Hardware Security

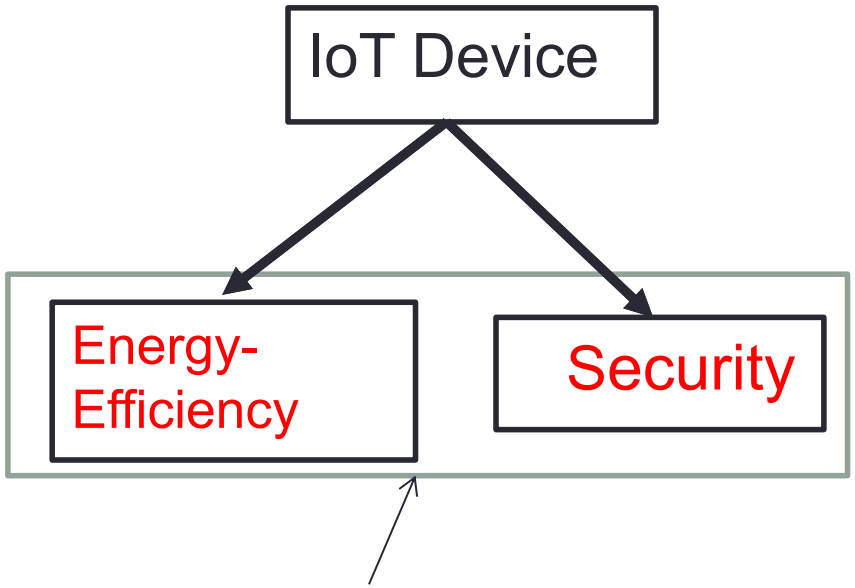
ICAN 2025

July 18,2025

Prof. Anirban Sengupta, FIET, FBCS, FIETE, SMIEEE
Professor, CSE, INDIAN INSTITUTE OF TECHNOLOGY INDORE

ACM Eminent Speaker, ACM India
IEEE Distinguished Visitor, IEEE Computer Society
IEEE Distinguished Lecturer, IEEE Consumer Electronics Society
Founder, IEEE CESoc Chapter – Bombay Section
Chair, IEEE Computer Society Distinguished Visitor Selection Committee
Editor-in-Chief, IET Computers & Digital Techniques (CDT)

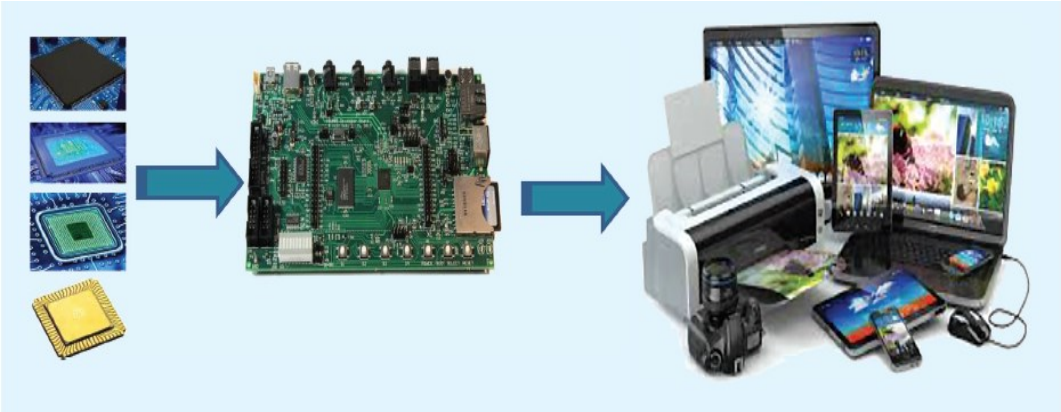
Challenges in Embedded and IoT Devices

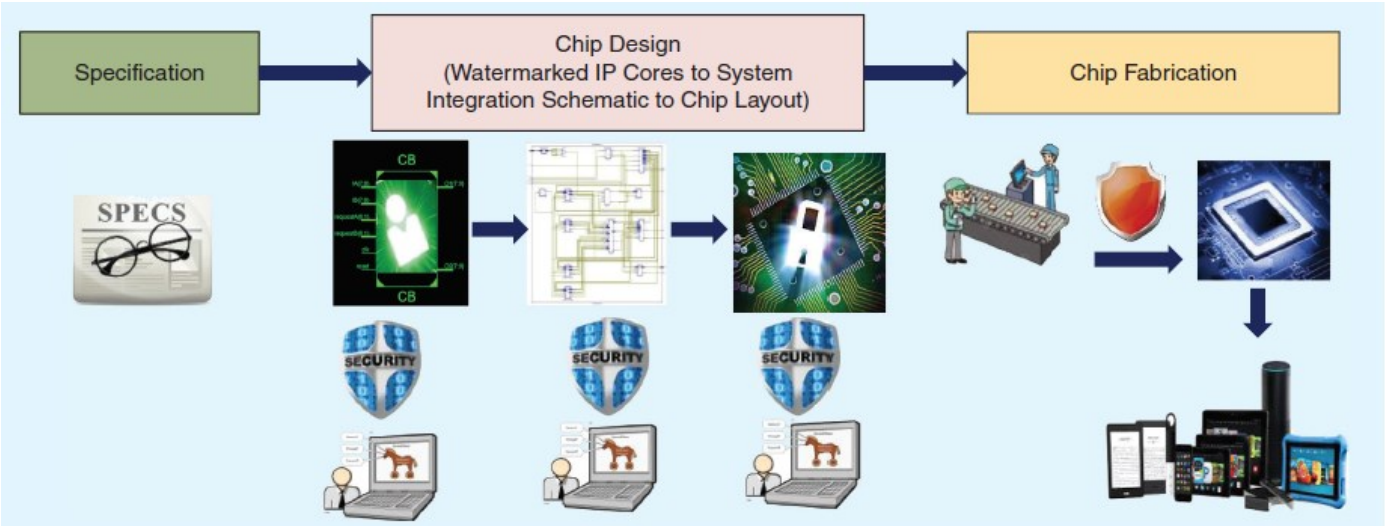


- Typically battery operated
  - Energy-efficient design
- Vulnerable to hardware/malware attacks
  - Power analysis attacks
  - IC piracy, IC counterfeiting, Hardware trojan

Cyberattacks are threat to reliability, safety, consumer's personal information and piracy or cloning of intellectual property (IP) core.

Consumer Electronics (CE) Device Vulnerabilities





Anirban Sengupta et. al "IP Core Protection and Hardware-Assisted Security for Consumer Electronics", **The Institute of Engineering and Technology (IET)**, 2019, Book ISBN: 978-1-78561-799-7, e-ISBN: 978-1-78561-800-0

INTRODUCTION

- Hardware Security and Intellectual Property (IP) Core protection is an emerging area of research for semiconductor community that focusses on protecting designs against standard threats such as reverse engineering, counterfeit, forgery, malicious hardware modification etc.

