http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (4): 870-876, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.870.876

The Design and FPGA Implementation of FSM-based Intellectual Property Watermark Algorithm at Behavioral Level

[1,2]Wei Liang, [1]Xingming Sun, [1]Zhiqiang Ruan and [2]Jing Long
[1]Hunan Provincial Key Laboratory of Network and Information Security,
Hunan University, Changsha, 410082, China
[2]School of Computer Science and Engineering, Hunan University of Science and Technology,
Xiangtan, 411201, China

Abstract: A Finite State Machine (FSM)-based Intellectual Property (IP) watermark algorithm at behavioral level is presented for the protection of IP reuse techniques in Very Large Scale Integration (VLSI). The proposed algorithm extracts the maximal delay state set through state transformation relations among circuit signals. The watermark is mapped into additional delay constraint sequence by constraint generator, and the value in the sequence is added into the maximal delay state set in the circuit for embedding watermark. The algorithm is tested on Virtex XCV600-6bg432 Field-Programmable Gate Array (FPGA), the experimental results show that the algorithms has lower impact on logical function, ensures better security and lower (resource) overhead in comparison with other methods.

Key words: Intellectual property reuse, finite state machine, IP watermark, delay state set, field-programmable gate array

INTRODUCTION

With the rapid development of deep sub-micron integrated circuit systems, SoC (System on Chip) has become the mainstream in IC (Integrated Circuit) design (Kamran *et al*., 2006; Zerigui *et al*., 2008). IP reuse has been widely used by more semiconductor companies, which is essential to shorten design time and reduce product risk (Martin and Chang, 2003). The problem of effective IP protection has been widely concerned.

Recently, digital watermarking has evolved as a mature technology to protect the copyright of multimedia content, such as text, image and video (Qureshi and Tao, 2006; Fiaidhi and Mohammed, 2003). The problem of IP protection has been addressed at all levels of VLSI design. Early in the 1990s (Lach *et al*., 1998, 1999, 2001) first proposed the concept of FPGA-based watermarking and conducted lots of studies on this field. The signature of IP owner is encrypted and then embedded into unused LUT(Look-up Table) of FPGA design. The watermarked LUTs will be incorporated into the design with some "don't care" interconnects. Kahng *et al*. (2001) presented a solution to satisfiability problem involved in IP design. It encodes an author's signature into an optimization problem and generates a unique watermarked design by limiting the overall solutions space to a certain area reflecting the given signature. Castillo *et al*. (2006, 2007) presented a method for embedding watermark at HDL (hardware description language) level. The authors propose to use the content of lookup table in an FPGA and embed watermark in unused LUTs or between used LUTs. The watermark extracting circuit results in an increasing hardware overhead. Once the watermark extracting circuit detects specific input sequence, it will route to the store address of watermark and then outputs the contents. In the constrained watermarking scheme proposed by Qu (2002), the watermark is divided into two parts: public and private. The public watermark can be detected in public and the third party is responsible for IP identification, while several authorised users to solve the difficulties in IP detection and authorisation can only detect private watermark. Jain *et al*. (2003) presented a zero overhead FPGA watermarking scheme by modifying time constraints of the nets for watermark embedding. Moreover, Fingerprinting techniques have emerged for IP protection Caldwell *et al*. (2004). The fingerprints of different users are inserted into the target circuits respectively. The proposed method can effectively ensure IP protection and easily track infringement, but increasing the power overhead and path delay.

Most constraint-based water marking scheme have been proposed at physical design level (Ni and Gao, 2004; Saha and Sur-Kolay, 2007; Saha *et al*., 2007; Nie *et al*., 2005; Newbould *et al*., 2002), while less at structural level

Corresponding Author: Xingming Sun, School of Computer and Communication, Hunan University, Changsha, 410082, China
Tel: 86-731-8821341 Fax: 86-731-8821780

and behavioral level (Cui *et al*., 2008; Yuan and Qu, 2004). By using these methods, unauthorized users are hard to detect, remove or modify the watermark, thus the security of watermark is high. However, the performance in terms of traceability, power and circuit delay may be partly affected.

