A New FSM Watermarking Method to Making Authorship Proof for Intellectual Property of Sequential Circuit Design Using STG

Arunkumar.P, Shangari.B
(Department Of ECE, Anna University, Tamilnadu
(Department Of ECE, Nandha Engineering College, Tamilnadu

ABSTRACT: *Finite state machines (FSMs) are mainly used for design an sequential circuits. In this paper, a new FSM watermarking method is introduced to make the authorship information of a designing circuits. To overcome the vulnerability attack and minimize the design error, the Digital watermark bits are seamlessly introduced into the outputs of the existing and free transitions of state transition graph (STG). To offers a high degree of tamper resistance and provides an easy and non invasive copy detection.The assignment of reserved literals is exploited to minimize the overhead of watermarking and make the watermarked FSM fallible upon removal of any pseudo input variable. A direct and convenient detection scheme is also proposed to allow the watermark on the FSM to be publicly detectable. Experimental results an acceptably low overheads with higher tamper resilience and stronger authorship owner proof in comparison with related watermarking schemes for sequential functions. IP providers are in pressing need of a convenient means to track the illegal redistribution of the sold IPs. This method is a great approach to protect a VLSI design against IP infringement has to embedding a signature that can only be uniquely generated by the IP author into the design during the process of its creation.*

Keywords: *Finite state machine (FSM), intellectual property (IP) protection, IP watermarking and state transition graph (STG).*

I. INTRODUCTION

A new dynamic watermarking method is proposed. The watermark is embedded in the state transitions of FSM at the behavioral level. As a FSM design is usually Specified by a STG or other than a behavioral descriptions that can be easily translated into STG, the watermark is embedded into the STG of any size and remains a property of FSM after the watermarked design is synthesized and optimized into circuit net list [6]. The authorship can be directly verified even after the downstream integrated circuit design processes by running the watermarked FSM with a specific code sequence. The proposed watermarking scheme is robust against state reduction attacks. It is different from other transition based embedding methods in that it has lower embedding overhead and has overcome the vulnerability of auxiliary inputs which are inevitably introduced if the embedding capacity is limited, especially for completely specified FSM. The weaknesses of the existing FSM watermarking scheme to be overcome in this paper . There is no easy way to publicly detect the Existence of watermark, once the FSM is integrated into a chip and packaged since the test signals can be traced after the chip is packaged and the scan path provides controlled accesses to all internal states [8]. This paper also proposes an alternative approach to allow the authorship proof of watermarked FSM to be verified off chip by making it a part of the test kernel. The proposed watermarking scheme thus makes the authorship proof harder to erase and the IP authorship easier to verify.

II. PRINCIPLE

A watermark on a bank note has a different transparency than the rest of the note when a light is shined on it. However, this method is useless in the digital world. Currently there are various techniques for embedding digital watermarks. Basically, they all digitally write desired information directly onto images or audio data in such a manner that the images or audio data are not damaged. Embedding a watermark should not result in a significant increase or reduction in the original data [7]. Digital watermarks are added to images or audio data in such a way that they are invisible or inaudible and unidentifiable by human eye or ear. Furthermore, they can be embedded in content with a variety of file formats. Digital watermarking is the content protection method for the multimedia era. Digital watermarking is applicable to any type of digital content, including still images, animation, and audio data [4]. It is easy to embed watermarks in material that has a comparatively high redundancy level such as color still images, animation, and audio data; however, it is difficult to embed watermarks in material with a low redundancy level, such as black-and-white still images. Solve this problem, we developed a technique for embedding digital watermarks in black and white still images and a softwareapplications.

