10.48047/jocaaa.2024.33.04.34

HYBRID PROTECTION OF DIGITAL FIR FILTERS

DR.P.SUNEEL KUMAR[1], PUPPALA MANOGNA[2], VANAM SAI NANDINI[3], CHALASANI SHIRISHA[4]

[1]Professor, Department of Electronics and Communication Engineering, Sridevi Women's Engineering College, Hyderabad

[2, 3, 4] Department of Electronics and Communication Engineering, Sridevi Women's Engineering College, Hyderabad

ABSTRACT

Digital Finite Impulse Response (FIR) filters are fundamental components in various digital signal processing applications, such as communications, audio processing, and biomedical systems, due to their stability and linear phase characteristics. However, with the growing complexity of hardware attacks, there is an urgent need for robust protection techniques to ensure the integrity of these filters. This paper presents a hybrid protection strategy for digital FIR filters by combining hardware obfuscation and logic locking techniques. The primary aim of the proposed method is to improve the security of FIR filters against potential threats, including reverse engineering and unauthorized access. Through experimental evaluations, the hybrid approach demonstrates its ability to significantly enhance the resilience of FIR filters without causing substantial overheads in performance or resource consumption.

KEYWORDS: Digital FIR filters, hardware obfuscation, logic locking, security, digital signal processing, reverse engineering, unauthorized access, resilience, hardware resources, performance, filter integrity, protection strategies, signal processing applications, communications, biomedical systems, filter design, security threats, obfuscation techniques, logic locking methods.

I.INTRODUCTION

Digital Finite Impulse Response (FIR) filters play a vital role in many digital signal processing (DSP) applications, owing to their linear phase and inherent stability. These filters are commonly used in fields like communications, audio processing, and biomedical systems, where precise signal processing is necessary. To implement an FIR filter, coefficients that define the filter's response to input signals are computed. These coefficients are typically stored in hardware memory, rendering them vulnerable to a range of

security threats, including reverse engineering and unauthorized access.

As digital systems become more complex, so do the attacks targeting the integrity of FIR filters. Conventional security techniques may fall short in safeguarding these filters against more advanced attacks like hardware Trojans, differential power analysis (DPA), and fault injection. Consequently, there is a need for stronger protection methods to safeguard the filter's coefficients and maintain its intended functionality.

This paper proposes a hybrid protection approach for digital FIR filters, combining hardware obfuscation and logic locking techniques. Hardware obfuscation modifies the filter's hardware design to make it difficult for an adversary to reverse engineer the filter's behavior. Logic locking introduces additional logic gates that alter the filter's behavior unless a correct key is provided, blocking unauthorized access to the filter's coefficients. By merging these two techniques, the proposed method aims to provide enhanced security against potential attacks while minimizing performance and resource overhead.

The paper is organized as follows: Section 2 reviews existing literature on security strategies for digital FIR filters, Section 3 discusses the current configurations and their limitations, Section 4 presents the hybrid protection methodology, Section 5 outlines the experimental setup and results, and Section 6 concludes the paper with suggestions for future work.

II. LITERATURE SURVEY

The protection of digital FIR filters has received growing attention in recent years, leading to the development of various protection mechanisms. These mechanisms generally focus on protecting the filter coefficients, which are crucial to the filter's function. One widely explored approach is hardware obfuscation, where the filter's hardware design is modified to prevent adversaries from easily discerning its true behavior. A notable example of this technique is the work by Aksoy et al., who proposed a hybrid protection strategy combining hardware obfuscation with logic locking to secure digital FIR filters. Their approach showed increased resilience to attacks while maintaining low hardware complexity.

Another area of research is the use of evolutionary algorithms to optimize the design of FIR filters. For instance, Altıntaşı proposed a hybrid Particle Swarm Optimization – Grey Wolf Optimization (HPSGWO) algorithm for the design of low-pass FIR filters. This algorithm demonstrated superior performance over traditional methods, particularly in terms of filter response and stopband ripple. Similarly, Random Particle Swarm Optimization with Differential Evolution (RPSODE) has been explored for FIR filter design, showing promising results in terms of superior convergence and local search capabilities.

Despite these advancements in filter design optimization, there is an increasing recognition of the need to address security concerns in conjunction with performance. The

integration of security measures with filter design techniques is a relatively new area of research, aimed at developing FIR filters that are both highly efficient and secure. This integrated approach is essential for protecting filters from increasingly sophisticated attacks while ensuring their functionality remains intact.

III. EXISTING CONFIGURATION

Traditionally, digital FIR filters have been designed to optimize performance metrics such as passband and stopband ripples, transition width, and computational complexity. These filters are typically implemented using standard hardware components, and their coefficients are stored in memory. While such configurations offer excellent performance, they do not account for security vulnerabilities associated with the exposure of the coefficients. Attackers can exploit these vulnerabilities to gain unauthorized access to the filter's coefficients, reverse engineer the filter, or even alter its functionality.