A FSM -based watermarking algorithm at behavioral level is proposed for IP protection. Finite state machine is introduced in the algorithm. The maximal delay state set can be extracted with state transformation relations among circuit signals. The constraint generator maps the watermark into a set of additional time constraints. The constraints are inserted into the maximal delay state set to obtain a unique watermarked design. The proposed scheme introduces lower resource overhead and has higher security in IP protection by comparing with other constraint-based watermarking methods.

PROBLEM DESCRIPTION AND DEFINITIONS

Finite state machine theory is introduced to improve the performance of IP watermark in terms of traceability, power and circuit delay. This section will firstly give the relevant definitions and then create a new watermarking mathematic model based on state transformation relations.

Definition 1: A Mealy type FSM is a six tuple $M=(\sum, \Omega, S, s_0, \theta, \lambda)$, where $\sum \neq \phi$ is a set of input symbols, $\Omega \neq 0$ is a set of output symbols, $S \neq \phi$ denotes a set of all states, $s_0 \in S$ represents the initial state, $\theta(s,a):S\times\sum \rightarrow S$ is the transition function and $\lambda(s,a):S\times\sum \rightarrow \Omega$ is the output function.

Definition 2: After applying a sequence $\alpha = (a_1,...,a_k)$ to state s, the output denoted by $\lambda(s,a)$ represents the output of FSM after the input sequence of $(a_1,...,a_k)$ applied to state s. The output can be defined as:

$$\lambda(s,a) = \lambda(\theta(\theta(...\theta(s,a_1)...),a_{k-1}),a_k \quad (1)$$

Definition 3: The destination state $\theta(s,a)$ of a sequence $\alpha = (a_1,...,a_k)$ represents the reachable state of FSM after the input sequence $(a_1,...,a_k$ applied to state s. The state is defined to be:

$$\theta(s,a)=\theta(\theta(...\theta(\theta(s,a_1),a_2)...),a_k) \quad (2)$$

Theorem 1: Given the set of current state variables $U=\{u^1,...,u^m\}$, a set of primary inputs $X=\{x^1,...,x^n\}$ and a set of next state delay variables $T=\{t^1,...,t^m\}$, we define the delay relation is:

$$\Psi(U,X,T)=\prod_{i=1}^{i=m}(t^i \equiv \theta^i(U,X)) \quad (3)$$

Proof: The equation $\Psi(U, X, T) = 1$ represents the sets of triples U, X, T, where each triple is a transition in state transition graph. Given the transition relation of a Mealy type FSM $M = (\sum,\Omega,S,s_0,\theta,\lambda)$, definition 2 and the delay state sequence in definition 3, we derive the expressions of delay state relation:

$$\Psi(U,X,T)=\prod_{i=1}^{i=m}(t^i \equiv \theta^i(U,X)) \quad (4)$$

This delay state relation is a significant characteristic of the FSM and can be widely used in the analysis of attacks to the method. Finally, by computing the set of delay states R(S), it is possible to embed the constraints into the delay state.

FPGA-BASED IP WATERMARKING

Principle of embedding watermark: During the overall design and development of IP circuit, we compute the values of all state transitions by using the delay state relation in theorem 1 and create a set of delay states R(S). By setting an appropriate threshold T_N, it is possible to select some specific delay value represented as the watermarked set of delay states. The signature of the design, such as company name, designer, is transformed as the watermark through encoding, encryption and hashing. Finally the watermark is inserted into the original design. Figure 1 shows the STG of the original design, $M = (\sum,\Omega,S.s_0,\theta,\lambda)$, where $\sum$ denotes the set of input symbols Ω the set of output symbols, $S = \{s_0,s_1,...,s_6\}$ the set of all the states s_0 the initial state, $\theta(s,a):S\times\sum \rightarrow S$ the state transition function and $\lambda(s,a):S\times\sum \rightarrow \Omega$ is the output function. Starting with initial state S_0, we traverse state set $S_0,S_1,...,S_m$ with input sequence $a_1,...,a_m$. By computing the set of all state transition edges and set of state delay with Watermark Embedding, it is possible to obtain the set of state delay information in STG, which meets all of the general conditions. Finally, we select the set of state delay met specific conditions for embedding watermark.