III. PROPOSED SYSTEM

Dynamic watermarking enables the embedded information to be detected from the output without reverse engineering by running the protected design with a specific code sequence. Dynamic watermarking is typically performed in the state transition graph (STG) of finite state machine (FSM), in the architectural level of digital signal processors or at the design-for-test ability stage[2]. FSM watermarking embeds the signature at a higher (behavioral/RT) level of design abstraction whereas the latter normally embeds the signature after logic synthesis. The authorship can be directly verified even after the downstream integrated circuit design processes by running the watermarked FSM with a specific code sequence. As extracting the STG from a gate level netlist is computationally impractical for large circuits, there are limited options for an attacker to remove or hide the watermark from the watermarked design netlist or netlist obtained by reverse engineering its downstream design. The proposed watermarking scheme is robust against state reduction attacks [5]. It is different from other transition based embedding methods in that it has lower embedding overhead and has overcome the vulnerability of auxiliary inputs which are inevitably introduced if the embedding capacity is limited, especially for completely specified FSM.

IV. RELATED WORK

A.WATERMARK LIFECYCLE

Depending on the ability of the watermark to withstand normal signal processing operations, digital watermarking can be categorized as robust, fragile and semi-fragile watermarking. Robust watermarks are detectable even after some image processing operations has been performed on the watermarked image such as image scaling, bending, and cropping, and so on. Robust watermarks are mainly used for copyright protection [2]. The implement was designed using similar methods that were used in the implementation of the MD5 hash algorithm which is to be published. Fragile watermarks became invalid even if a slight modification is done to the watermarked image. Fragile watermarks are mainly used for authentication purpose. Semi-fragile watermarks allow some acceptable distortion to the watermarked image [9]. Beyond this acceptance level if any modification is done to the watermarked image, the watermark will not be detected.

B.WATERMARK DETECTION PROCESS

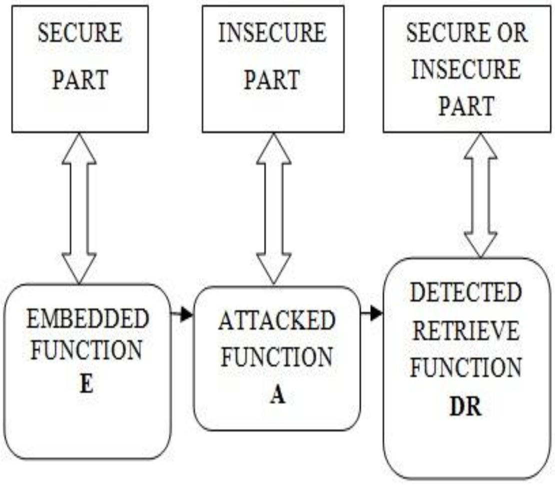


Fig1: Watermark Detecting Procedure

The original input image is not needed at the watermark detector. The watermarked image, the gain factor, and the seed value for creating the watermark are sufficient for the detection Fig.1 Block diagram of the detection process. We use two criteria for detection. A first criterion is similarity comparison result between *H* and *V* components for every 8x8 block. Second one is total average similarity measurement for every level [1]. The watermark detection in the DWT domain is implemented. The quotient is available in the register Q, and the remainder in A. The accumulator is implemented as a 14-bit register to accommodate a maximum value of 64 * 256. The maximum value occurs when each pixel in a 8 * 8 block assumes the value of pure white pixel gray value.

