Modified Counter Based Approach for Digital Watermarking of Sequential Circuits

Ankur Bhardwaj, Shamim Akhter

Abstract- Digital Watermarking techniques are applied on sequential circuits to track the misuse of Intellectual Property(IP) core of a design. Watermarking technique for sequential circuits was first proposed by Oliviera. The issue of duplicate states in the technique proposed by Oliviera was addressed by counter based approach given by Siddhant. Counter based approach also had its demerits and it was not very practical. In this paper, an improved counter based watermarking technique have been proposed which eliminates the drawbacks of previous watermarking techniques. The synthesis and simulation of proposed techniques has been done using Xilinx ISE and ModelSim simulator respectively.

Index terms- Watermarking; intellectual property; sequential circuits; counter

I. INTRODUCTION

With the rise of Internet of things, reuse of semiconductor IP cores in electronic devices and there interconnection to other devices in the network is increasing day by day. A semiconductor IP core is a block of logic that may be used for different application. As a particular IP core may be used by different users, there are high chances for unauthorized use and piracy. Hence the protection of these IPs should be the top priority to protect their illegal or unauthorized use. Its modification or illegal distribution may pose a serious threat to the economy of company.

There are different ways to protect the IPs and to prevent there unauthorized use[1]. When the owner uses legal means like copyright, patents etc. to prevent the illegal distribution of IP, it is called deterrent approach. This method when applied to semiconductor IP core cannot prevent it from physical attacks on IP, like modification of design. Another method is to protect the design by using some encryption. This allows only authorized user to use owner's IP core. It is called protection approach. This approach also has its limitations as one may not be sure that the user will not distribute the key to unauthorized parties. For the physical protection and to avoid illegal distribution of IP cores, it is important to detect and track the illegal usage of the design using techniques like watermarking and fingerprinting. This approach is known as detection approach. This paper focuses on Watermarking techniques for the detection of illegal use.

Watermarking is a technique of embedding some information in a signal to prevent its unauthorized use. It has been widely used to protect the copyright of texts, images and videos. The watermarking technique in digital sequential circuits was first coined by Oliviera[2]. In sequential circuits, watermarking is done by embedding a unique signature in the design, which is only known to the creator of IP core. In event of unauthorized use, this signature can be recovered using appropriate detection method and authorship can be established in court of law. There are different techniques to watermark an IP core available in open literature. Some techniques are used to watermark hard IP cores(IP cores present in the form of transistor level representation of circuit)[1-3] and some techniques are used to watermark soft IP cores(IP core present in the form of synthesizable HDL code)[4]. Watermarking can be classified as Static or Dynamic watermarking[1]. To detect static watermarking[5-9], the design needs to be reverse engineered till the abstraction level at which the watermark was embedded to check if the constraints of designer's watermark are satisfied. Reverse engineering is a difficult and expensive process especially for complex designs. So, dynamic watermarking is used [10-17], in which the embedded watermark can be detected by observing the output or state transitions of a particular design when a unique input is given. Dynamic watermarking is done at the architectural level of Finite state machines(FSM)[11-14] design by modifying its state transition graph(STG). Constraint based watermarking is an example of static watermarking whereas property implant [1] is an example of Dynamic watermarking. In constraint based watermarking, the signature used to watermark the design puts some constraints on the functionality of design. These constraints must be satisfied for watermark detection whereas in property implant the watermark is embedded within the design without changing its original functionality. In this paper, a new and better dynamic watermarking technique has been proposed and compared with other dynamic watermarking techniques.

This paper is divided in five sections. In section II, related work has been discussed. Proposed watermarking technique is discussed in section III. In section IV simulation results are presented. Section V concludes the paper.

II. RELATED WORK

The watermarking technique proposed by Oliviera[2] is known as property implanting. In this technique, the watermark is embedded in State Transition Graph(STG) of FSM in such a way that the original functionality of FSM is not altered. This is done by adding extra states in original state transition diagram, such that whenever a unique signature sequence is given as input to the FSM, it traverses unique sequence of states(watermarking states). If correct signature is not given, then there is no possibility that those sequence of states are

Revised Manuscript Received on June 10, 2019.

