Hierarchical Watermarking for Protection of DSP Filter Cores

Azra Rashid, Jeet Asher, William H. Mangione-Smith and Miodrag Potkonjak[†]

Departments of Electrical Engineering and [†]Computer Science
University of California, Los Angeles

Abstract

A hierarchical watermarking approach is developed that incorporates an ownership identification directly into the design development process. This approach offers a high degree of tamper resistance and provides easy, non-invasive copy detection. We present two FIR digital filter cores, one watermarked at the algorithm level and the second at the algorithm and architecture levels. A unique ownership signature (watermark) is placed at each level. At the algorithm level, the watermark is embedded in the filter coefficients during the development of the transfer function. At the architecture level, we use circuit transformations to watermark the design. Experimental results show approximately 7% area overhead of the algorithm-level watermarked design over a non-watermarked design. The cost of area for the design watermarked at both the algorithm and architecture levels is less than 40%.

Introduction

The move from transistor-based (or gate-level) ICs to integrating reusable circuit blocks (intellectual property) for systems-on-a-chip ICs in semiconductor industry, along with today's growing acceptance of Web commerce, have raised concerns regarding the opportunity for intellectual property theft. Consequently, there is a growing demand for secure property protection schemes. This paper presents watermarking techniques for intellectual property protection (IPP) of DSP filter cores. A design watermark is permanent information hidden into a design that identifies its creator, is largely imperceptible, offers a significant degree of tamper resistance, and provides easy, non-invasive copy detection. Our protection strategy incorporates design watermarking directly into the development process at various stages in the design hierarchy.

Traditional methods of IPP have included patents, copyrights, trademarks, trade secrets, and mask works (1). Companies currently rely on nondisclosure agreements, trade-secret litigation and encryption methods. However, these protection mechanisms are generally considered inadequate, especially for reusable IP cores and their electronic distribution. Recently several techniques for watermarking of hard and soft IP cores have been proposed. The key idea of watermarking for IPP is to impose a set of additional constraints during the design and implementation of IP which uniquely encodes the signature of the author. For example, one may vary or add additional timing constraints during the logic synthesis phase, or routing constraints at the physical design stage.

Since 1996, the effectiveness of the generic scheme for watermarking-based IPP has been demonstrated at the algorithm level (2), behavioral level (3), logic synthesis (4), in FPGA designs (5), at the physical design (6), and in the design hierarchy (7). An IP core which contains a watermark in the early stage of the design flow, for instance at the algorithm level, offers a greater degree of protection than one which is watermarked at a later stage, such as at the physical design stage. This fact is because the former requires undoing several layers of the design in order to recover the initial source of the watermark (8).

In this paper, we also propose, demonstrate, and evaluate the first algorithm-level watermarking technique for reusable DSP filter cores. The proposed method involves embedding the watermark directly into the filter specification. Since elimination of the watermark is virtually impossible without complete re-design of the core, this scheme will provide a significant degree of protection. In addition, this scheme involves an easy, non-invasive copy detection, that is, one can simply apply a unit impulse signal at the input. We present two FIR filter cores with IPP provided at different design levels and compare the benefits and limitations at each level.

Related Work

Data watermarking , also known as data hiding, a form of steganography, embeds data into digital media for the purpose of identification, annotation, and copyright. Throughout history, a multitude of methods and variations have been used to hide information. Recently, the proliferation of digitized media and the internet revolution are creating a pressing need for copyright enforcement schemes to protect copyright ownership.

Several techniques for data hiding in digital images, audios, videos and texts have been developed. Two methods for watermarking images are proposed in [Sch94a](9), which are highly sensitive to noise and are easily corrupted. A promising method based on spread-spectrum has been proposed [Cox96](10), which is difficult to intercept and remove but may introduce perceivable distortion into the host signal. Boney, Tewfik and Hamdy presented a technique for embedding digital watermarks into audio signals [Bon96](11).

The key difference of our proposed approach with these techniques is that all of them attempt to embed the watermark in the final object while our approach is incorporated in the design process.

0-7803-5443-5/99/$10.00©1999 IEEE

Hierarchical Watermarking Approach

We are primarily interested in protecting signal processing blocks, and in particular those used for signal filtering. While the techniques developed here are more broadly applicable, we will limit our discussion to the filtering context.