C.WATERMARK EXTRACT PROCESS

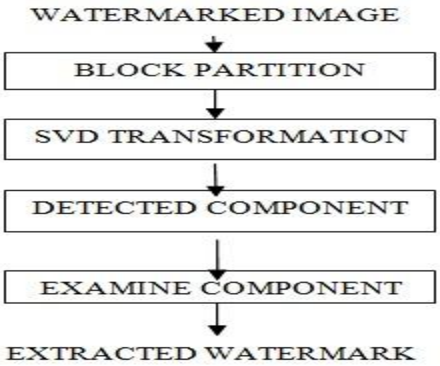


Fig2: Watermark Extracting Procedure

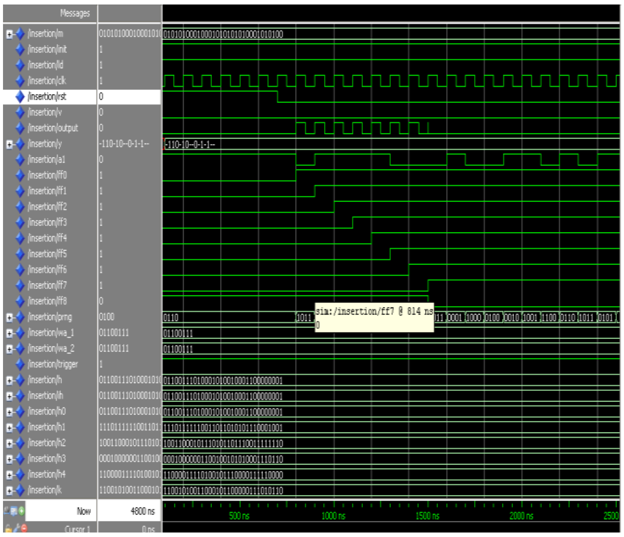
The watermark embedded at a higher level of design abstraction must survive the posterior optimizations so that the same IP distributed at all lower abstraction levels are protected. From the authorship verification perspective, IP watermarking can be classified into static watermarking and dynamic watermarking [3]. In the watermark detection phase, static watermarking requires the downstream design to be reverse engineered to the level where the watermark is embedded to show the additional constraints generated by the author's signature are satisfied. Digital watermarking can be categorized as robust, fragile and semi-fragile watermarking. Robust watermarks are detectable even after some image processing operations has been performed on the watermarked image such as image scaling, bending, and cropping, and so on.

V. APPLICATIONS AND ADVANTAGES

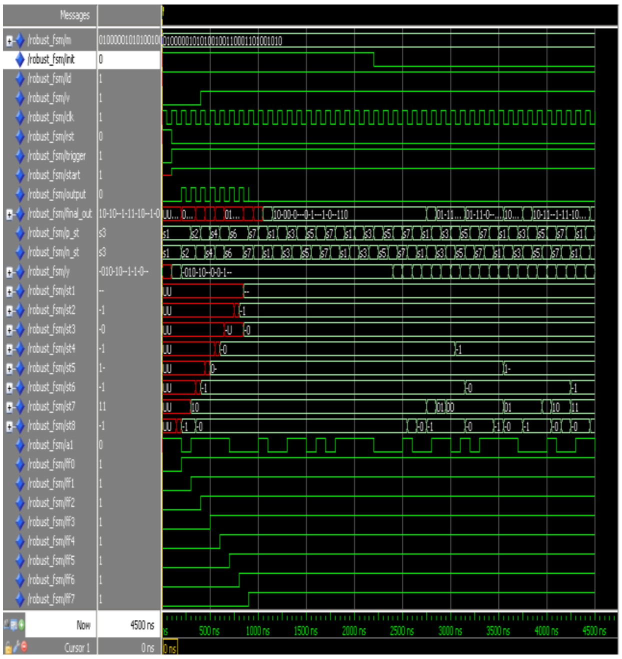
Depending on the ability of the watermark to withstand normal signal processing operations, digital watermarking can be categorized as robust, fragile and semi-fragile watermarking. Robust watermarks are detectable even after some image processing operations has been performed on the watermarked image such as image scaling, bending, and cropping, and so on. Robust watermarks are mainly used for copyright protection.

VI. SOFTWARE IMPLEMENTATION

WATERMARK INSERTION


```
Messages
/insertion/m        0101010001000101(  01010100010001010101010001010100
/insertion/init     1
/insertion/ld       1
/insertion/clk      1
/insertion/rst      0
/insertion/v        0
/insertion/output   0
/insertion/y        -110-10--0-1-1--   -110-10--0-1-1--
/insertion/a1       0
/insertion/ff0      1
/insertion/ff1      1
/insertion/ff2      1
/insertion/ff3      1
/insertion/ff4      1
/insertion/ff5      1
/insertion/ff6      1
/insertion/ff7      1
/insertion/ff8      0
/insertion/prng     0100               0110  1011  sim:/insertion/ff7 @ 814 ns 0
/insertion/wa_1     01100111           01100111
/insertion/wa_2     01100111           01100111
/insertion/trigger  1
/insertion/h        0110011101000101(  01100111010001010010001100000001
/insertion/lh       0110011101000101(  01100111010001010010001100000001
/insertion/h0       0110011101000101(  01100111010001010010001100000001
/insertion/h1       1110111111001101:  11101111110011011010101110001001
/insertion/h2       1001100010111010:  10011000101110101101110011111110
/insertion/h3       0001000000110010(  00010000001100100101010001110110
/insertion/h4       1100001111010010:  11000011110100101110000111110000
/insertion/k        1100101001100010:  11001010011000101100000111010110
Now       4800 ns    500 ns   1000 ns   1500 ns   2000 ns   2500
Cursor 1  0 ns
```

