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 12 (12): 2324-2332, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.2324.2332

A Survey of Techniques for VLSI IP Protection

[1,2]Wei Liang, [1]Dafang Zhang, [1]Zhiqiang You, [1]Wenwei Li and [3]Osama Hosam
[1]School of Information Science and Engineering, Hunan University, Changsha 410082, China
[2]School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China
[3]City for Scientific Research and Technology Applications, IRI, Alexandria, Egypt

Abstract: In order to reduce IP (Intellectual Property) infringements in VLSI (Very Large Scale Integration), many IP protection methods have been proposed. These methods have involved knowledge in fields of microelectronics, information hiding and embedded system. As a new field, IP protection can greatly reduce ownership misappropriation but it is faced with numerous challenges. On the basis of existing fundamental theories and engineering technologies, IP protection has rapidly developed in recent years. This study introduced IP protection in terms of concepts, characteristics and architecture. The challenges of IP protection technologies were analyzed. This study focused on the latest research improvement of IP protection technologies. The difficulties of digital watermarks on overhead, security, amounts were stated concretely. Meanwhile, this study presented some research methods for reference, such as multiple IP watermarking technology, models for watermark embedding and optimal computation, IP blind forensics technology and methods for evaluating watermark performance.

Key words: IP watermark, multiple IP watermark, optimal computation, blind forensics

INTRODUCTION

In the development of integrated circuit industry, low power and high integration are still the focus of technological competition (Girard, 2002; McCluskey *et al*., 2003). With the improvement of integration, the Moore's law still meets the demands of integration technology as before. However, in SoC (System on Chip), the contradiction between design ability and technological level has become a prominent obstacle of SoC development. If it starts all over again, it will not doubt increase difficulties and complexity and even the time to go public cannot be guaranteed. In this case, an IP reuse technology has been presented for solving this problem. The technology is to use predesigned, implemented and verified integrated circuit modules in SoC design, which has greatly reduced design level, complexity and design cycle. Recently, IP reuse technology has become a mainstream in Very Large Scale Integration (VLSI) (Abdel-Hamid *et al*., 2005). Meanwhile, application of the technology can bring the risk of misappropriation, which will damage the interests of IP designers seriously.

The statistics of Intel cooperation show that misappropriation of integrated circuit IP core could reduce the cost of development more than 80% and shorten the development time by one and a half years. The loss to industry caused by IP misappropriation has reached to five billion dollars. The disputes over intellectual property have brought not only huge financial loss but also damage to international reputation of enterprise brand and cooperation with customers. Confronting with masses of IP copyright disputes, the protection of reused IP core has been widely concerned all over the world.

To facilitate the development of VLSI, it is essential to reduce copyright disputes and misappropriation. In this case, the study on IP protection technologies has significant impact on sound development of national integrated circuit.

DEFINITIONS AND CHARACTERISTICS OF IP WATERMARKING TECHNOLOGY

IP watermarking technology is developed as a novel technology by inserting secret information into IP circuits for ownership identification. The concept was derived from the safety standard cell library provided by Foundry. At present, IP watermarking technology is primarily to hide specific information into reused modules of integrated circuit. The research results of IP watermarking

Corresponding Author: Dafang Zhang, School of Information Science and Engineering, Hunan University, Changsha 410082, China Tel/Fax: 86-731-88821570

