International Journal of Multidisciplinary and Current Educational Research (IJMCER)
ISSN: 2581-7027 ||Volume|| 2 ||Issue|| 5 ||Pages|| 82-95||2020||

Watermarking of Multi-mode Counter Circuit using Hardware Efficient Algorithm

[1,]Jeebananda Panda, [2,]Divant Jain, [3,]Lavi Tanwar, [4,]Sunil Kumar
[1,2,3]*Department of Electronics and Communication Engineering, Delhi Technological University, Delhi 110042, India* [4]*Department of Electronics and Communication Engineering, Maharaja Agrasen Institute of Technology, Delhi 110086, India*

ABSTRACT: The paper proposes a property implant watermarking technique for the hardware designers to protect their Intellectual Property (IP) in digital integrated circuits. The technique introduces some extra states in the State Transition Graph of the digital circuit to embed the watermark. These extra states can further be used to prove the ownership in case of IP theft. The proposed scheme is intended for Finite State Machine (FSM) sequential circuit only due to the omnipresence of FSM. The efficiency of the proposed scheme can be seen in terms of less number of additional gates requirement and tough detection and removal of watermark from the original circuit. To demonstrate the process of watermarking, the proposed algorithm makes use of a Multipurpose Counter as a vehicle. The paper also presents the HDL simulations for different length of signature bits to ease the comparison between watermarked and non-watermarked circuits.

KEYWORDS: Property Implant technique, State Transition Graph, Intellectual Property, Finite State Machine, Signature sequence.

I. INTRODUCTION

With the emergence of newer technologies in semiconductor processing, the complexity in IC design and fabrication has increased. The whole process of hardware designing, starting from the designing to fabrication, is cumbersome and expensive task. From an economical point of view, today most of the ICs are tested and verified using computer aided design tools before going for the fabrication processes. In the whole design process there are possibilities that some of the important and critical file generated by the computer software may get stolen or got in the wrong hands. The designer must protect his design by securing his design in the first place itself. This task can be accomplished by embedding a unique code, or watermark, exploiting the IP's unique features. Fundamental requirements for a watermark scheme are that it be 1) Invisible, i.e., the watermark should be invisible to the end user, and it should not disturb the functionality of the original circuit, 2) Robust, i.e., the watermark is hard to remove and if infringed upon, it will destroy the circuit's intended functionality, and 3) Detectable, i.e., the watermark can be easily detected by the owner, which can be used to prove the ownership in case of IP theft. The signature sequence is only known to the owner.

A short overview of different watermarking schemes and their comparisons are presented in [1]. The paper also discusses major considerations and issues related with watermarking schemes, such as possible attacks on watermark, embedding cost, etc. One of the most popular schemes suited for IP cores are the constraint-based watermarks introduced in [2] and [3]. In these schemes the watermark is applied by defining additional design constraints which do not interfere with the functionality of the IP core, but will be utilised for embedding the watermark. The concept of watermarking has been proposed for many different levels of the hardware design process. The paper [4] and [5] discusses different algorithms which can be used to generate and detect watermarks at different abstraction levels. Paper [5], in particular presents the watermarking scheme at physical design level, where the watermark is embedded by using features characteristics of physical design level.

In [6] to [13], schemes have been proposed to embed the watermark at the top abstraction level of design i.e. at the behavioral level, where the designer describes the functionality of the design. The papers [6] and [7], presents a watermarking scheme for the sequential circuits, here the watermark is embedded by duplicating all the states in the State Transition Graph (STG) of the original circuit and adding new watermarking states. The modified STG thus obtained, contains watermarking states plus the duplicate states. This methodology, however robust and easily detectable, is not hardware efficient i.e. it would be impractical to use this scheme when there is large no. of states in the sequential circuit. In [8], the whole watermarking procedure, for the scheme presented in [6] and [7], has been illustrated through a sequence detector circuit. A modification to the scheme proposed in [6] and [7] is presented in [9] and [10]. Here the watermarking scheme is proved to be hardware efficient as compared to the original one.

It has been shown that in order to embed the watermark it is not necessary to duplicate all the original states and the scheme can be implemented using lesser no. of additional states. This reduces the hardware requirement manifolds. The paper shows the comparison between the modified scheme and the scheme using the results from [8] as a reference.The approaches in [11], [12] and [13], presents the watermarking scheme for finite state machine (FSM), here the watermark is implanted by exploiting some unutilized input vectors and modifying the states corresponding to these vectors to store the watermarking information. The watermark is thus detected by triggering a specific response with known input sequence.

The paper [14] presents a robust watermarking method for the audio signals using the invariance property of exponent moments technique to watermark the audio signals. The paper [15] presents a reversible image watermarking scheme in DWT domain, the scheme besides being robust, protects the high quality of the image from being tampered. A novel watermarking scheme for the digital contents using phase congruency techniques is presented in [16]. The papers [14-16] present IP protection of digital cover medium like audio and image. Even the design of a sequential machine can be an another form of digital cover medium or digital content whose IP also needs to be protected. In this paper, we will focus on the kind of watermarking scheme presented in [6] to [13] i.e. watermarking in the sequential circuits. We propose a modification to the watermarking scheme presented in [6] and [7]. The proposed scheme has been implemented with lesser no. of additional states required to embed the watermark and thus hardware efficient. Moreover, the scheme fulfils all the fundamentals requirements i.e. 1) Invisible, 2) Detectable and 3) Robust.The paper is organised in six sections. Section II presents a detailed description of the watermarking scheme proposed. Section III discusses the detection of presence of watermark in the circuit, followed by a brief discussion on robustness of the watermark. The implementation details of the watermarked circuit with different signature key bits are presented in section IV. Section V gives the experimental results obtained by simulating the Verilog HDL designs. Finally, section V concludes the paper.

II. WATERMARKING PROCEDURE

The watermark is embedded in the sequential circuit by introducing some extra states in the original state transition graph of the circuit. These states would be unique and will be used to detect the presence of watermark in the circuit.

For a given FSM let the set S = {s0, s1, . . .} represent the original states which describes the behaviour of the FSM. The set R = {r1, r2, . . .} is used to represent the watermarking states that will be used for detection of presence of the watermark in the circuit.The first step in watermarking process is to identify the secret key or signature for the given circuit. The key can be any arbitrary sequence of primary input combinations of the circuit. For example if there primary inputs, {x0, x1, x2}, then the sequence of input combinations can be represented as {y1, y2, y3, . . .} where {yi} represents a unique combination of inputs {x0, x1, x2}. But care should be taken not to take such a combination which is very common for the intended behaviour of the circuit i.e. it is advisable to take a combination which causes such states transitions which are rarely traversed as far as the normal functionality of the circuit is concerned. After the sequence input combination is finalised, we need to find the states which are traversed on applying that input combinations, let us denote these states by S' = {s'1, s'2, . . .}.

