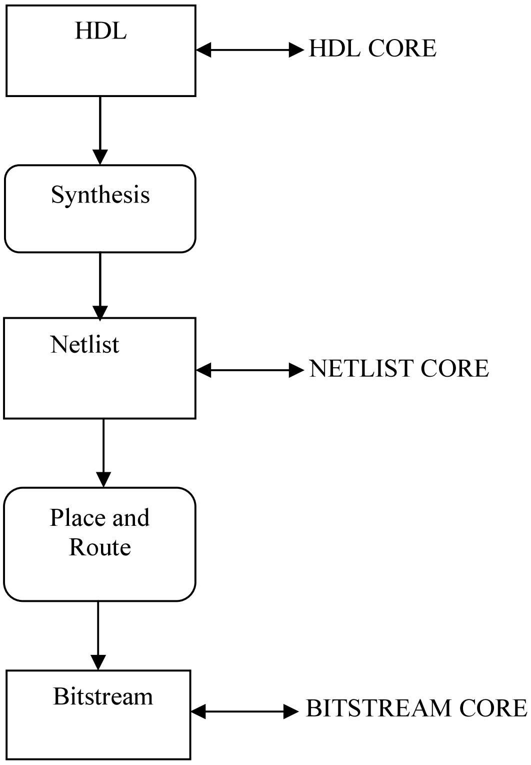

Figure 2: Types of IP Cores

1.1. Classification of IP Cores

IP cores are classified into three types which are given below.

Soft IP: They are delivered in the form of Hardware Description Language. They are more flexible and have increased Intellectual property risks because the RTL source code is required by the Integrator. It is also called as HDL core.

Firm IP: They are delivered in the form of the full or partial netlist. They do not include routing. They are more optimized in structure and topology for area and performance. It is also called as netlist core.

Hard IP: Hard IPs, delivered as GDSII files are optimized for power, size, or performance. From a security point of view, hard IP is the safest because they are hard to be reverse engineered or modified. It is also called as bitstream core.

1.2. Role of Cryptography in IP Protection

Cryptography plays an important role in generation of watermark bits which is to be inserted into state transition graph.VSI Alliance standards [5] describes standard cryptography techniques for the protection of data. The digital watermarking fundamentals and techniques are explained in [6]. Various encryption and authentication algorithms are explained by William Stallings in [7]. VLSI IP protection techniques are discussed by Gang Qu in [8]. Confidentiality, integrity and authentication are the important requirements for many cryptographic applications. Confidentiality is keeping information secret from all other who are unauthorized. Integrity is ensuring that the information has not been altered by unauthorized entities. Authentication is the assurance that the communicating party is the one that it claims to be.

In this paper, a new dynamic hierarchical watermarking scheme is proposed. The proposed approach is to be verified off chip by making it a part of the test kernel. The proposed watermarking scheme thus makes the authorship proof harder to erase and the IP authorship easier to verify.

2. RELATED WORKS

There are many watermarking techniques ıvailable for the protection of VLSI design IP cores ıt various design levels.

W.H. Mangione Smith et al. [9] proposed FPGA watermarking technique by using post processing constraints. The main theme of their approach is to encode the signature bits and embed them into the unused Look-Up Tables (LUTs) such as that they do not affect the original designs, and then reroute the design around these LUTs. The main limitation of this approach is that watermark is not embedded as a functional segment of the design. The watermark can be eliminated without affecting design functionality. Watermarked lookup tables do not reflect any functionality, thus they are susceptible to elimination if optimization algorithms are used. Gang Qu and Miodrag Potkanjak [10] investigated the effect of applying a watermark to the physical layout of a digital circuit when it is mapped into a FPGA.

Lin Yuan et al. [11] determined the delay on each net in the design and modified the delay by integrating necessary timing constraint on that net in user constraint file in ISE. This file is incorporated with the design during implementation and eventually it affects place and route result.

R.S. Chakraborty et al. [12] discussed a technique for hardware IP protection using netlist level obfuscation. This approach can be incorporated in the System-on-Chip design and manufacturing flow to simultaneously authenticate the design.

