ISSN: 2395-1680 (ONLINE)
DOI: 10.21917/ijme.2017.0063

IP PROTECTION USING WATERMARKING WITH OBFUSCATION

Nisha Elma Koshy and Binu K. Mathew
Department of Electronics and Communication Engineering, Saintgits College of Engineering, India

Abstract

The technology scaling allows complex systems to be placed on a single die with million transistors integrated into it. Intellectual Property (IP) cores are reusable logic blocks used for building such complicated systems. Secure IP designs that can protect authorship are needed to deter IP piracy. One widely used detection method is digital watermarking which provides proof of the ownership to the IP vendor. The proposed methods in this work can embed into the IP or system obfuscation enabled watermark and also provides techniques for access control and fingerprinting. These techniques were implemented in an 8 bit ALU that can perform 8 operations. The functionality of the system was analyzed using the Xilinx ISE Design suite 14.6.

Keywords:

Intellectual Property (IP), IP Protection, Watermarking, Obfuscation, Fingerprinting.

1. INTRODUCTION

In the new era of digital IC (Integrated Circuit) design, there are needs for design of complex and application specific chips in various domains. The only way to face this challenge is to follow a reuse based design methodology where reusable components called IP's are used for development of complex systems. The task of delivering high quality and cheaper devices within a given design time constrain can only be met by reuse of components.

IP designers, sharing their design and interacting with different parties, will have to encounter high security risks for their IP designs. Its reuse in several environments such as design house, foundries and application area has to be monitored, as unauthorized reuse by any manufacturer or buyer leads to economic damage to the genuine IP owner. Thus with popularity of IP oriented design, IP security becomes essential. IP protection techniques involve mechanisms like watermarking, fingerprinting, obfuscation and so forth. Of these, watermarking techniques were widely used in many application spheres, for copyright protection as well as data hiding [1].

In watermarking based IP protection, a watermark or a unique code is embedded into the IP core design and is detected during authentication of the IP copyrights. Several watermarking techniques that incorporate watermark at different abstraction levels have been proposed, over these years. This work aims at the design and implementation of watermarking methods which also provides provision for obfuscation and locking. An eight bit ALU that can perform eight operations is designed for the purpose of watermarking. Two proposed methods which uses the concept of using a controlling key as the watermark. This work when compared to other existing techniques also provides additional facilities for fingerprinting and access control.

The paper is organized as follows. A thorough discussion on IP's, different methods for IP protection, watermarking and different watermarking techniques is included in section 2. Section 3 provides the proposed watermarking techniques and its working. The implementation and simulation results are presented in section 4.

2. BACKGROUND

Globalization of IC designs caused provocation to security threats like IC piracy, overbuilding, counterfeit and RE (Reverse Engineering). The cost of counterfeiting and piracy for G20 nations was estimated as U.S. $450–650 billion in 2008 and was reckoned to grow to U.S. $1.2–1.7 trillion in 2015 [2]. IP cores should have robust and powerful ownership protection formats to thwart IP piracy.

2.1 IP CORES

IP core is a reusable unit of logic or chip layout design which is the intellectual property of designer and can be viewed as an independent subpart. They are used as building blocks within different chips created by same or different vendors. The newly developed subcomponents can be tested and saved as new design IPs in the IP library for future reuse.

IP blocks are available basically in three different types depending on design and applications. The Virtual Socket Interface (VSI) alliance document [3] classifies it as soft, firm and hard IP's. A circuit description of the system in Hardware Description Language (HDL) is a soft IP. Firm IPs may be of the form of full or partially placed netlist, while a hard IP can be delivered in the form of design layout.

Hardware design reuse is an effective design approach and it became the most practical solution to deal with the increasing design complications. The third party or buyer, knowing the interfaces and behavior, can simply repackage and sell the reusable IP even without grasping internal design or implementation details. Illegitimate copies of an IP are generated due to unlawful IP reselling by a third party or unauthorized over production of ICs in foundry [4].

The increasing damage that the hackers or competitors cause to the financial income and reputation of the IP owners asks for robust IP core protection methods.