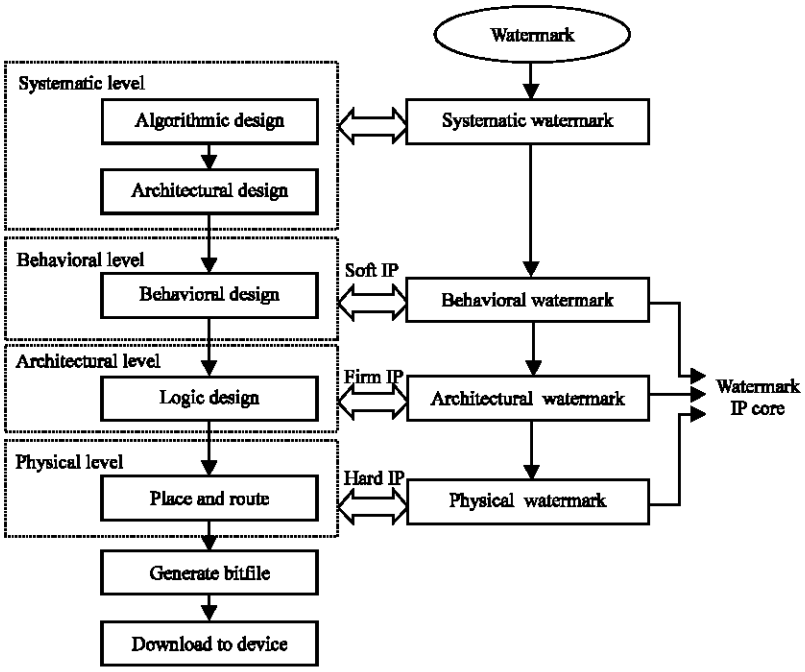

Fig. 1: Architecture of digital IP watermarking technology

technology can be applied in army, department of state secrets or company with core technology. As is shown in Fig. 1, IP watermarking technology is divided into four design levels. From high to low, they are systematic level, behavioral level, architectural level and physical level (Kahng *et al*., 2001; Lach *et al*., 1998). Accordingly, VSIA alliance classifies reused IP cores into three classes, respectively soft IP, firm IP and hard IP.

IP watermarking is different from multimedia watermarking since the user data cannot be altered. The features of IP watermarking are stated as follows:

- **Transparency:** It is a complicated task to design and verify IP cores. Since IP cores require strictly on correct functionality and precise timing, the watermark embedding of IP cores has no impact on functionality. Meanwhile, the invisibility of watermarks is necessary
- **Security:** The watermarks should be embedded into IP design in secret, protecting it from being found and removed by illegal users. In this case, resistance to attacks should be taken into account in design of IP watermarking algorithm
- **Reliability:** It is an important indicator for evaluating IP watermarking algorithm. Two aspects are included. One is robustness, which measures resistance of watermarks against illegal attacks and the number of undetected watermarks in IP design. The other one is false positive, which represents the probability of watermarks being found in a non-watermarked design
- **Watermark capacity:** The IP watermarking algorithm should insert enough ownership information for identifying copyright of IP design. The information will be extracted and considered as evidence in court. However, the size of embedded information should be small enough in order to reduce performance overhead. In this case, the watermark capacity is a contradiction, which needs a systematic consideration
- **Performance overhead:** The watermarking of IP design is one of the IP protection means, which will affect performance of IP design to some extent. Consequently, it is necessary to evaluate performances in terms of area (resource), timing, etc

CHALLENGES OF IP WATERMARKING TECHNOLOGY

At present, IP reuse technology has no universal and effective protection standard. The manufacturers of IP cores expect no misappropriation and illegal alteration on their products and less time and energy in maintenance and verification of IP cores as well. On the other hand, the customers hope IP cores they bought are creditable, which will improve the efficiency of SOC design and reduce design risks. The VSIA alliance brings great

Table 1: Performance comparison for several IP watermarking schemes

IP watermarking scheme	Watermarked level	Security	Transparency	Watermark capacity	Implemented overhead
Qu (2002)	Physical level	Medium	High	Medium	High
Saha and Sur-Kolay (2010)	Physical level	Low	High	Small	High
Kahng *et al.* (2006)	Physical level	Medium	High	Small	High
Kirovski *et al.* (2006)	Architectural level	Medium	High	Medium	Medium
Cui *et al.* (2008)	Behavioral level	Medium	High	Medium	Medium

convenience for IP manufacturers and SOC designers in IP protection and searching. However, IP design standards of these companies are various, which may cause the problems of long verification cycle, high failure rate and high cost. In this case, the research on reused IP protection technology cannot meet the demands for real-time protection and ownership verification in availability. Table 1 shows that present IP watermarking technologies are still confronted with three challenges:

- **Low security:** In majority of existing IP watermarking methods, watermark embedding always leaves trace of circuit alteration. The trace will be easily detected and found by users and related EDA tools. After suffering various conventional processing and hostile attacks, the embedded watermarks will be damaged or removed. In this case, the complete watermarks will be hard to extract for verification
- **Small watermark capacity:** As is known in Table 1, the majority of watermark embedding schemes will use large redundant structure for watermark embedding in order to exert no impact on performance. With restriction of watermark structure in existing IP watermarking methods, it is hard to improve watermark capacity in specific IP redundant structure
- **High performance overhead:** As is shown in Table 1, most of IP watermark will produce numerous additional constraints at various abstract design levels. These additional constraints always lead to extra hardware overhead. In this case, the overhead in terms of embedding time, circuit area, speed and power will accordingly increase

RESEARCH STATUS AND ANALYSIS

Research progress of FPGA-based IP watermarking technology: FPGA-based IP watermarking technology at physical design level:

