Hardware (IP) Security and Trust

PKIA 2025

Sep 4, 2025

Prof. Anirban Sengupta, Professor, FIET (United Kingdom), FBCS (United Kingdom), FIETE, SMIEEE

IEEE Distinguished Lecturer (IEEE Consumer Electronics Society)

Featured IEEE Distinguished Visitor (IEEE Computer Society)

ACM India Eminent Speaker

Chair, IEEE Computer Society Distinguished Visitor Selection Committee

Editor-in-Chief, IET Computers & Digital Techniques,

Former Editor-in-Chief, IEEE VLSI Circuits and Systems Letter

Ex-Officio Board of Governors, IEEE Consumer Electronics Society

Former Chair, IEEE Computer Society Technical Committee on VLSI

Founder & Former Chair, IEEE Consumer Electronics Society Bombay Chapter

Awardee, IEEE Chester Sall Memorial Consumer Electronics Award (IEEE CE Society)

Associate Editor - IEEE Transactions on Dependable and Secure Computing, IEEE Embedded System Letter, IEEE Transactions on VLSI Systems, IEEE Transactions on Aerospace and Electronic Systems, IEEE Transactions on Consumer Electronics, IEEE Letters of the Computer Society, IEEE Canadian Journal of Electrical and Computer Engineering, IEEE Access, IEEE Consumer Electronics Magazine, Elsevier Microelectronics Journal

General Chair, 37th IEEE International Conference on Consumer Electronics (ICCE), Las Vegas

General Chair, 23rd International Symposium on VLSI Design and Test (VDAT-2019), India

Executive Committee, IEEE International Conference on Consumer Electronics (ICCE) - Berlin and Las Vegas

IEEE Distinguished Lecturer Nominations Committee, IEEE CE Society

Computer Science and Engineering

Indian Institute of Technology Indore

Email: asengupt@iiti.ac.in

Web: http://www.anirban-sengupta.com

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.

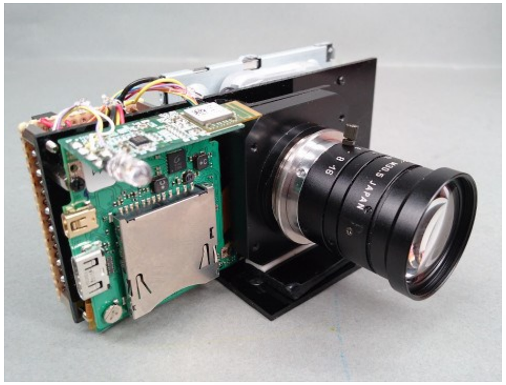
- Hardware security is broadly classified into two types: (a) authentication based approaches (b) obfuscation based approaches.
- The second type of hardware security approach i.e. obfuscation can again be further sub-divided into two types: (i) structural obfuscation (ii) functional obfuscation.
- Structural 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.

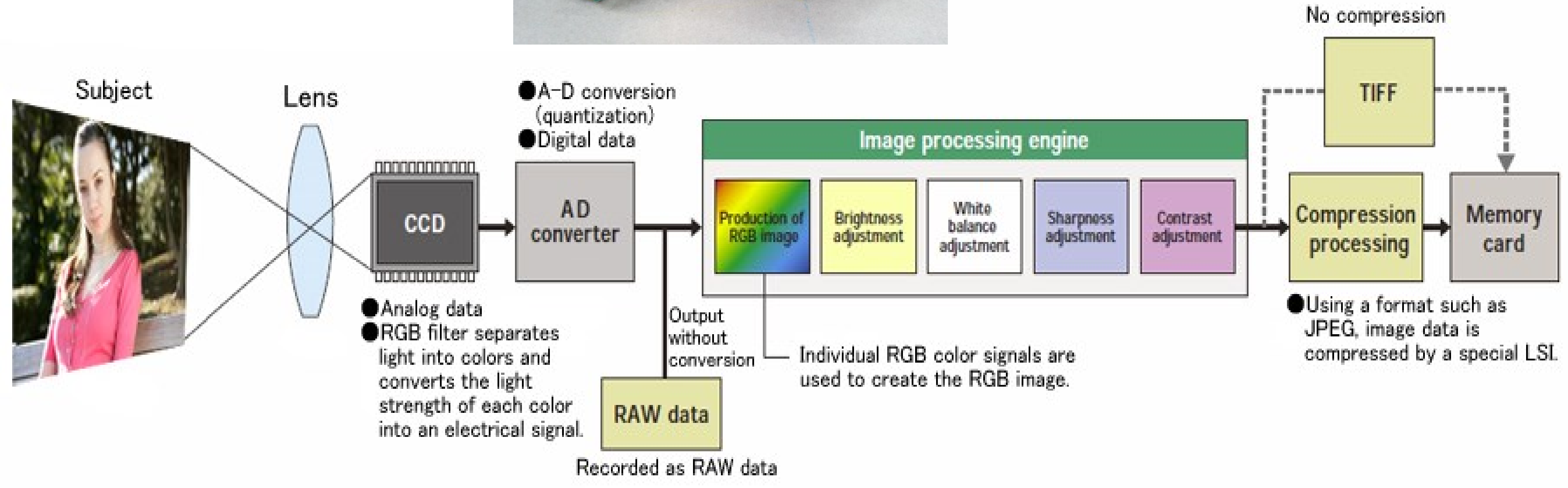
Anirban Sengupta, Saraju P. Mohanty "IP Core Protection and Hardware-Assisted Security for Consumer Electronics", **The Institute of Engineering and Technology (IET)**, 2019, Book ISBN: 978-1-78561-799-7, e-ISBN: 978-1-78561-800-0

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

Example of Consumer Electronics 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.