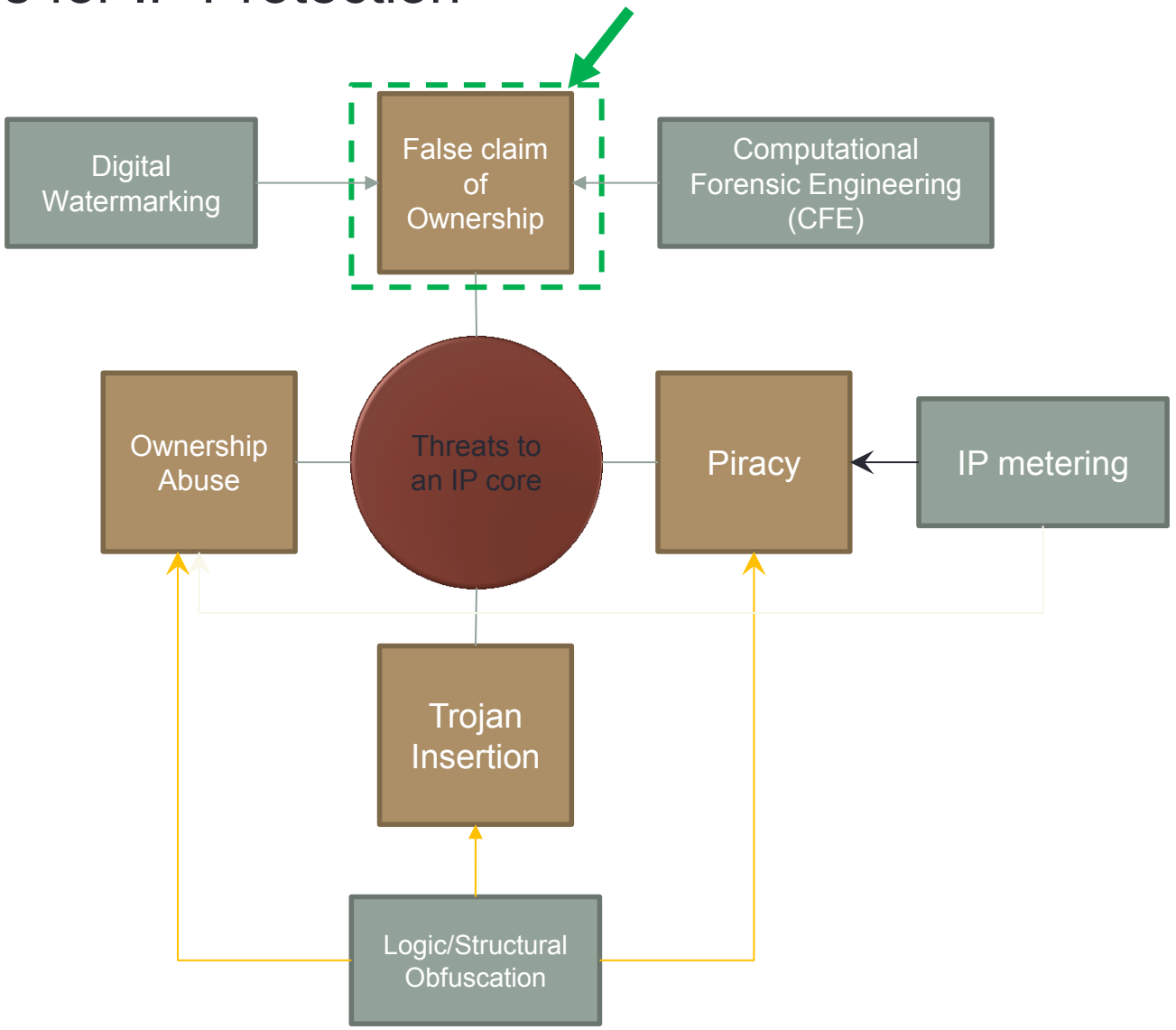
- Hardware security is broadly classified into two types: (a) authentication based approaches (b) obfuscation based approaches.

- The second type of hardware security approach i.e. obfuscation can again be further sub-divided into two types: (i) structural obfuscation (ii) functional obfuscation. Structural obfuscation transforms a design into one that is functionally equivalent to the original but is significantly more difficult to reverse engineer (RE), while the second one is active protection type that locks the design through a secret key.

Anirban Sengupta, Saraju P. Mohanty "IP Core Protection and Hardware-Assisted Security for Consumer Electronics", **The Institute of Engineering and Technology (IET)**, 2019, Book ISBN: 978-1-78561-799-7, e-ISBN: 978-1-78561-800-0

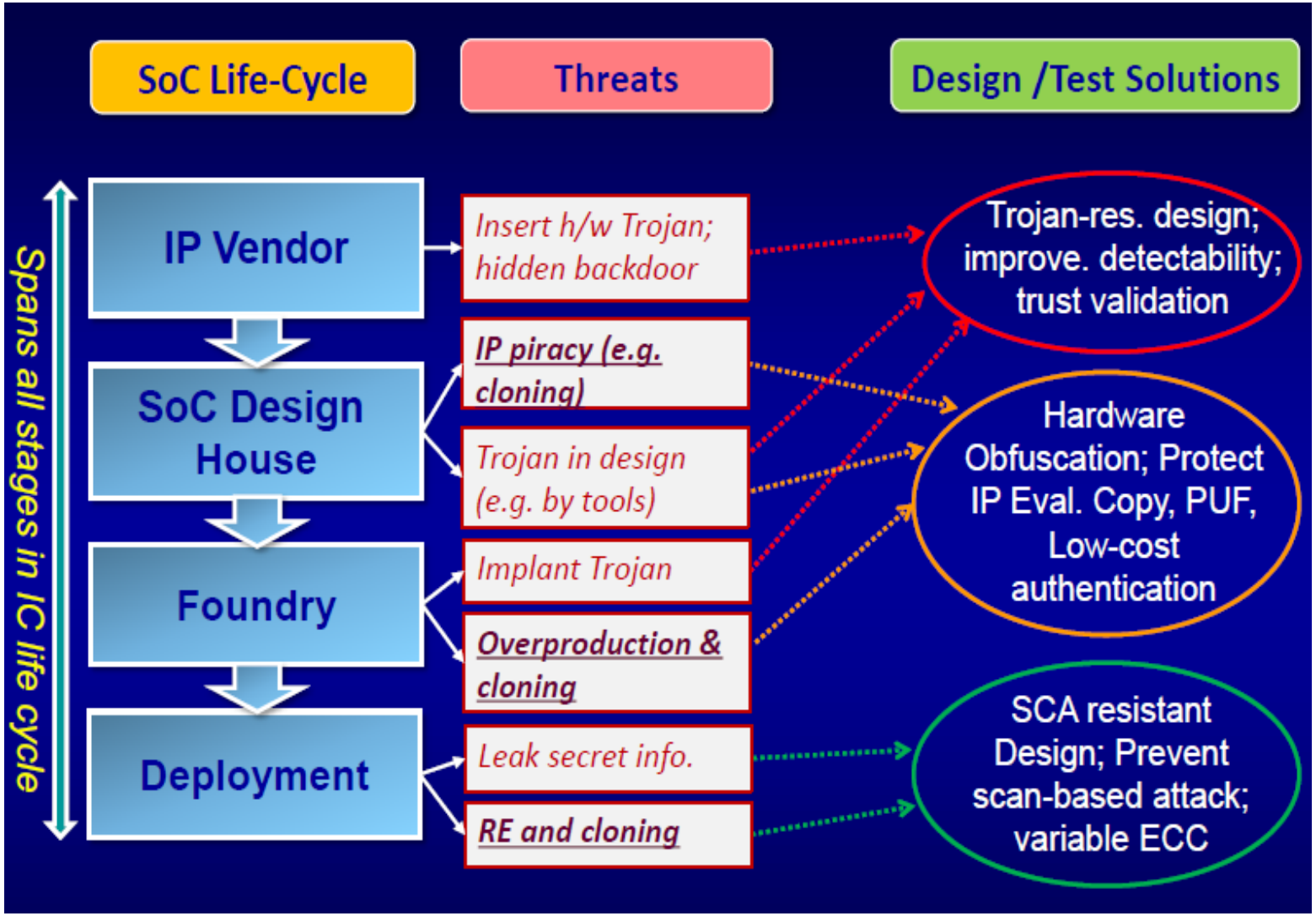
Anirban Sengupta, Mahendra Rathor "Protecting DSP Kernels using Robust Hologram based Obfuscation", **IEEE Transactions on Consumer Electronics**, 2019