Ziener et al. [13] proposed a novel approach that can attain the aim of zero overhead without affecting the task and performance of design. In this method, details of effectively not utilized LUTs (ILUTs) details are from post layout of FPGA design flow. Pseudo random number sequence determines the location where encrypted watermarks need to be encrypted. Tingyuan Nie et al. [14] proposed an approach to effectively hide the watermark bits in unused LUTs. In order to increase robustness, watermarking bits are integrated in the bitstream file.

Dasko Kirovski et al. [15] developed two protocols for embedding tool specific information into a logic network while performing multilevel logic minimization and technology mapping. Copyright information is hashed using a cryptographically secure hash function to create a key used to seed a pseudorandom number generator. Pseudo random number generator is used to generate unique set of design constraints. By superimposing these constraints to original network, new input is generated. It proves authorship of the design at levels of abstraction equal to lower than logic synthesis.

Aijiao Cui and C.H. Chang [16] suggested re-synthesis method for embedding the IP designer information into a distributed copy of master design. In [17] M.Schmid et al. modifies LUTs of netlist and converts functional LUTs in to shift registers or LUT- based RAMs to prevent deletion due to optimization. But overhead incurred is large.

Arvindo Olivera [18] introduced a technique for the watermarking of synchronous sequential circuits which determines the authorship of designs though digital watermark on the state transition graph of the circuit. In [19], an unused input/output symbol sequence is determined and it is used for watermark. This work can be performed by using an STG representation of the regular sequential function. After calculating the required input/output symbol sequence length that satisfies given uniqueness constraints, the user can generate sequences through selecting enough input/output symbols.

A.T. Abdel Hamid [20] proposed the first public-key IP watermarking scheme at the FSM level. Aijiao Cui et al. [21] presented a novel technique for watermarking IP designs based on the embedding of the ownership proof as part of the IP design’s FSM without increasing the number of states in STG. This technique utilizes coinciding as well as, un-used transitions in the state transition graph of the design. Encarnacion Castillo et al. [22] presented a technique to spread digital signature bits within memory structures or combinational logic that are part of the system at a high level description of the design. Wei Liang et al [23] discussed an approach to extract maximal delay set through state transformation and to add a watermark sequence to the maximal delay state set. Debapriya Basu Roy et al. [24] proposed an approach based on embedding ownership information as part of the IP design’s Finite State Machine. But this method increases number of states in STG.

The above discussed earlier methods show their advantages and disadvantages, to overcome the problems, a novel method called FSM is proposed here. The proposed method offers a high degree of tamper resistance and provides 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.

3. PROPOSED METHODOLOGY

The proposed approach is based on embedding IP designer information into multifaceted designs which is represented in the form of state diagram.

3.1. Materials Used

Finite state machines provide a powerful way to describe dynamic behavior of systems and components. A finite-state machine (FSM) or simply a state machine is a mathematical model of computation used to design sequential logic circuits. It is conceived as an abstract machine that can be in one of a finite number of states.

An FSM is a five-tuple [25]

$(Q, \sum , \Delta, \sigma, q_0)$

Where
Q Finite set of symbols denoting states
∑ Set of symbols denoting possible inputs
Δ Set of symbols denoting possible outputs
σ Transition function mapping $Q\times \sum$ to $Q\times \Delta$
q_0 Initial state

The finite state machine remains at one state at a time and it is called as current state. It can be transformed from one state to another when initiated by a triggering event or condition. This is called a transition. State diagrams are used to give an abstract illustration of the behavior of a system. This behavior is examined and represented in series of events that could occur in one or more possible states. State machine can be denoted in the form of mealy or Moore machine. In Mealy machine outputs are a function of inputs and current state. So, changes in input will be reflected in the output. In Moore machine outputs, are a function of current state only.

3.2. Hierarchical Method

Hardware designs are often designed in a Hierarchical way where the main system design is defined in one large block that is defined in terms of sub blocks described by smaller blocks and so on, until complete description of the system is completed. FSMs are nested inside other modules. Most practical systems have a very large number of states and transitions which is considered as a major limitation of the fundamental FSM. Representation and analysis becomes difficult in this case. Hierarchical approach solves these problems.