In recent years, IP watermarking technologies at physical design level have been widely researched. In University of Verginia, Lach *et al.* (1998) firstly presented FPGA-based IP watermarking method. Watermarks were mapped into additional constraints by using constraints generator and then inserted into the physical layout with the satisfiability in NP problem solving. In the constraints-based 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 private watermark can only be detected by several authorized users to solve the difficulties in IP detection and authorization. Since, watermark embedding in back-end process of physical design level is more secured, a watermarking scheme based on back-end process of physical design level was proposed by Lach *et al.* (2001) in Kochi University. The scheme abstracted physical layout as figure by using graph theory and topology. Watermarks were embedded into design with searching algorithm and optimizing algorithm (Nie *et al.*, 2005). For better flexibility of watermarking scheme based on physical layout, Halder *et al.* (2009) in University of Calcutta took graph corresponding to digital system design as input and embedded watermarks into encrypted graph by using LFSR-based locking scheme. However, this watermarking scheme imposed many restrictions on watermark embedding, making watermark detection much difficult (Halder *et al.*, 2009). In Indian statistical institute (Saha and Sur-Kolay, 2010) proposed a novel secure IP watermarking scheme at physical design level. VLSI design at physical design level could be protected directly and indirectly since the use of encryption algorithm and watermarking algorithm. The scheme has decreased difficulty of watermark detection and overhead caused by watermark embedding. Since FPGA platform has good performance on data processing and algorithm verification, FPGA-based IP watermarking algorithm at physical design level was proposed by Marolia (2008) in Georgia Institute of Technology. The watermarks were inserted by altering wires in FPGA-based design. Lu and Wang (2004) proposed timing constraints based FPGA watermarking scheme in front-end process. The watermarks were embedded into timing constrains of non-critical paths without affecting performance. After that, the bitfile of watermarked design was generated. Since security of watermarking algorithms based on designs at physical design level is much lower (Miao *et al.*, 2007) inserted ownership information into unique architecture of FPGA for protecting IP cores. Nie *et al.* (2010) designed a verification platform of IP watermarks. The design process was introduced concretely and the effect of the proposed platform in

IP watermark verification was analyzed as well. Liang *et al.* (2011a) proposed a chaotic mapping based IP watermarking algorithm at physical design level. The algorithm has low impact on performance in terms of circuit area, speed, etc.

FPGA-based IP watermarking technology at architectural design level: In this field (Ziener *et al.*, 2010; Schmid *et al.*, 2008) in the University of Erlangen-Nuremberg firstly introduced a new scheme for watermarking of IP cores for FPGA architectures. The watermark was detected at the power supply pins of FPGA. Moreover, the author's team presented an IP watermarking technology on the basis of netlist structure. The scheme restricted dynamically addressable part of the logic table in order to free spaces for watermark insertion. These two schemes will produce many extra traces of circuit alteration, causing a severe decline of watermark security. In the Southern Illinois University (Khan and Tragoudas, 2005) proposed a watermark embedding method in back-end process. The watermarks were embedded by altering netlist structure with redundancy addition and removal technology. Once a redundant connection was added to circuit, a series of new redundant connections may be generated. The function of new circuit will be the same with original circuit after removing these redundant connections. If the new circuit meets indicator of timing and some other indicators, the original circuit can be replaced with the new circuit. It is called redundancy addition and removing technology. In the scheme proposed by Kirovski *et al.* (2006), the watermarks were mapped into a set of additional constraints and then submitted to synthesis tool. The synthesis tool controlled logic synthesis, optimization and technology mapping of structure design level and finally generated unique output watermark vectors. The scheme requested strictly on the length of constraints. Shorter length of constraints will bring threat to security. On contrary, overlong length of constraints will cause larger hardware overhead. Xu *et al.* (2011) proposed an IP watermarking method by adding redundant logics into design. The ownership information was compressed and encrypted. With specific linear combination expression, the information was transformed into watermark bits and watermark positions. The watermark bits were finally inserted into FPGA based design dispersedly with method shown in Fig. 2. In this scheme, the performance in terms of watermark capacity, resource overhead and security was encouraging.