Approaches for IP Protection

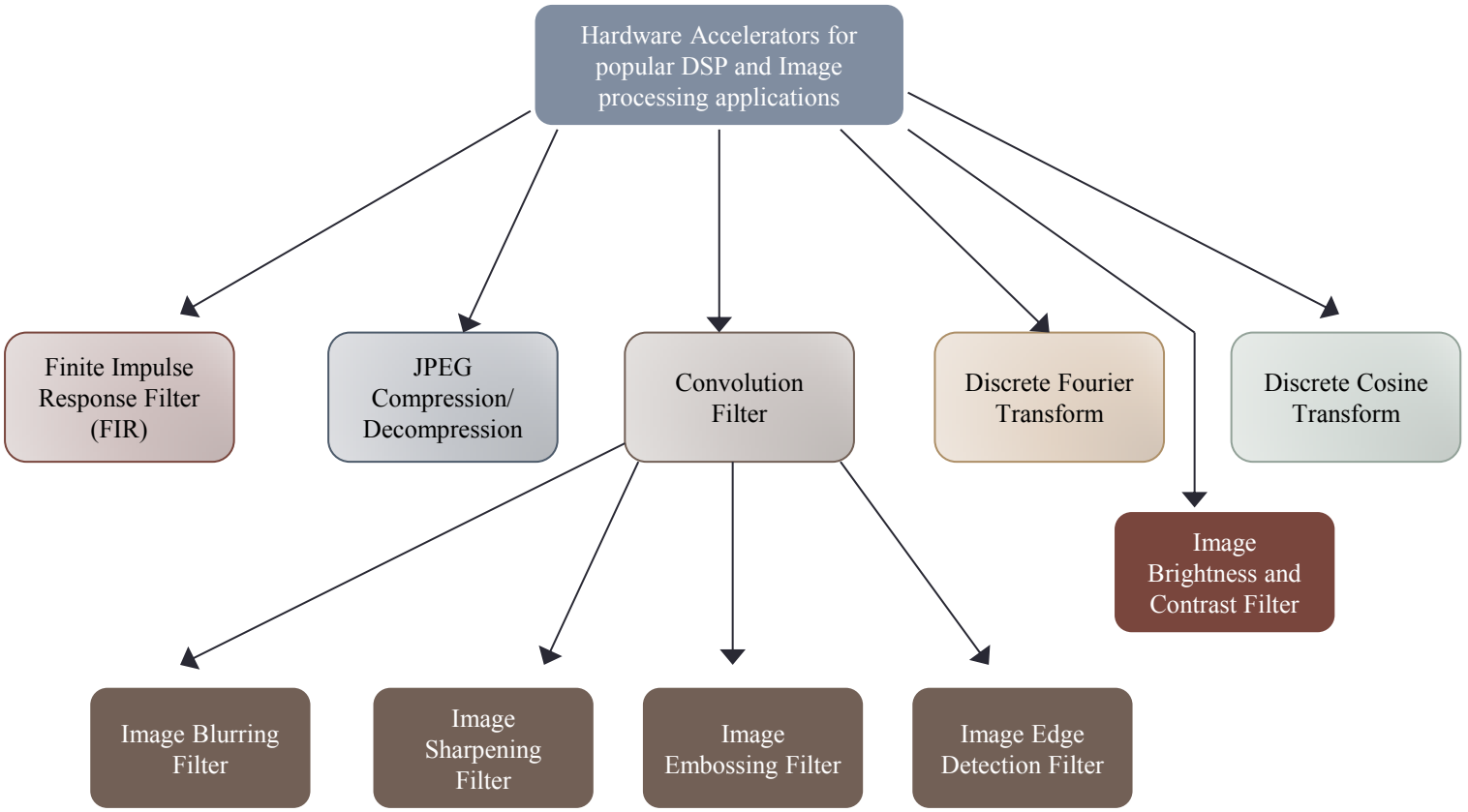


Anirban Sengupta, Dipanjan Roy, Saraju Mohanty, Peter Corcoran "DSP Design Protection in CE through Algorithmic Transformation Based Structural Obfuscation", **IEEE Transactions on Consumer Electronics**, Volume 63, Issue 4, November 2017, pp: 467 - 476

IP Core Protection and Hardware Security



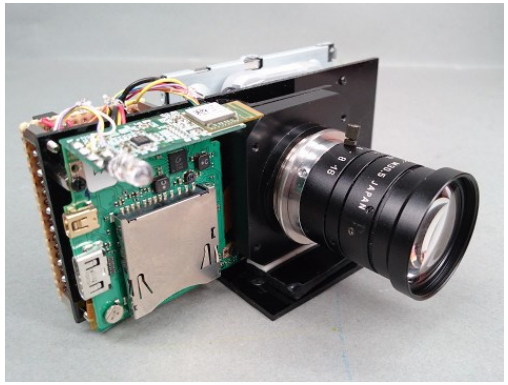
Real World Applications

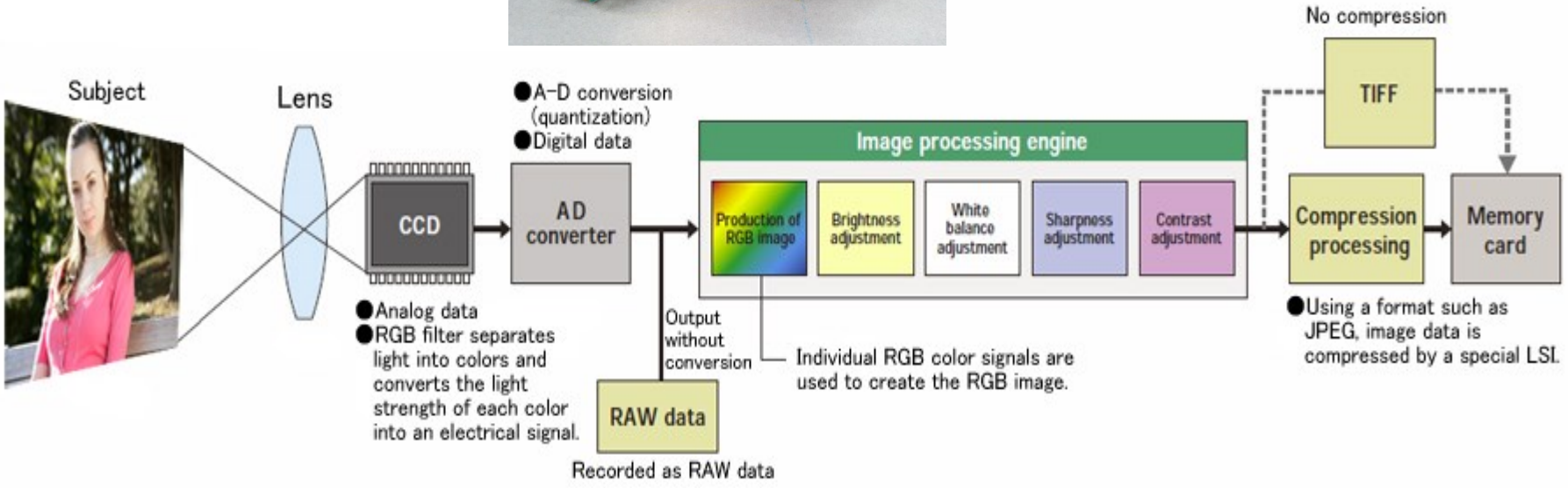


Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", The Institute of Engineering and Technology (IET), 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