FSM equivalent to main system design and sub block of the design is defined as master FSM and slave FSM respectively. Input alphabet for the slave FSM is defined to be a subset of the input alphabet of the master FSM. Similarly the output signals from the slave FSM are a subset of the output signals from its master. Slave FSM react to the reaction of their master FSMs. The reaction of the hierarchical FSM [26, 27] is defined as follows: if the current state is not refined, the hierarchical FSM behaves just like a basic FSM: If the current state is refined then the equivalent slave FSM reacts and then the master FSM reacts. Therefore, two transitions are triggered and two actions are taken. Slave FSM generally have one entry point and one or more exist points. The example hierarchical FSM is shown in Fig 3.

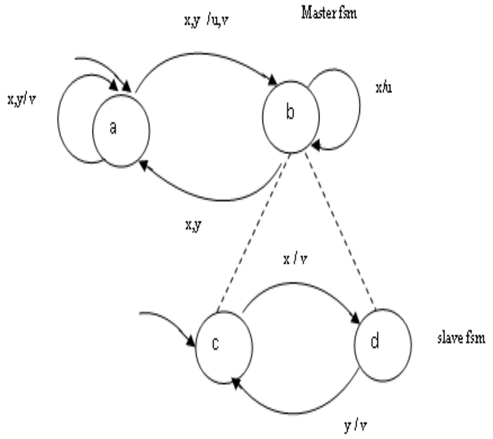

Figure 3: An Example Hierarchical FSM

3.2.1. Watermark Preparation

Before the FSM is being watermarked, a signature should be generated which identifies the owner of the core. The string is then encrypted using AES algorithm. In order to provide high data integrity, the encrypted output is given as input to MD5 hash generation block. It creates the hash output of the original message. MD5 is a widely used algorithm to verify data integrity through the creation of a 128 bit message digest from data input. The bits generated from MD5 are called as signature.

3.2.2. Watermark Insertion

The insertion approach in which existing and unused transitions in the FSM are used to insert the watermark information is described in this section. In case of completely specified FSM, extra input/output bits can be added to embed the information. In complex sequential designs, generally a number of such small FSMs exists which can be used to watermark the whole design by watermarking the entire or a selected subset of these FSMs. Original transitions can be utilized or additionally created transitions can be used to hide the watermark. Additional transitions are created based on satisfying constraints given in the algorithm. Let i be the number of inputs for the FSM and n be the number of flip flop states in FSM then there is a relationship between maximum number of transitions T and number of input i. T is calculated using the given formula

$$T=2^{i} *2^{n} \qquad (1)$$

The sequences of input and output bits in a FSM are represented by State Transition Graphs (STGs). The strength of the watermark increases because the attacker does not know the procedure to split the states.

The algorithm for insertion of watermarks in state transitions is given as:

1. Calculate the total states in STG.
2. Randomly select the initial state.
3. Check whether the state can be further refined or not.
4. If it is not atomic ie hierarchical state then there is a possibility of splitting the FSM into slave FSM.
5. Determine the entry and exit point for slave FSM.
6. Check whether both watermark bits and output bits coincide with each other. If it is not then check whether free inputs are available.
7. Add additional inputs to hide watermark. Increase in additional inputs adds automatically transitions also.
8. If the state is atomic then treat FSM as master FSM and check for output bits coincide.
9. Check the availability of free inputs. From the slave FSM create a transition to any of the discrete state in master FSM with no i/p dependence.
10. The algorithm will loop until all watermark bits are embedded.

4. ATTACK ANALYSIS

The proposed method is secure against removal attack and state encoding attack. As the watermark is embedded in the state transitions rather than the state's watermark will survive state encoding attack. The proposed watermarking method withstands logic resynthesis attack. If the protected IP is distributed at the gate level, attacker has to recover STG from the netlist which is computationally unfeasible for large designs. The existing and watermarked transitions are utilized for watermarking. Attacker may try to eliminate some transitions. There is no straightforward method to eliminate these transitions from the circuit netlist without modifying the correct behavior of FSM. The time and effort spent for this attack is large when compared with redesigning.

5. RESULTS AND DISCUSSION

In this research, a novel approach is proposed for watermarking sequential IP designs. The approach is based on the utilization of coinciding transitions as well as unused transitions in order to give higher robustness.

