TECHNIQUES FOR INTELLECTUAL PROPERTY PROTECTION OF DSP DESIGNS

Inki Hong and Miodrag Potkonjak

Computer Science Department, UCLA, Los Angeles, CA 90095-1596 USA

ABSTRACT

Recently, numerous watermarking-based techniques for intellectual property protection of DSP artifacts, such as images, compressed and uncompressed audio and video data, and text documents have been proposed. However, the applicability of all techniques proposed until now are limited to digital data and they either implicitly or explicitly exploit the imperfection of human perception to audio and video. We propose the first watermarking technique for protecting the intellectual property of DSP designs. The essence of the technique is the use of additional synthesis constraints to encode the authorship signature. The constraints are selected in such a way that they result in minimal hardware overhead while embedding the signature which is unique and difficult to detect and remove. The technique is applicable to all levels of design process, from the algorithm, system and behavioral synthesis to logic synthesis and physical design levels. The technique is illustrated on a set of DSP design examples on all levels of design process.

1. INTRODUCTION

The growing adoption of reuse-based design paradigms is creating a pressing need for the development of sound mechanisms to protect intellectual property rights of designers. The intellectual property protection (IPP) mechanisms play an important role as an enabling technology for reusable core-based design paradigm which has recently emerged as one of the most visible and important components on which future design approaches will be based [5].

Although there exist several legal intellectual property protection measures for DSP designs, they are insufficient or inapplicable for IPP of reusable DSP cores. We also note that watermarking techniques proposed for image, video, voice and text data do not provide an adequate solution for IPP of DSP designs since these techniques alter a large number of components in watermarked objects. While in multimedia this alteration is invisible to human eyes or ears, in the case of DSP designs it will have unacceptable impact on the functionality and correctness of the designs.

We propose a new watermarking-based approach which is specifically developed for IPP of DSP designs. The approach embeds encoded messages in designs at all levels of design process with minimal hardware overhead while maintaining the correctness and functionality of designs. It is based on the key property of design space exploration in design process such that there are numerous competitive solutions. The idea is to select one of the competitive solutions which encodes a signature. Searching for such solution with the embedded signature is difficult, if not an impossible task. However, generating such a design that satisfies the original specified constraints as well as additional watermarking constraints is both easy and time efficient.

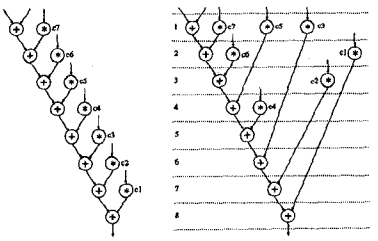
The rest of the paper is organized in the following way. In Section 2 we provide a motivational example for the new approach. In Section 3, we outline the related work. In Section 4, we identify the criteria for effective watermarking of DSP designs. In Section 5, a generic approach for IPP of DSP designs and its application to all levels of design process are described. In Section 6, we provide the experimental results. Finally, we summarize the key contributions.

2. MOTIVATIONAL EXAMPLE

To illustrate the key ideas behind the new approach, we consider the design shown in Figure 1(a). We explain using the example that how the approach is applied to scheduling in behavioral synthesis. In scheduling, the set of operations in the control data flow graph (CDFG) are partitioned into groups of operations so that the operations in the same group can be executed concurrently in one control step. The author's signature is embedded by adding a set of constraints such that two operations with no dependencies are enforced to be scheduled in one specific order, i.e., an additional edge is added in the CDFG. The periods between as soon as possible control step and as late as possible control step that an operation can be scheduled to satisfy the timing constraints must be overlapped in at least 2 control steps for the two operations. Otherwise, adding an edge between the operations is not a new constraint. Whenever an edge is added, the periods for operations must be updated accordingly. The CDFG with the extra edges must satisfy the timing requirements with minimum hardware overhead.