2.2 IP PROTECTION TECHNIQUES

As per VSI Alliance IP protection development working group [5] there are three main approaches to secure IPs. First, a deterrent approach where the theft is deterred using legal means such as patents, copyrights and trade secrets. Second is an active protection approach where the owner tries to prevent IP piracy using license agreements and encryption techniques. Protection techniques cannot secure designs or track them in case they are stolen or reused without permission [1]. Third approach of detection, involves the facilities for determining the unauthorized use and tracing of the source of the theft. It includes methods like watermarking and fingerprinting. The process of adding the authorship proof of IP vendor in form of watermark is known as watermarking, whereas including identity of IP buyer is termed as fingerprinting. Obfuscation based protection can also be preferred to thwart infringement.

2.2.1 *Obfuscation of Designs:*

Obfuscation of IP is an effective technique that converts an IP to functionally similar design but significantly hard to reverse engineer. A combinatorial logic obfuscation method with additional key gates (XOR or XNOR) inserted in original design is proposed in [6]. Another method for modifying the functionality by adding certain data path components is given in [7]. The possibility of using multiplexer as obfuscation cell is applied in [8] where the select line input is the key input. The obfuscated design will exhibit a correct function only when a correct key is applied. These obfuscation techniques can protect the IC from piracy and overbuilding.

2.2.2 *Watermarking as Authorship Proof:*

This task of adding a representation of ownership can be accomplished by embedding a unique code, or watermark in IP. Primary prerequisites for any watermark are listed in [9]. Watermark must be transparent, i.e. it should not indulge in the functionality of the design It has to be robust or resistant to deletion attack, and detectable, i.e., easy to extract from the design. In [10] a technique for embedding watermark circuit in test circuit is discussed. It uses the test mode signal '*t*' to control the watermark generating circuit, where the chip sends out the watermark followed by test pattern in test mode. Several watermarking techniques based on FSM's are present in existing literature which use unused states and transitions to store watermark [9], [11]. There are high chances for different attacks [1] against watermark. The removal and masking attack tries to delete the watermark or disables its extraction. The best method for handling this is to embed watermark or sign as the functional part of design. An HDL level watermarking method uses the combinational logic and memory cells for signature hosting and embedding [12]. Embedding attacks add another watermark into the design. The concept of using a governing body to handle the case of infringement is discussed in [1], [11] and [13]. This legal body records the watermark data securely with a time stamp. The date of generation of watermark stored by this authorized legal body can thus be used to tackle embedding attacks.

Combining fingerprint with watermark to form a signature that can prove authorship and buyers identity is used in [14], [13].

3. PROPOSED TECHNIQUES

Several schemes and architectures were proposed by different researchers for securing the IP core. They include methods for embedding watermarks at different abstraction levels of design. The proposed work incorporates watermark into high level of design of a system. The architecture chosen for the work is an 8 bit ALU (Arithmetic Logic Unit) that can perform 8 operations.

The architecture of the ALU is as shown in Fig.1, where *A* and *B* are the 8 bit operands and OP CODE selects the desired ALU. The SUB signal is taken into the ADD/SUB module which can perform either addition or subtraction. It gets asserted whenever a subtraction is to be performed by the ALU. Comparator performs the comparison between two operands. The result of subtraction is also taken into this module so that, whenever both operands are same, comparator uses the zero difference to give the result of comparison. Multiplier performs 3 bit multiplication by taking the last three bits of both *A* and *B*, while the decoder decodes the last four bits of operand *A*.

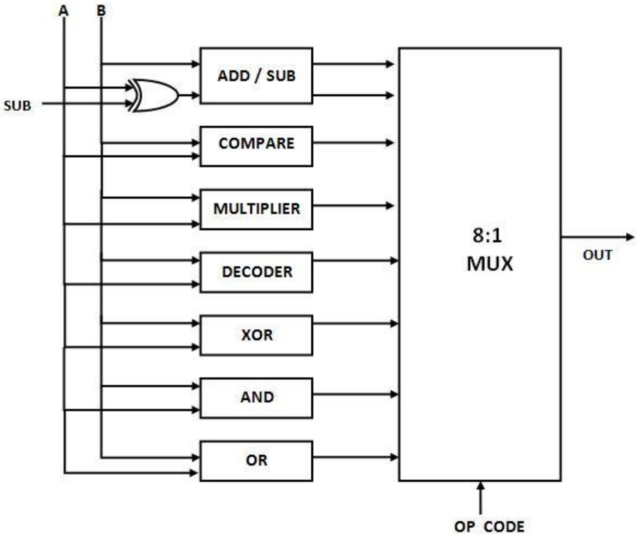

Fig.1. Architecture of 8 bit ALU

The operations XOR, AND and OR are for bitwise logic operations. The functioning of ALU is summarized as in Table.1.

