Survey on Security based Watermarking Techniques in FPGA Design

[1]R.Senthil Ganesh, [2]A.Keerthana Priyaa, [3]S.A.Sivakumar, [4]Dr.R.Naveen
[1,3]Assistant professor, [2]PG Scholar (M.E., VLSI Design), [4]Associate Professor & Head
[1,2,3,4] Department of Electronics and Communication Engineering
[1,2,3,4] Info Institute of Engineering, Coimbatore, Tamilnadu, India

Abstract : The Watermarking is an intellectual property (IP) protection technique. It can protect field-programmable gate array (FPGA) IPs from infringement. IP protection of hardware designs is the most important requirement for many FPGA intellectual property vendors. Digital watermarking has become an innovative technology for IP protection in recent years. This paper proposes the publicly verifiable watermarking for intellectual property protection in FPGA design. The chaos-based zero knowledge verification protocol is used in this watermarking detection technique. The time stamping is also used and it can resiliently resist the sensitive information leakage and embedding attacks, and is thus robust to the cheating from the prover, verifier, or third party. The synthesis tool Xilinx ISE 9.1 and different types of Xilinx FPGA chips are used to verify and implement the watermarking scheme. The zero-knowledge protocol proposed in this paper is implemented by MATLAB and C programming language, running on a PC.

Index Terms **– Intellectual property (IP) protection, field-programmable gate array (FPGA), publicly verifiable watermarking, zero-knowledge protocol.**

I. INTRODUCTION

With the prevalence of reusable design methodology in the IC design field, intellectual property (IP) infringement becomes increasingly serious. The modular designed IP cores are easy to be copied or sold by third parties without reverse engineering, which results in huge economic losses to IP owners and reduces the market share of their products. Therefore, how to prevent the IP infringement effectively has become a huge challenge for field-programmable gate array (FPGA) vendors and IC designers.

However, existing watermarking techniques may give away sensitive information during the public verification, which enables malicious verifiers or third parties to remove the embedded watermark and resell the design. Various watermarking verification schemes can address the sensitive information leakage issue but are vulnerable to embedding attacks, which makes them ineffective in preventing the infringement denying of untrusted buyers (verifiers).

In this paper, a new publicly verifiable watermarking detection scheme based on chaotic sequences is proposed to address the issues that the FPGA watermarking technique may leak the sensitive information and the existing zero-knowledge FPGA watermarking detection scheme is vulnerable to embedding attacks. In this scheme first, a watermark is generated with the signature information and then the watermark is embedded into the benchmark circuits based on the embedding algorithm. Next the watermarking overhead and the robustness of position permutation of zero-knowledge protocol are analyzed.

The verification scheme proposed in this paper can not only prove that the watermark does exist in IP without revealing its content and position, but any verifier (including untrusted verifier) can verify the legitimacy of the watermark and resist embedding attacks against the cheating from the prover, verifier, or third party effectively. The experimental results show that the random permutation algorithm has a higher robustness.

II. PUBLICLY VERIFIABLE WATERMARKING SCHEME

2.1 Watermarking Generation and Embedding

The process of watermarking generation and embedding are as follows.

Step 1: Watermarking generation - First, the signature S is encrypted with an encryption algorithm. Second, the encrypted S is imputed into a one-way Hash function (such as SHA-2) to generate an abstract S with fixed length. Finally, the watermark W is obtained by scrambling S with hashed chaotic sequence (the initial value of the chaos is used as the key K1).

Step 2: Locating watermark positions - Using a pseudorandom number generator (such as chaos K2 as the key) to generate a pseudorandom sequence as the watermark embedding positions.

Step 3: The watermark is grouped according to the maximum value of the watermark in an LUT and then embedded into unused LUT of used Slice.

Step 4: The input and output of watermarked ILUTs are connected with the “do not care” inputs of the original circuit in order to disguise the embedded watermark.