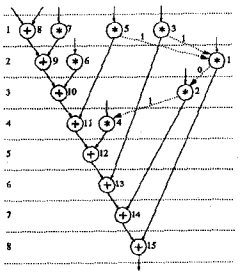
Using this set of additional constraints, the author's signature is encoded. For example, the following encoding scheme can be used: All the operations in a design are sorted and numbered based on the degrees of their scheduling freedom in a decreasing order. The scheduling freedom of an operation is defined to be the length between as soon

0-7803-4428-6/98 $10.00



(a) Original CDFG

(b) Scheduled CDFG with watermark



(c) Added edges with encoded values

Figure 1: An example of watermarking scheduling solutions

as possible control step and as late as possible control step that the operation can be scheduled to satisfy the timing constraints. An added edge (x, y) represents 1 if x and y are either both even numbers or both odd numbers. It represents 0, otherwise. Following the order in this sorted list, for each operation x, we search the first operation y from the beginning of the list that an edge (x, y) can be added and represent the desired value.

Suppose that 6 clock cycles are available. Its scheduled CDFG is shown in Figure 1(b). The design is embedded with a signature "7". Figure 1(c) shows how the watermarking is achieved. The number in the right side of each node represents the position in the sorted list. The set of additional edges is (1,2), (2,4), (3,1), (5,1), as shown in dotted lines. The set encodes "0111", i.e., "7" in the BCD code.

3. RELATED WORK

In this Section, we review the most relevant related work to IPP: data watermarking and cryptographic techniques.

Data watermarking, also known as data hiding, embeds data into digital media for the purpose of identification, annotation, and copyright. Several techniques for data hiding in digital image [3], audio [2], video [6] and text [1] have been developed. The key difference of our proposed approach with those techniques is that all of them attempt to

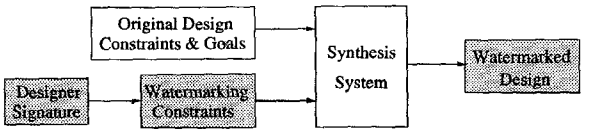


Figure 2: The generic approach to IPP of DSP designs

embed the watermark in the final object while our approach is incorporated in the design process.

Cryptographic techniques can be used to supplement the watermarking methods, for example, by encrypting the watermark. Cryptography puts "signature" by restricting access to information. Once the information is decrypted, the "signature" is removed and there is no proof of ownership.

4. DSP INTELLECTUAL PROPERTY DESIDERATA

We set out the criteria which a watermarking-based IPP technique should satisfy in order to be considered effective.

- **Correctness of Functionality.**
- **Low Hardware Overhead.**
- **Transparent to Existing CAD Tools and Designs.**
- **Strong Proof of Authorship.**
- **Difficult to Detect.**
- **Resiliency (Difficult to Remove).**
- **Proportional Component Protection.**

5. WATERMARKING DSP DESIGNS

5.1. Generic Approach

The generic approach to watermarking DSP designs is shown in Figure 2. The essence of the approach is the addition of constraints which encode the authorship signature. The constraints are selected such that they result in minimal hardware overhead while embedding the signature difficult to detect and remove. The technique is transparent to manual and automatic design processes and therefore can be used in conjunction with any available or future DSP design tools. The technique is applicable to all design abstraction levels.

5.2. Algorithm Level

Covert channels are hidden communication mechanism embedded in designs. Traditionally covert channels have been used for circumventing security barriers. We propose a new use of covert channels for IPP of DSP designs in algorithm level. The idea is to embed a covert channel into a design in such a way that only the authors of a design can observe and interpret information obtained through the channel. The information encodes watermarking signatures. Note that intellectual property protection at the higher levels of the design abstraction is in particular attractive, because regardless of how much a unauthorized user of the design changes the implementation on the lower levels of abstraction (e.g. during behavioral, logic and physical synthesis) the proof of the authorship is not affected.