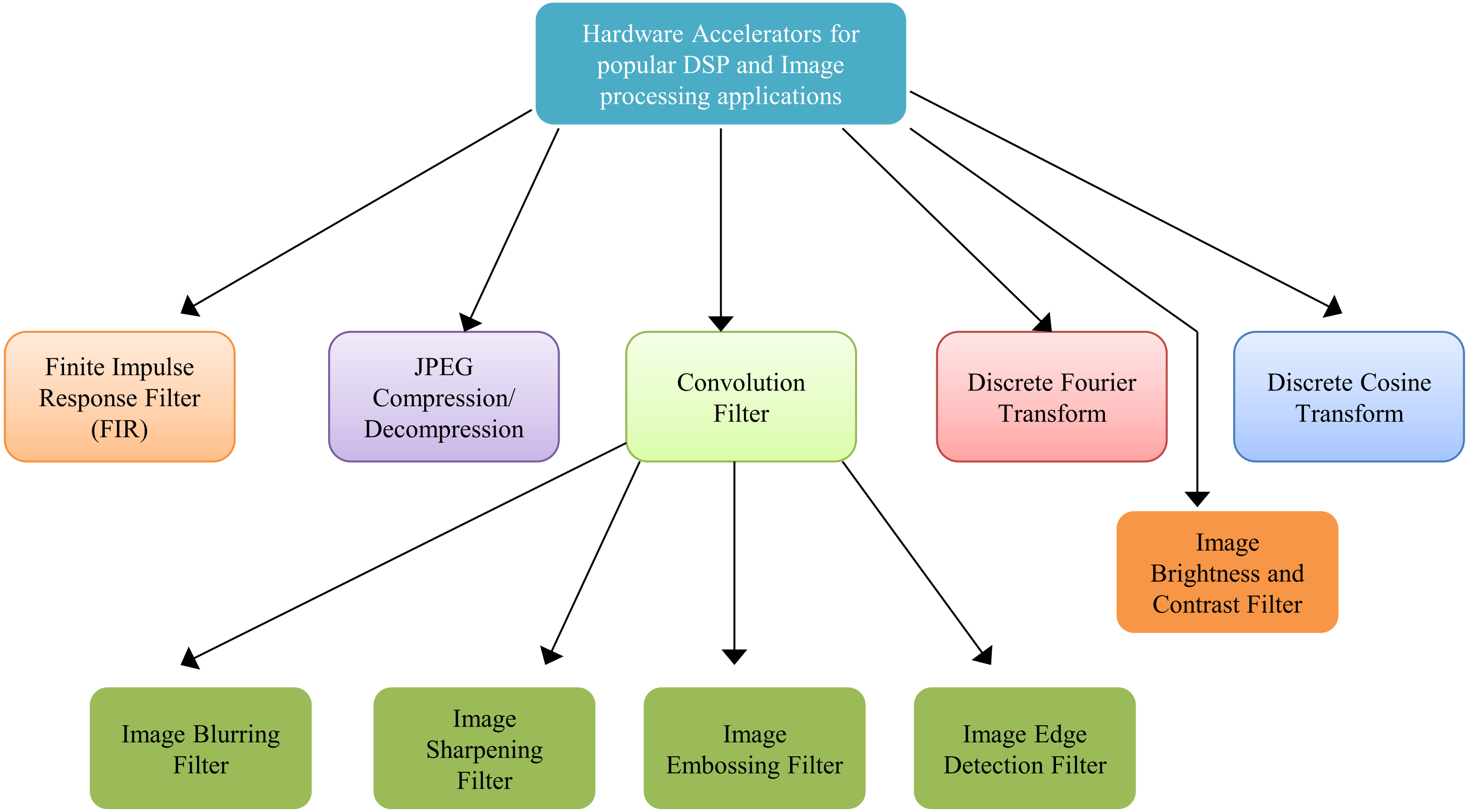

No compression
TIFF
Subject
Lens
●A-D conversion (quantization)
●Digital data
Image processing engine
CCD
AD converter
Production of RGB image
Brightness adjustment
White balance adjustment
Sharpness adjustment
Contrast adjustment
Compression processing
Memory card
●Analog data
●RGB filter separates light into colors and converts the light strength of each color into an electrical signal.
Output without conversion
RAW data
Recorded as RAW data
Individual RGB color signals are used to create the RGB image.
●Using a format such as JPEG, image data is compressed by a special LSI.

Complex JPEG codec

Anirban Sengupta, Dipanjan Roy, Saraju P Mohanty, Peter Corcoran "Low-Cost Obfuscated JPEG CODEC IP Core for Secure CE Hardware", **IEEE Transactions on Consumer Electronics,** Volume: 64, Issue:3, August 2018, pp:365-374.