Table.1: Implementation Result of Benchmark Circuits

Benchmark Circuits	No of LUTS Occupied for Watermark			No of slices Occupied for Watermark			No of FFS Occupied for Watermark		
	16 bits	32 bits	64 bits	16 bits	32 bits	64 bits	16 bits	32 bits	64 bits
bbara	49	65	66	26	35	35	6	7	9
Dk15	41	47	42	22	25	25	7	8	8
Dk17	32	34	30	17	18	16	6	8	6
ex4	45	64	81	24	34	43	13	22	17
S27	36	36	36	19	19	19	7	7	7
S386	156	156	190	82	82	99	20	20	27

The structure of signature generation using Encryption and hashing function is simulated by Modelsim 6.0 SE and it is shown in Fig. 4. The six sequential benchmark circuits are taken from IWLS93 benchmark suite and it is synthesized by Xilinx ISE 9.1 software. .kiss2 file format of sequential benchmark circuit is watermarked. We have chosen XC 5003Se-5-FG20 family of FPGA for implementation. The circuits are analyzed for three different sizes of watermarks. The resource utilization details for 16 bit, 32 bit and 64 bit watermark bits are tabulated in Table I. The proposed algorithm was evaluated for different attacks.

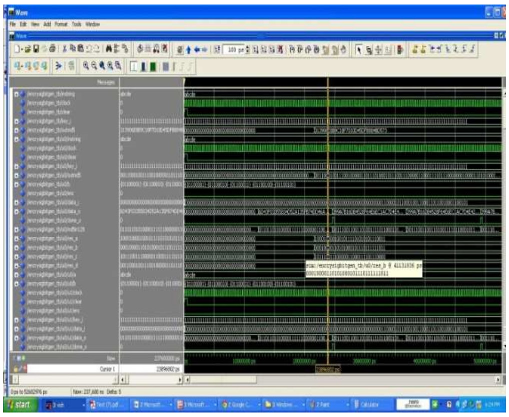

Figure 4: Simulation waveform of signature Generation

The simulation result of original sequential benchmark circuit S27 is shown in Fig.5. The resource utilization by implementation for 16 bit, 32 bit and 64 bit watermark bits are shown in Fig 6, Fig 7 and Fig 8 respectively.