Ankur Bhardwaj, Electronics and Communication Engineering, Jaypee Institute of Information Technology, Noida, India.

Shamim Akhter, Electronics and Communication Engineering, Jaypee Institute of Information Technology, Noida, India.

traversed. These watermarking states are added by using an algorithm[2] which decides the number of watermarking states and their connection with original STG, so that original functionality of our design is not changed. The property implanting approach was applied on a sequence detector by Shaila[18] as shown in Fig.1**.** In this technique all the original Q states are copied and V states are created. Both original and copied states are interconnected via R states as shown in Fig.1. These R states are traversed completely only when signature sequence is applied.

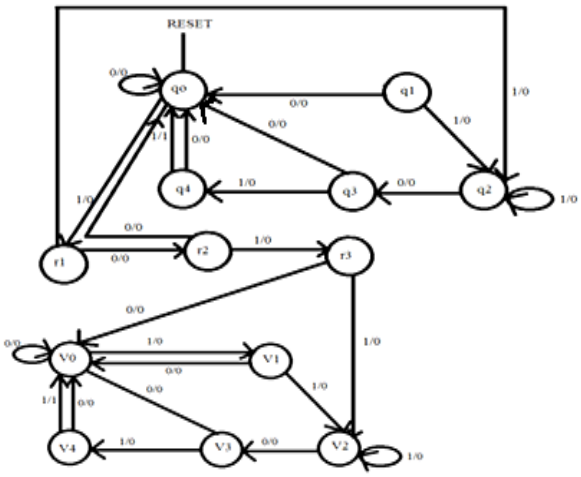

Fig. 1 Property implanting watermark[18]

The issue in this technique is that it requires need to duplicate all the original states of STG which increases the hardware over head as well as complexity in a design. Also this technique requires separate detection circuit to monitor the state traversal of R states. To monitor the R states the state variables must be taken as output pins, which is not a practical thing when we are trying to hide the signature. The strength of this type of watermarking depends on the strength of signature sequence and the encryption technique applied on signature. To reduce the number of states used in this technique, a counter based watermarking approach was suggested by Sidhhant Malik[3] as shown in Fig. 2.

In this technique, the watermarking sequence is an iteration of input sequence of a particular length. A counter is designed to count the number of times this sequence is traversed. In Fig. 2 “100” is taken as the input sequence for watermark. At state c if “0” is given as input ,the counter increases by 1. Now, the length of this sequence and count value is decided by the required signature complexity. For example, if count is taken as 3 and watermarking sequence is taken as “100”, then the signature will be “100100100”. Once count equals 3, output z becomes high , indicating the detection of watermark.

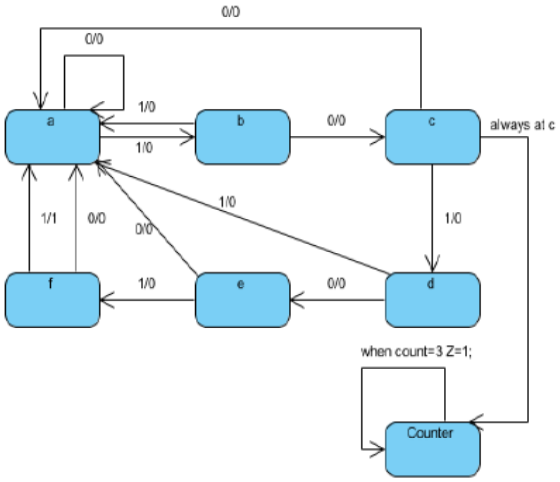

Fig. 2 Counter based watermarking

There are some problems with counter based approach. Firstly, count value may increase at input sequence other than, “100”. In Fig. 2 , if we give an input sequence ”11100” then also count value will increase and false watermark detection may occur. So, there must be some logic to check that uniqueness of sequence is preserved. According to the algorithm, even if the watermark sequence is not given successively, counter value can still increase by 1, since counter increments every time state c is reached. Hence the watermark strength becomes too weak. The limitations of counter based technique and property implanting technique has been removed in proposed technique.