FPGA-based IP watermarking technology at behavioral design level: In research results of FPGA IP watermarking schemes at behavioral design level

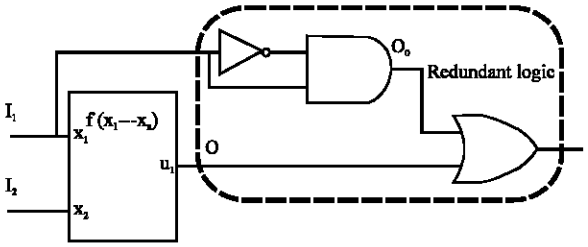

Fig. 2: Example for watermark embedding

(Castillo *et al.*, 2006) made use of the special internal architecture of FPGA and inserted watermarks into interspaces in used LUTs (Table 1) and unused LUTs. The hardware overhead is mainly caused by the circuit logic for extracting watermarks. The logic will write watermarks to output port after detecting specific input sequence. By comparing with scheme proposed (Raj *et al.*, 2011), watermark extraction is more convenient. However, the circuit for watermark extraction is vulnerable as well. Yu and Zhu (2011) proposed a watermarking method for protecting soft IP cores. The data of image and text are embedded into soft IP design in forms of specific bit stream. The on-site detection is implemented with low overhead. In method presented by Cai *et al.* (2007), the watermark constraints were dispersedly inserted into a set of watermark positions which were randomly selected in physical layout. Moreover, the author's team implemented a constraints-based watermarking system for protecting soft IP cores and hard IP cores. Their schemes are applicable for VLSI design and full-custom designs, which were superior to traditional constraints-based watermarking schemes. Sun *et al.* (2006) introduced an IP watermarking method by using buffer insertion technique. In addition, a hierarchical IP watermarking technology at behavioral design level on basis of constraints-based watermarking methods. Lin *et al.* (2007) proposed a HDL-based IP module protection method by inserting module of watermark detection into HDL code. The method has better ability against forgery attacks.

FPGA-based IP watermarking technology at systematic design level: Research results of IP watermarking technologies are rarely reported at systematic design level. (Chapman and Durrani, 2000) in the Strathclyde University proposed an IP protection for DSP algorithm implemented on SOC. The watermark was generated and embedded into partitions of high level filter design. The illegal users cannot obtain the watermark easily. However, the security is lower due to the short length of watermarks.

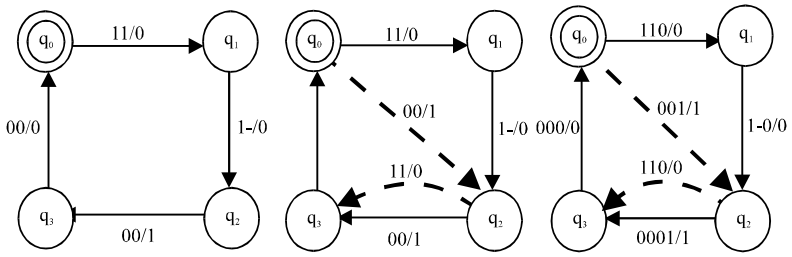

Fig. 3: Example for embedding watermarks into FSM-based IP core

Research progress of FSM-based IP watermarking technology: IP watermarking technologies based on FSM (Finite State Machine) have been widely researched in field of digital watermark. As is shown in Fig. 3 Torunoglu and Charbon (2000) added some unused transitions into original STG (State Transition Graph) and constructed an Euler path with the newly added transitions for indicating watermark. Oliveira (2001) divided 128bit watermarks into a set of watermark fragments according to the bit wide of input signal. These fragments, taken as an input sequence, were embedded by altering state of STG. For strengthening performance of watermark detection. Abdel-Hamid and Tahar (2008) proposed to insert watermarks into sequential circuit on basis of FSM in succession. This kind of watermarking algorithm shows certain randomness under control of key K. In this case, different schemes to add transitions will be generated if different designers input different keys. In watermark detection, given specific initial state and watermark input sequence, it is easily to read output sequence of watermarks.

In order to improve security of FSM based IP watermarking methods at behavioral design level Xu and Zhu (2011) proposed a FSM based watermarking scheme for soft IP protection. It is an improvement of original FSM-based IP watermarking technology, with some problems like low security and high power overhead still remaining. Cui *et al.* (2008) proposed to embed watermarks into architecture of single scan chain with FSM reduction technique. The traceability is guaranteed since FSM reduction technique does no damage to watermarks. The watermarks will be detected at lower design levels even in a packaged chip. In FSM base watermarking schemes, the team proposed a simple-designed IP protection scheme, which embedded watermarks by reordering scan cells between scan chains but its security and overhead remains to be improved. Liang *et al.* (2011b) introduced an FSM based IP watermarking algorithm with better performance on security and hardware overhead.