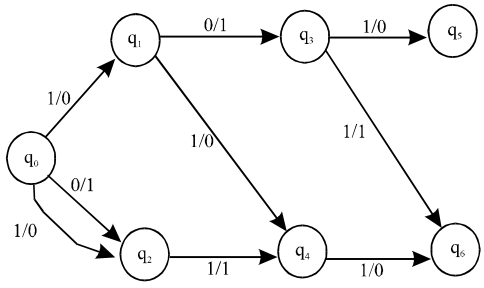

Fig. 1: The STG of original design

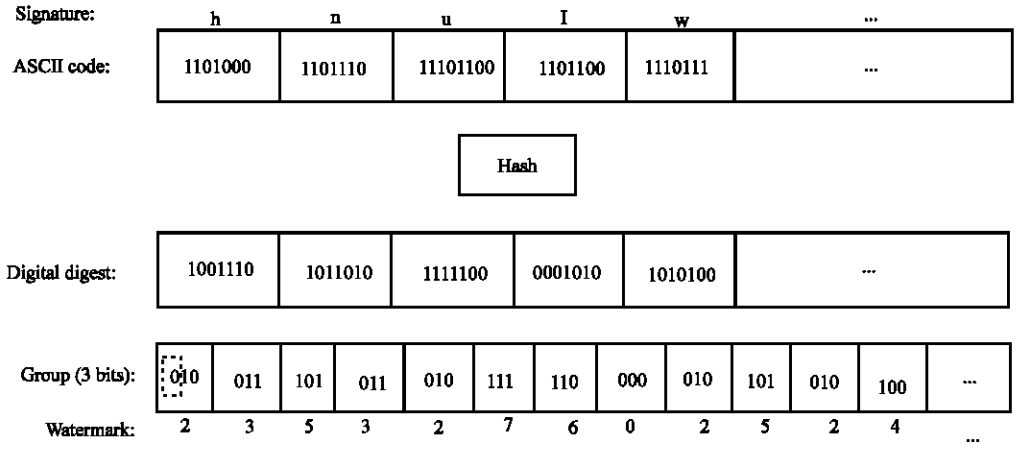

Fig. 2: The generation of watermark

Watermark generation: Since only the binary signals can be traced in IP circuit design, the signature should be preprocessed before embedding. To enhance the security of the method, the signature such as company name, trademark is encoded into ASCII (America Standard Code for Information Interchange) codes. These codes are orderly linked into a binary string. By using hash function, the binary string is scrambled, after that we group the scrambled string with 3 bits (with left zero padding to ensure the length of the string is divisible by 3 if necessary). Finally, each group of 3 bits is transformed into decimal value 0-7. Suppose the signature is "hnulw..." Figure 2 shows the generation of the watermark, where the 0 within the dotted rectangle denotes zero padding.

Watermark embedding: For the proposed algorithm, the watermark is inserted by the modification of state delay information in STG. With the watermark generated in (B.W atermark Generation), we perform the following steps to embed watermark.

Input: The watermark Wand the IP core
Output: IP core with watermark

- **Step 1:** Traverse each state $s_i \in S$ in STG with a sequence of inputs $a_1,...,a_m$ and obtain the set of all state transitions, denoted by $\Gamma=\{1<i,j<m \mid s_i \neg s_j\}$;
- **Step 2:** For each state transition in Γ, compute the delay of each state transition with the state delay expression in theorem 1, thus obtain the set of delay states R(S);
- **Step 3:** Analyze all the state delay information in the set of delay states R(S), set an appropriate delay threshold T_N as criteria for selecting set of states $R_T(S)$ which is suitable for modification. The selection of the delay threshold T_N depends on type of the core;
- **Step 4:** Randomly select γ state delay values according to the length of watermark and create a set of delay states R_w to embed watermark;
- **Step 5:** Analyze all delay values in $R_w(S)$, replace the last number of each state delay value with corresponding watermark;
- **Step 6:** Generate the watermarked IP core

Watermark extraction: When the IP core is suspicious to be misappropriation, the author could apply to the third party for the verification of watermark by the following steps.