The steps to be followed to modify the state transition graph, in order to obtain a watermarked circuit are as follows:

a. Each state {ri} is formed by duplicating the state {s'i} and all its outgoing edges. Note that it is not necessary that all the states corresponding to the set {s'i} are different.

b. The outgoing edge from the starting state i.e. {s0} which corresponds to the transition {y1} is directed towards the state {r1}.

c. For the states {r1, r2, . . . , rn-1} the outgoing edge which corresponds to the transition {y2, y3, . . . , yn} is directed towards the states {r2, r3, . . . , rn}. Therefore every state {ri} has only one incoming edge, corresponding to the transitions {y1, y2, . . . ,yn}, and that also originating from the state {ri-1}.

d. All the outgoing edges from the states {r1, r2, . . . ,rn} which do not corresponds to the transitions {yi} are directed towards the original states {si}.

After the completion of the above procedure, we have a modified STG, which has watermark embedded in it. This modified sequential circuit follows all the fundamental requirements i.e. it is:

a. Invisible, meaning that the modified circuit has the same functionality as that of the original circuit.

b. Detectable, meaning that the watermark is easy to detect and prove the ownership in case of piracy.

c. Robust that is the watermark is hard to remove from the design.

In this paper we have used a multi-mode counter to demonstrate the watermarking procedure. A counter is a relatively simple sequential circuit and is easily available in the IC format by various vendors. Our multi-mode synchronous counter counts in three modes namely, 1) Binary, 2) Grey Code and 3) BCD Counter. It is a bidirectional counter i.e. it can count in both forward and backward directions. Further it has a synchronous reset and count enable pins, reset is used to set the counter in zero state and count enable is used to start or stop the counting. The STG of the counter is shown in figure 1 and the modified STG for an 18 bit watermark is shown in figure 2. Table 1 presents the relation between the present state, next state and the output for the circuit. We have shown the input as a three bit binary number, in which the LSB represents the "direction" input and the first two bits are for the "counter_type" i.e. the type of counting that the counter performs. The binary number {00} is assigned for binary counting, {01} is assigned for grey code counting and {10} is assigned for BCD counting. Further in figure 1, we have used colour scheme as – Blue, when output is '1'; Red, for grey code counting up; Magenta, for grey counting down; Black, for binary and BCD counting up and down. In figure 2, apart from these colours we have used colours – Green, for the transitions corresponding to the key or signature as input sequence i.e. {001, 011, 101, 010, 000, 100}; Orange, for the outgoing transitions from the watermarking states that do not result in a watermarking state as next state. The watermarking states are shown with a Yellow colour.