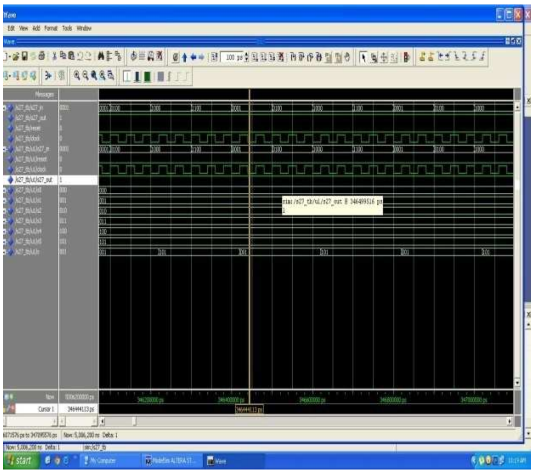

Figure 5:.Simulation result of S27 benchmark circuit

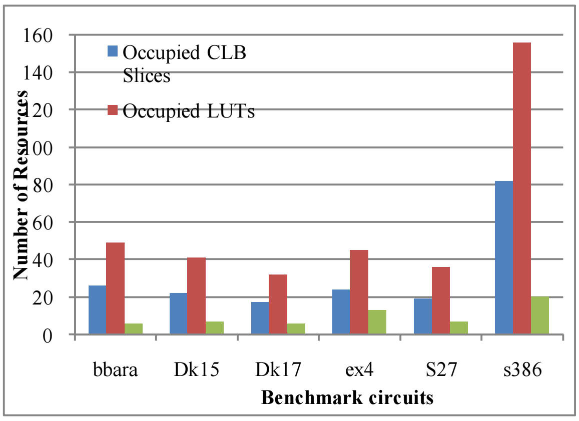

Figure 6: Comparison of Re source Utilization for 16 bit *Watermark*

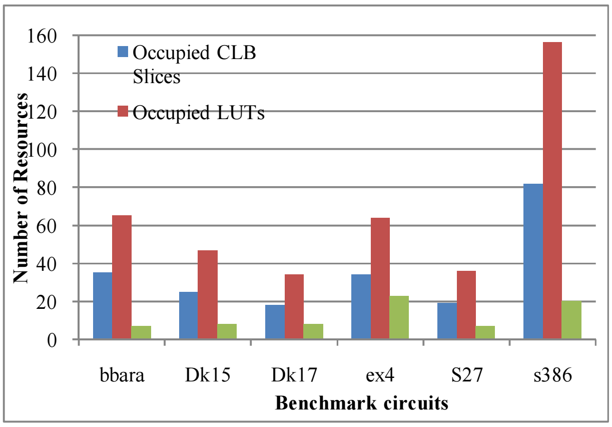

Figure 7: Comparison of Resource Utilization for 32 bit Watermark

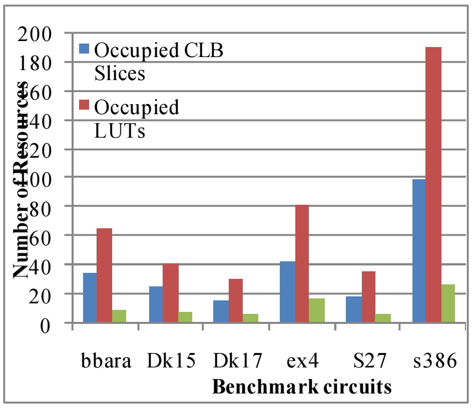

Figure 8: Comparison of Resource Utilization for 64 bit Watermark

6. CONCLUSION

A new robust dynamic watermarking scheme by embedding the authorship information on the transitions of STG at the behavioral synthesis level is proposed. This proposed approach provides a high degree of tamper resistance and offers simple and not tending to spread undesirably copy detection. The FSM watermark is extremely flexible to all imaginable watermark removal attacks. The redundancy in the FSM has been efficiently used to reduce the embedding overhead. The proposed approach can be used publically without the fear of canceling watermark.The experimental result shows that the proposed approach provides a robust solution for FPGA IP protection. This embedded information to protect the data is embedded as watermark. In furutre, beyond the copyright protection, Digital watermarking is having some other applications as fingerprinting, owner identification etc.

REFRENCES:

[1] H.Chang, L. Cooke, M. Hant and G. Martin, “Surviving the SOC revolutions: A Guide to Platform-Based design”, Kluwer Academic publishers, 1999.

[2] T.Abdel Hamid, Sofiene Tahar and El Mostapha Aboulhamid, “IP Watermarking Techniques Survey and Comparison“, *Proceedings of Third International Workshop for System-On- Chip for Real Time Applications,* 30 June-2 July, 2003, pp. 60 - 65.

[3] M.Meenakumari and G.Athisha,”A Survey on Protection of FPGA based IP Designs”, *International Journal of Advanced Electrical and Electronics Engineering*, Vol.2, Issue.2, March 2013, pp 93-99.

[4] Lin Yuan and Gang Qu, “VLSI Design IP Protection: Solutions, New Challenges Opportunities”, *Proceedings of the first NASA / ESA Conference on Adaptive Hardware's and Systems* (AHS ‘06), 2006, pp. 469-476.

[5] VSI Alliance, “Intellectual Property Protection White Paper: Schemes Alternatives and discussion Version “, *Intellectual Property Protection Development Working Group* ver. 1.1 Released.

[6] I.J.Cox, M.L. Miller and J.A. Bloom,. “Digital Watermarking”, Morgan Kaufmann publishers, 1998.

[7] William Stallings, “Cryptography and Network Security: Principles and Practices”, Third Edition, Pearson Education, 2003.

[8] Gang Qu, Miodrag Potkanjak, “Intellectual Property Protection in VLSI designs Theory and Practice”, Kluwer Academic publishers, 2003.

[9] John Lach and W.H. Mangionnationale Smith, ”Fingerprinting Techniques for FPGA Intellectual Property Protection”, *IEEE Transaction on Computer Aided Design of Integrated Circuits and System*, Vol. 20, No.10, October 2001, pp. 1253-1261.

[10] Gang Qu, Miodrag Potkanjak, “Fingerprinting IPs in Constraint Addition case study“, in *Proceedings 37th ACM/IEEE Design* Automation Conference,2000, pp.587-592.