2.2Chaos-Based Zero-Knowledge Verification Protocol

1) Protocol Overview: Zero-knowledge public verification is to prove that the watermark of IP owner exists in the bitstream of FPGA design without revealing the watermarking content and position. Assume the prover is Alice and the verifier is Bob. According to the watermark generation and embedding algorithm mentioned, Alice gets W based on S. Then W is embedded into I (FPGA design) to get I^. Alice wants to prove the existence of W without leaking its position. The process of zero-knowledge verification protocol is shown in Fig. 2.1

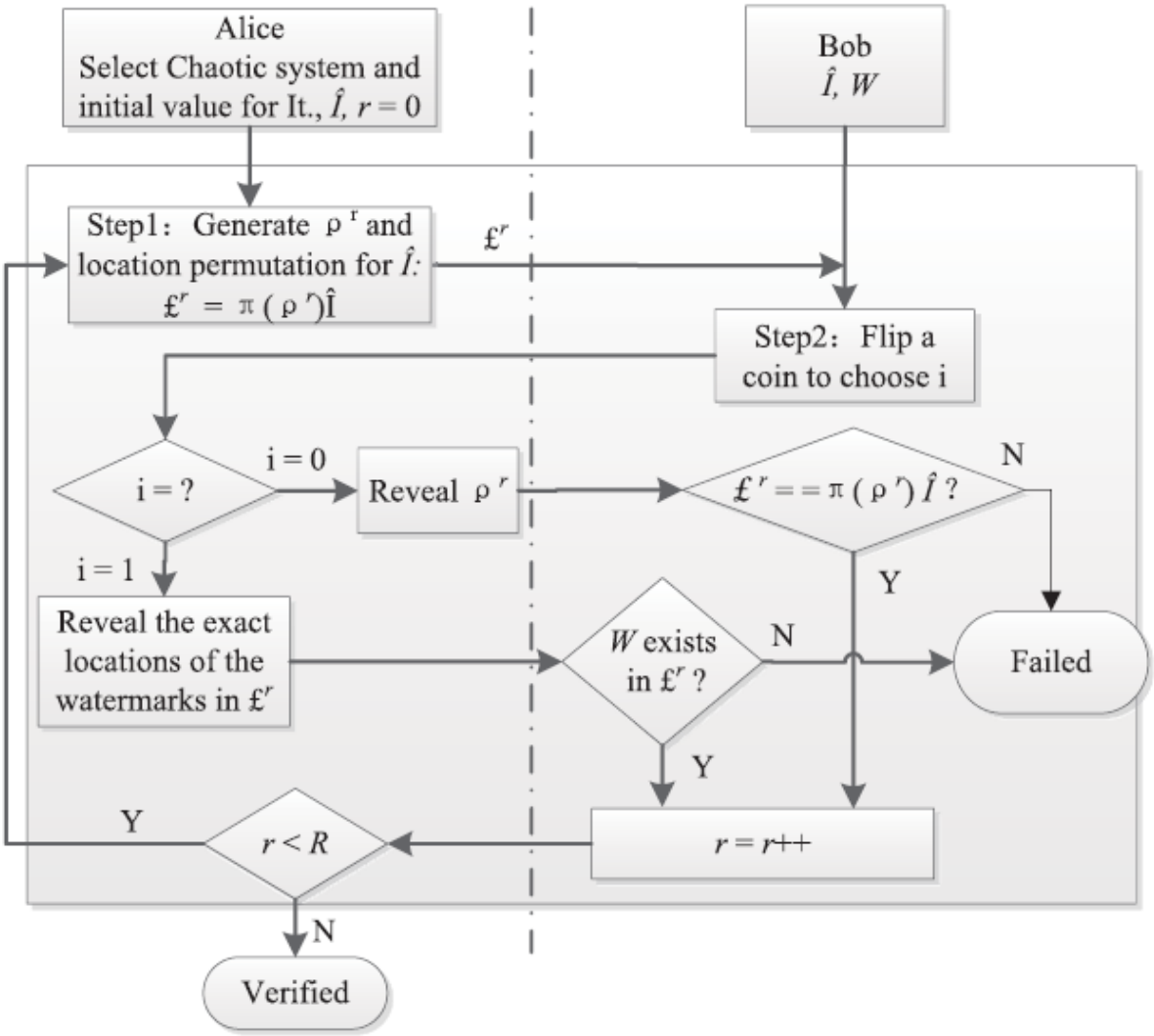

Fig.2.1 Zero-knowledge verification protocol between prover Alice and verifier Bob [2]