Table.1. ALU Operations

Op code	Function
000	A+B
001	A-B
010	1 if A=B 2 if A>B 3 if A<B
011	A[2:0] * B[2:0]
100	Decode ([A[3:0]])
101	A exor B
110	A and B
111	A or B

3.1 OBFUSCATION USING MULTIPLEXERS

The ALU shown in Fig.1 is subjected to obfuscation by inserting multiplexers which can act as obfuscation cells. The modified ALU shown in Fig.2 is functionally equivalent to the original ALU only when the correct key, *K*[8:0], is given to the system. The obfuscated ALU is designed in such a way that it functions as per Table.1 only when *K*='01100011'. Inserted multiplexers, with one of its inputs the actual entry and other the fake input, are controlled by bits of the key acting as the select lines. When a key other than '01100011' is entered the circuit gives a different functionality.

Only those IP's approved by the designer can assure the correct operations. An intruder without knowing the key cannot use the pirated or overproduced IP's as it can only be unlocked with the proper key provided by the IP author. Nonvolatile on-chip memories, preferably one time programmable, can be used to store the key [8].

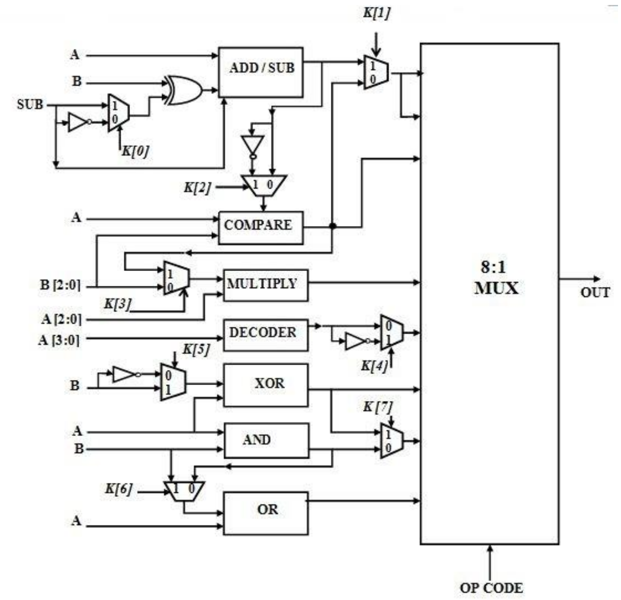

Fig.2. Obfuscated ALU

3.2 PROPOSED WATERMARKING METHODS

Watermark is a mechanism for proving the identity or copyright of the IP designer and must be embedded as an vital part of the design for making it strong against removal attacks. The proposed method in this section utilizes key, the inevitable part of the design, as the unique mark for proving the ownership.

3.2.1 Proposed Watermarking - Method 1:

This method employs the idea of using the unavoidable key as watermark. The Fig.3 demonstrates the architecture of proposed system. During normal functioning the value of ‘*t*’ signal is ‘0’ and during validation of authorship it takes the value ‘1’.

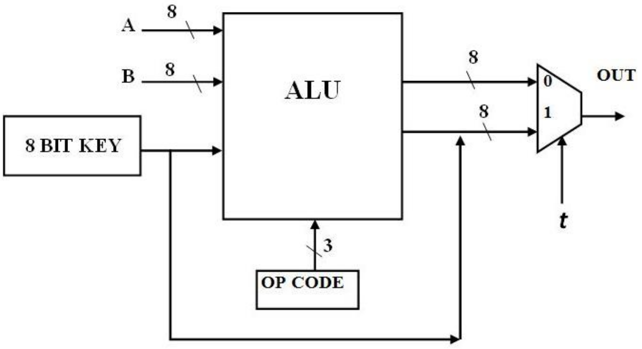

Fig.3. Proposed watermarking method 1

Thus output multiplexer passes the value of controlling key or the watermark as the system output during authentication. During normal operation the output multiplexer forwards the typical ALU response to the output port. The normal behavior of the system is not disturbed by the existence of the watermark, i.e. the transparency of watermark is ensured in this proposed system.