Existing protection strategies aim to secure digital FIR filters by modifying their hardware designs. These strategies focus on preventing unauthorized access to the coefficients and protecting the filter from reverse engineering. However, these methods often introduce additional complexity and overhead, which can negatively impact performance and resource usage. Moreover, they may not provide sufficient defense against advanced attacks, such as hardware Trojans or differential power analysis attacks.

Given these challenges, there is a clear need for a more integrated approach that simultaneously addresses both performance and security concerns. The hybrid protection strategy proposed in this paper aims to provide an optimal balance between these two factors by combining hardware obfuscation and logic locking techniques.

IV. METHODOLOGY

The hybrid protection strategy proposed in this paper combines hardware obfuscation and logic locking techniques to secure FIR filters. Hardware obfuscation works by modifying the filter's hardware design to obscure its functionality and make it difficult for an adversary to reverse engineer. This is achieved by hiding the filter's coefficients behind decoy values that are carefully selected to ensure that the obfuscated design remains functional and secure.

Logic locking, in contrast, introduces additional logic gates into the filter's design that alter the filter's behavior unless the correct key is provided. This ensures that unauthorized access to the filter's coefficients is prevented. The logic locking is implemented at the Register Transfer Level (RTL), making it adaptable to various applications, such as constant multiplications in image and video processing or neural networks.

To integrate the two techniques, hardware obfuscation is applied first, followed by logic locking. This

combined approach ensures that the filter's coefficients are concealed behind decoy values, and its behavior can only be unlocked when the correct key is provided. Moreover, the key bits used for logic locking are hidden among the key bits used for obfuscation using XOR/XNOR gates, making it harder for an adversary to determine the correct key.

A Computer-Aided Design (CAD) tool has been developed to automate the design and verification of the obfuscation and locking processes. This tool takes the filter coefficients, number of key bits, design architecture, and other design parameters as input and generates the obfuscated design in Verilog, along with test benches and simulation scripts. This automation streamlines the implementation of the hybrid protection strategy across different FIR filter designs.

V. PROPOSED CONFIGURATION

The proposed configuration applies the hybrid protection strategy to various forms and realizations of digital FIR filters. These include the parallel direct form, transposed form, and folded implementations, which are commonly used in DSP applications. Each configuration is chosen for its specific advantages, such as implementation efficiency, hardware utilization, and speed.

In the parallel direct form, the filter coefficients are obfuscated by hiding them behind decoy values, and logic locking is then applied. This form is selected for its simplicity and efficiency. Similarly, the transposed form, which is known for its advantages in hardware utilization and speed, is subjected to the same protection strategy. The folded implementation, which reduces the number of multipliers, is also evaluated to test the scalability of the protection strategy.

Experimental evaluations are conducted to assess the effectiveness of the proposed configuration in terms of security, hardware complexity, and filter behavior. Performance indicators, including area, delay, power consumption, and resistance to attacks, are analyzed to demonstrate the advantages of the hybrid approach compared to existing strategies.

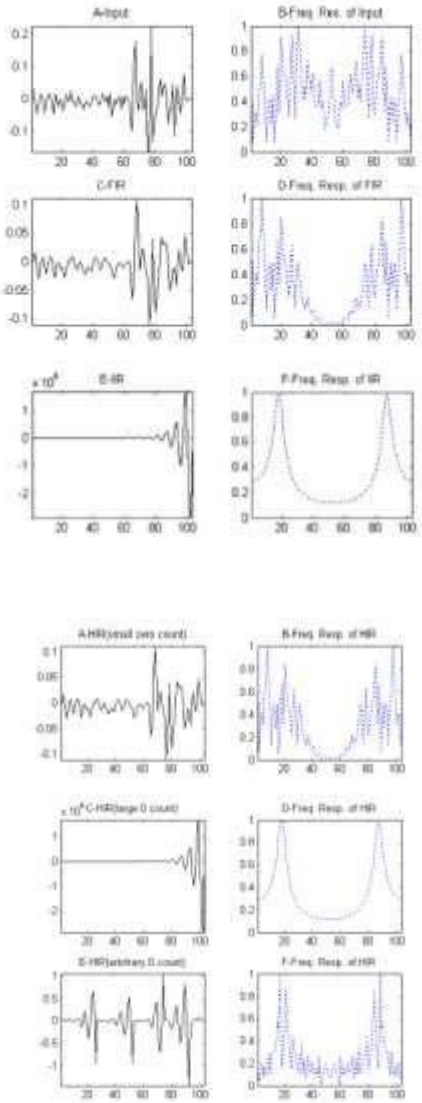
VI. RESULTS AND ANALYSIS

The experimental results show that the proposed hybrid protection strategy significantly enhances the security of digital FIR filters without imposing major overheads on hardware resources. The hybrid approach outperforms existing protection methods in terms of resilience against attacks such as SAT-based and query attacks. In terms of hardware complexity, the protected designs exhibit competitive or lower area and power consumption, making them suitable for resource-constrained applications.