Input: The watermarked IP core
Output: Digest of watermark W

- **Step 1:** Extract and analyze the STG of the watermarked IP core
- **Step 2:** traverse each state $s_i \in S$ in STG with a sequence of inputs $a_1,...,a_m$ and obtain the set of all state transitions, denoted by $\Gamma'=\{1<i,j<m \mid s_i \neg s_j\}$;
- **Step 3:** Obtain the set of delay states R(S)' after the circuit being placed and then analyses the STG after watermark
- **Step 4:** Determine γ watermarked state delay information with the random rules used in watermark embedding
- **Step 5:** Analyze the γ watermarked state delay information, extract the last values and transform them into binary codes
- **Step 6:** Recombine the binary codes in Step 5, and generate the embedded digest

In the identification of IP misappropriation, we could extract the embedded digest following the above steps. With the comparison with the generated digest before embedding, the original copyright could be verified if consistent. Due to the one way hash function, the security of the watermark is greatly enhanced.

EXPERIMENTAL RESULTS AND ANALYSIS

Functional simulation: We have simulated the RSA core before and after watermark on Modelsim 6.2SE. The RSA core is described by VHDL and performed compiling, synthesis, place and route on ISE tool. Finally, we conduct the function verification by loading the generated bitfile into FPGA device.

Given the initial key, input ds, output data odata and clock clk, Fig. 3 shows the functional simulation results before and after watermark. The simulation waveforms of the original core are shown as Fig. 3 a and b is the simulation waveform after watermark. It is revealed that the embedded watermark has low impact on circuit function.

Resistance to attacks: Resistance to attacks refers to the ability that the inserted watermark can be extracted correctly under various unauthorized attacks. For the general watermarking methods, the attackers cannot obtain the original watermark through the delay state of the inserted watermark when embedding. However, the attackers would damage the delay states reflecting that the watermark by using the power attacks, while not affecting the functionality of the IP circuit. Here the resistance to power attack is principally analyzed.

In order to evaluate the resistance of the watermarking component to power attack and improve the robustness and security, the EDA tool Hspice is used to simulate the transient power when working and quantified its resistance during the design and implementation of the watermarking method. Assume, when embedding, that at each moment of state delay, the transient power is a random variable having a normal distribution. At this moment, the attackers only need to guess the key. With the plain text, cipher text and the guessed key, it is possible to compute the SNR (Signal to Noise Ratio) of power attack. Suppose that the cipher arithmetic unit and SNR of transient power have a normal distribution, the sample number is n, σ_1,σ_2 are respectively mean square deviation, ε denotes the mean attack deviation. As known from (Abdel-Hamid *et al*., 2006), the formula to compute SNR of power attack is defined as:

$$SNR = \frac{\varepsilon}{\sqrt{(\sigma_1^2 + \sigma_2^2)/n}} \quad (5)$$

Formula (5) indicates that as the sample number increasing, SNR of power attack gradually increases. Therefore, it is more possible for attackers to perform power attack successfully. We perform power attack to RSA core after place and route. Figure 4 shows the results of power attack (known as power deviation) with the sample number 2000. If the key guessed correctly, the power deviation can be distinctly observed. Therefore, it is easy to obtain the correct key.

Therefore, multithreading power simulation technique is used to quantify the resistance of watermarking