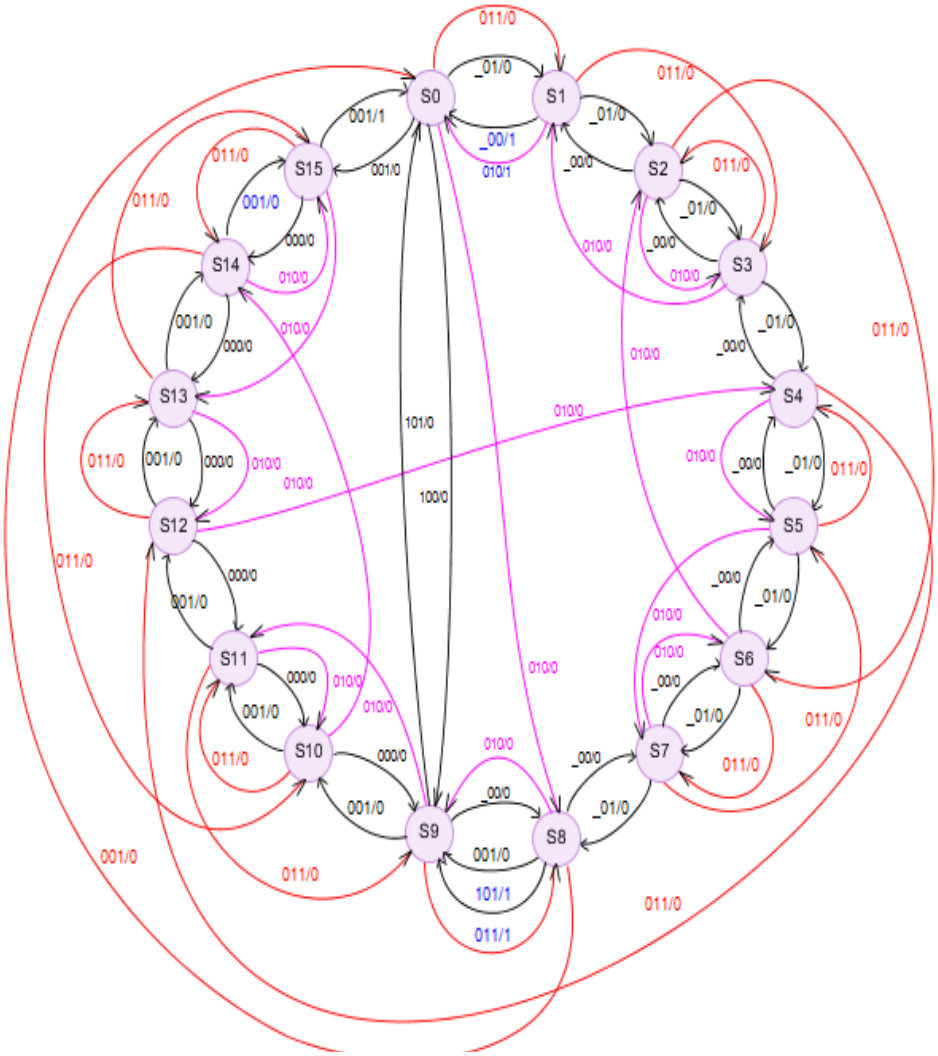

Figure 1. STG for the multipurpose counter circuit

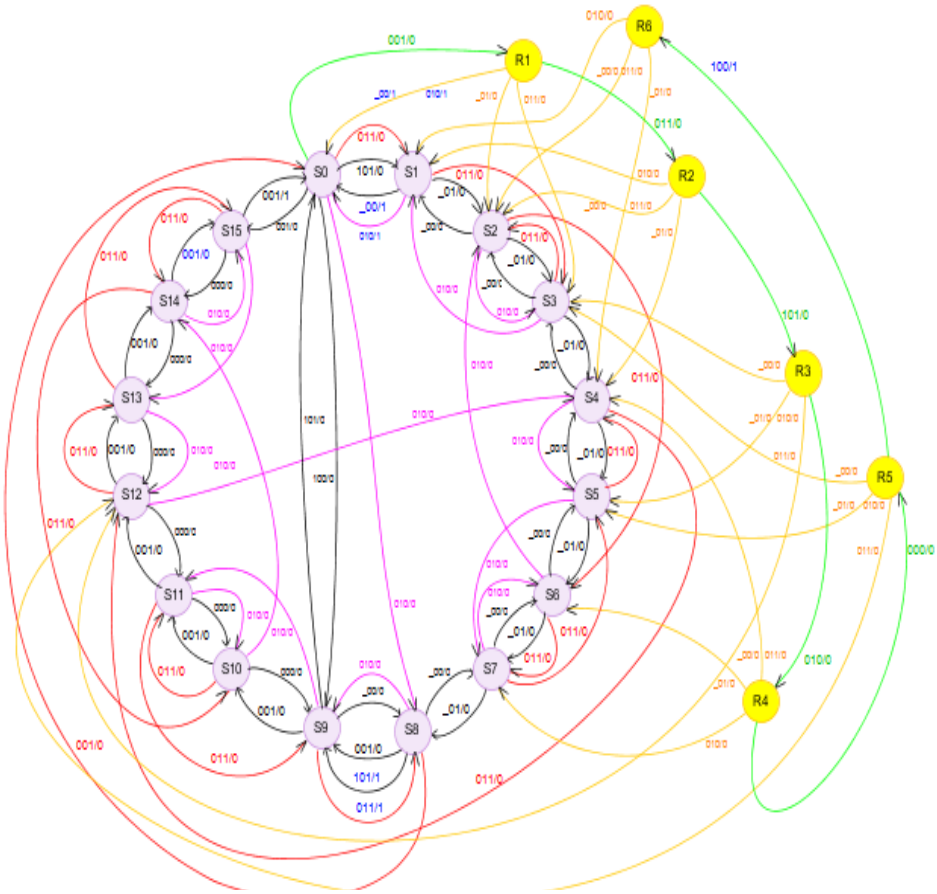

Figure 2. Modified STG for the multipurpose counter with 18-bit Watermark embedded in it

Table 1. State Table for the multipurpose counter

PRESENT STATE	NEXT STATE / OUTPUT						
	INPUTS						
	001	000	011	010	101	100	11_
S0	S1/0	S15/0	S1/0	S8/0	S1/0	S9/0	S0/0
S1	S2/0	S0/1	S3/0	S0/1	S2/0	S0/1	S0/0
S2	S3/0	S1/0	S6/0	S3/0	S3/0	S1/0	S0/0
S3	S4/0	S2/0	S2/0	S1/0	S4/0	S2/0	S0/0
S4	S5/0	S3/0	S12/0	S5/0	S5/0	S3/0	S0/0
S5	S6/0	S4/0	S4/0	S7/0	S6/0	S4/0	S0/0
S6	S7/0	S5/0	S7/0	S2/0	S7/0	S5/0	S0/0
S7	S8/0	S6/0	S5/0	S6/0	S8/0	S6/0	S0/0
S8	S9/0	S7/0	S0/0	S9/0	S9/1	S7/0	S0/0
S9	S10/0	S8/0	S8/1	S11/0	S0/0	S8/0	S0/0
S10	S11/0	S9/0	S11/0	S14/0	S0/0	S0/0	S0/0
S11	S12/0	S10/0	S9/0	S10/0	S0/0	S0/0	S0/0
S12	S13/0	S11/0	S13/0	S4/0	S0/0	S0/0	S0/0
S13	S14/0	S12/0	S15/0	S12/0	S0/0	S0/0	S0/0
S14	S15/1	S13/0	S10/0	S15/0	S0/0	S0/0	S0/0
S15	S0/0	S14/0	S14/0	S13/0	S0/0	S0/0	S0/0

As can be seen from the figure there are four watermarking states which are represented as {r1, r2, r3, r4, r5, r6}. There are two primary inputs. These two inputs make up three bits in total which are represented as {x0, x1, x2}, the first two bits represent the two bit input – "count_type" and the third bit is for the second input – "direction". Now the sequence of input combination or the signature or key chosen for the circuit shown in figure 2 is {y1, y2, y3, y4, y5, y6} = {001, 011, 101, 010, 000, 100}. On application of

this sequence of input the sequence of states traversed will be {s0, r1, r2, r3, r4, r5, r6}. Note that these states can only be traversed by this particular key and cannot be traversed by any other sequence of inputs.

III. DETECTION OF WATERMARK

The additional states, that are added to the STG of the original circuit, will be used for the detection of watermark embedded in the circuit and hence to prove the ownership in case of piracy. These additional states are thus also termed as watermarking states. From figure 2 it can be observed that states denoted by {r1, r2, r3, r4, r5, r6} represents the watermarking states. Further, it can be observed that these states have only one incoming edge and multiple outgoing edges. Moreover, every transition corresponding to the incoming edge in the watermarking states corresponds to the sequence of inputs {yi} i.e. the signature or the key. The above two properties can be stated as:

a. Every watermarking state can be reached only by its previous state i.e. the state {ri} can only be reached from the state {ri-1}.

b. Each and every watermarking state can only be traversed if and only if we apply the signature or key at the input correctly.

These two properties will be used to detect the presence of watermark. Note also that no other input sequence can result in transition through all the watermarking states. Thus only the secret key or the signature, which only the designer knows, can make the circuit transit through the watermarking states. Hence in case of piracy, the designer can use this key in the court-of-law and claim the ownership of the design.Figure 3 shows the simulation result of detection of watermark present in the modified circuit presented in figure 2. In this case, we have assigned binary value to the watermarking states as {r1 = 10000, r2 = 10001, r3 = 10010, r4 = 10011, r5 = 10100, r6 = 10101}. As can be seen from the figure 3, that on application of the input sequence as {001, 011, 101, 010, 000, 100}, which is the key chosen for this circuit, the sequence of states traversed are {s0, r1, r2, r3, r4, r5, r6} and the output will be 1 on the next rising edge of the clock after the state {r6} is reached, this is used only as an indication that the end of watermarking states has been reached. The states are represented in hexadecimal numbers in the figure as {00, 10, 11, 12, 13, 14, 15}. Similarly simulation for different keys sizes are shown in figure 4-8. For a 15 bit signature, the sequence of states traversed will be {s0, r1, r2, r3, r4, r5} on applying {001, 011, 101, 010, 000} as signature, this has been shown in figure 4. For a 12 bit signature, the sequence of states traversed will be {s0, r1, r2, r3, r4} on applying {001, 011, 101, 010} as signature, this has been shown in figure 5. Similarly for 9 and 6 bit signatures the sequence of states traversed will be {s0, r1, r2, r3} and {s0, r1, r2} on applying {001, 011, 101} and {001, 011} as signatures respectively, this has been depicted in figures 6 and 7. It should be noted that the robustness of the circuit decreases with decreasing size of the key.