2) Protocol Implementation: In the zero-knowledge water-marking detection protocol, the random permutation of the FPGA bitstream is an important component of the zero-knowledge protocol. Random permutation must meet two requirements: (i) the number of random permutations should be enough and (ii) the correlation between random permutations should be extremely low.The implementation of protocol is described in detail as follows.

Algorithm: Chaos-based position permutation algorithm

Step 1: Confirm 1-D chaotic system [use the logistic mapping] and the initial value x(0).

Step 2: Generate the chaotic sequence x(k)(k= 0, 1, 2, . . . ,n)

Step 3: Perform the binarization of chaotic sequence x(k)(k= 0, 1, 2, . . . ,n)to get

ρ (k)(k=0, 1, 2, …,n).

Step4: Determine the value of M and N in IM×N . Set k= 0.

Step 5:
```
for i= 0 to M/2-1
for j= 0 to N-1
Swapρ (k)( f (i, j ), f (i + M/2, j ));
k = k +1;
end
end
```

Step 6:
```
for i= 0 to M-1
for j= 0 to N/4-1 and N/2 to (3/4)*N-1
Swapρ (k)( f (i, j ), f (i, j + N/4));
k = k + 1;
```

```
                end
                end
Step 7:         for i= 0 to M/4-1 and M/2 to (3/4)*M-1
                for j= 0 to N-1
                Swapρ (k)( f (i, j ), f (i + M/4, j ));
                k = k +1;
                end
                end
Step 8:         for i= 0 to M-1
                for j= 0 to N/2-1
                Swapρ (k)( f (i, j ), f (i, j + N/2));
                k = k +1;
                end
                end

Step 9:         Position permutation is done.
```

III. PROTOCOL ANALYSIS

3.1 Analysis of Embedding Attacks

A dishonest IP buyer (verifier) uses an unauthorized IP. An honest IP owner (prover) wants to prove that the IP contains his watermark. In the actual public verification process, the verifier is often untrusted because the verifier will strive to make an honest IP owner unable to prove his illegal use of IP, i.e., even though the verifier uses the IP illegally, the IP owner is unable to prove it. Since FPGA IP is essentially a bitstream file, a malicious attacker is able to embed the watermark into the file. Therefore, the existing FPGA zero-knowledge watermarking detection systems are vulnerable to embedding attacks.

In order to prevent embedding attacks and denial of infringement, we not only need to watermark the FPGA bitstream, but also ensure the existence of the watermark before certain time. We address the problem using the linking or distributed trust time-stamping scheme. The two time-stamping schemes can guarantee that no matter how unscrupulous the time-stamping service (TSS) is, the times it certifies will always be the correct ones, and that it will be unable to issue incorrect time-stamps.

The distributed trust time-stamping scheme even could be implemented without the need for a centralized TSS at all. When a copyright dispute occurs, the time that an attacker copies the IP illegally and launches the embedding attack to embed the forged watermark would lag in the genuine time. In the Analysis ofProtocol Properties, the zero-knowledge protocol should satisfy three properties - completeness, soundness and zero-knowledge.

3.2 Watermarking Overhead

The resource and time overhead are measured by the used Slice and minimum clock period. The method proposed in this paper does not affect the minimum clock cycle of the design. This is because we embed the watermark in the physical layout of the circuit, the routing modification for original design is very small. The routing influence on the design will cause the design to partly change (“hold to clock clk,” “setup to clock clk,” and “clock clk to pad”), but the minimum clock period keeps unchanged . Therefore, the overhead is almost 0 for our proposed watermarking method, which is an obvious advantage compared with the previous watermarking methods.