Research progress of testable IP watermarking technology: In recent years, testable IP watermarking technology has been a research hotspot at home and abroad, which concentrate on scan chains based IP watermarking. For instance Fan (2008) added watermark generation circuit in reusable IP design and proposed five feasible watermark hiding methods. According to embedding rules, watermark can be detected at output pin of the chip on site. However, once make the embedding rule public, the watermark generation circuit is easy to remove. In watermarking schemes based on scan chains and scan forest, the method by Saha and Sur-Kolay (2010) proposed to protect IP by altering both the scan tree and single scan chain, separately embedding signatures of the owner of physical design tool and that of the logic design tool, in which watermark detection was difficult. In methods proposed by Cui and Chang (2009), Chang and Cui (2010) and Cui *et al.* (2011) watermark was inserted by reordering the scan cells in scan chains, which is described in Fig. 4. Additional constraints generated by the owner's digital signature have been imposed on the NP-hard problem of ordering the scan cells to achieve a watermarked solution which minimizes the penalty on power and cost of testing. The ownership legitimacy can be publicly authenticated on-site by IP buyers after the chip has been packaged. Liang *et al.* (2011a) proposed an IP protection method by watermarking minimum correlation of vectors based multiple scan chains. It provides an effective approach for improving fraction of coverage. However, the ability against collusion attacks and performance on hardware overhead still exist room for improvement.

Research progress of other IP protection technologies: "Tag" technology: To identify authenticity of chip by inserting an electronic "tag" into chip with good reliability and traceability. An EPIC (Ending Piracy of Integrated Circuit) technology was proposed by Roy *et al.* (2008) for supervising chip manufacture. The key is embedded into circuit in advance. The chip cannot enter into market through routine test without activation. Furthermore, a bus based "lock and unlock" scheme was proposed for hardware IP protection. Its implementation requires certain hardware overhead (circuit, pins, etc.) but with good concealment and security. Even so, the scheme can still only supervise chip manufacture and test but not involve traceability of IP watermarks after chip is sold.