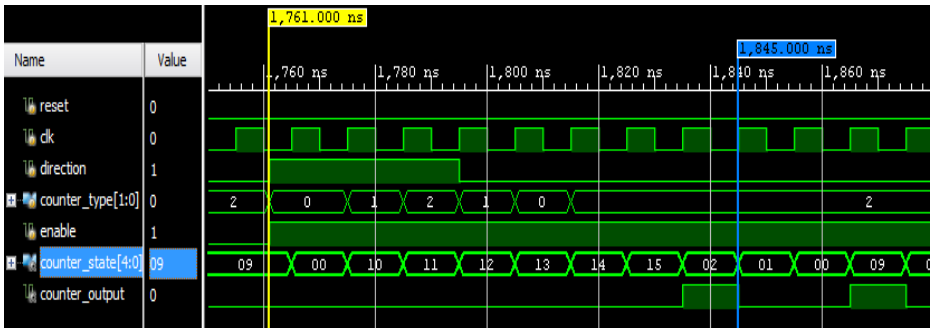

Figure 3. Detection of Watermark (18-bit watermarked circuit)

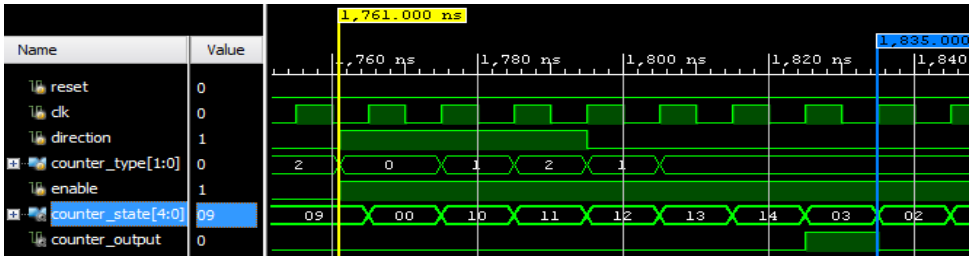

Figure 4. Detection of Watermark (15-bit watermarked circuit)

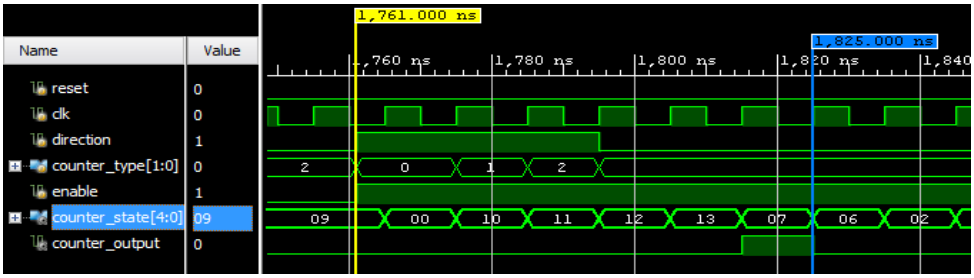

Figure 5. Detection of Watermark (12-bit watermarked circuit)

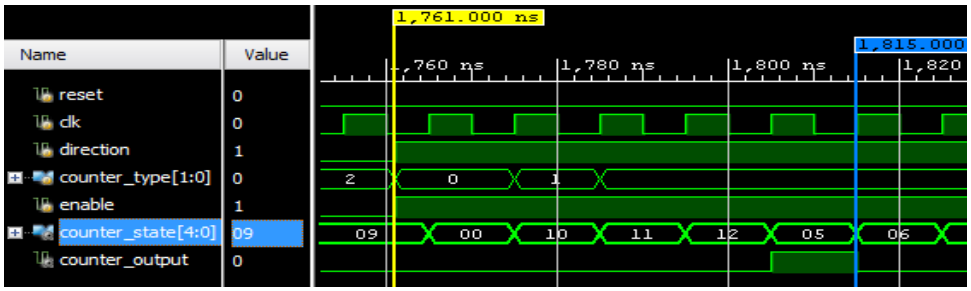

Figure 6. Detection of Watermark (9-bit watermarked circuit)

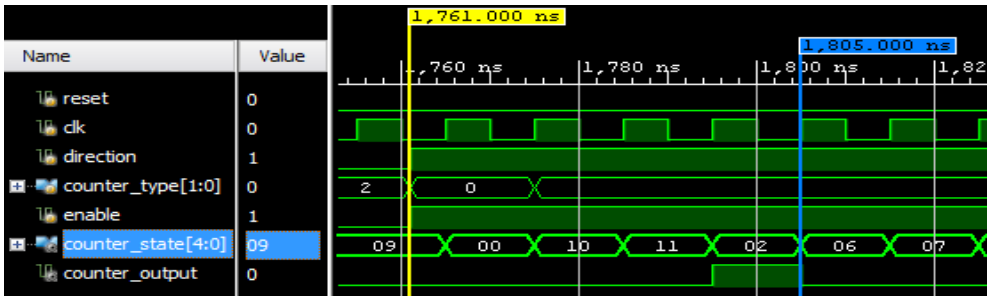

Figure 7. Detection of Watermark (6-bit watermarked circuit)

Thus, the watermark is easy to detect and at the same time is robust i.e. if it is infringed upon, that will result in damage to the circuit and its functionality. The watermarking states form an integral part of the circuit and are necessary for the normal functioning of the circuit. This property can be verified from the simulations (presented in section V) of the watermarked circuit for various operations. Here the difference between the state transition of the watermarked and non-watermarked circuits should be noted. Thus, due to combinatorial complexity, it is not feasible to erase or delete the watermark from the FSM with finite resources and time. Therefore, the presented watermark scheme is robust to attacks and easy to apply.

IV. IMPLEMENTATION OF WATERMARK

To illustrate the formulation of an efficient watermarking signature sequence, we have used multi-mode counter as the base sequential circuit. The modified STG of the counter circuit for five different sizes of keys (that varies from 6 to 18 bits) were simulated and analysed in order to formulate a most efficient signature sequence with minimal hardware overweight and as efficient as un-watermarked circuit in terms of timing parameters. Although the security of the circuit increases with the size of the key, but care should be taken that the watermark is embedded with minimal hardware overhead. Thus there is a trade-off between the key size and hardware overhead associated with it. Figures 8-11 and figure 2, shows the modified STG for different sizes of keys. Hardware requirements and timing specifications for each of the modified circuit is given in section V. For an 18 bit watermark, we have selected the key as input sequence {001, 011, 101, 010, 000, 100}. This input sequence is a rare set of input combination for anyone to imagine and hence can be used as a signature to watermark the design. On the other hand, for a 6 bit watermark the signature sequence selected is {001, 011}, although it is not a common operation, but it is less secure as compared to the 18 bit watermark because of less no. input sequence. Thus, as far as the security of the watermark is concerned, the watermark with more no. of input bits is more secure.

As can be seen from the figure 2 and 8-11 with increasing signature sizes the number of watermarking states, shown in yellow, increases and this will increase the overall hardware requirement for the circuit.