3.2.2 Proposed Watermarking - Method 2:

The second method also makes use of the proposal of using the controlling key as watermark. In case of first proposed method, the adversaries, if somehow get knowledge about the presence of output multiplexer, can remove the multiplexer or bypass the result. In this method the functionality of the ALU is exploited to give the watermark or the key as the output of the system, avoiding the output multiplexer present in first proposed method, during authentication.

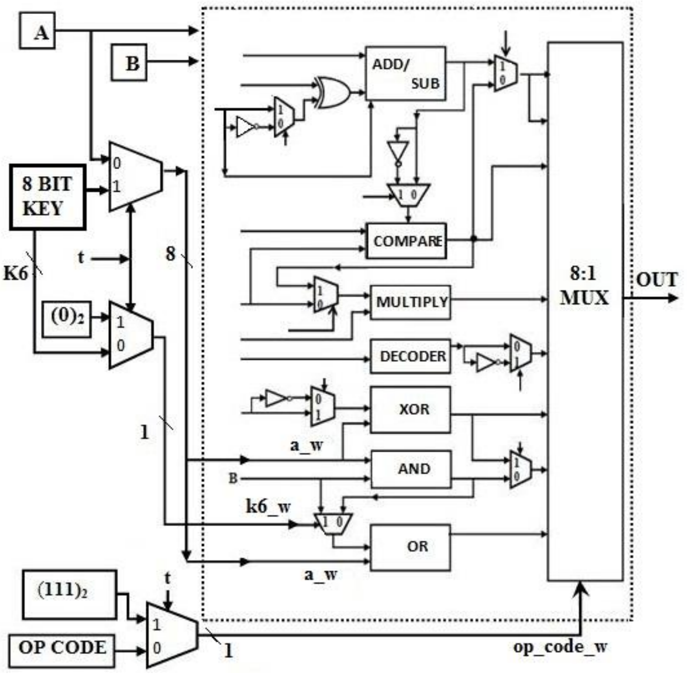

Fig.4. Proposed watermarking Method 2

In this ALU, the boolean operation of A+(A.B)=A is employed to deliver the watermark, the key, as the output of the system. For that, some modifications are made in system as shown in Fig.4. The ‘*t*’ signal which takes the value ‘1’ during verification, controls three multiplexers, an 8 bit multiplexer, a 1 bit multiplexer and a 3 bit multiplexer. During validation the 8 bit multiplexer forwards the key, instead of operand A, to the blocks performing AND and OR operation. Similarly 1 bit and 3 bit multiplexers forwards ‘0’ as ‘*k*6_*w*’ and ‘111’ as ‘*op_code_w* to’ the ALU. Here ‘111’ corresponds to OR operation. By this modification the ALU performs the operation (*key* + (*key B*)) to give ‘*key*’ at the output.

3.3 USER IDENTIFICATION TECHNIQUE

The idea of combining creator’s and consumer’s information in one signature was put forward in [12] and [13]. In order to incorporate the user identification facility, the fingerprinting scheme and model of watermarking authority is used in this work [13].

The watermark which is a sequence of binary bits of controlling key can be subjected to a function F, say multiplication, with a fingerprint ID to generate a signature that can be embedded in IP. A data set (WM_X, FP_Y, S_{XY}) corresponding to each officially authorized buyer of IP, is recorded in a database as shown in Table.2. Here, WM_X denotes the watermark of designer *X*, FP_Y denotes the fingerprint ID of legal user *Y* and S_{XY} indicates the signature located in the IP purchased by user *Y* from designer *X*.

Table.2. Signature for different users

IP	User	Water mark	Fingerprint	Signature
IP 1	User A	WM_1	FP_A	$S_{1A} = F(WM_1, FP_A)$
	User B	WM_1	FP_B	$S_{1B} = F(WM_1, FP_B)$
	User C	WM_1	FP_C	$S_{1C} = F(WM_1, FP_C)$
IP 2	User D	WM_2	FP_D	$S_{2D} = F(WM_2, FP_D)$
	User E	WM_2	FP_E	$S_{2E} = F(WM_2, FP_E)$
	User F	WM_2	FP_F	$S_{2F} = F(WM_2, FP_F)$