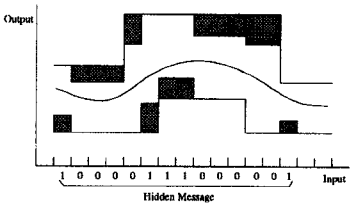


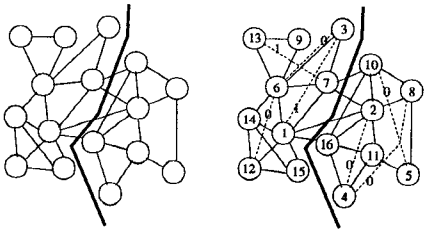
Figure 3: Algorithm level IPP: Covert channel-based scheme for a digital bandpass filter

We now illustrate the key idea using a digital bandpass filter. Figure 3 shows a typical specification for a digital bandpass filter using a transfer function profile [4]. For both stopbands and passbands, in addition to the required amplification level specification, the allowable margin of imperfection is also stated. The idea is to add additional constraints in the filter structure which encode a designer signature. In our example, we reduce the margin of error by 25% on lower or upper bound of the margin for some input segments. By observing the outputs for the specific input segments, we can identify the embedded messages. For example, in Figure 3, the first 14 consecutive input segments encode "10000111000001" in binary which is equal to "CA" in ASCII code, where additional lower bound constraint means 1 while additional upper bound constraint means 0. The way to detect from the design under examination for possible intellectual property right violation is to apply proper input signals to the pins of the design and observe the outputs. Essentially, in our example, one can unit-impulse [7] and store the outputs. After the application of Fast Fourier transform on the output signals, he/she will obtain the transfer function of the filter. The examination of the transfer function will indicate the probability that the examined design is indeed his/her intellectual property.

5.3. System Synthesis

We can apply the new approach to system synthesis tasks such as cache line coloring and multiprocessor DSP code partitioning. We show its application to the latter task which is formulated as a graph partitioning problem.

We embed the authorship signature by providing such constraints that particular two nodes should remain in the same partition. The following encoding scheme can be used. All the nodes in a design are randomly numbered. In the increasing order of node numbers, each node is considered for embedding a single bit. After all nodes are considered, we repeat the process from the first node in the order. For each bit in the watermark, the terminal node is chosen such that the terminal node number represents the bit value. 1 is embedded if the terminal node has odd number. 0 is embedded, otherwise. The first feasible node in the increasing order of node numbers, starting from the position right after the terminal node of the last edge added, is selected as the terminal node to embed the bit value.



(a) Partitioned graph with watermark

(b) Pairs of nodes with encoded values

Figure 4: An example of watermarking graph partitioning solutions

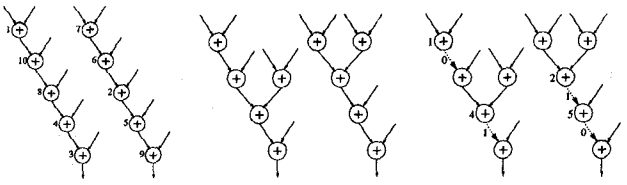
Consider the graph in Figure 4(a). The balance requirement is that one partition can have at most 20% more nodes than the other partition. Its partitioned graph is shown in Figure 4(a). The design is embedded with a signature "A". Figure 4(b) shows how the watermarking is achieved. The number in each node represents the position in the randomly ordered list. The pairs of nodes to remain in the same partition are (1,3), (2, 4), (3, 6), (4,8), (5,10), (6,12), and (7, 13). The pairs are connected by dotted lines. The set encodes "1000001", i.e., "A" in the ASCII code.

5.4. Compilation and Behavioral Synthesis Level

The generic approach can be applied to all compilation and behavioral synthesis tasks, such as scheduling, assignment, allocation, transformations and template matching. We show how the approach is applied to transformations, which is an important step in both compilation and behavioral synthesis.

Variables in the original design often disappear after the application of transformations. We embed the author's signature by providing such constraints that particular variables should remain after the application of transformations. For example, we consider associativity transformation. The following encoding scheme can be used: All the operations in a design are randomly numbered. A variable v_x from operation x represents 1 if x is even. It represents 0, otherwise. Following the order in the list, for each bit, we search the first variable that can represent the value of the bit. Suppose the BCD encoding for a decimal digit is used.

Consider the CDFG in Figure 5(a). Suppose that 4 clock cycles are available. Its transformed CDFG after applying associativity is shown in Figure 5(b). The design is embedded with a signature "6". Figure 5(c) shows how the watermarking is achieved. The number in the left side of each node represents the position in the randomly ordered list. The set of variables to be untouched by transformations is 1,2,4,5, as shown in dotted lines. The set encodes "0110",



(a) Original CDFG

(b) Transformed CDFG with watermark

(c) Variables with encoded values

Figure 5: An example of watermarking transformation solutions

i.e., "6" in the BCD code.