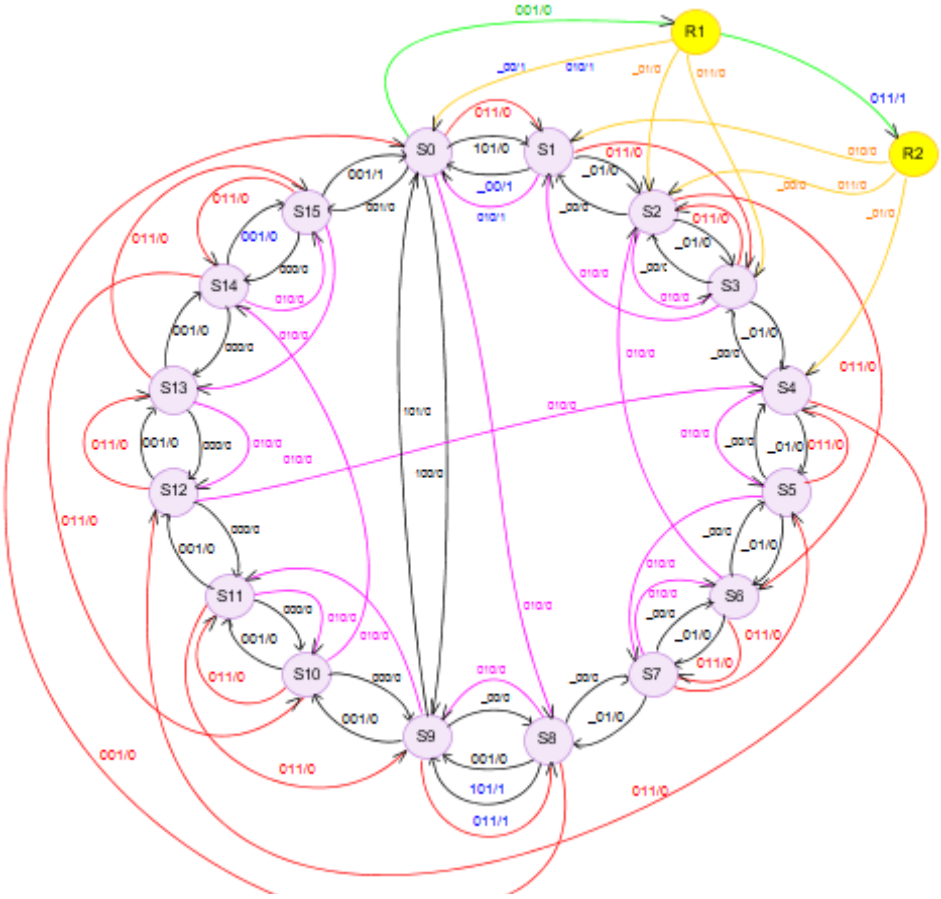

Figure 8. Modified STG for the multipurpose counter with 6-bit Watermark embedded in it

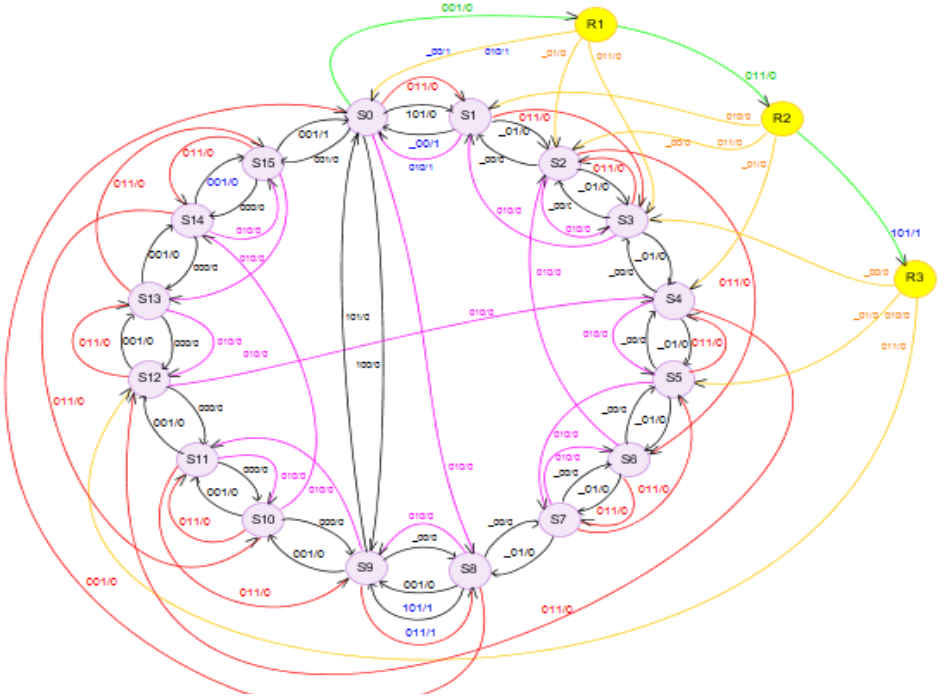

Figure 9. Modified STG for the multipurpose counter with 9-bit Watermark embedded in it

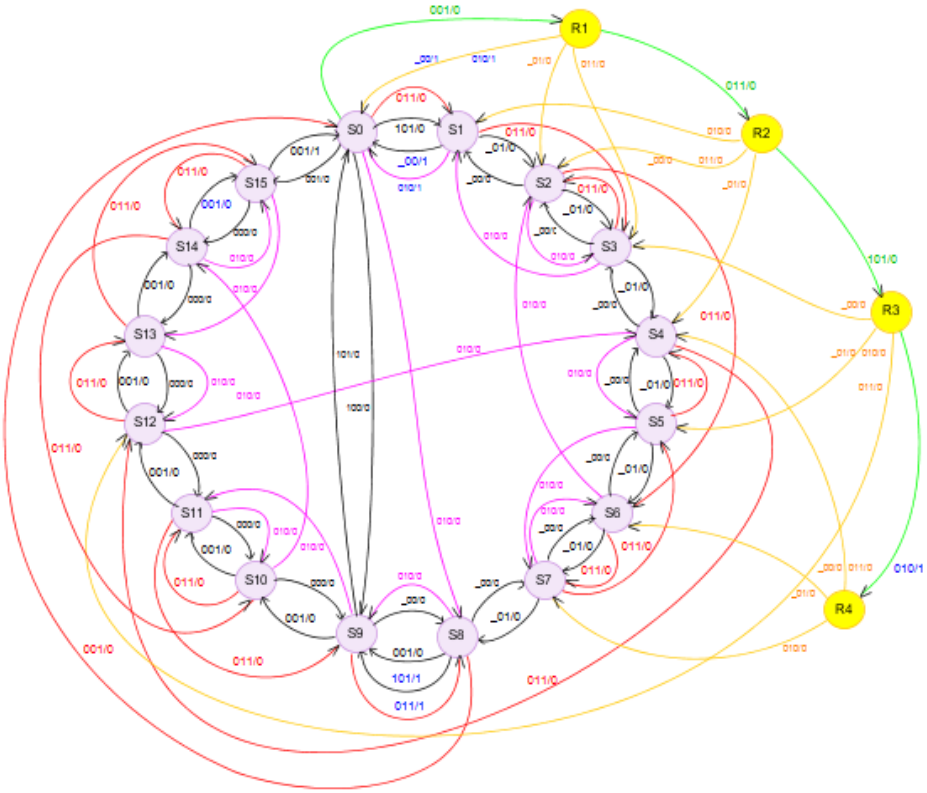

Figure 10. Modified STG for the multipurpose counter with 12-bit Watermark embedded in it