3.3 Robustness of Position Permutation

Position permutation is an important metric to evaluate the security of the verification protocol. We use the average Manhattan distance ($\mu N(\delta L)$), Manhattan standard deviation ($\sigma N(\delta L)$), and the correlation coefficient ($\rho N(l, \delta L)$) between the LUT position and Manhattan distance to measure the robustness of the position permutation. The larger the value of $\sigma N(\delta L)$ and the smaller the value of $\rho N(l,\delta L)$ are the higher the robustness of the position permutation. (xk ,yk) and (xk , yk) are the positions of the Kth LUT before and after position permutation, respectively.

IV. LITERATURE REVIEW ON WATERMARKING

4.1Publicly detectable watermarking for intellectual property authentication in VLSI design

G.Qu[2002] developed the publicly detectable watermarking for IP authentication in VLSI design. This paper proposes a publicly detectable VLSI watermarking technique that embeds an independent public watermark for public verification and the watermark is publicly detected without losing its strength and security [1]. The idea is to create a cryptographically strong pseudo-random watermark embed it into the original problem as a special constraint and make it public.

4.2 Fingerprinting techniques for field-programmable gate array intellectual property protection

J.Lach et al [2001] developed a technique for FPGA IP protection. This paper proposes the technique that leverages the unique characteristics of FPGA to protect commercial investment in IP through fingerprinting [2]. The hidden encrypted mark is embedded into the physical layout of a digital circuit when it is placed and routed onto the FPGA. This mark uniquely identifies both the circuit origin and original circuit recipient.

4.3Secure public verification of IP marks in FPGA design through a zero-knowledge protocol

D. Saha et al [2012] developed the publicverification of IP marks in FPGA designs. This paper proposes the zero-knowledge protocol in which it is an interactive two-person game between the prover and the verifier. This protocol satisfies zero- knowledge property and introduce statistical metrics to measure its robustness [3]. The protocol used in this is fast, incurs no additional design overhead and needs no centralized signature database.

4.4 Ultra-low overhead dynamic watermarking on scan design for hard IP protection

A. Cui et al [2015] developed the ultra-low overhead dynamic watermarking on scan design for hard IP protection. This paper proposes ultra-low overhead watermarking scheme to protect hard IPs, the dominating form of commercial IPs. An optimized scan design uses two complementary connections between two adjacent scan cells and such scan design flexibility in the section of local connection styles provides a vehicle to embed watermarking constraints [4]. It can conveniently be implemented by local rewiring and/or introducing dummy scan cells.

4.5 A blind dynamic fingerprinting technique for sequential circuit intellectual property protection

C.H. Chang et al [2014] developed a blind dynamic fingerprinting technique for sequential circuit IP protection. This paper proposes the first dynamic fingerprinting technique on sequential circuit IPs to enable both the owner and legal buyers of an IP embedded in a chip to be readily identified in the field and the fingerprint in this is an oblivious ownership watermark independently endorsed by each user through a blind signature protocol [5]. Thus the authorship, can also be proved through the detection of different users fingerprints without the need to separately embed an identical IP owner's signature in all fingerprinted instances.

V. COMPARATIVE ANALYSIS

Table 5.1 Comparative analysis on various watermarking techniques

AUTHOR	YEAR	ALGORITHM	ADVANTAGE	DISADVANTAGE
G. Qui	2002	The combine data-integrity technique isused in which it is compatible and resulting public-private watermark maintains the strength of watermark.	Easy detectability and high credibility.	Low robustness is obtained.
J. Lach et al	2001	The technique of cryptographically encoded marks to FPGA digital designs is used.	Capable of encoding long messages.	Performance and area impacts are minimal.
D. Saha et al	2012	The zero-knowledge based FPGA digital signature verification scheme is used.	Good robustness and overhead can be achieved.	Vulnerable to embedding attacks.
A. Cui et al	2015	The ultra-low overhead watermarking scheme is used inorder to protect hard IPs.	Easy detectability.	Low performance and vulnerable to embedding attacks.
C.H. Chang et al	2014	The blind signature protocol is used for sequential circuit IP protection.	Applicable to both application specific integrated circuit (ASIC) and FPGA IPs.	The robustness is low when compared with zero-knowledge protocol.