Example of CE Device : Digital Camera

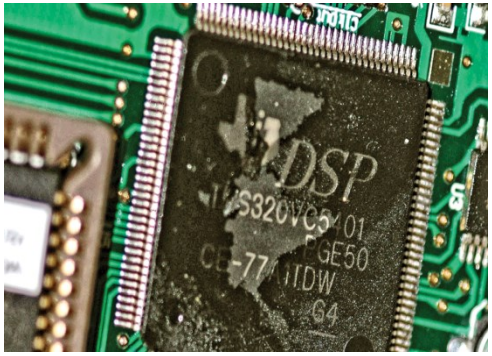
- ✓ Simply converting an analog image that is captured by the CCD into digital data does not create a digital image.
- ✓ Only after the image processing engine and CODEC engine performs a variety of calculations on a huge amount of digital image data can we see a completed color/grayscale image.





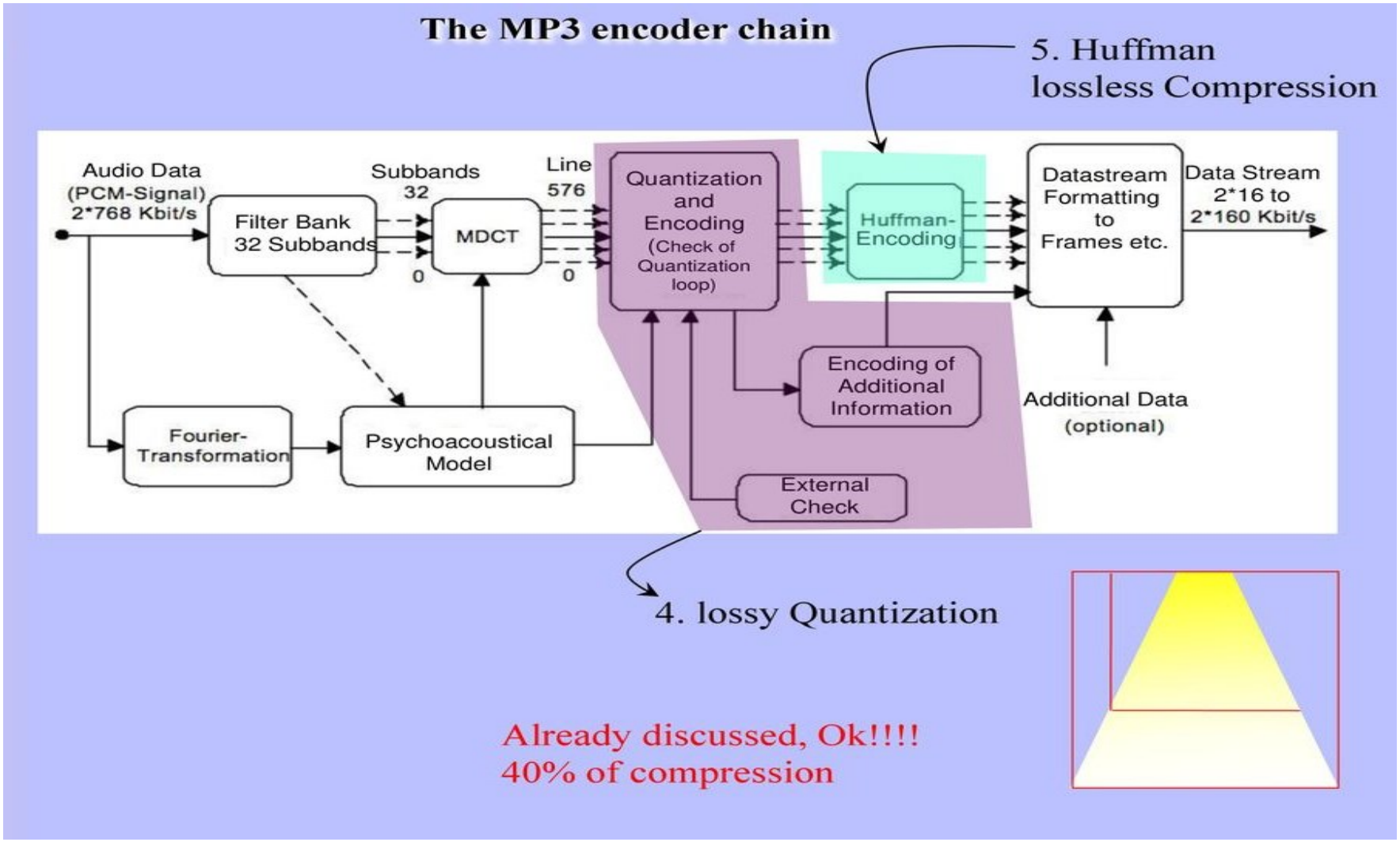
Example of DSP Core in Digital Camera

- ✓ But when you're recording video, if the videos are not processed fast, then you start missing frames.
- ✓ This is why digital video cameras almost always have a second microprocessor built-in, dedicated to video calculations. This is a Digital Signal Processor or DSP — the job of which is to perform repetitive mathematical tasks in real time.
- ✓ So, while your iphone's main microprocessor is checking to see if you have an incoming call, running your email in the background and managing your Wi-Fi signal, when video is coming through the lens, those calculations are handed off to a second microprocessor.