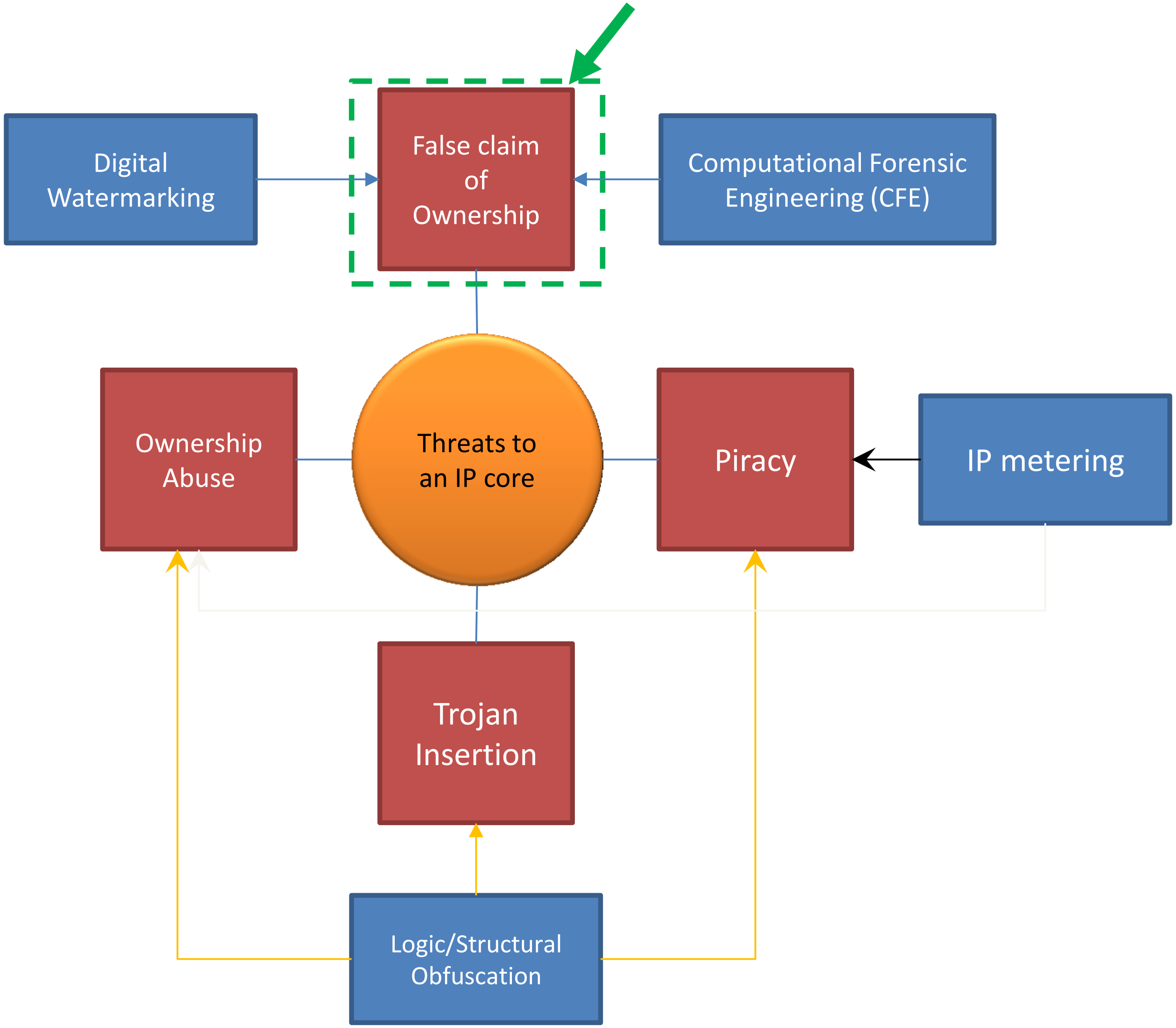
Anirban Sengupta "**Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques**", **The Institute of Engineering and Technology (IET),** 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

Hardware accelerators for popular DSP and image processing applications


Hardware Accelerators for popular DSP and Image processing applications
Finite Impulse Response Filter (FIR)
JPEG Compression/ Decompression
Convolution Filter
Discrete Fourier Transform
Discrete Cosine Transform
Image Brightness and Contrast Filter
Image Blurring Filter
Image Sharpening Filter
Image Embossing Filter
Image Edge Detection Filter

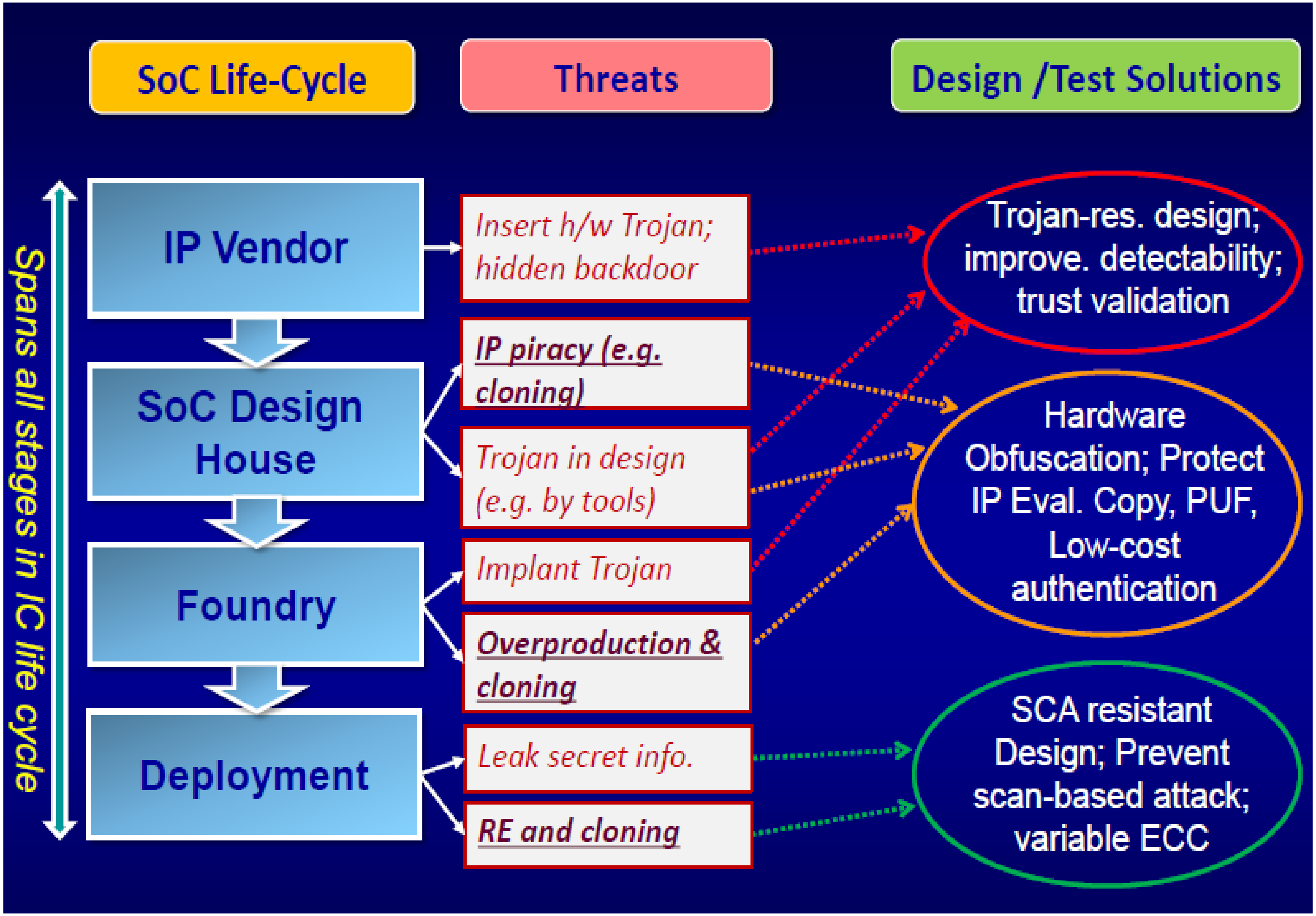
Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", **The Institute of Engineering and Technology (IET),** 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