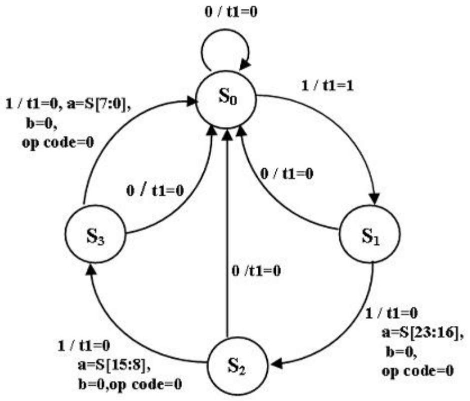

Fig.5. State Diagram for sign generation

The state diagram of the FSM is as shown in Fig.5. When input '*t*' to the FSM becomes '1' it starts to transit from S_0 to S_1 and so on. During first transition, the watermark is generated at output as '*t*1' signal acting as internal '*t*' signal is made one by FSM control. For rest of transitions, generated op code is '000' which corresponds to the addition operation. Thus '*a*' taking values of the sign bits and '*b*' equals to zero gives the sum as sign itself at output.

The ALU is redesigned as in Fig.6 to take the '*a*', '*b*' and '*op code*' inputs from FSM instead of normal inputs '*A*', '*B*' and '*OP CODE*'. Functionalities other than addition can also be used for sign generation through FSM control.

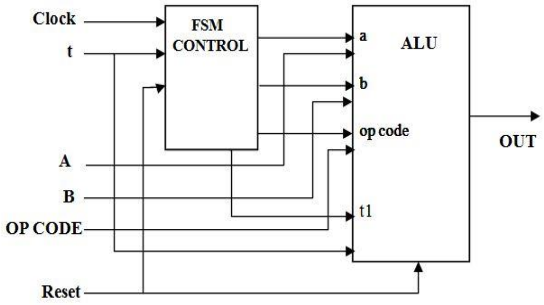

Fig.6. Arrangement for User Identification

As soon as a suspect issue happens, IP designer can immediately request the watermarking authority for the confirmation. The authority then access IP and retrieve the signature. If the signature obtained is the same to a signature S_{XY}, then the FP_Y is used to perform inverse of function *F*, to obtain the watermark *WM*. If obtained watermark *WM* is equivalent to WM_X, it confirms that the IP core is designed by the designer *X* and is illegally distributed by buyer *Y*. The entire process of authentication is done confidentially by the authority to secure the watermark and fingerprint details. Consequently, the proposed technique facilitates both user recognition, to track the source of illegal circulation of an IP, and watermarking for ownership proof.

4. RESULTS

This section presents the FPGA simulation results and implementation details obtained when different methods discussed in the previous section were implemented on different FPGA families.

The FPGA simulations and implementations were done using ISE version 14.6 and synthesized for Artix-7, Spartan-3, Spartan-6, Virtex-4, Virtex-5 and Virtex-6 families. Through this analysis, the implementation results of the proposed techniques could be obtained for different families of FPGA. The design entry was done using Verilog HDL.

The Fig.7 shows the graphical illustration of device utilization of method 1 in different FPGA families. It shows the LUT utilization of 8 bit ALU, watermarked ALU and that of ALU with fingerprinting ability, using method 1.

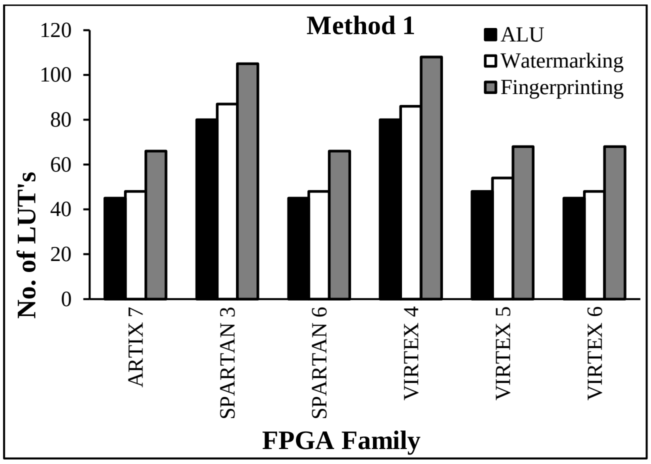

Fig.7. Device utilization of Method 1

The Fig.8 shows the device utilization details of method 2 in different FPGA families. It shows the LUT utilization of 8 bit ALU, watermarked ALU and that of ALU with fingerprinting ability, using method 2.