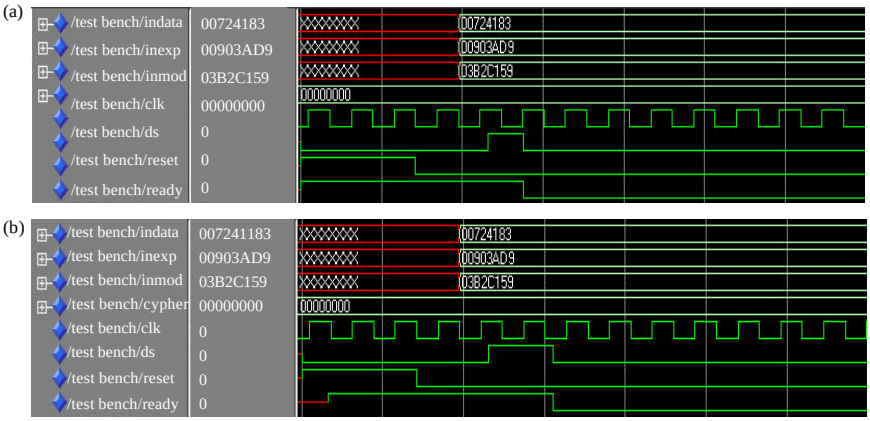

Fig. 3: Functional simulation waveforms before and after watermark. (a) The original vector function simulation waveforms and (b) Watermarked vector functional simulation waveforms

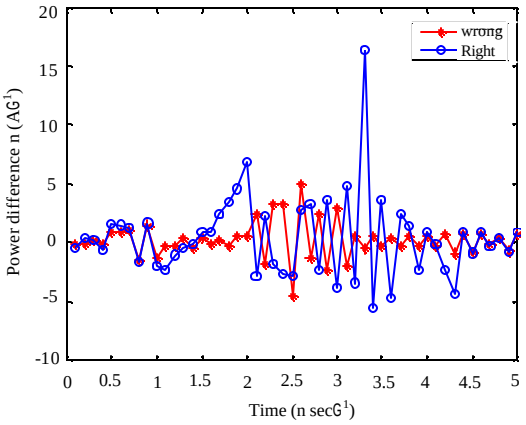

Fig. 4: Result of power analysis attacks after place-route

component to power attack. In this way, it has no interfere with the functionality and performance of original design, the resistance of the watermark position to power attack is enhanced as well.

EXPERIMENTAL RESULTS AND DISCUSSION

The proposed method has been tested on Xilinx VirtexII device XCV600 by watermarking three public cores with 128bits watermark: DES56 (Opencores.org, 2009a), ALU (Opencores.org., 2009b), RSA (Opencores.org, 2009c). The performances in the form of timing, SNR and resources are primarily verified. The test results are shown in Table 1.

Table 1 reveals that DES core utilizes the most CLBs, while ALU the least for the three cores. The core with the maximal delay is DES occupied the most resources, followed by RSA, ALU. By comparison with methods (Yuan and Qu, 2004; Abdel-Hamid *et al*., 2006), the proposed method is not the best in terms of timing performance. While the SNR and the occupied resource relative to original circuit are both lower. Therefore, the proposed method has lower impact on circuit function, better security and resource overhead.

Figure 5 shows the experimental results for RSA core. The physical layouts reveal that, the watermarked layout in Fig. 5b has higher density of occupied resource, but lower impact on circuit function in comparison with the original in Fig. 5a.

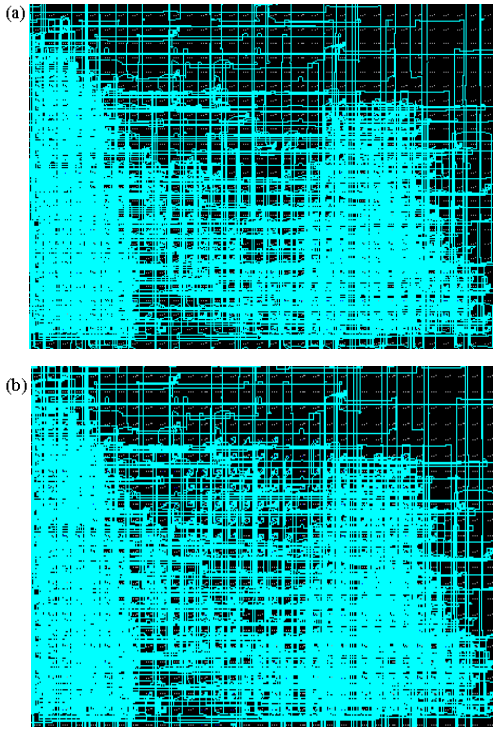

Fig. 5: Original DES design layout and the layout with 128 bitwatermark. (a) Original DES design layout and (b) DES design layout with 128 bitwatermark