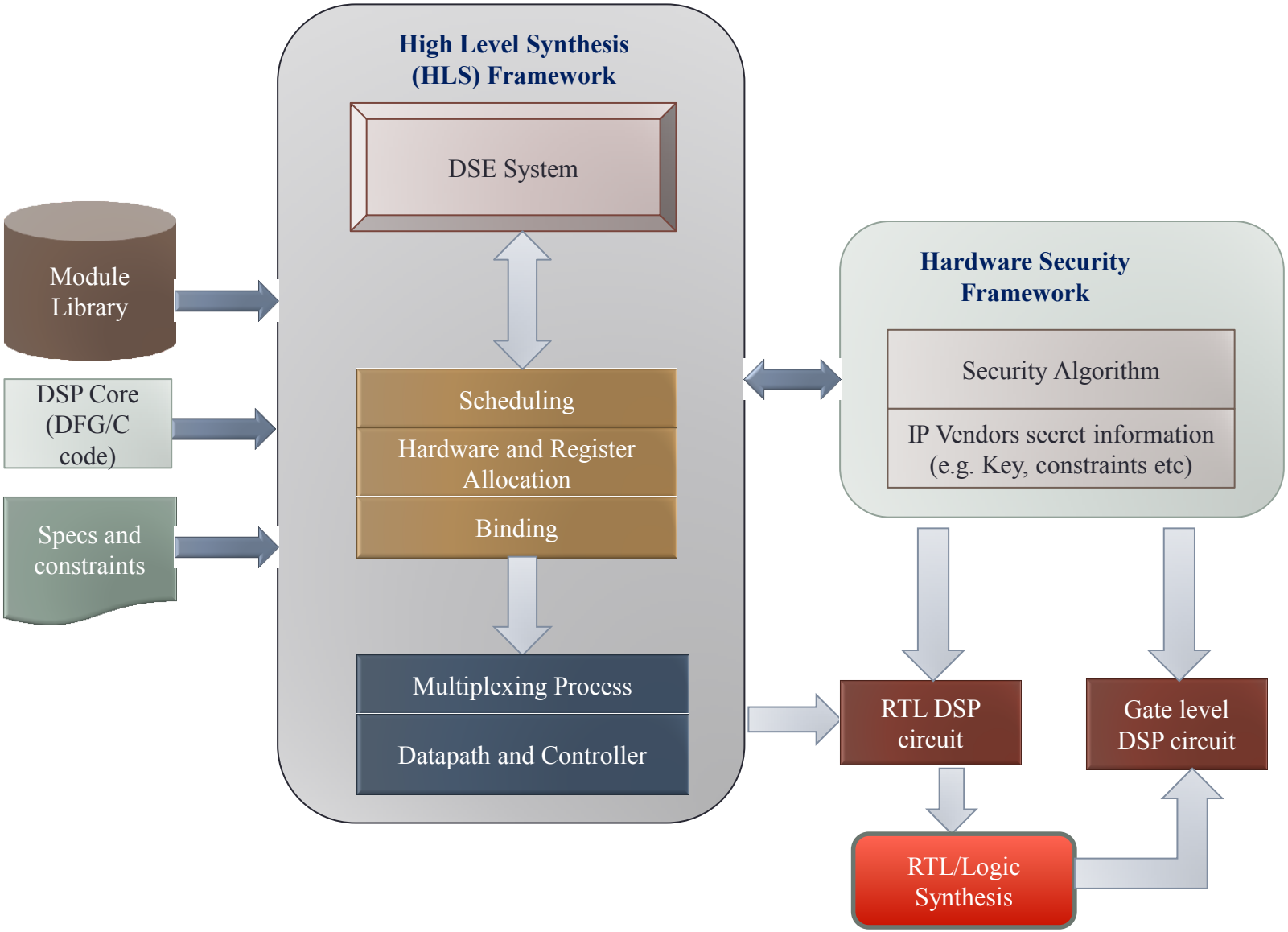


Nikon EXPEED, a system on a chip including an image processor, video processor, digital signal processor (DSP) and a 32-bit microcontroller controlling the chip