A. Watermarking at the Algorithm Level

The process of watermarking at the algorithm level involves hiding the owner's identification in the filter specification during the development of the transfer function. The identity signature code is encoded into the filter's magnitude response by manipulating the magnitude vector within the passband region. Fig. 1 shows how a 7-bit signature *011010* can be embedded into the filter specification. Since the MATLAB *remez* function allows specification of the magnitude response in a piecewise linear manner, we divide the passband region into seven approximately equal bands and vary the magnitude by a small amount, δ, between bit transitions. Small positive offsets code the value 1, while small negative offsets code the value 0. The resulting magnitude response is shown in Fig. 2. Notice the slight degradation in filter response. To improve this response, we could either vary the filter order and/or the transition band width. Note the ripple behaviour in the passband region. Herein lies the essense of our watermarking technique: constrain the extremes of the passband ripple to a bit pattern that exactly matches our 7-bit signature code.

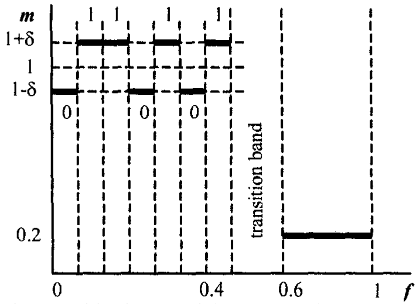

Fig. 1 Filter specification containing watermark sigunature 0110101

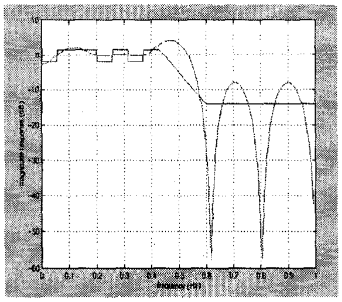

Fig. 2 Magnitude response of the filter specified in Fig. 1

B. Watermarking at the Architecture Level

We provide here a method for watermarking the transpose form FIR filter structure. However, we believe that the techniques we present here apply to other FIR form structures. The transpose form FIR filter structure is a pipelined structure, with each pipeline stage consisting of a multiplier-adder-delay basic block functions. The key in watermarking at the architecture level is to make circuit transformations using the basic blocks of each pipeline stage without altering the transfer function of the filter. Fig. 3 illustrates two basic block transformations. Each structure can encode a 2-bit code: 00, 01, 10.

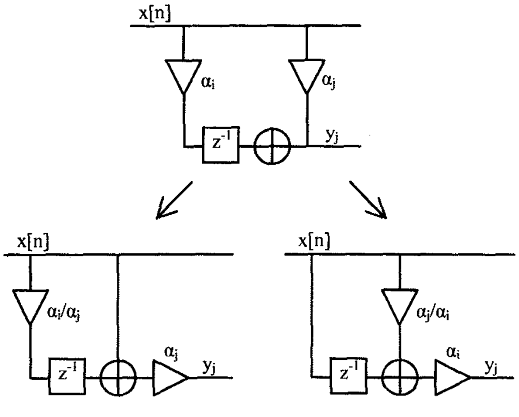

Fig. 3 Architecture level circuit transformations

C. Experimental Results

Three filter cores were designed according to the following criteria (12):

Passband	0.0 – 3.0 kHz
Stopband 1	4.0 – 4.6 kHz
Stopband 2	› 4.6 kHz
Passband ripple	± 0.125 dB
Stopband 1 ripple	- 14 dB
Stopband 2 ripple	- 32 dB

The magnitude response of the filter based on this specification, a sampling frequency of 16000 samples/second, and 31 taps is shown in Fig. 4.

To watermark this filter, we initially increased the number of taps from 31 to 63, and embedded a 12-bit signature *100110101001* by dividing the passband region into twelve equal frequency bands of 250 Hz each (Fig. 5). This gave us a starting point from which we could then vary filter parameters and the watermark bit length in order to observe their impact on the filter performance. Fig. 6 illustrates the effects of varying the filter length parameter on the watermark. As the number of taps decreases, so does the quality of the watermark. At 41 taps, the signature is still decipherable. However, at 31-taps, which is the length of the non-watermarked filter, the passband ripple behavior no longer follows the signature pattern.