The device utilization results show that the area of system increases when a watermark is added to the design. There is further increase in area when the provision for buyer identification is combined to the watermarked design. But these come at the cost of elevated protection to the IP core design which if not present, cause IP infringement and thereby revenue loss to designer.

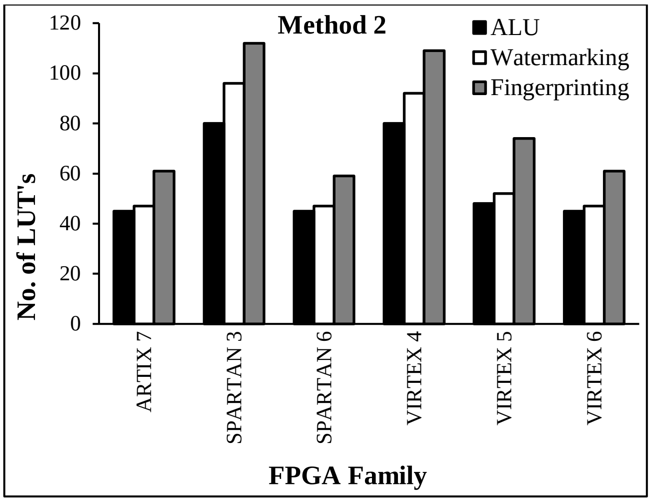

Fig.8. Device utilization of Method 2

The simulation results of architectures proposed is shown from Fig.9 to Fig.12. The response ALU of Fig.1 to different op codes is shown in Fig.9. It shows the operation of ALU with no watermarking.

The simulated waveform of watermark retrieval during authentication using system in Fig.3 is demonstrated by Fig.10. As revealed by the figure, watermark is generated when ‘*t*’ signal is made high during verification. During normal operation the ‘*t*’ signal will be low and the ALU performs its usual operations as given in Table.1. In this work the key or the watermark of the ALU is ‘01100011’.

The simulation waveform of Fig.11 shows the second proposed watermarking method. When ‘*t*’ is made high ‘*k*6_*w*’ takes the value ‘0’, ‘*op_code_w*’ takes the value ‘111’and ‘*a_w*’ takes the value of key. The output gives the watermark when ‘*t*’ is high.