Table 1: Performance comparison of different IP core physical layouts

Method	Core	Devices	Used CLBs (Slices)	Timing (nsec)	SNR	Resources (%)
Yuan and Qu (2004)	DES	XCV600	972	7.706	0.432	0.786
	RSA	XCV600	668	9.103	0.503	1.899
	ALU	XCV600	481	15.122	0.422	2.591
Abdel-Hamid *et al.* (2006)	DES	XCV600	958	8.416	0.716	0.558
	RSA	XCV600	683	9.706	0.706	2.793
	ALU	XCV600	485	16.231	0.231	2.883
Our method	DES	XCV600	947	7.802	0.602	0.367
	RSA	XCV600	656	9.901	0.491	1.707
	ALU	XCV600	479	17.998	0.368	2.165

CONCLUSION

A FSM-based IP watermark algorithm at behavioral level is presented for IP protection in reusable designs. The proposed algorithm extracts the maximal delay state set through state transformation relations among circuit signals. The optimal delay paths are selected in the set of delay states for watermarking. The watermark embedding and extraction are discussed. Meanwhile, we verify the circuit function before and after watermarking by Modelsim 6.2SE tool and the resistance of watermark to power attack by Hspice. Finally, the algorithm is tested on

Virtex XCV600-6bg432 FPGA, and the experimental results show that the algorithm has lower impact on logical function. Although the area overhead slightly increases, the traceability and security are better.

ACKNOWLEDGMENTS

This study is partially supported by National Basic Research Program of China (973 Program) under Grant No. 2009CB326202 (2009.4-2011.8, Hunan University) and 2010CB334706 (2010.4-2013.3, Hunan University). Key Program of National Natural Science Foundation of China under Grant No. 60736016 (2008.1-2011.12, Hunan University). National Natural Science Foundation of China under Grant No. 60873198 (2009.1-2011.12, Hunan University), 60973128 (2010.1-2012.12, Hunan University), 61070196 (2011.1-2013.12, Hunan University), 61073191 (2011.1-2013.12, Hunan First Normal University) and 60973113 (2010.1-2012.12, Hunan University). Scientific Research Fund of Hunan Provincial Education Department under Grant No. 09C403 (2009.6-2012.6, Hunan University of Science and Technology), National Natural Science Foundation of Hunan Province and Xiangtan united Foundation under Grant No. 09JJ9006 (2009.6-2012.6, Hunan University of Science and Technology), Key Program of Scientific Research Fund of Hunan Provincial Education Department under Grant No. 09A027 (2009.6-2012.6, Hunan University of Science and Technology).

REFERENCES

Abdel-Hamid, A.T., S. Tahar and E.M. Aboulhamid, 2006. Finite state machine IP watermarking : A tutorial. Proceedings of the 1st NASA/ESA Conference on Adaptive Hardware and Systems (AHS), June 15-18, Istanbul, pp: 457-464.

Caldwell, A.E., H. Choi, A.B. Kahng, S. Mantik, M. Potkonjak, G. Qu and J.L. Wong, 2004. Effective iterative techniques for fingerprinting design IP. IEEE Trans. Comput. Aided Design Integ. Circuits Syst., 23: 208-215.

Castillo, E., L. Parrilla, A. Garcia, A. Loris and U. Meyer-Baese, 2006. IPP watermarking technique for IP core protection on FPL devices. Proceedings of International Conference on Field Programmable Logic and Applications, FPL' 06, Madrid, pp: 487-492.

Castillo, E., U. Meyer-Baese, A. Garcia, L. Parrilla and A. Lloris, 2007. IPP@HDL: Efficient intellectual property protection scheme for IP cores. IEEE Trans. Very Large Scale Integration (VLSI) Syst., 15: 578-591.

Cui, A., C.H. Chang and S. Tahar, 2008. IP watermarking using incremental technology mapping at logic synthesis level. IEEE Trans. Comput. Aided Design Integ. Circuits Syst., 27: 1565-1570.