III. PROPOSED WORK

The proposed watermarking technique uses a watermarking module as shown in Fig. 3, which consists of a sequence detector(shown by STG of FSM1) for detection of sequence and a counter for counting number of times sequence is detected. The FSM that is watermarked is also taken to be a sequence detector which detects ”11011” shown as FSM2 in Fig.4. FSM2 operates on enable signal E1. This watermarking technique does not require separate detection circuit as it is a part of watermarked circuit. An enable input (E0) is provided, whenever watermark detection is required. Complete architecture of the proposed watermarking technique for a signature sequence”1010101” is shown in Fig. 3. The algorithm of proposed technique can be described by following steps-

i. Watermarking module will start working only when E0=1.
ii. Every time the sequence is detected by sequence detector FSM1, counter increments by 1.
iii. When count equals the pre-decided number of iterations of sequence, signal x goes high.
iv. If at any point of time before competing n iterations, wrong sequence is entered, counter is reset to 0.
v. If x=1, CL i.e, the clock signal for FSM to be watermarked is disabled by clock gating and FSM2 will store its present state and next state.
vi. If the Next state of FSM2 is Qsxc, where Qsxc is the state reached in Q on applying the signature sequence

n times successively, the output pin gives an output.

vii. If Next state is not equal to Qsxc, it means entered signature is not correct and detection will fail.

viii. The msb of output(OUT[n]) obtained during watermark detection will be complement of the output msb during normal operation(O[n]) of FSM2, if same sequence was applied

ix. In case of false detection of watermark, the shortest sequence which gives the desired output will be the signature sequence.

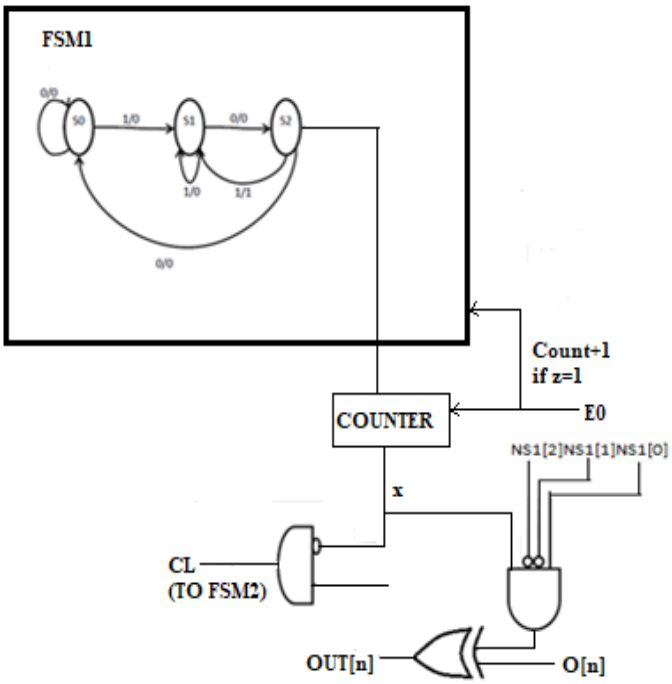

Fig. 3 Watermarking module for proposed technique

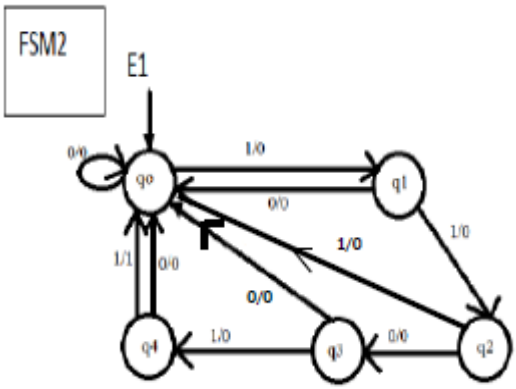

Fig. 4 STG of sequence detector for sequence "11011"