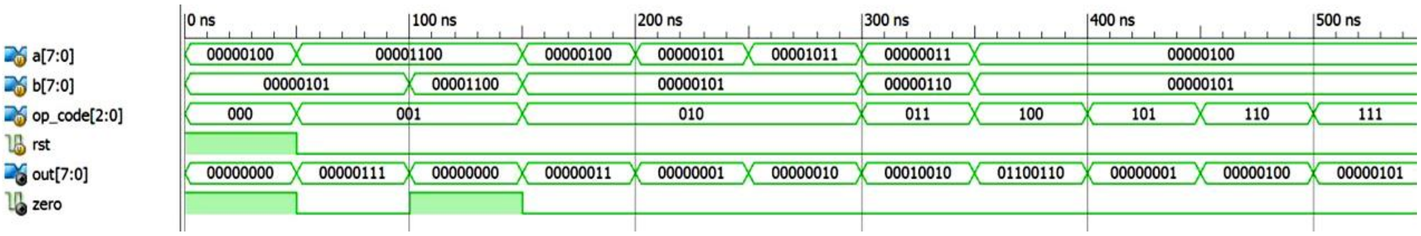

Fig.9. Simulation result showing normal ALU operation

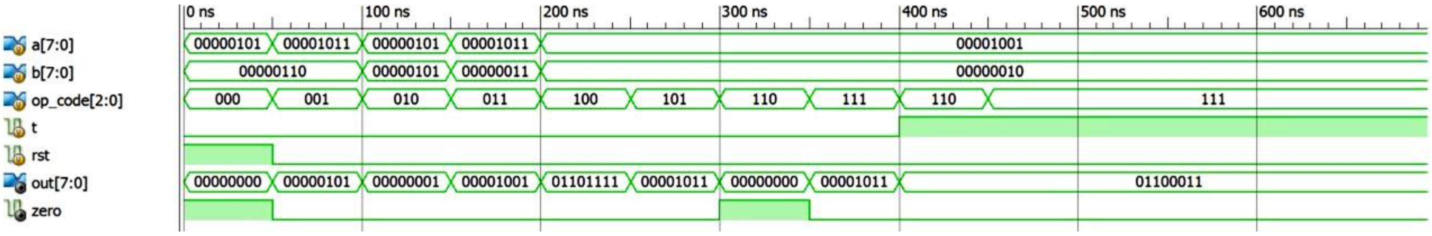

Fig.10. Simulation of Proposed watermarking Method 1

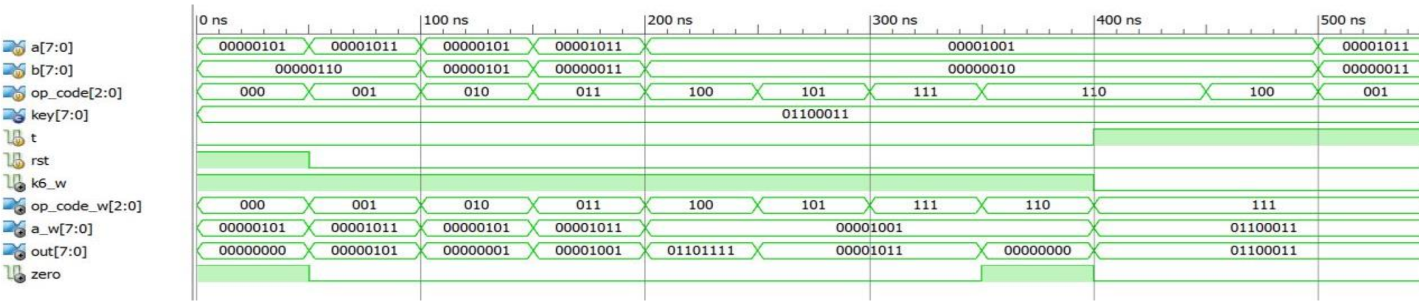

Fig.11. Simulation of Proposed watermarking Method 2

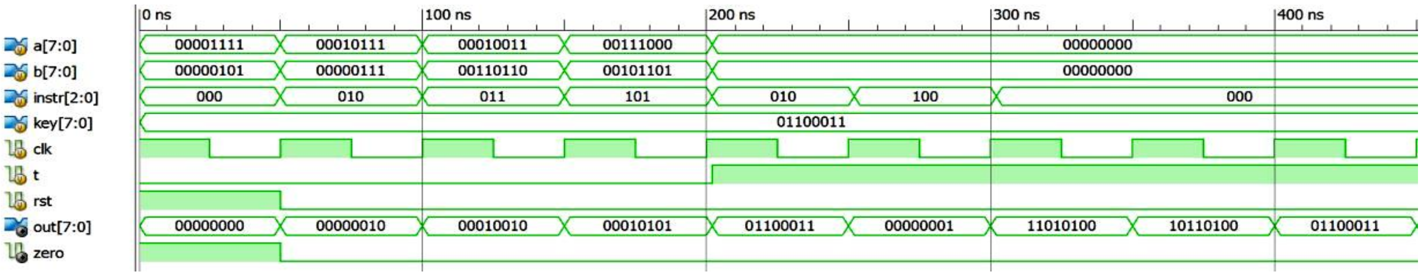

Fig.12. Simulation of user identification technique

In this work the function chosen for combining watermark and fingerprint to generate signature is multiplication. The Table.3 gives an illustration of data to be stored by watermarking authority for an IP. Three different buyers *A*, *B* and *C* are considered and their corresponding fingerprints are shown in Table.3. The product of fingerprint and watermark gives the signature for each IP instance.

Table.3. Signature for different users of an IP

User	Watermark	Fingerprint	Signature
User *A*	01100011	1001 0110 1100	0000 0011 1010 0100 1100 0100
User *B*	01100011	0100 1011 1100	0000 0001 1101 0100 1011 0100
User *C*	01100011	1001 1111 0001	0000 0011 1101 1000 0011 0011

Signature generation for user and designer identification is performed by asserting '*t*' signal during validation and is illustrated in Fig.12. During verification the system generates the watermark at the beginning followed by the signature. Comparing the data from the waveform with that in Table.3 shows a match in signature with that of user *B*. Hence the IP subjected to buyer identification in this case can be confirmed to be purchased or illegally redistributed by user *B*. The watermark '01100011', obtained initially can be used as proof of ownership of the IP. The fingerprint used in this case is twelve bits long and thus it is possible to distribute IP to 2^{12} consumers.