Approaches for IP Protection

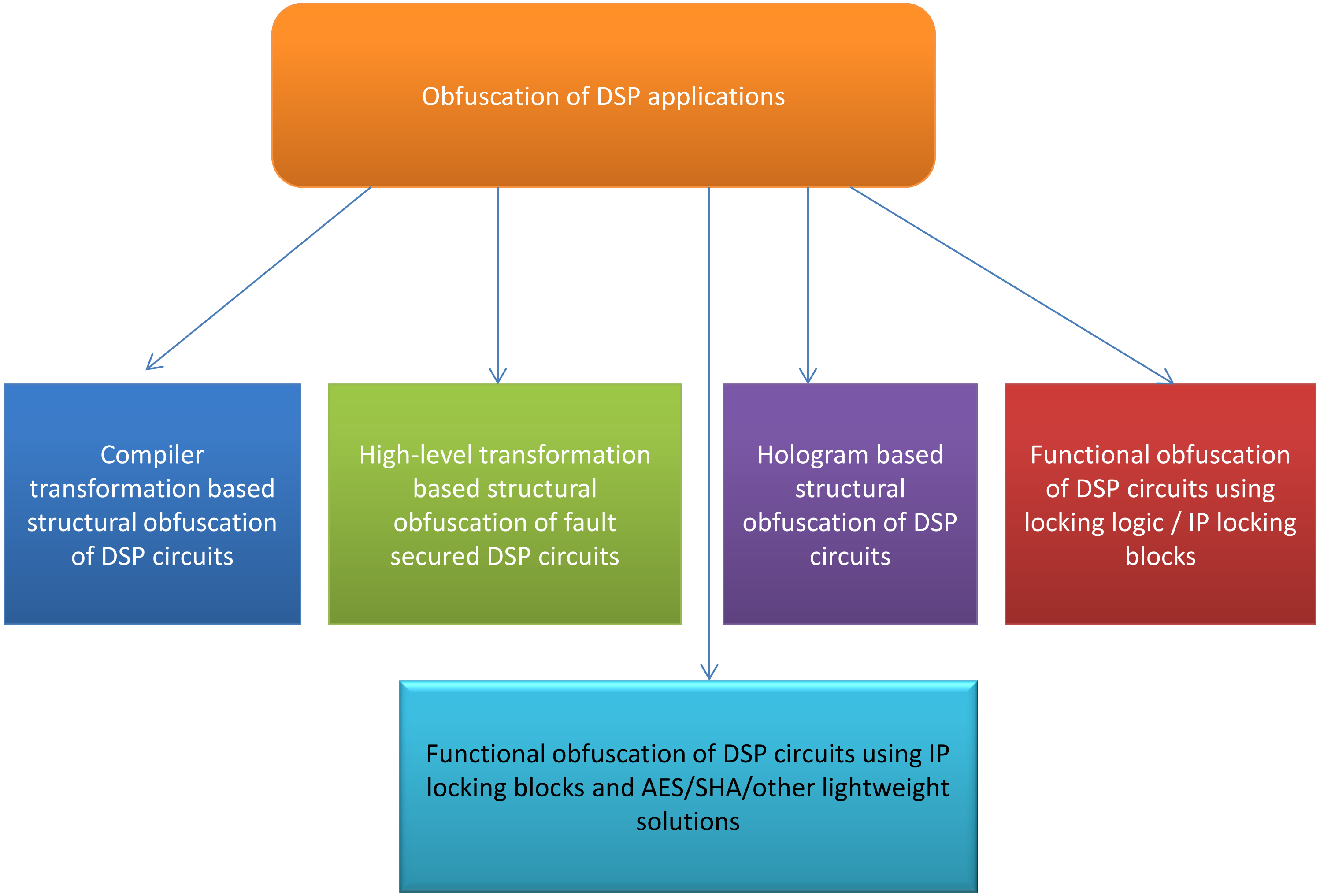


Anirban Sengupta, Dipanjan Roy, Saraju Mohanty, Peter Corcoran "DSP Design Protection in CE through Algorithmic Transformation Based Structural Obfuscation", **IEEE Transactions on Consumer Electronics**, Volume 63, Issue 4, November 2017, pp: 467 - 476

IP Core Protection and Hardware Security


SoC Life-Cycle
Threats
Design /Test Solutions
Spans all stages in IC life cycle
IP Vendor
SoC Design House
Foundry
Deployment
Insert h/w Trojan; hidden backdoor
IP piracy (e.g. cloning)
Trojan in design (e.g. by tools)
Implant Trojan
Overproduction & cloning
Leak secret info.
RE and cloning
Trojan-res. design; improve. detectability; trust validation
Hardware Obfuscation; Protect IP Eval. Copy, PUF, Low-cost authentication
SCA resistant Design; Prevent scan-based attack; variable ECC

Hardware Security of DSP applications using Obfuscation



Obfuscation of DSP applications

Compiler transformation based structural obfuscation of DSP circuits

High-level transformation based structural obfuscation of fault secured DSP circuits