When compared to property implanting algorithm, proposed algorithm eliminates the use of separate detection circuit, as watermark is detected through the msb of FSM2 output. Also, only one extra input(E0) is required for enabling watermark detection and there is no need for extra outputs to monitor State transitions as in case of property implanting watermarking technique[2]. For complex designs, the number of states and hardware overhead is considerably reduced in proposed technique as there is no need to copy all the states of FSM2. The strength of watermark can be increased by increasing signature length or by increasing count value or both as in case of counter based technique[3]. The proposed technique reduces the possibility of false detection as the counter gets reset every time wrong sequence is entered. If somehow counter counts to desired value and x becomes high , in that case the current next state value of FSM2 is compared to predetermined next state value and if both are not same , it means that signature sequence was wrong and detection will fail. This way the proposed algorithm eliminates the limitation of the property implanting and counter based watermarking technique.

IV. SIMULATION AND SYNTHESIS RESULTS

The proposed technique is applied on the sequence detector of Fig. 4. The sequence is taken as "101" and count value is taken as 3. So, complete signature sequence will be "1010101" and the simulation for watermark detection is shown in Fig. 5. PS and NS are present states and next states of FSM1, PS1 and NS1 are present states and next states of FSM2. Rest of the signals has same function as explained in the proposed algorithm.

A. Watermark Detection

For detection of watermark, both E0 and E1 are kept high. An input sequence "1010101" is given at the input. The count increases by one each time "101" is detected. When count becomes"11", x becomes high and CL is disabled by clock gating. Both PS1 and NS1 will be stored and OUT will become high indicating the detection of watermark.

B. Normal Operation

For normal operation of FSM2, watermarking module is disabled by making E0=0. The simulation result for normal operation for input sequence "11011" is shown in Fig. 6. The watermarking module is disabled in this case and FSM2 gives a high output once sequence is detected.