5. CONCLUSION

This paper proposes novel IP protection techniques using watermarking. IP cores are secured using key based access control which implements obfuscation by inserting multiplexers as obfuscation cells into the design. The controlling key utilized here also act as the watermark representing the authorship of the IP. Due to the unavoidability of key the watermark is resistant to removal threats. The role of watermarking authority further reduces the threat of embedding attacks. The paper also suggests technique to locate the source of illegal redistribution of the IP core. These capabilities for watermarking and fingerprinting come at the cost of increase in area. The provision for buyer identification is optional and can be used for securing large systems. The existing IP protection methods based on watermarking and fingerprinting are passive protection methods which cannot prevent illegal access. This paper provides an activation mechanism using a key such that the proposed IP protection approach becomes an active protection method with facilities for access control, obfuscation, watermarking and fingerprinting.

REFERENCES

[1] Amr T. Abdel-Hamid, Sofiene Tahar and El Mostapha Aboulhamid, "A Survey on IP Watermarking Techniques", *Design Automation for Embedded Systems*, Vol. 9, No. 3, pp. 211-227, 2014.

[2] Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy, Available at: http://www.inta.org/Communications/Documents/2017_Frontier_Report.pdf.

[3] VSI Alliance, "VSI Alliance Architecture Document: Version 1.0", Available at: http://www.fpga.world/_hdl/1/VSI/vsi-or.pdf, 1997.

[4] Debasri Saha and Susmita Sur-Kolay, "SoC: A Real Platform for IP Reuse, IP Infringement, and IP Protection", *VLSI Design*, Vol. 2011, No. 5, pp. 1-10, 2011.

[5] VSI Alliance, "Intellectual Property Protection: Schemes, Alternatives and Discussion", Available at: http://www.univ-st-etienne.fr/salware/Bibliography_Salware/IP%20Watermarking/Article/VSIAlliance2000WhitePaper.pdf.

[6] Jarrod A. Roy, Farinaz Koushanfar and Igor L. Markov, "EPIC: Ending Piracy of Integrated Circuits", *Proceedings of Conference on Design, Automation and Test in Europe*, pp. 1069-1074, 2008.

[7] Rajat Subhra Chakraborty and Swarup Bhunia, "RTL Hardware IP Protection using Key-based Control and Data Flow Obfuscation", *Proceedings of 23rd International Conference on VLSI Design*, pp. 405-410, 2010.

[8] Jiliang Zhang, "A Practical Logic Obfuscation Technique for Hardware Security", *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 24, No. 3, pp. 1193-1197, 2016.

[9] I. Torunoglu and E. Charbon, "Watermarking based Copy-Right Protection of Sequential Functions", *IEEE Journal of Solid State Circuits*, Vol. 35, No. 3, pp. 434-440, 2016.

[10] Y.C. Fan and H.W. Tsao, "Watermarking for Intellectual Property Protection", *Electronics Letters*, Vol. 39, No. 18, pp. 1316-1318, 2003.

[11] Aijiao Cui, Chip-Hong Chang, Sofiene Tahar and Amr T. Abdel-Hamid, "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, pp. 678-690, 2011.

[12] Encarnacin Castillo, Uwe Meyer-Baese, Antonio Garcia, Luis Parrilla and Antonio Lloris, "IPP@ HDL: Efficient Intellectual Property Protection Scheme for IP Cores", *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 15, No. 5, pp. 578-591, 2014.

[13] Qiang Liu, Wenqing Ji, Qi Chen and Terrence Mak, "IP Protection of Mesh NoCs using Square Spiral Routing", *IEEE Transactions on Very Large Scale Integration Systems*, Vol. 24, No. 4, pp. 1560-1573, 2016.

[14] Chip-Hong Chang and Li Zhang, "A Blind Dynamic Fingerprinting Technique for Sequential Circuit Intellectual Property Protection", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 33, No. 1, pp. 76-89, 2014.