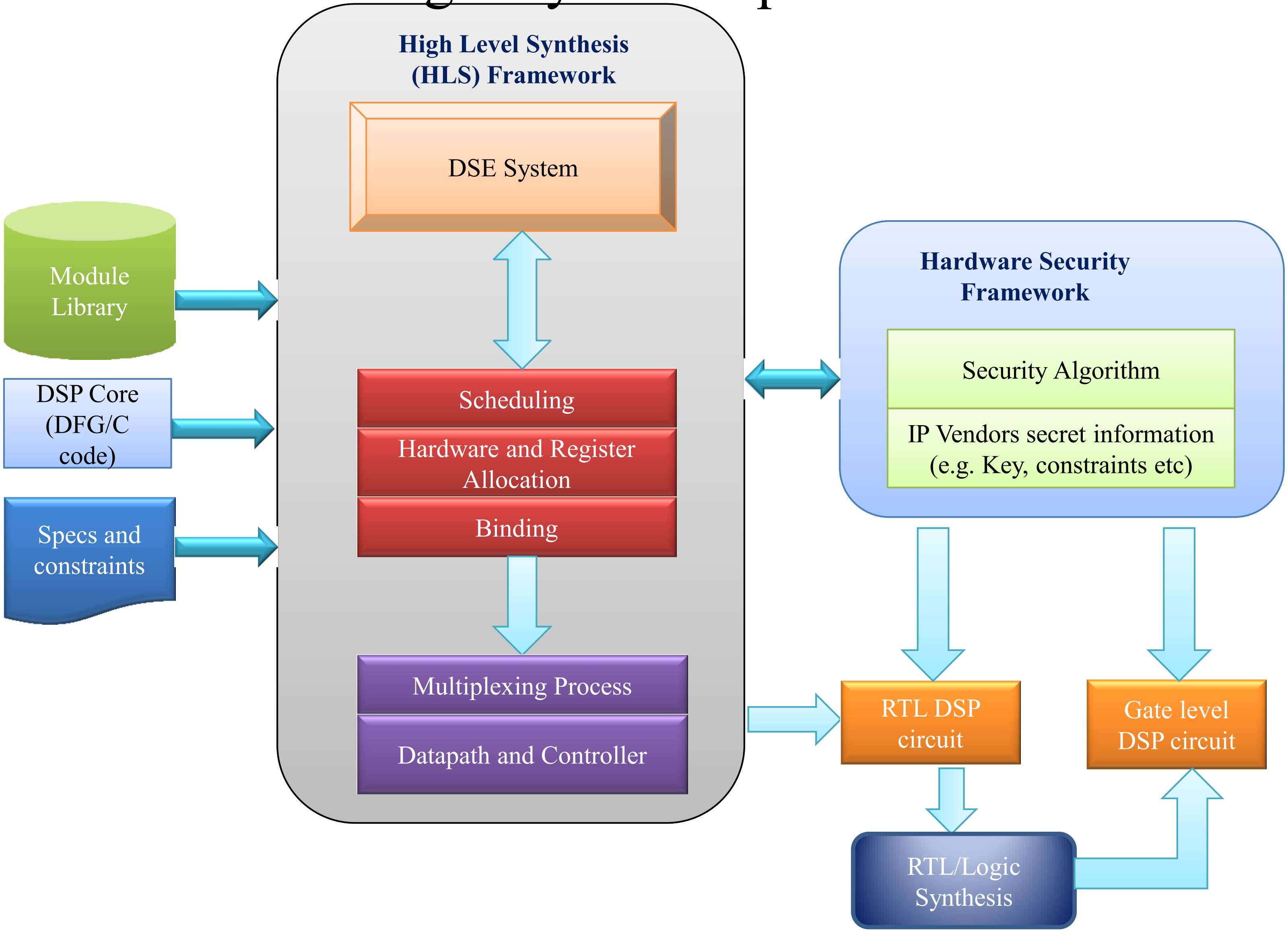
Hologram based structural obfuscation of DSP circuits

Functional obfuscation of DSP circuits using locking logic / IP locking blocks

Functional obfuscation of DSP circuits using IP locking blocks and AES/SHA/other lightweight solutions

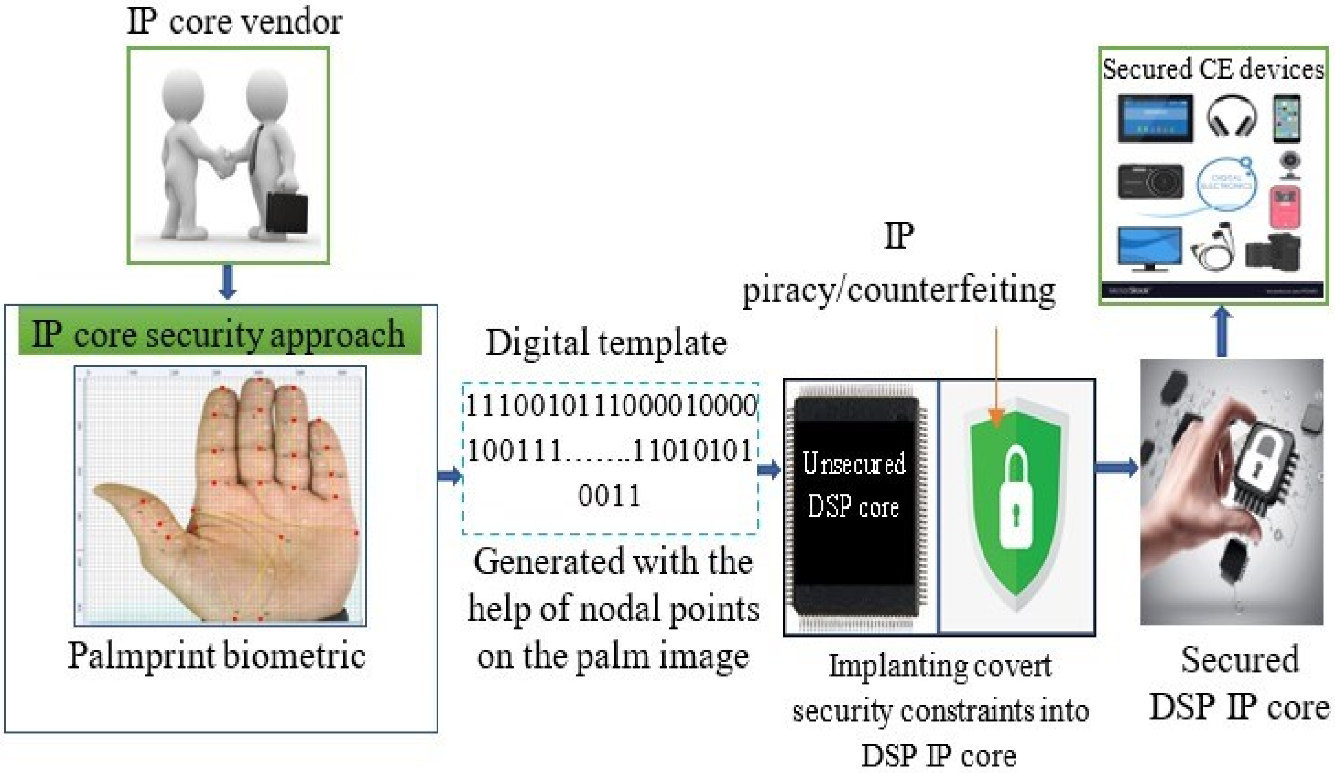
Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", **The Institute of Engineering and Technology (IET),** 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

