Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Forensic engineering for resolving ownership problem of reusable IP core generated during high level synthesis

Anirban Sengupta *, Deepak Kachave

Computer Science & Engineering, Indian Institute of Technology Indore, India

HIGHLIGHTS

- A novel methodology for resolving ownership problem of IP cores.
- A CFE methodology that protects IP core generated during HLS.
- Offers 0% hardware overhead and minimal implementation runtime.

ARTICLE INFO

Article history:
Received 8 February 2017
Received in revised form 21 June 2017
Accepted 1 August 2017
Available online xxxx

Keywords:
High level synthesis
Protection
Forensic engineering
IP core

ABSTRACT

Reusable Intellectual Property (IP) cores have become an obligatory mandate for combating conflicting objectives of maximizing design productivity and minimizing design cycle time. However, a reusable IP core needs protection against false (illegal) claim of ownership. In this paper, we propose a novel computational forensic engineering (CFE) based approach for resolving ownership problem of a reusable IP core generated during high level synthesis (HLS).

Some of the major contributions of the proposed approach are as follows: (a) a novel methodology based on multiple design feature set (technology & control parameter independent) that is capable of resolving false claim of vendor ownership problem for an IP core generated during HLS (b) novel algorithms for extracting design features (from register transfer level (RTL) hardware description language (HDL)) of an IP core for determining the rightful owner (c) a novel signature free approach (with avg. runtime ∼2 s) that offers 0% hardware overhead and 0% degradation of IP functionality/quality compared to watermarking based IP ownership resolution techniques.

1. Introduction

With the escalation in demand of electronics in consumer market along with rapid proliferation of newer system-on-chip technologies such as multi-core systems, 4K display, wearable devices [1,2] etc., reusable IP cores have become an inevitable solution. Multi-vendor third party IP cores have become a viable solution for reuse based design methodologies. This is because an IP core simplifies the complex demand of maximizing design productivity while minimizing design cycle time [3–13]. However, a reusable IP core requires protection from vendor's perspective against threats that are non-trivial. Some major threats related to ownership of an IP core used in applications such as system-on-chip, ad-hoc networks [14] etc. are shown in Fig. 1. One of the central threats to an IP core used in IoT application [15] is abuse of ownership [16] where a licensee may have been granted license for a limited number of uses, but the licensee may have exceeded the number of agreed uses without permission of the licensor. IP metering technique [17] is used to protect the creator or vendor from ownership abuse in such a case. As we know an IP core is a creation of intellect for which the law provides monopoly right to the owner. Although techniques such as patent, copyright, trademark etc. provide the right to enjoy ownership, however these are not applicable for reusable IP cores [16,18,19]. Hence for these type of entities, ownership problem is a major concern. In this context, piracy [20,21] is a major ownership threat to an IP core where an adversary can falsely claim ownership. In such a case, fraudulent means or reverse engineering may allow direct theft/copying of an IP for re-use without permission. As a result of stealing, the adversary may even claim the IP to be its own. Thus means of nullifying false claims of IP ownership is needed. Traditionally to protect against ownership abuse of reusable IP cores, signature is inserted into the design without disturbing its functionality and performance. For the owners of an IP core or a complete chip, it is both difficult and expensive to prove that their IP is being illegally used in a product. In the case of silicon chips, the

* Corresponding author.
E-mail address: asengupt@iiti.ac.in (A. Sengupta).

http://dx.doi.org/10.1016/j.future.2017.08.001
0167-739X/

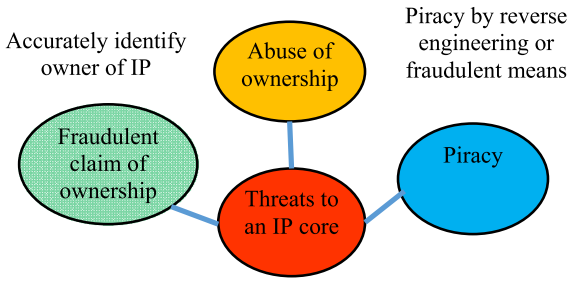

Fig. 1. Ownership related threats to an IP core.

only practical method of detecting an IP core is to obtain a sample of the product under suspicion and send it to a specialist laboratory for analysis and reverse engineering. The ownership protection deals with identifying the creator of an IP core, as there may be several false claimants. Therefore, there is a threat to an IP creator about losing ownership to some false claimant.

Another class of IP threat is Trojan [22,23] where an adversary in the third party IP vendor house may embed a malicious logic (called 'hardware Trojan') in an IP core for seeking information or affecting functionality. There is recently some work done that tries to detect presence of hardware Trojans in an IP [22,23]. Trust [24,25] is another important threat that plays a major role in deciding whether to buy an IP from a respective IP vendor. If there are two competitive vendors providing similar IP cores, generally the client prefers to buy an IP from trusted vendor i.e. the vendor who has strong reputation in the market.