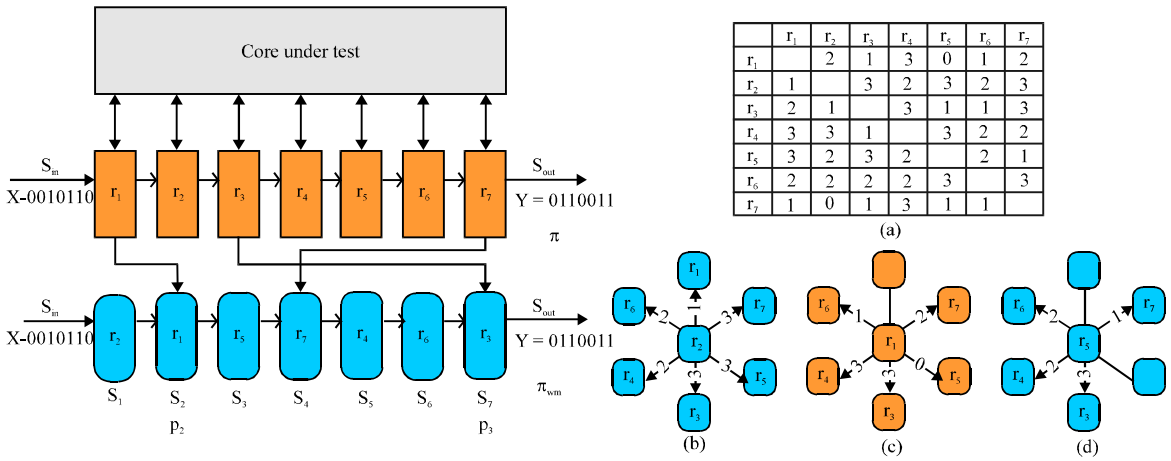

Fig. 4(a-d): Example for embedding watermarks into testable IP core

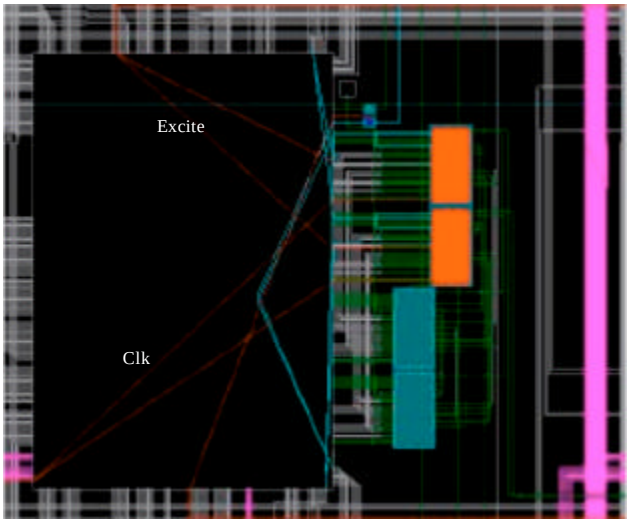

Fig. 5: BPUF Cell Displayed by FPGA Editor

A tag technology for protecting ASIC (Application Specific Integrated Circuit) IP core was proposed by (Goren *et al*, 2010). A "secure tag", with ownership information stored, is placed in IP core. Meanwhile, an "external receiver" is set for detecting the existence of the tag. The independency of "tag" can deter misappropriation to some extent but the "tag" may be easy to be removed or damaged. Methods in Kumar *et al*. (2008), Guajardo *et al*. (2007) and Kumar *et al*. (2008) used the unique physical feature and variability of single silicon slice in IC manufacture and generated RFID (Radio Frequency Identification Devices) "tag". After that, the "tag" is integrated into chip for preventing chip clone. As shown in Fig. 5, security has been greatly improved but high design cost and RFID work environment restrict the development of this technology.

Fingerprint technology. Various users can obtain different versions of IP cores with identification. The use of this technology can identify responsibility in property dispute due to the uniqueness of fingerprint. The difficulty lies in generation of many different IP cores with the same function and technology indicators in design process. Lach *et al*. (2001) proposed an IP fingerprint technology based on partition of problem solving. An initial problem solving is divided into many parts, each one of which is realized with different forms. The IP

module with user fingerprint is generated by selecting and combining forms of different parts. However, this technology can only be implemented on certain VLSI design level. Furthermore, high design cost and low ability against collusion attacks make its application be limited.

OUTSTANDING ISSUES IN IP WATERMARKING TECHNOLOGY

To make reusable IP watermarking technology be safely applied in practice, it is necessary to design a more effective IP watermarking method. However, the research on this aspect remains in primary stage. To develop into mature application technology need further innovative research. Consequently, there are several problems in digital IP watermarking technology to be solved, which will provide guidance for future watermarking technology.

Multiple IP watermarking technology: In research fields of digital IP watermarking, multiple IP watermarking can always perform several application functions, which is impossible for traditional watermarking technology to replicate. Multiple IP watermarking has great improvement in applied range and extensibility, making it applicable in more complicated environment. Nevertheless, it gives transparency of system away since more watermarks will be embedded into design than that in single watermarking scheme. The more design levels are watermarked, the larger hardware overhead it takes. At present, multiple IP watermarking technology still stays on simple superimposition of several watermarks. Although with strengths in watermark number and robustness, multiple IP watermarking technology will bring certain complexity as well. Consequently, research on this aspect will provide approaches for the development of IP watermarking in integrated circuit, such as watermark capacity, security, etc.

IP watermark embedding models and optimization models: To build models of IP watermark embedding and optimization is a critical part of IP watermarking technology. Correlation and compatibility between IP watermark vectors are related to watermark structure in watermarked circuit and watermark structure depends on size of redundant information in circuit carrier. Consequently, real application of IP watermarking scheme will consider logic synthesis and optimization of circuit in various abstract design levels. In original circuit, states of redundant information and ordering of signal names may be altered, which will lead to larger structure of some redundant information and lower security of watermarks. Study on methods of watermark embedding and optimization, construction of watermark architecture, optimal condition of watermark embedding based on good security and reliability will be development trend of IP watermarking technology.

Watermark detection: In general, user information or identification of IP core will be used for generation of unique fingerprint with specific encryption algorithm. The fingerprint information is then inserted into IP attribute document secretly, which will be distributed to various users. Once a user is suspected to reuse IP design illegally, the fingerprint information will be extracted for ownership authentication. If succeed, the illegal IP user will be found by decrypting the extracted information. Since this method requires participation of the third party, it will bring many difficulties for IP forensics. To study on blind forensics technology will be crucial in IP forensics.

Watermark evaluation: Performance evaluation is an important part in IP watermarking technology. In order to fully evaluate strengths of IP watermarking and compensate for drawbacks of other watermarking methods, evaluation method of watermark performance will be researched at various abstract levels. Furthermore, corresponding standards will be established as well. At present, performance evaluation of IP watermark mainly consists of security and robustness, which is contradictory mutually. The capacity and strength of embedded watermarks have impact to security and robustness inordinately. For this reason, the compromise scheme among watermark capacity, robustness and security should be overall considered.