Hardware Security Algorithms integrated with HLS and Logic Synthesis phases



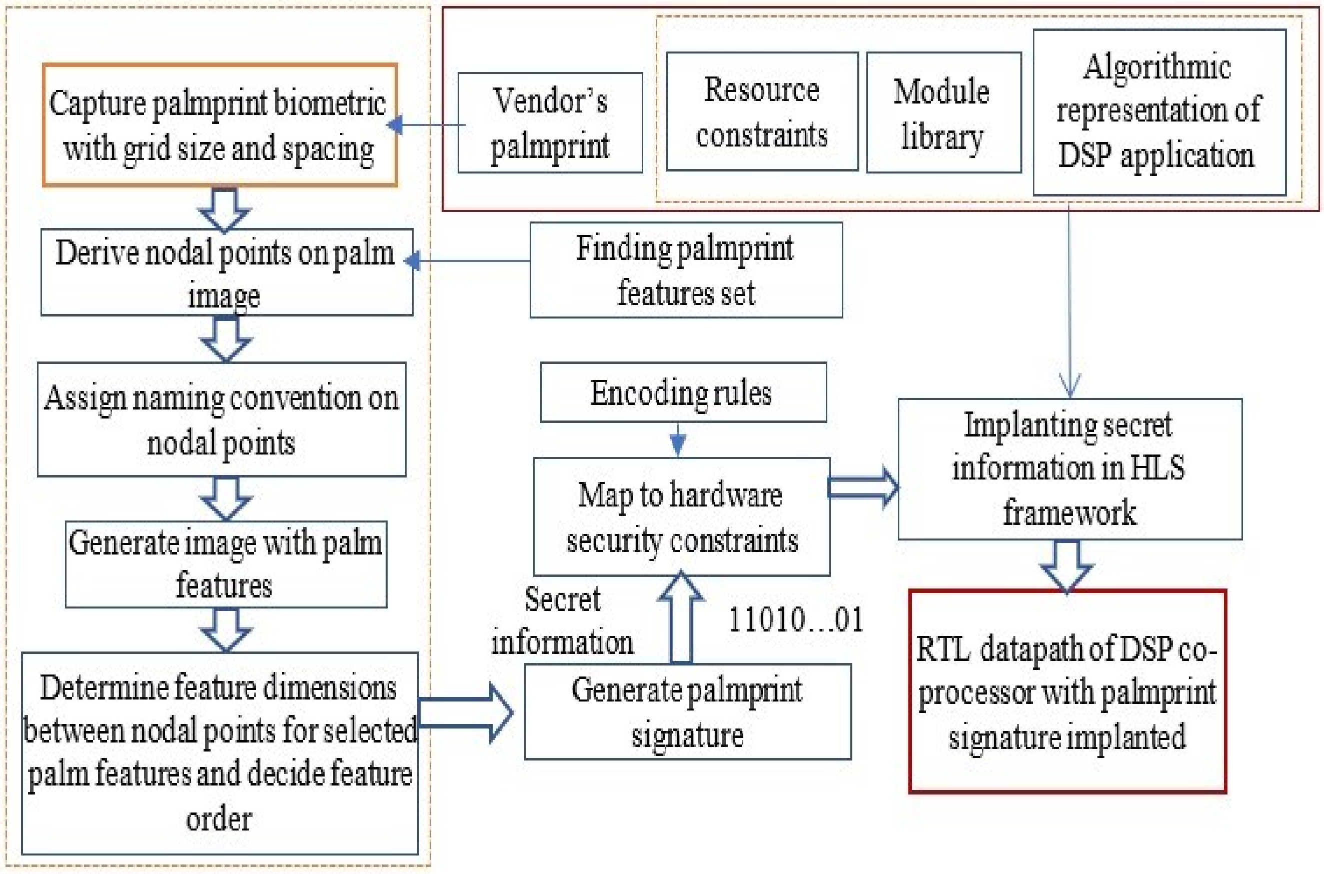
Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", **The Institute of Engineering and Technology (IET),** 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