WATERMARK DETECTION



VII. CONCLUSION

A new robust dynamic watermarking scheme by embedding the authorship information on the transitions of STG at the behavioral synthesis level. The proposed method offers a high degree of tamper resistance and provides an easy and noninvasive copy detection. The FSM watermark is highly resilient to all conceivable watermark removal attacks. The redundancy in the FSM has been effectively utilized to minimize the embedding overhead. By increasing the length of input code sequence for watermark retrieval and allowing the output compatible transitions to be revisited to embed different watermark bits, the watermarks are more randomly dispersed and better concealed in the existing transitions of FSM. The new approach to the logic state assignments of pseudo input variables also makes it infeasible to attack the watermarked FSM by removing the pseudo inputs[8].Without compromising the watermark strength, the length of verification code sequence can be adapted to reduce the area overhead of watermarked design to a reasonable bound within a preset number of iterations.

VIII. FUTURE WORK

The copying of digital content without quality loss is not so difficult. Due to this, there are more chances of copying of such digital information. So, there is great need of prohibiting such illegal copyright of digital media. Digital watermarking (DWM) is the powerful solution to this problem. Digital watermarking is nothing but the technology in which there is embedding of various information in digital content which we have to protect from illegal copying. This embedded information to protect the data is embedded as watermark. Beyond the copyright protection, Digital watermarking is having some other applications as fingerprinting, owner identification etc.

REFERENCES

[1] Mangione-Smith.W.H, Mantik.D (Aug 2001) "Intellectual Property Protection Development Working Group, Intellectual Property Protection: Schemes, Alternatives and Discussion", VSI Alliance, white paper, version 1.1. Page.no:25.

[2] Abdel-Hamid.A.T, Tahar.S, and Aboulhamid.E.M (Jul 2005), "A survey on IP watermarking techniques", in Design Automation for Embedded Systems, vol. 10. Berlin, Germany: Springer-Verlag, Page.no:26 .

[3] Cui.A, Chang.C.H, and Tahar.S (Sep 2008) "IP watermarking using incremental technology mapping at logic synthesis level", IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 27, no. 9, Page.no:1.

[4] Cui.A and Chang.C.H (May 2006) "Stego-signature at logic synthesis level for digital design IP protection", in Proc. IEEE Int. Symp. Circuits Syst., Page.no:37.

[5] Kahng.A.B, Lach.J, Mangione-Smith.W.H, Mantik.D, Markov.I.L, Wang.H, Potkonjak.M, and Wolfe.G (Oct 2001) "Constraint-based watermarking techniques for design IP protection" , IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 20, Page.no:34.

[6] Kim.H.J, Mangione-Smith.W.H and Potkonjak.M (Oct 1998) "Protecting ownership rights of a lossless image coder through hierarchical watermarking", in Proc. Workshop Signal Process. Syst., Page.no:23.

[7] Rashid.A, Asher.J, Mangione-Smith.W.H, and Potkonjak.M (May 1999) "Hierarchical watermarking for protection of DSP filter cores". in Proc. IEEE Custom Integr. Circuits Conf., Page.no:25.

[8] Oliveira.A.L (Jun 1999) "Robust techniques for watermarking sequential circuit designs", in Proc. IEEE/ACM Des. Autom.Conf., Page.no:15.

[9] Torunoglu.I and Charbon.E (Feb 2000) "Watermarking-based copyright protection of sequential functions", IEEE J. Solid-State Circuits, vol. 35,. Page.no:3.