CONCLUSION

This study summarized the background, concept and features of IP watermarking technology and analyzed problems in current IP watermarking. Moreover, many challenges and latest progress of IP watermarking are discussed. On the basis of existing theories and research results, some critical research problems, like multiple IP watermarking, model design of watermark embedding optimization, IP detection and performance evaluation, etc., are presented for practical application. These introductions are expected to provide references for researchers in the field of VLSI based IP protection.

ACKNOWLEDGMENTS

This study is partially supported by National Basic Research Program of China (973 Program) under Grant No. 2012CB315801 (2012.1-2015.12, Hunan University). National Natural Science Foundation of China under Grant No.61202462 (2013.1-2015.12, Hunan University of Science and Technology) and No. 61173167,61173169 (2012.1-2015.12, Hunan University), National Natural Science Foundation of Hunan Province and Xiangtan united Foundation under Grant No. 11JJ9014 (2011.1-2013.12, Hunan University of Science and Technology), the planned science and Technology Project of Hunan Province, China under Grant No. 2011 Gk 3156 (2011.6-2013.6, Hunan University of Science and Technology), National Natural Science Foundation of Hunan Province Foundation under Grant No. 13JJ3091 (2014.1-2016.12, Hunan University of Science and Technology).

REFERENCES

Abdel-Hamid, A.T., S. Tahar and E.M. Aboulhamid, 2005. A survey on IP watermarking techniques. Des. Autom. Embedded Syst., 9: 211-227.

Abdel-Hamid, A.T. and S. Tahar, 2008. Fragile IP watermarking techniques. Proceedings of the NASA/ESA Conference on Adaptive Hardware and Systems, June 22-25, 2008, Noordwijk, China, pp: 513-519.

Cai, X., Z. Gao, F. Bai and Y. Xu, 2007. A watermarking technique for hard IP protection in post-layout design level. Proceedings of the 7th International Conference on ASIC, October 22-25, 2007, Guilin, China, pp: 1317-1320.

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 the 16th International Conference on Field Programmable Logic and Applications, FPL`06, Madrid, pp: 487-492.

Chang, C.H. and A. Cui, 2010. Synthesis-for-testability watermarking for field authentication of VLSI intellectual property. IEEE Trans. Circuits Syst., 57: 1618-1630.

Chapman, R. and T.S. Durrani, 2000. IP protection of DSP algorithms for system on chip implementation. IEEE Trans. Signal Process., 48: 854-861.

Cui, A. and C.H. Chang, 2009. An improved publicly detectable watermarking scheme based on scan chain ordering. Proceedings of the IEEE International Symposium on Circuits and Systems, May 24-27, 2009, Taipei, Taiwan, pp: 29-32.

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.

Cui, A., C.H. Chang, S. Tahar and A.T. Abdel-Hamid, 2011. A robust FSM watermarking scheme for IP protection of sequential circuit design. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., 30: 678-690.

Fan, Y.C., 2008. Testing-based watermarking techniques for intellectual-property identification in SOC design. IEEE Trans. Instrum. Meas., 57: 467-479.

Girard, P., 2002. Survey of low-power testing of VLSI circuits. Des. Test Comput., 19: 80-90.

Goren, S., H.F. Ugurdag, A. Yildiz and O. Ozkurt, 2010. FPGA design security with time division multiplexed PUFs. Proceedings of the International Conference on High Performance Computing and Simulation, June 28-July 2, 2010, Caen, France, pp: 608-614.

Guajardo, J., S.S. Kumar, G.J. Schrijen and P. Tuyls, 2007. FPGA intrinsic PUFs and their use for ip protection. Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems, September 10-13, 2007, Vienna, Austria, pp: 63-80.

Halder, R., P. Dasgupta, S. Naskar and S.S. Sarma, 2009. An internet-based IP protection scheme for circuit designs using Linear Feedback Shift Register (LFSR)-based locking. Proceedings of the 22nd Annual Symposium on Integrated Circuits and System Design: Chip on the Dunes, August 31-September 03, 2009, Natal, Brazil, pp: 384-389.

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.

Khan, M. and S. Tragoudas, 2005. Rewiring for watermarking digital circuit netlists. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., 24: 1132-1137.

Kirovski, D., Y. Hwang, M. Potkonjak and J. Cong, 2006. Protecting combinational logic synthesis solutions. IEEE Trans. Compu. Aided Des. Integr. Circuits Syst., 25: 2687-2696.

Kumar, S.S., J. Guajardo, R. Maes, G.J. Schrijen and P. Tuyls, 2008. Extended abstract: The butterfly PUF protecting IP on every FPGA. Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust, June 9-9, 2008, Anaheim, CA., USA., pp: 67-70.