Palmprint Biometrics for Hardware IPP



Securing reusable DSP IP core used in CE systems

Palmprint Biometrics for Hardware IPP

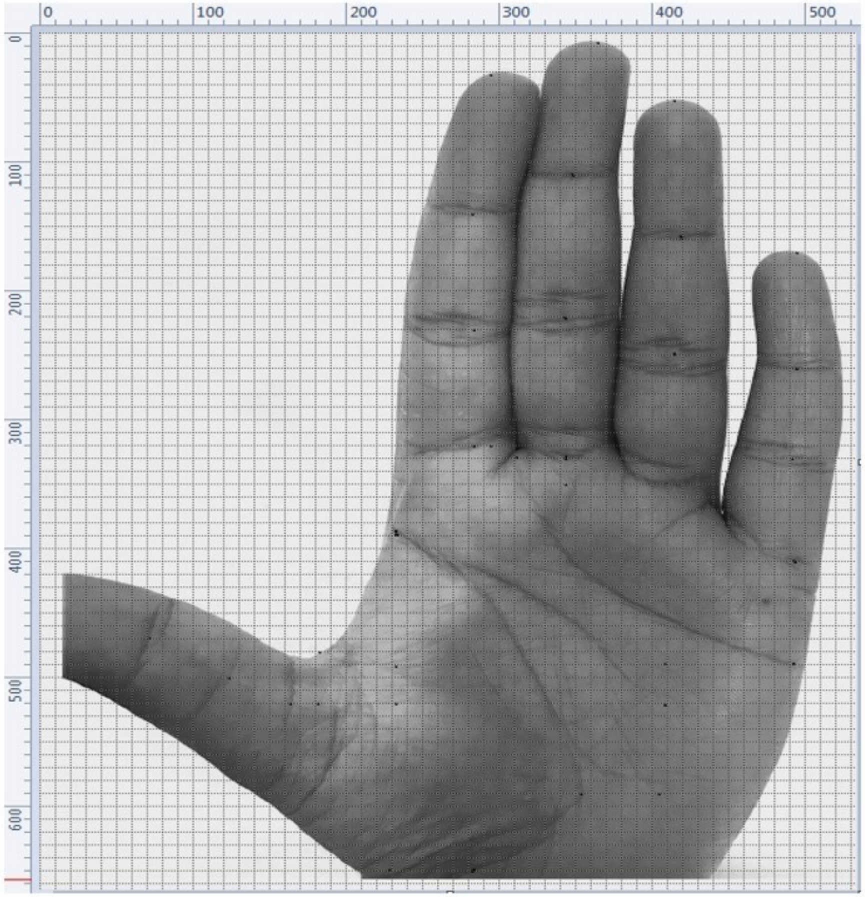

Capture palmprint biometric with grid size and spacing
Vendor's palmprint
Resource constraints
Module library
Algorithmic representation of DSP application
Derive nodal points on palm image
Finding palmprint features set
Assign naming convention on nodal points
Encoding rules
Implanting secret information in HLS framework
Map to hardware security constraints
Generate image with palm features
Secret information
11010…01
RTL datapath of DSP co-processor with palmprint signature implanted
Determine feature dimensions between nodal points for selected palm features and decide feature order
Generate palmprint signature

Proposed palmprint biometric for securing DSP co-processors

Palmprint Biometrics for Hardware IPP

➢ Capturing palm image

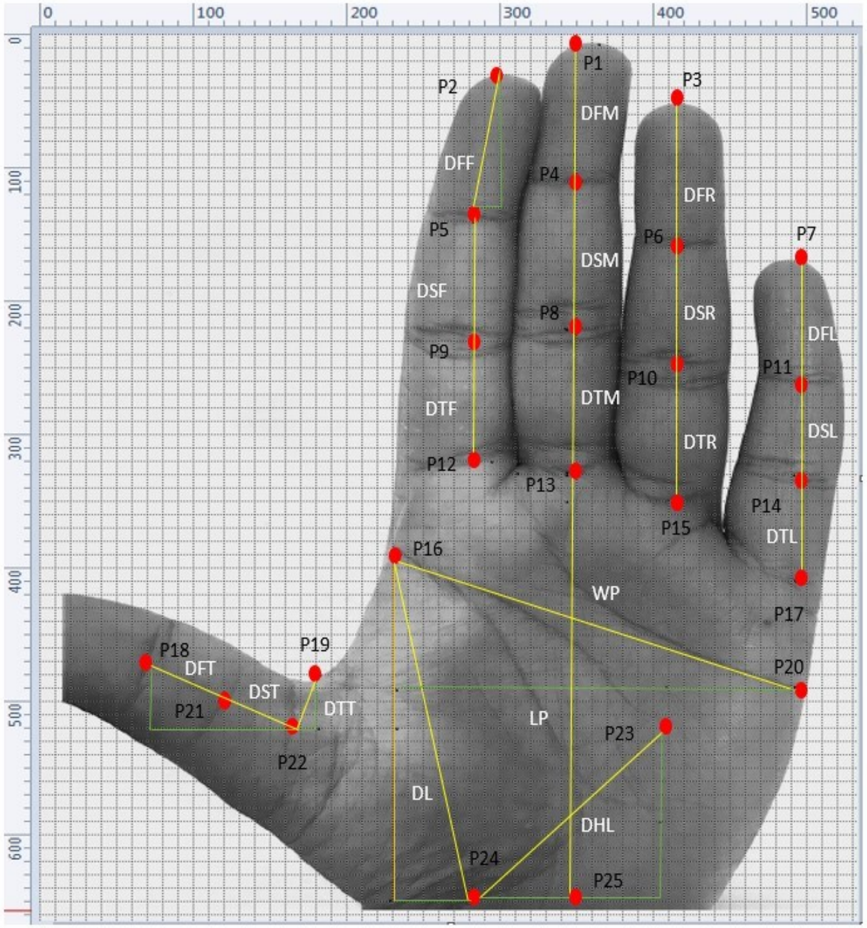
- At first the palmprint biometric of the authentic vendor or designer is captured and subsequently image of the captured palmprint is subjected to a specific grid size/spacing.
- This helps in generating the nodal points precisely.