5.5. Logic Synthesis

The new approach can be applied to all logic synthesis tasks such as two-level and multi-level logic minimization and cell-library binding. We show its application to cell-library binding which is the task of transforming an unbound network into an interconnection of components that are instances of elements of a given library. The author's signature is embedded by adding a set of design constraints such that some particular cells should be bound together. For example, the following encoding scheme can be used: All the cells in a design are randomly numbered. Any two cells i and j connected with an edge can be required to be bound together, if the two cells belong to at least one of the elements in a cell library. The pair of cells is numbered by (i, j), where $i < j$. All such pairs are *lexicographically* sorted. Each pair represents a binary number. For a pair (x, y), if x and y are both even numbers or both odd numbers, then the pair represents 1, else it represents 0.

5.6. Physical Design

We have considered the application of the new approach to placement problem in standard-cell physical design. For row-based placement, we can constrain individual cells to be placed with specified cell row parity. For example, cell $x(y)$ might be constrained to be placed in a cell row that has even(odd) index. Note that very few constraints are needed to make a strong signature. For example, if the signature constrains 50 cells with specific row parities, the chances are 2^{-50} that this could have occurred by accident.

6. EXPERIMENTAL RESULTS

We have applied our approach to register allocation formulated as graph coloring on 5 DSP designs which include an adaptive modem, an LMS audio formatter, a CORDIC, a speech compressor, and a 2D Lee DCT. For the register allocation problem, the watermarking constraints are imposed such that a set of variables are forced to be stored in different registers which result in extra edges in the interval graph to be colored. Let P_C denote the probability of generating the same coloring solution with the signature of k watermarking edges accidentally, given the solution uses the same number of colors. $P_C = (1 - \frac{1}{c})^k$. The probability P_C for the 5 designs is extremely low with little overhead. For example, the P_C of a speech compressor with the overhead of 3 registers is 1.3×10^{-78}.

Design	# of Variables	# of Registers	# of Edges Added for k More Registers		
			$k = 1$	$k = 2$	$k = 3$
adaptive modem	200	48	600	830	1045
LMS Audio Formatter	464	122	1435	2340	2880
CORDIC	827	65	2050	4670	5760
Speech Compressor	1257	45	2895	6475	7980
2D Lee DCT	2048	184	3675	9975	13635

Table 1: Watermarking designs in register allocation

7. CONCLUSION

We proposed the first watermarking technique for protecting the intellectual property of DSP designs. We proposed the methods to apply the technique to all levels of design process abstraction, from the algorithm, system synthesis and behavioral synthesis to logic synthesis and physical design levels. The technique was illustrated on a set of DSP design examples on all levels of design process.

8. REFERENCES

[1] H. Berghel and L. O'Gorman. Protecting ownership rights through digital watermarking. *IEEE Computer*, 29(7):101–103, 1996.

[2] L. Boney, A.H. Tewfik, and K.N. Hamdy. Digital watermarks for audio signals. In *International Conference on Multimedia Computing and Systems*, pages 473–480, 1996.

[3] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon. A secure, imperceptible yet perceptually salient, spread spectrum watermark for multimedia. In *Southcon*, pages 192–197, 1996.

[4] R.E. Crochiere and A.V. Oppenheim. Analysis of linear digital networks. *Proceedings of the IEEE*, 63(4):581–595, 1975.

[5] E. Girczyc and S. Carlson. Increasing design quality and engineering productivity through design reuse. In *Design Automation Conference*, pages 48–53, 1993.

[6] F. Hartung and B. Girod. Digital watermarking of raw and compressed video. In *SPIE - The International Society for Optical Engineering*, volume 2952, pages 205–213, 1996.

[7] A.V. Oppenheim and R.W. Shafer. *Discrete-Time Signal Processing*. Prentice Hall, Englewood Cliffs, NJ, 1989.