1.1. Motivation: CFE for IP core protection

Signature based watermarking is a well-known technique for protecting vendor ownership in IP core [3,5,15]. In case of protecting an IP core through watermarking during high level synthesis, the vendor signature insertion is performed at the register allocation step that has every chances of affecting the performance while incurring hardware overhead. Further, watermarking techniques mandate reverse engineering during signature detection which is highly vulnerable to threats. Other IP protection approaches such as IP metering [6] and obfuscation [26,27] are not able to determine the original owner of an IP core. This is because IP metering is developed to limit the number of IP cores used by a licensee, while obfuscation is used to enhance complexity of reverse engineering process.

In such scenarios, CFE based approach for owner identification is very useful as it does not involve signature insertion, design overhead and reverse engineering. In the proposed CFE approach, there is no need of signature, unlike watermarking based ownership resolution process (which embeds signature during HLS or logic level or silicon). Table 1 shows advantages of proposed CFE approach for IP core protection over watermarking based IP protection approach [5] in terms of parameters: (a) overhead (b) quality of design (c) complexity (d) security (e) threats. As evident from Table 1, it is clear that the proposed CFE approach offers zero hardware overhead, zero degradation of quality of design, lower complexity of implementation, higher security and lesser vulnerability to threats compared to watermarking based IP core protection such as [5] during high level synthesis.

1.2. Background on CFE

CFE can be understood as follows: given a solution S to the problem P having a finite set of algorithms/tools $A\_n\,(n = 1, \ldots, i)$ applicable to problem P that can generate solution S, the aim of CFE is automated identification with a certain degree of confidence that the algorithm/tool A_i has been applied to generate solution S [28,29]. The generic CFE approach consists of four steps namely (a) Feature and data collection (b) Feature extraction (c) Algorithm clustering and (d) Validation. The first step feature and data collection involves identifying particular properties/features of algorithms which may be able to distinguish it from other algorithms. The next step involves extracting those properties/features from the solution. Please note that the terms features and properties may have been used interchangeably. The third optional step involves clustering of solutions on basis of their features. Note: this step is needed in case the number of competing claimants is extremely large which is not pertinent in case of the problem addressed in this paper, as claimants in our case are always limited. This is because in practical scenario, the number of HLS tool IP vendors for digital signal processing (DSP) applications available in the market is handful. Thus for solving this specific case, adding clustering step is redundant and would only result in increasing runtime for CFE process. Even if number of competing vendors increase, it will not require the use of clustering which is typically used when the number of instances is very large. In the context of the domain where proposed CFE is applied, number of competing vendors may not exceed seven as there are not many HLS tool IP vendors for digital signal processing (DSP) applications available in the market. Thus, even without using algorithm clustering step, the CFE for IP core protection problem may accurately identify the creator of IP. In summary, the CFE approach for IP core protection does not require statistical knowledge base as it typically does not involve large number (instances to be analyzed through digital evidence) of IPs. As reported later in Fig. 10, the time complexity is represented through average extraction runtime which is in the order of few milli-seconds, irrespective of the IP core size and number of competing vendors (though as explained above typically in practical scenario, number of competing vendors may not exceed seven). Finally, the solution is validated to be originated from an algorithm on basis of how closely the features of solution match to the features of the algorithm.

We note the following key points about the proposed approach:

- The proposed CFE for IP protection is applicable in scenarios where 'n' IP vendors are claiming ownership of a given IP core and rightful owner has to be ascertained. It is assumed that each IP vendor has a unique HLS tool for generating their respective IP design. Scenario, where two (or more) IP vendors uses a common third party tool for generating respective IP cores, does not fall within the scope of this approach.
- The CFE approach for IP core protection for validation requires the following as *inputs*: Executable version of HLS tools corresponding to 'n' claiming IP vendors and the given IP core (in RTL hardware description language) whose owner is to be identified. This is analogous to signature detection step in watermarking where the signatures from claiming vendors are taken as input to determine which matches the signature present in the given IP core. Similarly for proposed CFE, the feature set (extracted from RTL description) of IP core corresponding to ith HLS tool which fully matches the feature set of the given IP core is the rightful owner.

  Note: procuring the RTL HDL of given IP core is practical because the given IP core can be obtained from any of the claimants (competing IP vendors), as they all claim ownership of the same IP core (and have copies of the same IP core. Except the original vendor, all others have stolen/counterfeit copies, but we do not know who produced the original version). The ith HLS tool vendor whose IP feature set fully matches with the given IP core, is the rightful owner of the given IP core.

Please cite this article in press as: A. Sengupta, D. Kachave, Forensic engineering for resolving ownership problem of reusable IP core generated during high level synthesis, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.08.001.