Fiaidhi, J.A.W. and S.M.A. Mohammed, 2003. Towards developing watermarking standards for collaborative e-learning systems. Inform. Technol. J., 2: 30-34.

Jain, A.K., L. Yuan, P.R. Pari and G. Qu, 2003. Zero overhead watermarking technique for FPGA designs. Proceedings of the 13th ACM Great Lakes Symposium on VLSI, April 28-29, Washington, DC, USA., pp: 147-152.

Kahng, A.B., J. Lach , W.H. Mangione -Smith , S. Mantik and I.L. Markov *et al*., 2001. Constraint-based watermarking techniques for design IP protection. IEEE Trans. Comput. Aided Design Integrated Circuits Syst., 20: 1236-1252.

Kamran, M., S. Feng and S. Qureshi, 2006. Serial ALU simulation with timing and signal constraints. Inform. Technol. J., 5: 198-203.

Lach, J., W.H. Mangione-Smith and M. Potkonjak, 1998. Signature hiding techniques for FPGA intellectual property protection. Proceedings of the IEEE/ACM International Conference on Computer-Aided Design, Nov. 8-12, San Jose, California, USA., pp: 186-189.

Lach, J., W.H. Mangione-Smith and M. Potkonjak, 1999. Robust FPGA intellectual property protection through multiple small watermarks. Proceedings of the 36th ACM/IEEE Design Automation Conference, June 21-25, New Orleans, LA, USA., pp: 831-836.

Lach, J., W.H. Mangione-Smith and M. Potkonjak, 2001. Fingerprinting techniques for field-programmable gate array intellectual property protection. IEEE Trans. Comput. Aided Design Integrated Circuits Syst., 20: 1253-1261.

Martin, G. and H. Chang, 2003. Winning the SoC Revolution: Experiences in Real Design. Kluwer Academic Publishers, Massachusetts, USA..

Newbould, R.D., J.D. Carothers, J.J. Rodriquez and W.T. Holman, 2002. A hierarchy of physical design watermarking schemes for intellectual property protection of IC designs. IEEE Int. Symp. Circuits Syst., 4: 862-865.

Ni, M. and Z. Gao, 2004. Constraint-based watermarking technique for hard IP core protection in physical layout design level. 7th Int. Conf. Solid-state Integ. Circuit Technol. Proc., 2: 1360-1360.

Nie, T., T. Kisaka and M. Toyonaga, 2005. A post layout watermarking method for IP protection. Proceedings of International Symposium on Circuits and Systems (ISCAS), May 23-26, Kobe, pp: 6206-6209.

Opencores.org., 2009a. Basic DES crypto core: www.opencores.org/projects.cgi/web/basicdes.

Opencores.org., 2009b. Basic RSA encryption engine: popencores.org/projects.cgi/web/basicrsa.

Opencores.org., 2009c. HCSA adder and generic ALU based on HCSA: Downloads. opencores.org/project, hcsa_adder,overview.

Qu, G., 2002. Publicly detectable watermarking for intellectual property authentication in VLSI design. IEEE Trans. Comput. Aided Design Integ. Circuits Syst., 21: 1363-1368.

Qureshi, M.A. and R. Tao, 2006. A comprehensive analysis of digital watermarking. Inform. Technol. J., 5: 471-475.

Saha, D. and S. Sur-Kolay, 2007. Fast robust intellectual property protection for VLSI physical design. Proceedings of 10th International Conference on Information Technology, Dec. 17-20, Orissa, India, pp: 1-6.

Saha, D., P. Dasgupta, S. Sur -Kolay and S. Sen-Sarma, 2007. A novel scheme for encoding and watermark embedding in VLSI physical design for IP protection. Proceedings of the International Conference on Computing: Theory and Applications, March 5-7, Kolkata, pp: 111-116.

Yuan, L. and G. Qu, 2004. Information hiding in finite state machine. Proceedings of the 6th International Workshop on Information Hiding, May 23-25, Toronto, Canada, pp: 340-354.

Zerigui, A., X. Wu and Z.Q. Deng, 2008. Communication of mobile rover based on FPGA, DSP and wireless communication. Inform. Technol. J., 7: 374-377.