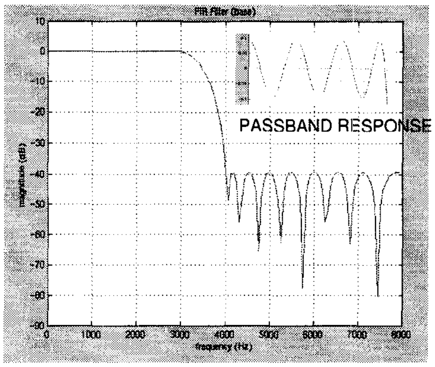

Fig. 4 31-tap non-watermarked filter

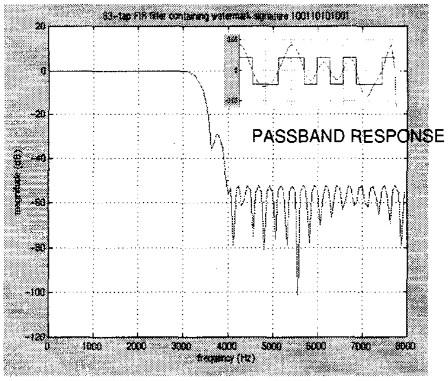

Fig. 5 63-tap watermarked filter

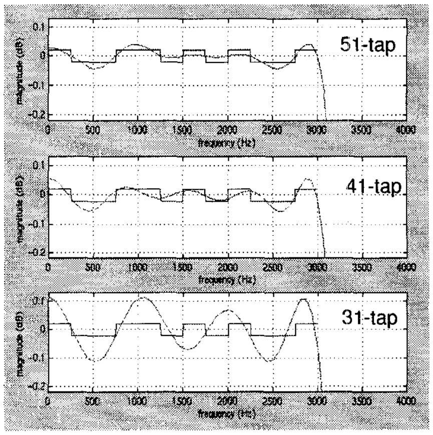

Fig. 6 Effects of varying filter lengths on the watermark

Fig. 7 shows a 33-tap filter with a 6-bit signature *101101*. In this algorithm watermarking scheme, we allow a single maximum to occur between consecutive 1s. Fig. 8 shows an architecture model of this filter. Note we used a different signature to watermark at the architecture level. The filter design was verified with a DSP simulation tool, *DSP Canvas*. The simulation testbench consisted of a software (algorithm) model of the FIR filter using the filter coefficients (floating point precision) generated from MATLAB, and two schematic (architecture) models: a floating-point model and a fixed-point (CSD) model. The simulation results showed both architecture models to be within the required filter specification. The circuit was implemented in VHDL. The data word length was arbitrarily set to 20 bits and the internal word length set to twice the data word length.

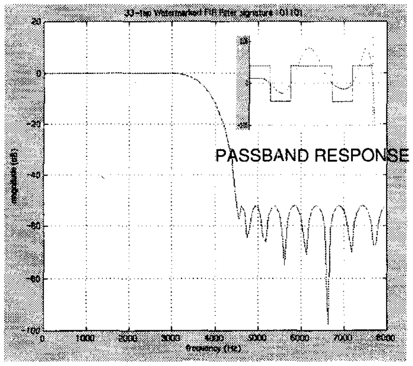

Fig. 7 Experimental watermarked 33-tap filter

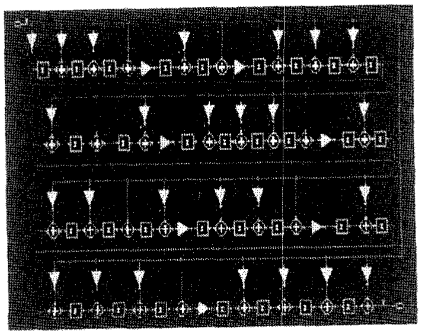

Fig. 8 Architecture model of the watermarked 33-tap FIR filter

Fig. 9 shows the core layout of the non-watermarked and watermarked designs. The watermarked core shown here contains watermarks at both the algorithm and architecture levels. Table 1 shows the areas of the filter cores after running the designs through Cadence place and route tools. The cost in area incurred by the design watermarked at only the algorithm level is about 7%, whereas the cost for watermarking at both the algorithm and architecture levels is approximately 38%. In the later case, the increase in area was primarily due to a higher internal word precision required as result of dividing coefficients.