[11] Adarsh K. Jain, Lin Yuan, “Zero overhead Watermarking Technique for FPGA Designs”, *13th IEEE/ACM Great Lake Symposium on VLSI, Washington*, USA, April 28-29,2003, pp. 147-152.

[13] Chakraborty R.S., S. Bhunia, “HARPOON: An Obfuscation based SOC design methodology For hardware Protection“, *IEEE Transaction on Computer Aided Design of Integrated Circuits and Systems*, Oct .2009, Vol .28, No.10, pp. 1493-1502.

[14] Schmid. M, Ziener. D, Teich. J, “Netlist –level IP Protection by Watermarking for LUT-based FPGAs“ in *Proceedings of IEEE International Conference on Field Programmable Technology* Taipei (Taiwan), 2008, pp. 209-216.

[15] Tingyuan Nie, Lijian Zhou and Yansheag Li,” Hierarchical Watermarking Method for FPGA IP Protection”, *IETE Technical Review*, Sep.2013, Vol.30, Issue. 5, pp 367-374.

[16] Dasko Kirovski, Yean- Yow Kwang, “Protecting Combinational Logic Synthesis Solutions”, *IEEE Transaction on Computer Aided Design of Integrated Circuits*, December 2006, Vol. 20, No. 9 pp. 2687-2696.

[17] Aijiao Cui and C.H. Chang, “Stego-Signature at Logic Synthesis Level for digital design IP Protection“, *in proceedings of IEEE Intenational Symposium on Circuits and Systems,* 2006, pp. 4611-4614.

[18] Moiz khan M. and Spyros Tragoudas, ”Rewiring for Watermarking Digital Circuit Netlists “, *IEEE Transaction on Computer Aided Design of Integrated Circuits and Systems*, July.2005,Vol.24, No.7, pp. 1132-1137.

[19] Arvindo Olivera, "Techniques for the Creation of Digital Watermarks in Sequential Circuit Designs", *IEEE Transaction on Computer Aided Design of Integrated Circuits Systems*, Sep. 2001Vol .25, No .12, pp. 661-686.

[20] I.Torino and E. Charbon," Watermarking based Copyright Protection of Sequential Functions" *IEEE Journal of Solid State Circuits*, February 2000,Vol 35, No.3, pp.434-440.

[21] Abdel Hamid A.T., S. Tahar, EL.M. Aboulhamid, "A Public Key Watermarking Technique of IP Designs" *, in proceedings of Design Test and Automation in Europe (DATE '05*), 2005, p.330-335.

[22] Aijiao Cui, Chip-Hong Chang, Sofiene Tahar and Amr.T. Abdel-Hamid"A Robust FSM Watermarking Scheme for IP Protection in Sequential Circuit Designs", *IEEE Transaction on Computer Aided Design of Integrated Circuits and Systems*, May. 2011Vol.30, No..5, pp. 678- 690.

[23] Encarnacion Castillo, Antonio Garcia, Luis Parrilla and Antonio Lioris "IPP @ HDL: Efficient Intellectual Property Protection Scheme for IP Cores", *IEEE Transaction on Very Large Scale Integration Systems,* May. 2007,Vol .15, No.5, pp. 578-591.

[24] Wei Liang, Xignug Sun, Zhiquang Rian and Jing Long"The Design and FPGA Implementation of FSM based Intellectual property watermark at Behavioral level, *Information Technology Journal*, 2011, Vol.10, No.4, pp. 870-876.

[25] Abishek Basu, Debapriya Basu Roy and S.K. Sarkar, "FPGA Implementation of IP Protection through Visual Information Hiding", International *Journal of Engineering Science and Technology*, May .2011,Vol.3, No.5 pp. 4191-4199.

[26] J.Hopecropt and J. Ullman , Introduction to Automata Theory, Languages, and Computation, Reading, MA:Addision-Wesley,1979.

[27] Alian Girault, Bilung Lee and Edward A.Lee " Hierarchical Finite state Machine with multiple concurrency models" , *IEEE Transaction on Computer Aided Design of Integrated Circuits and systems* June.1999, Vol. 18, No. 6 pp 742-760.