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, 2001. Fingerprinting techniques for field-programmable gate array intellectual property protection. IEEE Trans. Comput. Aided Design Integrated Circuits Syst., 20: 1253-1261.

Liang, W., X. Sun, Z. Ruan and J. Long, 2011a. The design and FPGA implementation of FSM-based intellectual property watermark algorithm at behavioral level. Inform. Technol. J., 10: 870-876.

Liang, W., X. Sun, Z. Ruan, J. Long and C. Wu, 2011b. A sequential circuit-based IP watermarking algorithm for multiple scan chains in design-for-test. Radioengineering, 20: 533-538.

Lin, M.C., G.R. Tsai, C.R. Wu and C.H. Lin, 2007. Watermarking technique for HDL-based IP module protection. Proceedings of the 3rd International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Volume 2, November 26-28, 2007, Kaohsiung, Taiwan, pp: 393-396.

Lu, J. and S. Wang, 2004. An FPGA based IP watermarking method based on timing constraints. J. Electron. Inform., 26: 1882-1887.

Marolia, P. M., 2008. Watermarking FPGA bitstream for IP protection. M.S. Thesis, Georgia Institute of Technology, Atlanta.

McCluskey, E.J., D. Burek, B. Koenemann, S. Mitra, J. Patel, J. Rajski and J. Waicukauski, 2003. Test data compression. IEEE Des. Test Comput., 20: 76-87.

Miao, S., G. Dai, D. Mu and M. Li, 2007. A watermark protecting method for IP core based on FPGA. Microelectron. Comput., 24: 30-33.

Nie, T., T. Kisaka and M. Toyonaga, 2005. A watermarking system for IP protection by a post layout incremental router. Proceedings of the 42th Annual Design Automation Conference, June 13-17, 2005, Anaheim, California, USA., pp: 218-221.

Nie, T., Y. Li, X. Xu and M. Toyonaga, 2010. Performance evaluation for watermarking techniques. Proceedings of the International Conference on Biomedical Engineering and Computer Science, April 23-25, 2010, Wuhan, China, pp: 1-4.

Oliveira, A.L., 2001. Techniques for the creation of digital watermarks in sequential circuit designs. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., 20: 1101-1117.

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

Raj, N.D., Josprakash, A. Kumar, Daniel and J. Thomas, 2011. Behavioural level watermarking techniques for IP identification based on testing in SOC design. Proceedings of the International Conference on Information Technology and Mobile Communication, April 21-22, 2011, Nagpur, Maharashtra, India, pp: 485-488.

Roy.J.A., F. Koushanfar and I.L. Markov, 2008. EPIC: Ending piracy of integrated circuits. Proceedings of the Design, Automation and Test in Europe, March 10-14, 2008, Munich, Germany, pp: 1069-1074.

Saha, D. and S. Sur-Kolay, 2010. A Unified approach for ip protection across design phases in a packaged chip. Proceedings of the 23rd International Conference on VLSI Design, January 3-7, 2010, Bangalore, India, pp: 105-110.

Schmid, M., D. Ziener and J. Teich, 2008. Netlist-Level IP protection by watermarking for LUT-based FPGAs. Proceedings of the International Conference on ICECE Technology, December 8-10, 2008, Taipei, Taiwan, pp: 209-216.

Sun, G., Z. Gao and Y. Xu, 2006. A watermarking system for IP protection by buffer insertion technique. Proceedings of the 7th Symposium on Quality Electronic Design, March 27-29, 2006, San Jose, USA., pp: 671-675.

Torunoglu, I. and E. Charbon, 2000. Watermarking-based copyright protection of sequential functions. IEEE J. Solid-State Circuits, 35: 434-440.

Xu, J., J. Long, W. Liang and W. Huang, 2011. A DFA-based distributed IP watermarking method using data compression technique. J. Convergence Inform. Technol., 6: 152-160.

Xu, W. and Y. Zhu, 2011. A digital copyright protection scheme for soft-IP core based on FSMs. Proceedings of the International Conference on Consumer Electronics, Communications and Networks, April 16-18, 2011, XianNing, China, pp: 3823-3826.

Yu, T. and Y. Zhu, 2011. A new watermarking method for soft IP protection. Proceedings of the International Conference on Consumer Electronics, Communications and Networks, April 16-18, 2011, XianNing, China, pp: 3839-3842.

Ziener, D., F. Baueregger and J. Teich, 2010. Using the power side channel of FPGAs for communication. Proceedings of the 18th IEEE Annual International Symposium on Field-Programmable Custom Computing Machines, May 2-4, 2010, Charlotte, USA., pp: 237-244.