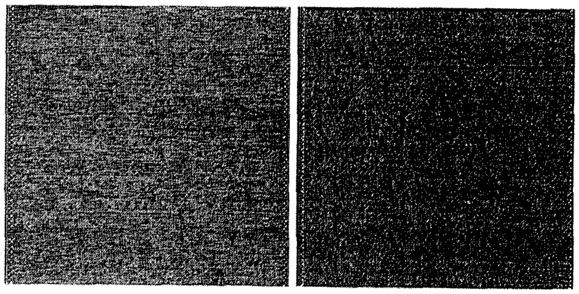

Fig. 9 Non-watermarked and watermarked filter cores

Table 1. Area results of filter cores after place and route

Core	Chip Area (μm^2)	Cell Area (μm^2)
31-tap FIR filter (non-watermarked)	5080516	3306920
33-tap FIR filter (watermarked at algorithm level)	5484964	3575920
33-tap FIR filter (watermarked at algorithm and architecture levels)	8145316	5383360

Summary

We have presented a hierarchical watermarking scheme for the intellectual property protection of DSP filter cores. This approach requires a unique watermark at each level of the design process or hierarchy. We have also proposed and demonstrated the first algorithm-level watermarking technique for reusable DSP filter cores which embeds a watermark directly into the filter coefficients during the filter specification phase. We believe that the protection mechanisms we provide here offer a high degree of tamper resistance, and provide easy, non-invasive copy detection.

References

(1) D.L. Drinkwater, "Intellectual property: rich by-product of intellectual capital," *Thirteenth Annual Applied Power Electronics Power and Exposition,* vol.1, pp. 41-45, February 1998.

(2) I. Hong and M. Potkonjak, "IPP Techniques for Behavioral Specifications," unpublished manuscript, 1998.

(3) I. Hong and M. Potkonjak, "Behavioral synthesis techniques for intellectual property protection," unpublished, 1997.

(4) D. Kirovski, Y-Y. Huang, M. Potkonjak and J. Cong, "Intellectual property protection by watermarking combinational logic synthesis solutions," *Proc. ACM/IEEE Design Automation Conf.*, pp. 194-198, November 1998.

(5) J. Lach, W.H. Mangione-Smith and M. Potkonjak, "FPGA fingerprinting techniques for protecting intellectual property," *IEEE Custom Integrated Circuits Conference,* 1998.

(6) A.B. Kahng, S. Mantik, I.L. Markov, M. Potkonjak, P. Tucker, H. Wang and G. Wolfe, "Robust IP watermarking methodologies for physical design," *Proc. ACM/IEEE Design Automation Conf.*, pp. 782-787, June 1998.

(7) E. Charbon, "Hierarchical watermarking in IC design," *IEEE Custom Integrated Circuits Conference*, 1998.

(8) K. Hodor, "Adopting methods to protect intellectual property from pirates," *Silicon Strategies*, pp. 35-40, February 1998.

(9) B. Shneir, *Applied Cryptography: Protocols, Algorithms, and Source Code in C,*" New York: John Wiley & Sons, 1998.

(10) I.J. Cox, et al., "Secure spread spectrum watermarking for images, audio, and video," *International Conf. On Image Processing*, 1996.

(11) L. Boney, et al., "Digital watermarks for audio signals," *International Conf. On Multimedia Computing and Systems,* 1996.

(12) L. Claesen, et al., "Automatic synthesis of signal processing benchmark using the CATHEDERAL silicon compilers," *IEEE Custom Integrated Circuits Conference*, pp. 14.7.1-14.7.4, 1988.

(13) J.G. Proakis and D.G. Manolakis, *Digital Signal Processing: Principles, Algorithms and Applications*, Prentice-Hall, 1996.

(14) S.K. Mitra, *Digital Signal Processing: A Computer-Based Approach*, McGraw-Hill, 1998.

(15) R. Jain, P.T. Yang, and T. Yoshino, "FIRGEN: A computer-aided design system for high performance FIR filter integrated circuits," *IEEE Trans. On Signal Processing*, vol. 39, no. 7, pp. 1655-1668, July 1991.

(16) MATLAB, *Signal Processing Toolbox*, The Math Works, Inc.

(17) T.W. Parks and J.H. McClellan, "Chebyshev approximation for non-recursive digital filters with linear phase," *IEEE Trans. On Circuit Theory,* CT-19:189-194, 1972.

(18) DSP Canvas, Angeles Design Systems, Inc.