Another example of DSP in CE

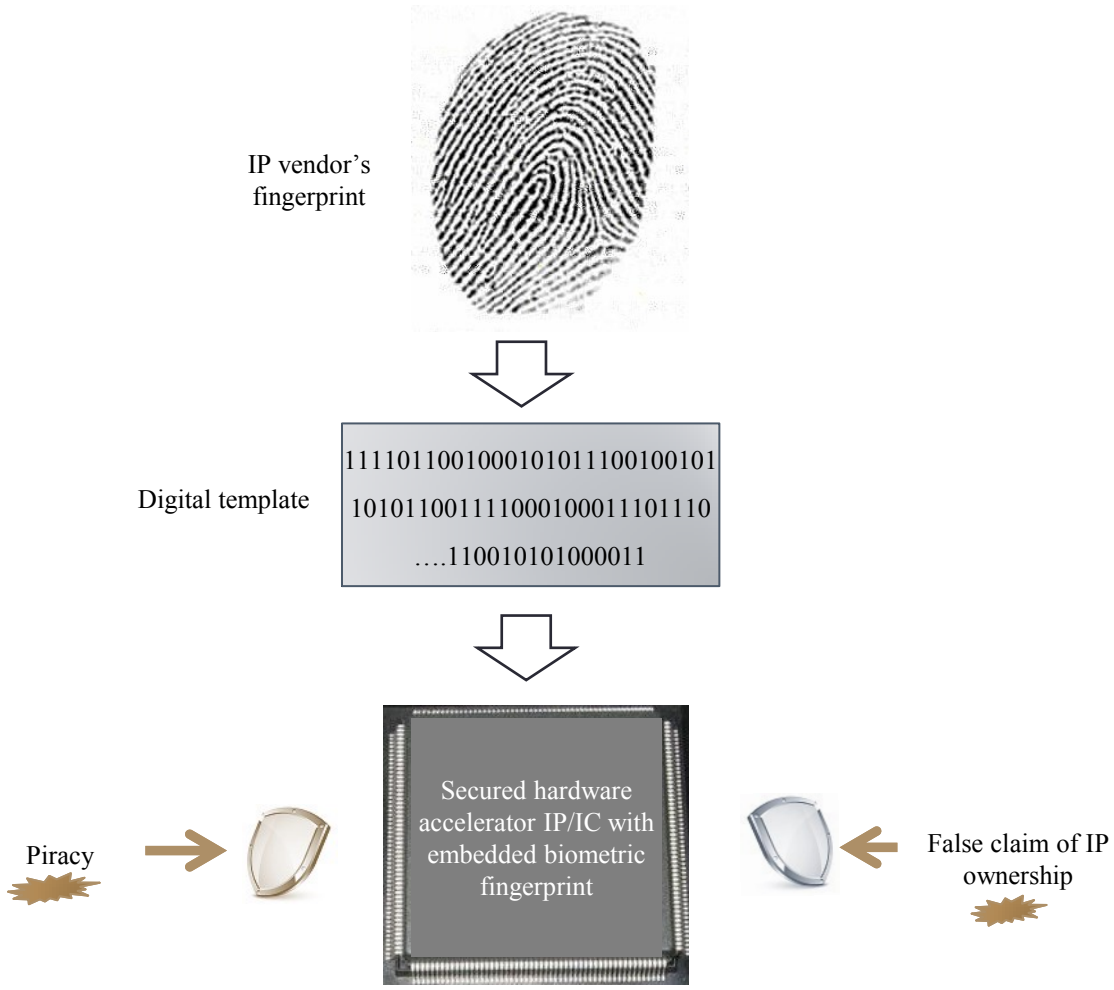


Hardware Security Algorithms integrated with HLS and Logic Synthesis phases



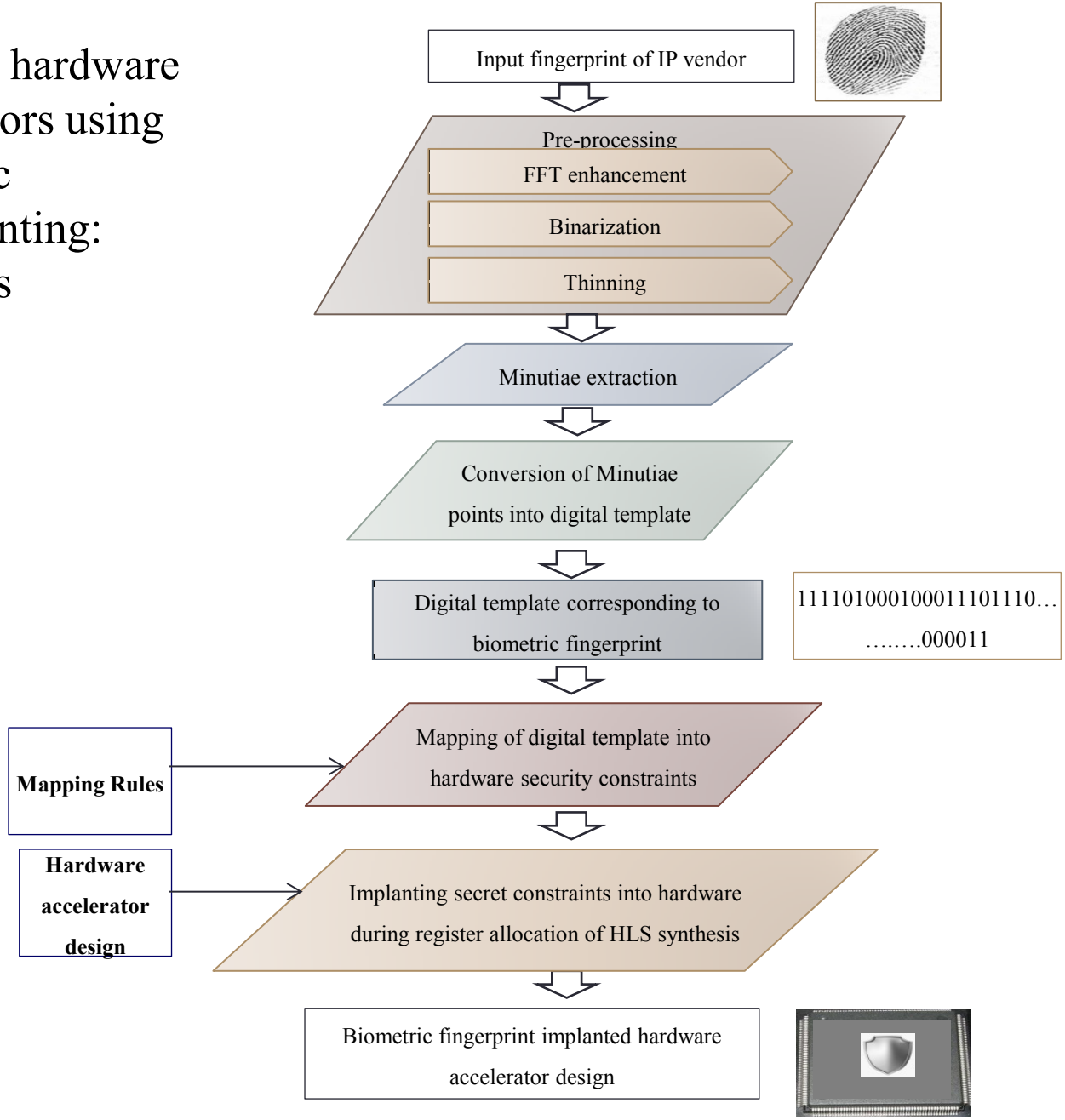
Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", The Institute of Engineering and Technology (IET), 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

Securing hardware accelerators using biometric fingerprinting: Forensics



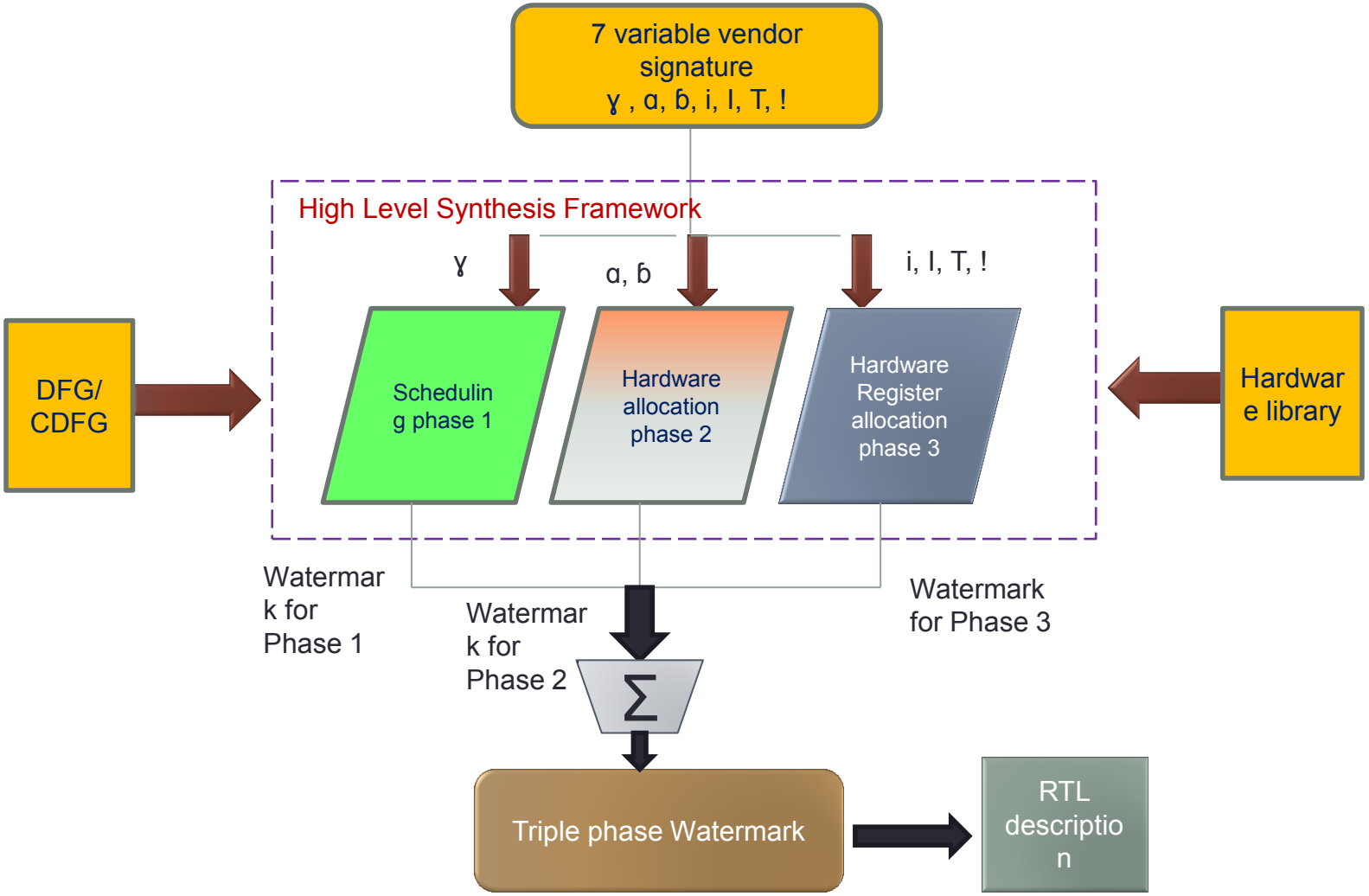
Anirban Sengupta, Mahendra Rathor "Securing Hardware Accelerators for CE Systems using Biometric Fingerprinting", **IEEE Transactions on Very Large Scale Integration Systems (TVLSI)** , Accepted, 2020