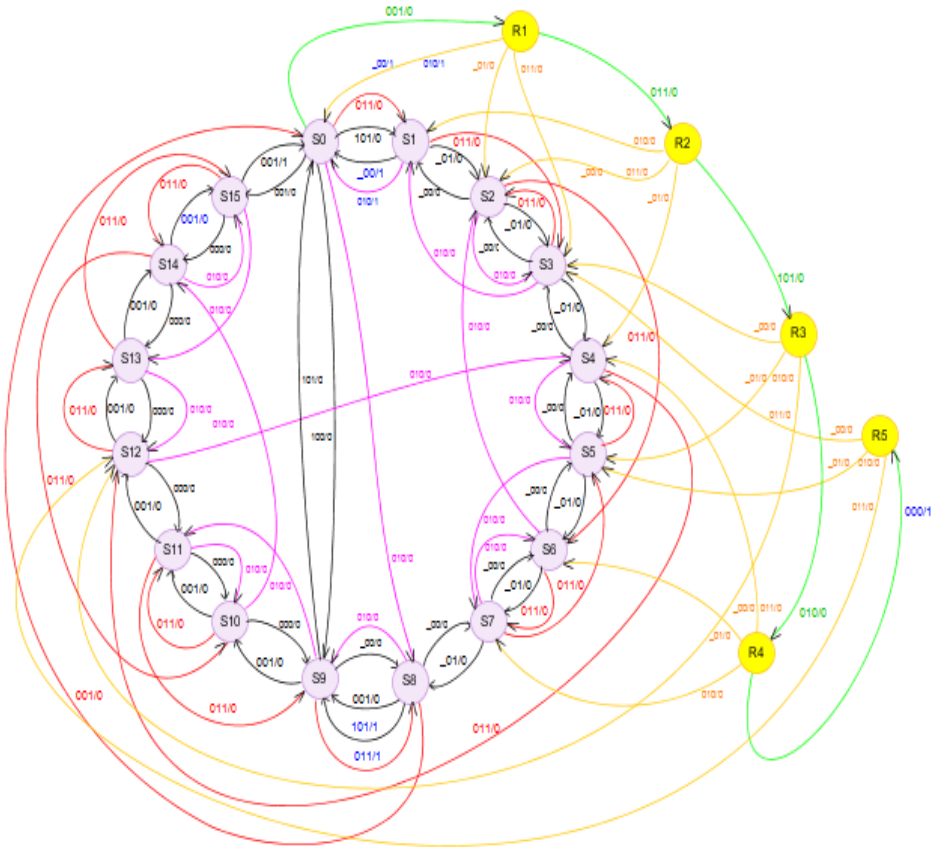

Figure 11. Modified STG for the multipurpose counter with 15-bit Watermark embedded in it

V. EXPERIMENTAL RESULTS

The design of the multi-mode counter was implemented using the Verilog HDL. The Xilinx Vivado Suit software was used synthesize and simulate the design. Two separate modules for the watermarked and non-watermarked circuit were made. The simulation result for the three modes of counting, shown in figure 12-17, are for the original circuit i.e. non-watermarked circuit. Figure 18-23 shows the simulation results for the watermarked circuit. It can be observed that simulations for original circuit exactly match the simulations for the watermarked circuit as far as the functionality of the circuit is concerned. It is an important result that verifies the invisibility of the watermark i.e. the end user should not be aware that a watermark is embedded in the circuit. However, it should be noted that the states that are traversed on applying the same input to both the circuits vary greatly.

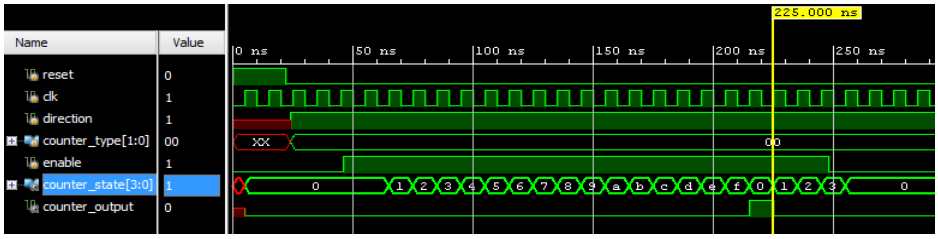

Figure 12. Binary counting up (original circuit)

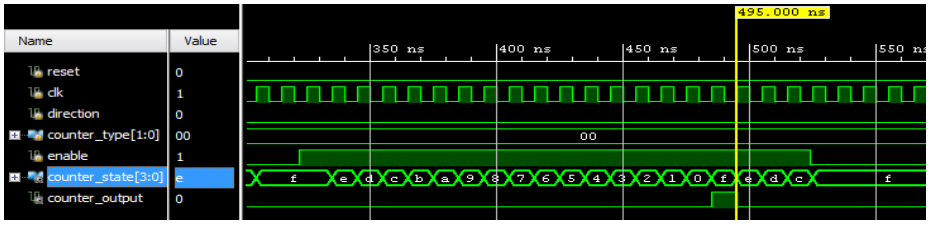

Figure 13. Binary counting down (original circuit)

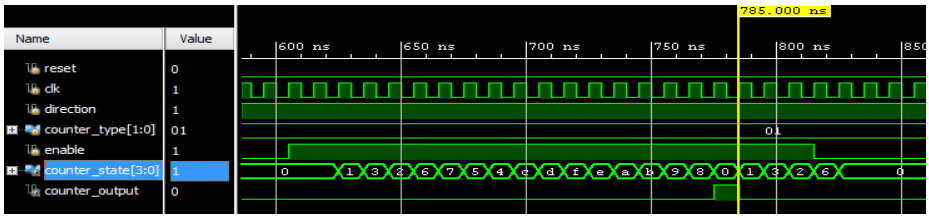

Figure 14. Gray code counting up (original circuit)

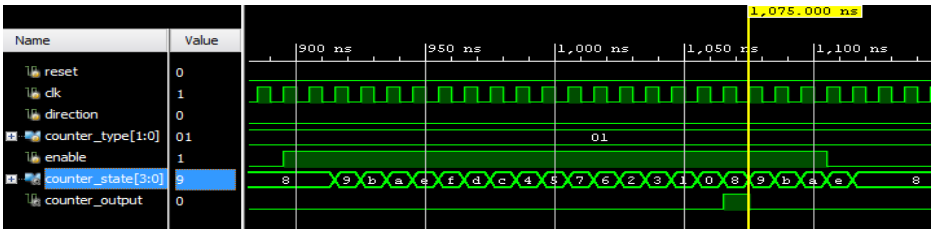

Figure 15. Gray code counting down (original circuit)

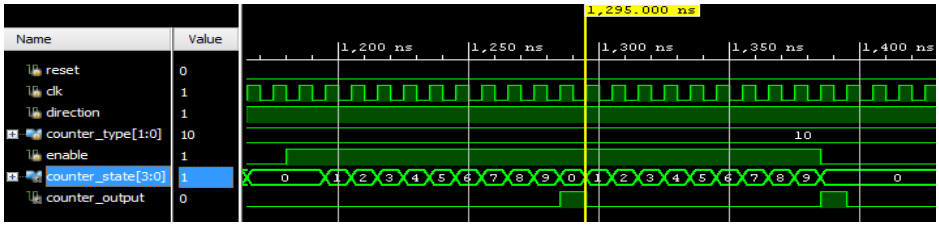

Figure 16. BCD counting up (original circuit)