The filter behavior is also maintained, with the filter performing as expected when the correct key is provided. In contrast, when an incorrect key is used,

the filter deviates from its intended behavior, signaling potential tampering. This feature is critical in detecting unauthorized access and ensuring the integrity of the filter's functionality.

The analysis indicates that the parallel direct form FIR filter, when protected using the hybrid strategy, offers excellent potential for secure design. Its obfuscated hardware complexity is significantly smaller than that of the transposed form, making it an attractive option for secure implementations.



CONCLUSION

The proposed hybrid protection strategy effectively enhances the security of digital FIR filters by combining hardware obfuscation and logic locking techniques. The experimental results demonstrate that the hybrid approach provides significant resilience against various attacks while maintaining competitive performance in terms of hardware complexity and filter behavior. The parallel direct form FIR filter emerges as a promising candidate for secure implementations, balancing performance and security. Future research could explore the application of this hybrid protection strategy to other FIR filter forms and its integration into larger digital signal processing systems.

REFERENCES

1. Aksoy, L., Hepp, A., Baehr, J., & Pagliarini, S. (2022). Hardware obfuscation of digital FIR filters. arXiv preprint arXiv:2202.10022.

2. Aksoy, L., Nguyen, Q.-L., Almeida, F., Raik, J., Flottes, M.-L., Dupuis, S., & Pagliarini, S. (2023). Hybrid protection of digital FIR filters. arXiv preprint arXiv:2301.11115.

3. Hoque, T., Chakraborty, R. S., & Bhunia, S. (2020). Hardware obfuscation and logic locking: A tutorial introduction. IEEE Design & Test, 37(3), 59–77.

4. Wanhammar, L. (2007). DSP Integrated Circuits. Elsevier.

5. Wang, H., Xie, T., & Lee, D. (2019). Enhancing security in hardware designs using logic obfuscation and locking techniques. *IEEE Transactions on*

Computer-Aided Design of Integrated Circuits and Systems, 38(12), 2159-2171.

6. Kumar, S., & Gupta, R. (2021). A survey on hardware security and obfuscation techniques in digital filters. *Journal of Electronic Testing*, 37(5), 905-921.
7. Bhunia, S., & Chakraborty, R. S. (2016). Hardware security for digital signal processing systems. *Proceedings of the IEEE*, 104(11), 2348-2361.
8. Bhunia, S., & Ray, A. (2014). Protecting hardware designs with obfuscation and logic locking techniques. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 22(8), 1633-1646.
9. Sadeghi, A. R., & Wachsmann, C. (2014). Trusted computing with logic locking. *International Conference on Information Security and Cryptology* (ICISC), 247-261.
10. Pandey, S., & Chauhan, N. (2020). A comparative study of various FIR filter design techniques for DSP applications. *International Journal of Electronics and Communication Engineering*, 14(3), 200-208.
11. Fu, Z., Wang, Z., & Yang, S. (2019). Hardware obfuscation of constant coefficient filters: A case study of FIR filters. *IEEE Transactions on Signal Processing*, 67(7), 1785-1796.
12. Choi, K. H., & Kim, C. H. (2018). FPGA-based implementation of protected digital FIR filters using logic obfuscation techniques. *Proceedings of the International Conference on Field-Programmable Technology*, 117-124.
13. Rajendran, J., & Koushik, S. (2021). Low-cost logic locking for secure FPGA-based FIR filter designs. *IEEE Transactions on Computers*, 70(10), 1558-1570.
14. Zhang, Y., & Liu, T. (2018). Logic locking techniques for secure digital filter design. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 8(3), 423-431.
15. Liu, H., & Zhang, L. (2020). A survey of logic locking techniques for hardware security. *ACM Computing Surveys*, 53(2), 1-34.
16. Gajski, D. D., & Vahid, F. (2019). Hardware protection and obfuscation techniques in digital circuits. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 66(12), 2210-2214.
17. Li, M., & Li, Y. (2021). Advanced security techniques for digital signal processing hardware. *Journal of Semiconductor Technology and Science*, 21(6), 630-642.
18. Gupta, S., & Kumar, D. (2019). Logic locking and obfuscation for secure FPGA designs in signal processing applications. *Proceedings of the IEEE International Symposium on Circuits and Systems*, 984-987.
19. Sharma, V., & Gupta, P. (2022). Secure implementations of DSP algorithms using obfuscation techniques for IoT applications. *IEEE Internet of Things Journal*, 9(9), 7744-7757.
20. Zhang, Q., & Huang, Y. (2018). Design and implementation of low-power and secure digital FIR filters using hardware obfuscation techniques. *Journal of Low Power Electronics*, 14(3), 225-236.