VI. CONCLUSION

The chaos-based publicly verifiable watermarking detection scheme proposed in this paper will not give away sensitive information such as the content and the position of embedded watermarks. In addition, the linking or distributed trust time-stamping mechanism is used to address the issue that the existing FPGA watermarking detection schemes are vulnerable to embedding attacks. Since the inherent advantages of the chaotic system exactly meet the special requirements of random position permutation in the zero-knowledge protocol, our proposed scheme has high position permutation robustness. The experimental results also show that the proposed watermarking scheme incurs almost zero overhead and analysis show that the proposed method has better robustness than the previous watermarking techniques. Thus this paper present the work on the use of watermarking technique for the IP protection in FPGA design.

VII. ACKNOWLEDGMENT

Our sincere thanks to the management of Info institute of Engineering for providing the research lab for our work.

REFERENCES

[1] G. Qu, "Publicly detectable watermarking for intellectual property authentication in VLSI design," IEEE Trans. Comput.-Aided Des.Integr.Circuits Syst., vol. 21, no. 11, pp. 1363–1368, Nov. 2002.

[2] J. Lach, W. H. Mangione-Smith, and M. Potkonjak, "Fingerprinting techniques for field-programmable gate array intellectual property pro-tection," IEEE Trans. Comput.-Aided Des.Integr. Circuits Syst., vol. 20, no. 10, pp. 1253–1261, Oct. 2001.

[3] D. Saha and S. Sur-Kolay, "Secure public verification of IP marks in FPGA design through a zero-knowledge protocol," IEEE Trans.Very Large Scale Integr. (VLSI) Syst., vol. 20, no. 10, pp. 1749–1757,Oct. 2012.

[4] A. Cui, G. Qu, and Y. Zhang, "Ultra-low overhead dynamic watermark-ing on scan design for hard IP protection," IEEE Trans. Inf. ForensicsSecurity, vol. 10, no. 11, pp. 2298–2313, Nov. 2015.

[5] C.-H. Chang and L. Zhang, "A blind dynamic fingerprinting technique for sequential circuit intellectual property protection," IEEE

Trans.Comput.-Aided Des. Integr. Circuits Syst., vol. 33, no. 1, pp. 76–89,Jan. 2014.

[6] J. Lach, W. H. Mangione-Smith, and M. Potkonjak, "Robust FPGA intellectual property protection through multiple small watermarks," in Proc. 36th Annu.ACM/IEEE Design Autom. Conf., Jun. 1999,pp.831-836.

[7] J. Zhang, Y. Lin, Q. Wu, and W. Che, "Watermarking FPGA bitfile for intellectual property protection," Radioengineering, vol. 21, no. 2,pp.764-771, Jun.2012.

[8] A. Adelsbach and A.-R.Sadeghi, "Zero-knowledge watermark detection and proof of ownership," in Proc. 4th Int. Workshop Inf. Hiding, Apr. 2001, pp. 273–288.

[9] W. Liang, K. Wu, Y. Xie, and J. Duan, "TDCM: An IP watermarking algorithm based on two-dimensional chaotic mapping," Comput. Sci. Inf.Syst., vol. 12, no. 2, pp. 823–841, 2015.

[10] Q. Liu, W. Ji, Q. Chen, and T. Mak, "IP protection of mesh NoCs using square spiral routing," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 24, no. 4, pp. 1560–1573, Apr. 2016.