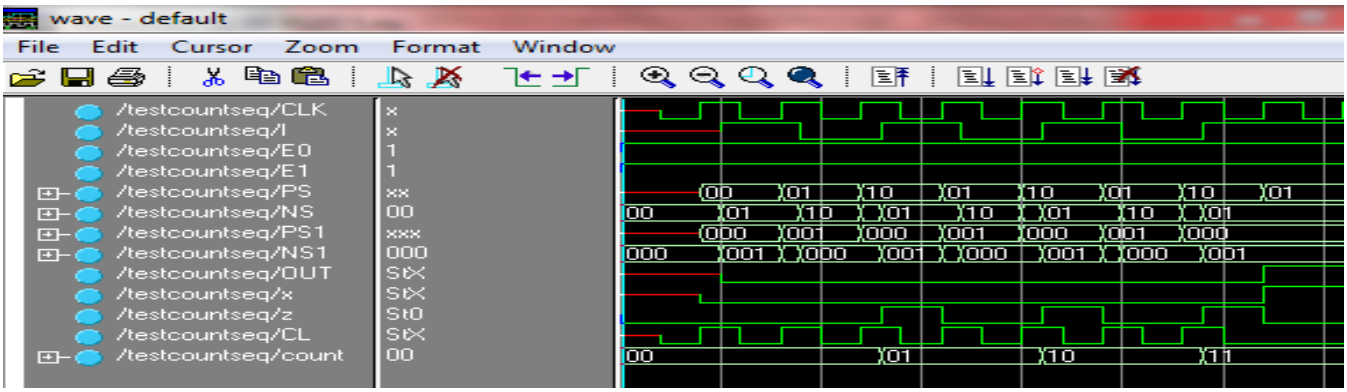

Fig. 5 Simulation result for watermark detection

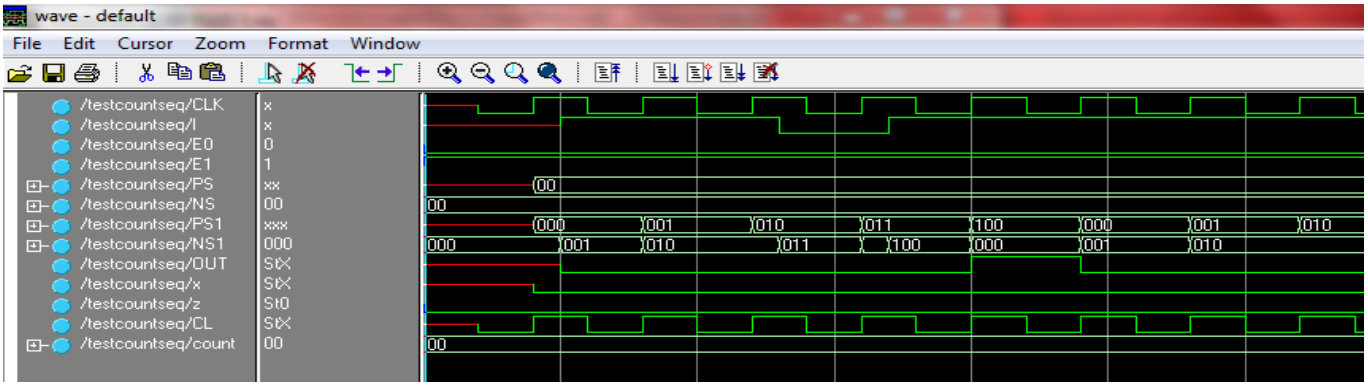

Fig. 6 Simulation result for normal operation of Sequence detector(FSM2) for input "11011"

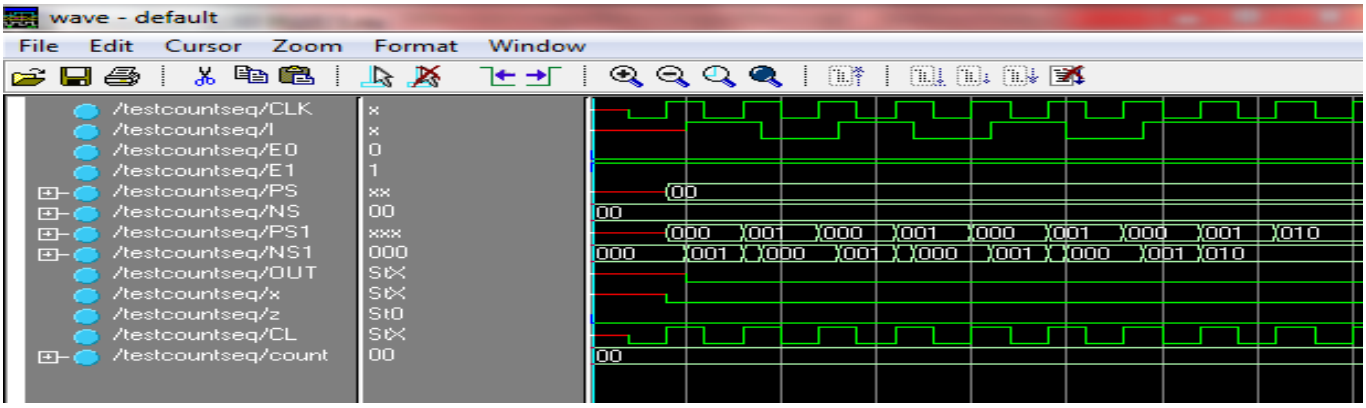

Fig. 7 Simulation result for normal operation of Sequence detector(FSM2) for input"1010101"