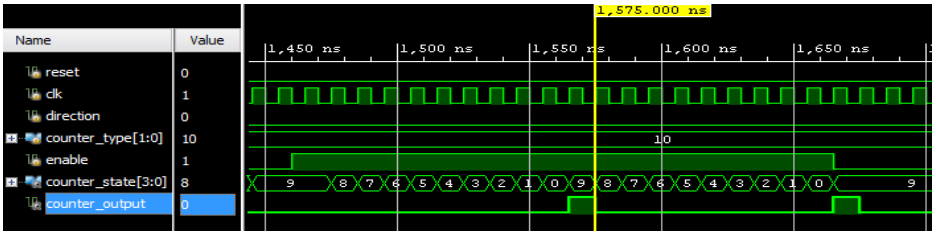

Figure 17. BCD counting down (original circuit)

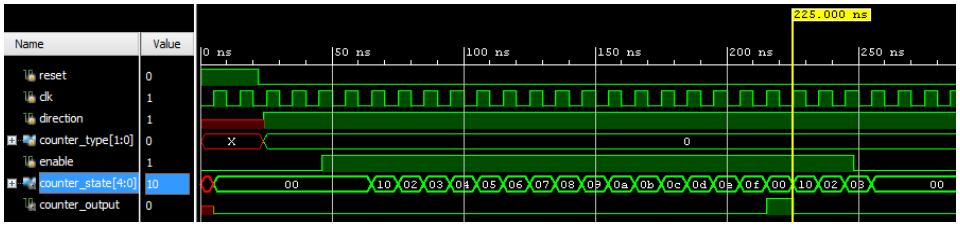

Figure 18. Binary counting up (watermarked circuit)

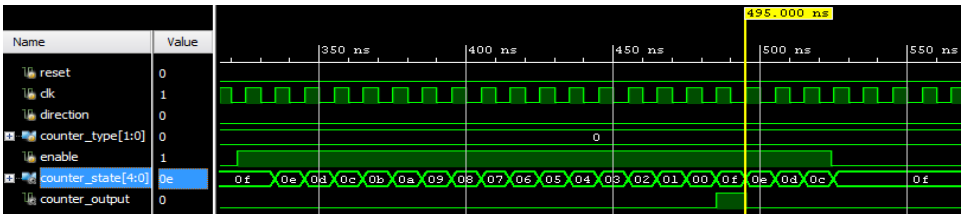

Figure 19. Binary counting down (watermarked circuit)

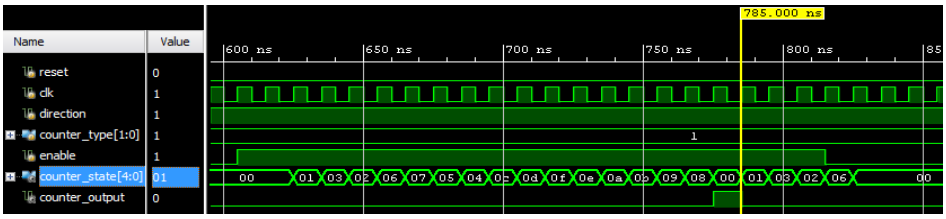

Figure 20. Gray code counting up (watermarked circuit)

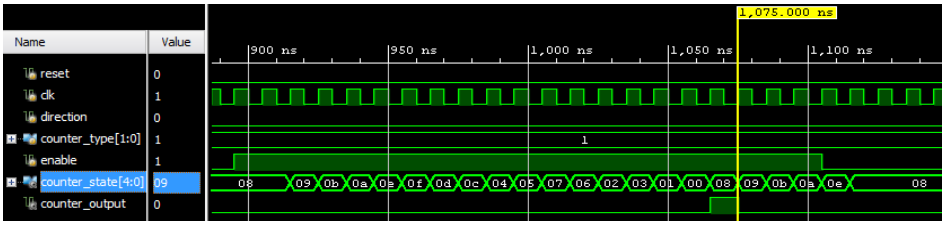

Figure 21. Gray code counting down (watermarked circuit)

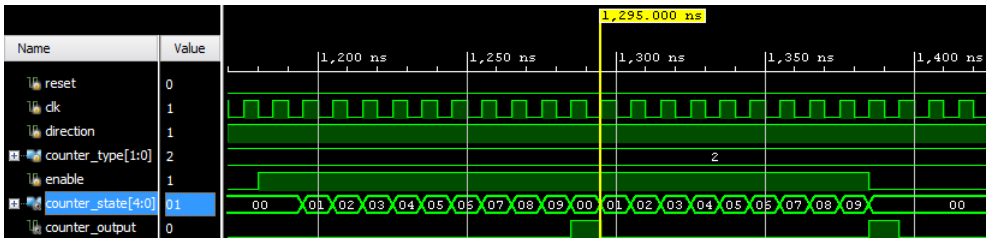

Figure 22. BCD counting up (watermarked circuit)

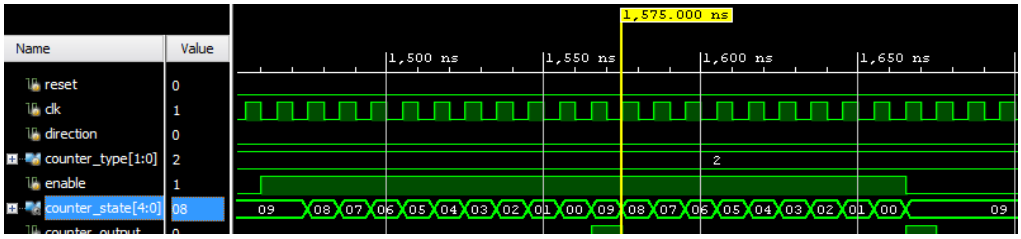

Figure 23. BCD counting down (watermarked circuit)

The hardware requirements and timing specifications for the original design and the watermarked design with different key sizes are given in table 2 and table 3. It can be seen that the modified circuit requires only few extra hardware components as compared to the original circuit. Further, it should be emphasized on the fact that among the different watermarked designs, the best would be to use the one with 12 bit watermarking key. From table 2, it can be observed that among the five available signatures the 12 bit and 15 bit watermarked circuits can be used efficiently. For others signatures, either the lengths are too short (6 and 9 bit) or the signature hardware requirements are more (15 bit). From table 3, we see that among the 12 bit and 15 bit signature, the 12 bit signature is more close to the original design parameters. Thus, the watermarked design with 12 bit signature has its parameters more close to the original design and also 12 bit signature length is large enough that it can be efficiently used to watermark the circuit.

Table 2. Hardware Requirements

Functional Unit	Original Design	Watermarked design				
		6 bit	9 bit	12 bit	15 bit	18 bit
Flip Flop & Latches	7	8	8	8	8	8
IO Buffers	12	12	12	12	12	12
Clock Buffers	1	1	1	1	1	1
Multiplexers	1	0	1	0	2	4
LUTs	27	40	41	42	40	50

Table 3. Timing Specifications

Timing Specification	Original Design	Watermarked design				
		6 bit	9 bit	12 bit	15 bit	18 bit
Maximum Frequency (MHz)	269.26	262.64	268.40	265.91	263.07	265.51
Minimum input arrival time before clock (ns)	5.088	5.143	5.722	5.135	5.388	5.333
Maximum output required time after clock (ns)	4.089	4.131	4.110	4.131	5.731	5.786

It should be noted that if the counter circuit presented in this paper would have been watermarked using the scheme presented in [6] and [7], we would require double the original states plus the watermarking states as the total number of states for the watermarked circuit, which would be 36 states. The proposed method, on the other hand, requires only the watermarking states as the additional states i.e. a total of 20 states for the watermarked STG. Thus the proposed scheme requires much less states and therefore can be implemented with minimal hardware overhead.