Securing hardware accelerators using biometric fingerprinting: Forensics



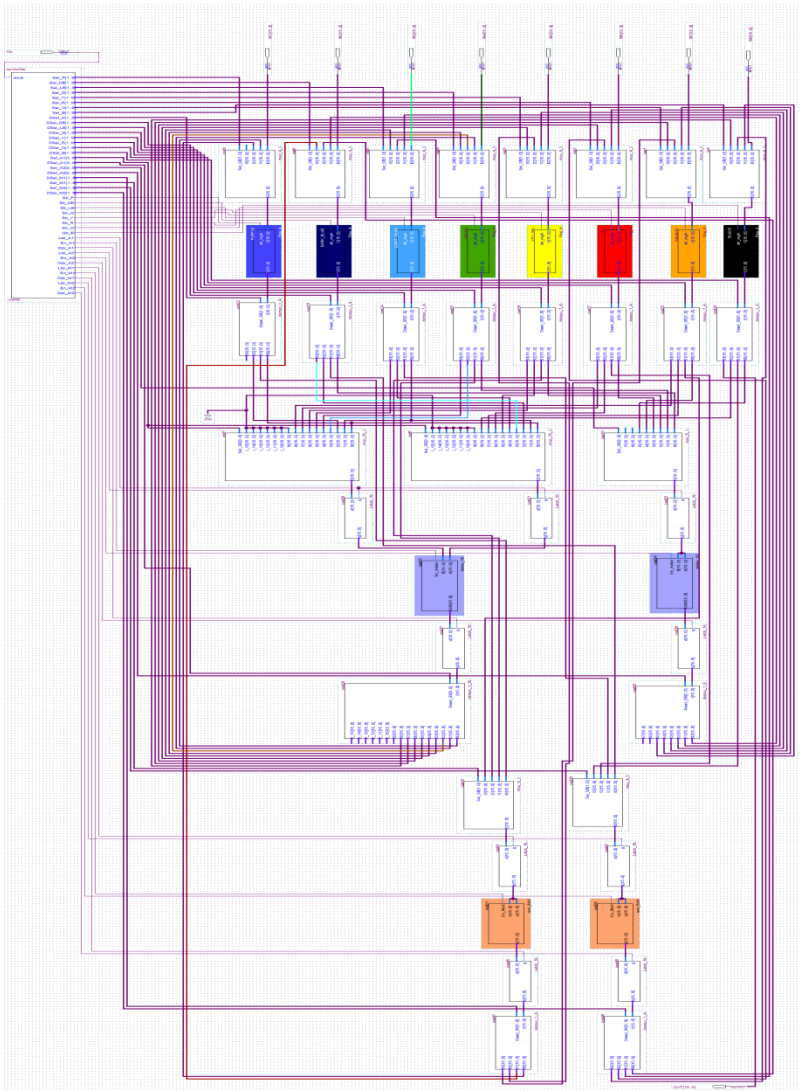
Anirban Sengupta, Mahendra Rathor "Securing Hardware Accelerators for CE Systems using Biometric Fingerprinting", **IEEE Transactions on Very Large Scale Integration Systems (TVLSI)** , Accepted, 2020

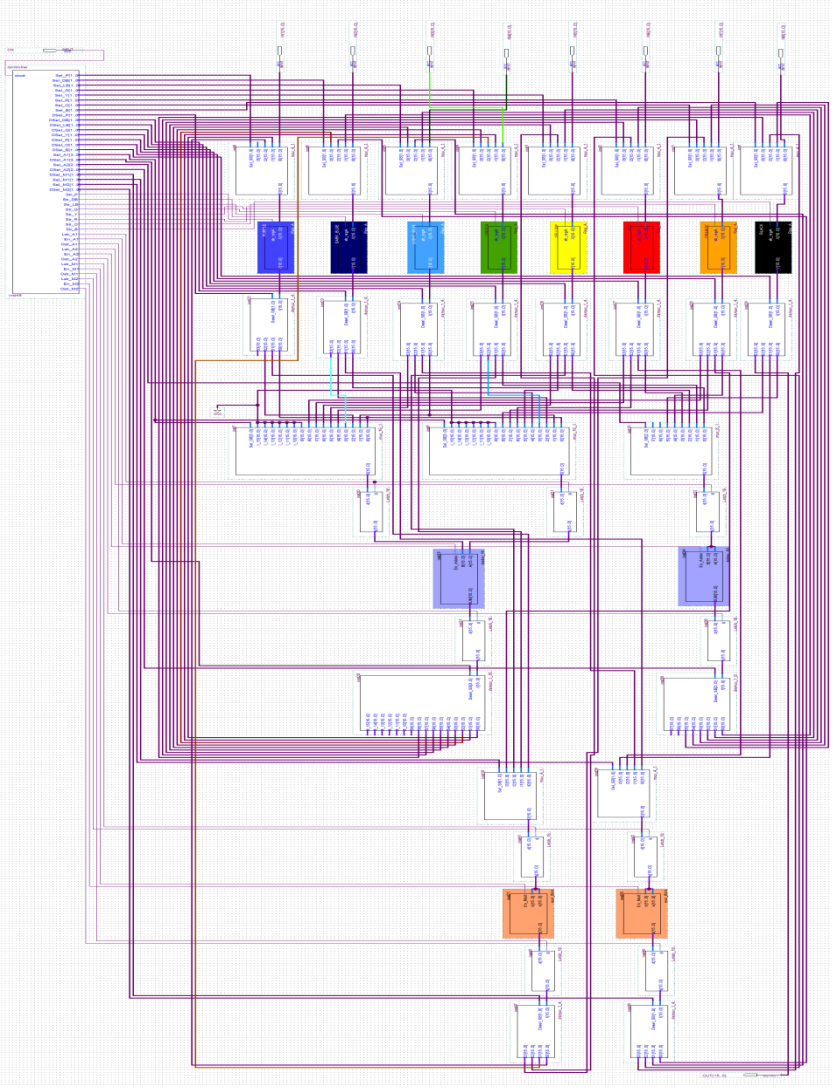
High level overview of triple phase watermarking



Anirban Sengupta, Dipanjan Roy, Saraju P Mohanty, "Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD),** Volume: 37, Issue: 4, April 2018, pp. 742 - 755