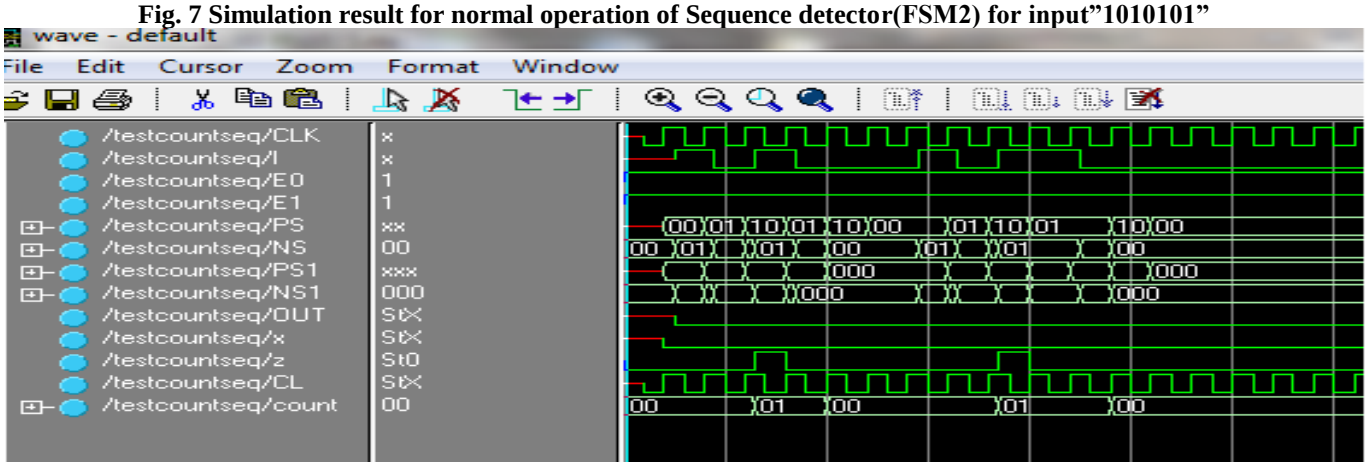

Fig. 8 Simulation result for wrong signature input

When an input sequence "1010101" equivalent to signature sequence is applied to FSM2 during normal operation, the output of FSM2 comes out to be 0 as shown in Fig. 7.

This shows that during watermark detection the output after giving signature sequence was complement of the output for same input sequence during normal operation. In case the signature is not given correctly, the counter will get reset and FSM2 will perform normal operation as shown in Fig. 8.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

V. CONCLUSION

It can be seen from simulation results that the proposed algorithm creates and detects the watermark using same circuit instead of using a separate detection module as in the case of property implanting algorithm. Also the possibility of false detection is reduced significantly as counter gets reset every time wrong signature is given and the detection depends on count value as well as state variables of FSM2. In case of counter based algorithm, counter can increment even if signature bits "101" is not given successively and there is no provision of counter reset. Further, the synthesis results of Table I show that the hardware utilization of watermarking module of Fig.4 with signature sequence"10101" is approximately same as that of property implanting technique with signature sequence"101". The input to output path delay, however is significantly reduced in proposed technique as compared to property implanting technique a shown in Table II. Hence, proposed technique is better in terms of area, delay and watermark strength as compared to both property implanting and counter based watermarking technique.

Table I- Cell usage comparison

Cell Usage	Property Implanting(watermark creation)	Proposed Technique(water mark creation and detection)
BEL	21	23
Flip Flops/Latches	13	12
Clock Buffers	2	2
IO Buffers	2	3

Table II- Input to Output path delay comparison

Data Path	Property Implanting	Proposed Technique
Input to Output	5.868 ns	4.104 ns