VI. CONCLUSION

The Verilog HDL simulation for all the five modified STGs with different length of signature sequence proves the functional similarity of the watermarked and non-watermarked circuits, which fulfils the foremost condition of any watermarking scheme. It also has been shown that the watermark can be easily applied and detected to prove the ownership in case of any kind of piracy of the original design.

Moreover, the watermarking scheme is robust and if it is infringed upon, it will destroy the intended behaviour of the design and hence the whole circuit. Finally, it has been shown that the signature key should be selected in such a way that it minimise the hardware overhead caused and at the same time rare and large enough that it is not possible for anyone, except the owner, to access the key and use it to prove the authorship of the design. Base on the simulation results, it is observed that the modified STG with 12 bit signature sequence needs very few additional hardware overhead with very close timing parameters to that of un-watermarked circuit.As a future scope, this type of analysis can be applied to any FSM to obtain an efficient watermark signature sequence, which can be used to watermark the original FSM in order to obtain a hardware efficient watermarked FSM by property implant scheme. The similar technique can also be adopted for watermarking of commonly used digital blocks in digital system design.

REFERENCES

[1] A.T.A. Hamid, S. TaharE.M.Aboulhamid,"IP Watermarking Techniques: Survey and Comparison", 3rd IEEE International Workshop on System-on-Chip for Real-Time Applications, IEEE, Canada,**(2003)**, pp. 60–65.

[2] A.B. Kahng, J. Lach,W.H.M. Smith, S.Mantik,L.L. Markov,M. Potkonjak, P. Tucker, H. Wang, G. Wolfe, "Watermarking Techniques for Intellectual Property Protection", 35th Design Automation Conf., IEEE, USA,**(1998)**,pp. 776–781.

[3] D. Kirovski, Y.Y. Hwang,M. Potkonjak,J. Cong, J,"Intellectual Property Protection by Watermarking Combinational Logic Synthesis Solutions", IEEE/ACM Int. Conf. on Computer Aided Design, IEEE, USA,**(1998)**,pp. 194–198.

[4] E. Charbon, "Hierarchical Watermarking in IC Design", Proceedings of IEEE Custom Integrated Circuit Conf., IEEE, USA,**(1998)**, pp. 295–298.

[5] E. Charbon, I. Torunoglu,"Watermarking Layout Topologies",Proceedings of IEEE Asia and South-Pacific Design Automation Conf., IEEE, Hong Kong,**(1999)**, pp. 213–216.

[6] A.L. Oliveira,"Techniques for the Creation of Digital Watermarks in Sequential Circuit Design", IEEE Transactions on Computer-aided Design of Integrated Circuits and Systems, vol. 20, no. 9,**(2001)**, pp. 1101–1117.

[7] A.L. Oliveira,"Robust Techniques for Watermarking Sequential Circuit Designs", Proceedings of 36th IEEE Design Automation Conf., IEEE, USA,**(1999)**, pp. 837–842.

[8] S. Subbaraman, P.S. Nandgawe,"Intellectual Property Protection of Sequential Circuits Using Digital Watermarking", 1st Int. Conf. on Industrial and Information Systems, IEEE, Sri Lanka,**(2006)**, pp. 556–560.

[9] J. Panda, S. Malik, N. Pandey, A. Bhattacharyya,"A Modified Hardware Efficient Watermarking Scheme for Intellectual Property Protection in Sequential Circuits", Int. Journal of Electronics Communication and Computer Engineering, vol. 5, no.4, **(2014)**, pp. 741– 746.

[10] J. Panda, A. Bharadwaj, N. Pandey, A. Bhattacharyya,"Hardware efficient watermarking technique for finite state sequential circuit using STG", Int. Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, vol. 2, no. 7, **(2014)**, pp.1670–1674.

[11] I. Torunoglu, E. Charbon,"Watermarking-Based Copyright Protection of Sequential Functions", IEEE Journal of Solid-State Circuits,vol. 35, no. 3, **(2000)**, pp. 434-440.

[12] A. Cui, C.H. Chang, S. Tahar, A.T.A. 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, **(2011)**, pp. 678–690.

[13] M. Lewandowski, R. Meana, M. Morrison, S. Katkoori, "A Novel Method for Watermarking Sequential Circuits", IEEE International Symposium on Hardware-Oriented Security and Trust, IEEE, USA,**(2012)**, pp. 21–24.

[14] X.Y. Wang, Q.L. Shi, S.M. Wang,H.Y. Yang, "A blind robust digital watermarking using invariant exponent moments", International Journal of Electronics and Communications, vol. 70, no. 4, **(2016)**, pp. 416-426.

[15] T.S. Nguyen, C.C. Chang, X.Q. Yang,"A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain", International Journal of Electronics and Communications, vol. 70, no. 8,**(2016)**, pp. 1055–1061.

[16] M.R. Nayak, J. Bag, S. Sarkar, S.K. Sarkar, "Hardware implementation of a novel water marking algorithm based on phase congruency and singular value decomposition technique", International Journal of Electronics and Communications, vol. 71, **(2017)**,pp. 1–8.

Authors

Jeebananda Panda born on 15th Feb, 1968 in Odisha, India. He got graduated in Electrical engineering and subsequently in Electronics and Communication Engineering in 1988 and 1989 respectively. He got his M.E degree in Applied Electronics specialization from Bharathiyar University in 1992 and got his Ph.D. degree from University of Delhi. Presently working as Professor in the Department of Electronics and Communication Engineering, Delhi Technological University, Delhi, India. His field of research is Watermarking of Digital Data.

Divant Jain born in Delhi, India, in 1995. He did hisB.Tech in Electronics and Communication Engineering from Delhi Technological University, Delhi, India. His areas of interests are in RISC processors and computer architecture.

Lavi Tanwar born in Delhi, India, in 1992.Presently working as an Assistant Professor in the Department of Electronics & Communication Engineering,Delhi Technological University, Delhi, India and also pursuing PhD in the field of Digital Watermarking from Delhi Technological University. She received 5-year Integrated B.Tech (Electronics and Communication Engineering) + M.Tech (Intelligent Systems and Robotics) degree from Gautam Buddha University, Greater Noida, Uttar Pradesh, India in 2015.

Sunil Kumar born on 10th March 1970. He graduated in Electronics and Communication Engineering from Nagpur University. He got his M.Tech in ECE from Delhi University and Ph.D from Singhania University. Presently working as Professor and Head of the Department of Electronics and Communication Engineering, Maharaja Agrasen Institute of Technology, Delhi, India. His field of research are image processing and digital watermarking.