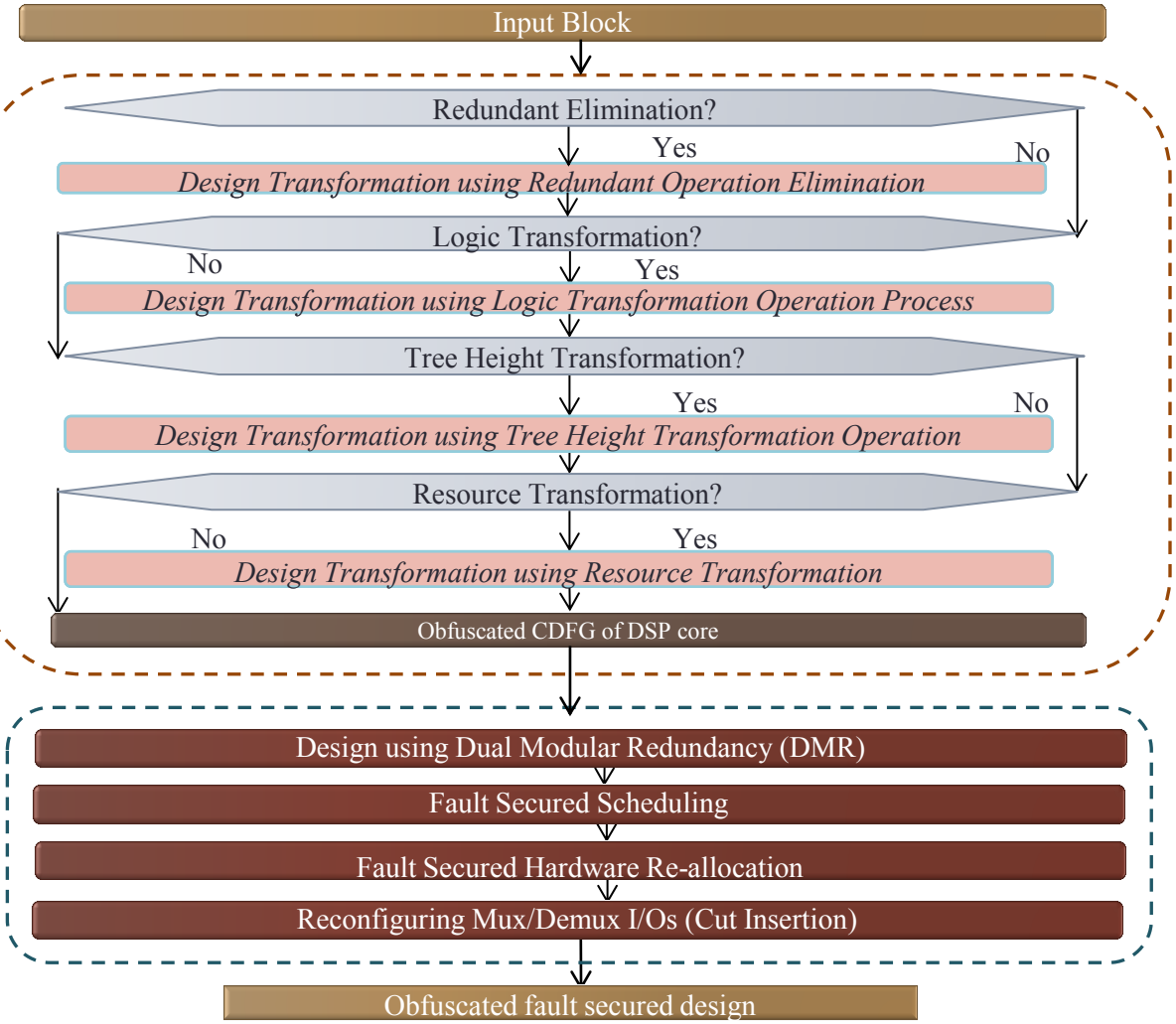
Watermarked FIR Vs Non-Watermarked FIR at RTL





Anirban Sengupta, Dipanjan Roy, Saraju P Mohanty, "Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD),** Volume: 37, Issue: 4, April 2018, pp. 742 - 755

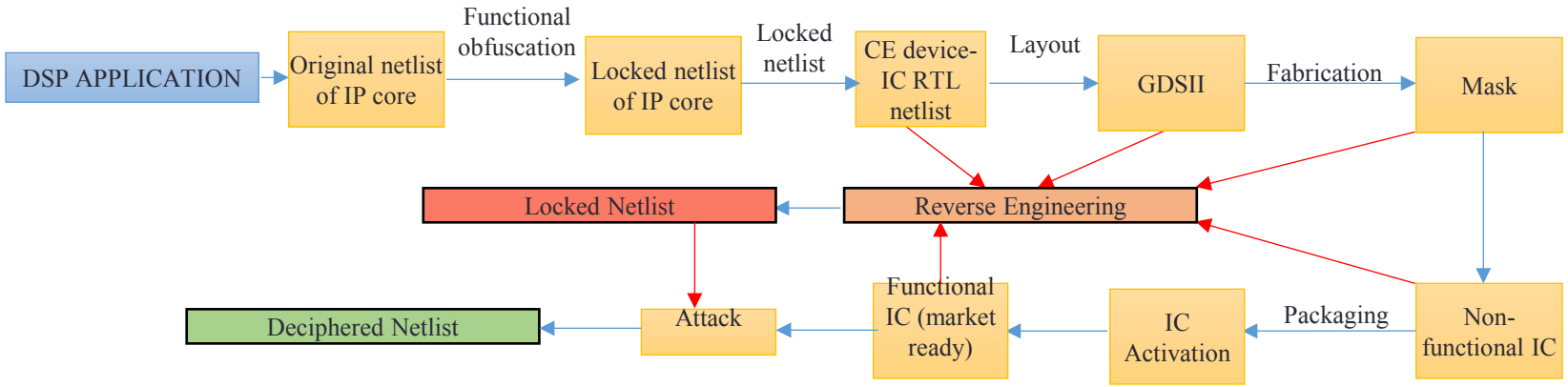
GENERIC DESIGN FLOW OF THE OBFUSCATION PROCESS



Obfuscation for fault Secured IP Designs

Anirban Sengupta, Saraju P Mohanty, Fernando Pescador, Peter Corcoran "Multi-Phase Obfuscation of Fault Secured DSP Designs with Enhanced Security Feature", **IEEE Transactions on Consumer Electronics**, Volume: 64, Issue:3, August 2018, pp: 356-364

How Hardware of a CE device can be compromised ?



- Reverse engineering (RE) of a DSP core is a process of gaining the complete understanding of its **functionality**, **design** and **structure**.
- However, RE can be used for dishonest intention such as **overbuilding**, **piracy**, or **counterfeiting** a DSP core or inserting a **hardware Trojan**.

Anirban Sengupta, Deepak Kachave, Dipanjan Roy "Low Cost Functional Obfuscation of Reusable IP Cores used in CE Hardware through Robust Locking", **IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD),** 2019

Conclusion

The future of CE system / IoT design / CPS design / Autonomous vehicle design is Energy-Security Tradeoff !

References

- Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", The Institute of Engineering and Technology (IET), 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9
- Anirban Sengupta, Mahendra Rathor "Protecting DSP Kernels using Robust Hologram based Obfuscation", IEEE Transactions on Consumer Electronics, Volume: 65, Issue: 1, Feb 2019, pp. 99-108
- Anirban Sengupta, Saraju P. Mohanty "IP Core Protection and Hardware-Assisted Security for Consumer Electronics", The Institute of Engineering and Technology (IET), 2019, Book ISBN: 978-1-78561-799-7, e-ISBN: 978-1-78561-800-0
- Anirban Sengupta, Dipanjan Roy, Saraju P Mohanty, "Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis", IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD), Volume: 37, Issue: 4, April 2018, pp. 742 – 755
- Anirban Sengupta, Saraju P Mohanty, Fernando Pescador, Peter Corcoran "Multi-Phase Obfuscation of Fault Secured DSP Designs with Enhanced Security Feature", IEEE Transactions on Consumer Electronics, Volume: 64, Issue:3, August 2018, pp: 356-364.
- Anirban Sengupta, Mahendra Rathor "Securing Hardware Accelerators for CE Systems using Biometric Fingerprinting", IEEE Transactions on Very Large Scale Integration Systems, Vol 28, Issue: 9, 2020, pp. 1979-1992
- https://cadforassurance.org/tools/ip-ic-protection/faciometric-hardware-security-tool
- Anirban Sengupta, Deepak Kachave, Dipanjan Roy "Low Cost Functional Obfuscation of Reusable IP Cores used in CE Hardware through Robust Locking", IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD), Volume: 38, Issue 4, April 2019, pp. 604 - 616

Thank You