REFERENCES

1. Intellectual Property Protection Development Working Group, " intellectual Property Protection: Schemes, Alternatives and Discussion", VSI Alliance**,** White Paper version 1.1, August 2001.
2. Arlindo L. Oliveira," Techniques for the Creation of Digital Watermarks in Sequential Circuit Designs", IEEE Transactions On Computer-Aided Design Of Integrated Circuits And Systems, Vol. 20, No. 9, pp: 1101-1116, September 2001.
3. Siddhant Malik," Counter Based Approach To Intellectual Property Protection In Sequential Circuits And Comparison With Existing Approach", 2014 International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), pp: 48 – 53, 2014.
4. TingtingYu, Yuesheng Zhu "A new watermarking method for soft IP protection", International Conference on Consumer Electronics, Communications and Networks (CECNet), pp.: 3839 – 3842, 2011.
5. D. Kirovski, Y. Y. Hwang, M. Potkonjak, and J. Cong, "Protecting combinational logic synthesis solutions," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 25, no. 12, pp. 2687–2696, Dec. 2006.
6. A. Cui, C. H. Chang, and S. Tahar, "IP watermarking using incremental technology mapping at logic synthesis level," IEEE Trans. Comput.- Aided Design Integr. Circuits Syst., vol. 27, no. 9, pp. 1565–1570, Sep. 2008.
7. A. Cui and C. H. Chang, "Stego-signature at logic synthesis level for digital design IP protection," in Proc. IEEE Int. Symp. Circuits Syst., pp. 4611–4614, May 2006.
8. A. Cui and C. H. Chang, "Watermarking for IP protection through template substitution at logic synthesis level," in Proc. IEEE Int. Symp. Circuits Syst., pp. 3687–3690, May 2007.
9. A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Constraintbased watermarking techniques for design IP protection," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 20, no. 10, pp. 1236– 1252, Oct. 2001.
10. H. J. Kim, W. H. Mangione-Smith, and M. Potkonjak, "Protecting ownership rights of a lossless image coder through hierarchical watermarking," in Proc. Workshop Signal Process. Syst., pp. 73–82, Oct. 1998.
11. A. Rashid, J. Asher, W. H. Mangione-Smith, and M. Potkonjak, "Hierarchical watermarking for protection of DSP filter cores," in Proc. IEEE Custom Integr. Circuits Conf., pp. 39–42, May 1999.
12. A. L. Oliveira, "Robust techniques for watermarking sequential circuit designs," in Proc. IEEE/ACM Des. Autom.Conf., pp. 837– 842 Jun. 1999.
13. I. Torunoglu and E. Charbon, "Watermarking-based copyright protection of sequential functions," IEEE J. Solid-State Circuits, vol. 35, no. 3, pp. 434–440, Feb. 2000.
14. A. T. Abdel-Hamid, S. Tahar, and E. M. Aboulhamid, "A public-key watermarking technique for IP designs," in Proc. Des.Autom. Test Eur., vol. 1, pp. 330–335, Mar. 2005.
15. A. Cui and C. H. Chang, "Intellectual property authentication by watermarking scan chain in design-for-testability flow," in Proc. IEEE Int. Symp. Circuits Syst, pp. 2645–2648, May 2008.
16. A. Cui and C. H. Chang, "An improved publicly detectable watermarking scheme based on scan chain ordering," in Proc. IEEE Int. Symp. Circuits Syst., pp. 29–32 May 2009.
17. C. H. Chang and A. Cui, "Synthesis-for-testability watermarking for field authentication of VLSI intellectual property," IEEE Trans. Circuits Syst.-I, vol. 57, no. 7, pp. 1618–1630, Jul. 2010.
18. Shaila Subbaraman , P. S. Nandgawe," Intellectual Property Protection of Sequential Circuits Using Digital Watermarking", First International Conference on Industrial and Information Systems, ICIIS 2006, Sri Lanka, pp.556-560, 8 - 11 August 2006.

AUTHORS PROFILE

Ankur Bhardwaj was born at Meerut, Uttar Pradesh, India on January 04,1990. He received B.Tech degree from Gautam Buddh Technichal University, Lucknow (June 2011), M.tech degree from DTU Delhi(2013) and currently pursuing PhD degree from Jaypee Institute of Information Technology, Noida**.** He joined Jaypee Institute of Information Technology, Noida, in July 2013 as a Lecturer. Presently he is Assistant Professor in the Department of Electronics and Communication Engineering, Jaypee Institute of Information Technology, Sector 62, Noida.

Shamim Akhter was born at Chittaranjan, West Bengal, India on January 15, 1979. He received B.Tech degree from ZHCET, AMU(June 2001), M.Tech degree from IIT Delhi (Dec 2002) and Ph.D degree from Jaypee Institute of Information Technology, Noida, India(March 2015). He joined Jaypee Institute of Information Technology, Noida, in April 2003 as a Lecturer. Since then he is engaged in teaching, research and development in the field of VLSI digital circuits design. He has published research papers in reputed International Journals. Besides he has also published papers in International Conferences in India and abroad. Presently he is Assistant Professor in the Department of Electronics and Communication Engineering, Jaypee Institute of Information Technology, Sector 62, Noida.