Palmprint Biometrics for Hardware IPP

- **Generating image with chosen palm features and nodal points**

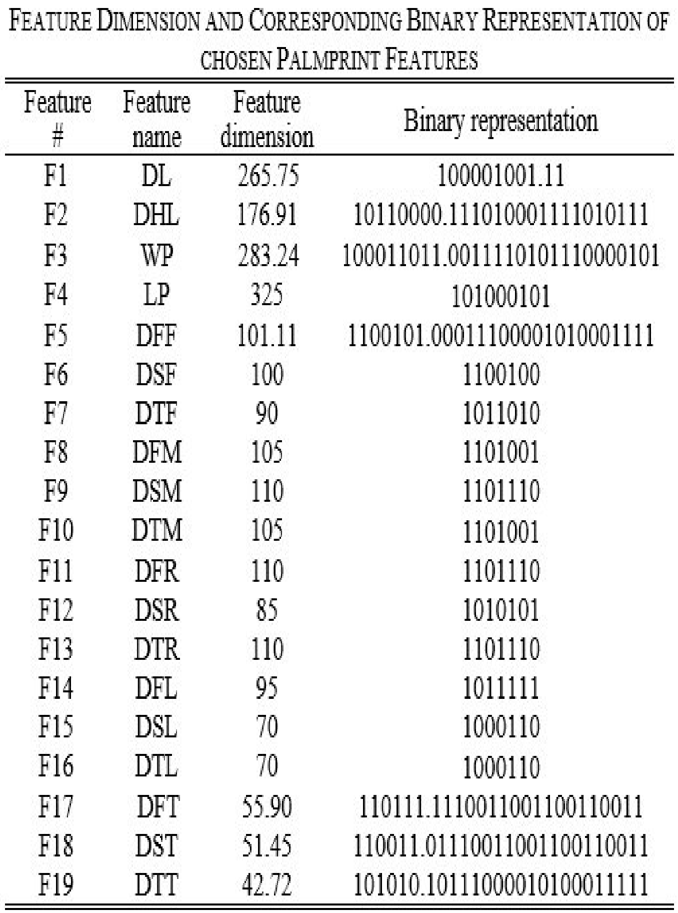
- Finding Palmprint Feature Set and Deriving Nodal Points for Captured Palmprint Biometric.
- Assigning Naming Convention and Deriving Palmprint Image with Selected Feature set.



Palmprint Biometrics for Hardware IPP

- **Finding Feature Dimensions and Deriving Palmprint Signature Based on the Selected Feature Order**
- For example, a palmprint signature for the selected order of palmprint features (“DL╪ DHL --- ╪ DTT”. Where, ‘╪’ represents the concatenation operator) after concatenation is as follows:
- Palmprint Signature:

  “100001001.1110110000.111010001111010111.---.11111”



FEATURE DIMENSION AND CORRESPONDING BINARY REPRESENTATION OF CHOSEN PALMPRINT FEATURES

Feature #	Feature name	Feature dimension	Binary representation
F1	DL	265.75	100001001.11
F2	DHL	176.91	10110000.111010001111010111
F3	WP	283.24	100011011.0011110101110000101
F4	LP	325	101000101
F5	DFF	101.11	1100101.00011100001010001111
F6	DSF	100	1100100
F7	DTF	90	1011010
F8	DFM	105	1101001
F9	DSM	110	1101110
F10	DTM	105	1101001
F11	DFR	110	1101110
F12	DSR	85	1010101
F13	DTR	110	1101110
F14	DFL	95	1011111
F15	DSL	70	1000110
F16	DTL	70	1000110
F17	DFT	55.90	110111.1110011001100110011
F18	DST	51.45	110011.01110011001100110011
F19	DTT	42.72	101010.10111000010100011111

Note: Size of the palmprint signature varies based on the number of chosen palm features by the vendor for signature generation (depending on the required security strength corresponding to target application).

Palmprint Biometrics for Hardware IPP

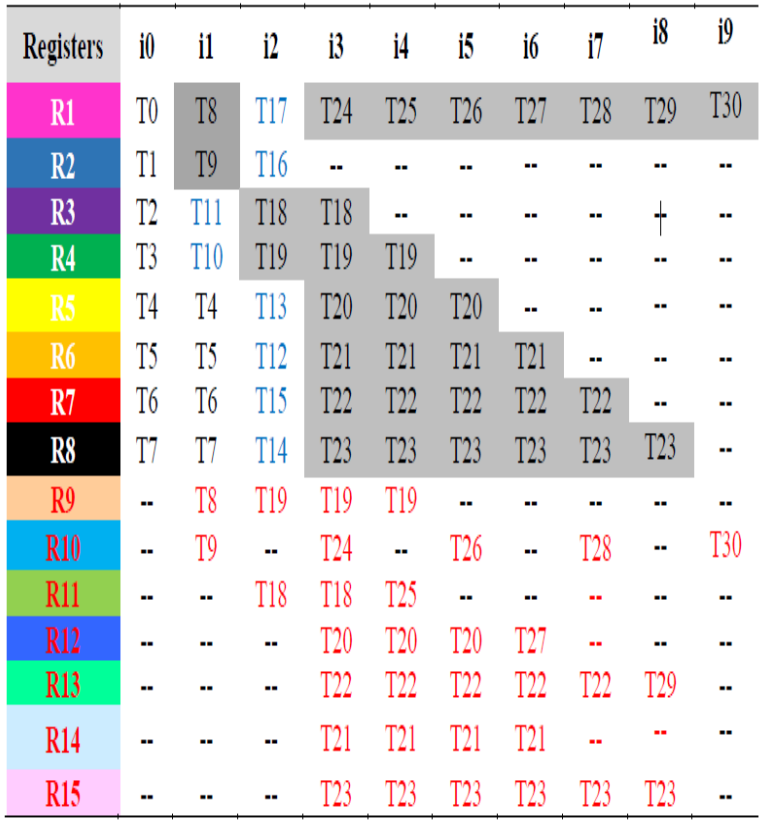
Deriving the Covert Security Constraints and Implanting into Target IP core Design

- Post obtaining the digital template of palmprint signature, corresponding hardware security constraints are generated based on the encoding rules.
- The encoding rules for the signature bits are as follows:

The bit ‘1’ embeds an edge between node pair (odd-odd), bit ‘0’ embeds an edge between node pair (even-even). Moreover, the binary bit ‘.’ embeds an edge between node pair (0, integer) into the CIG of target DSP design.

- For example, for a sample design having 31 storage variables (T0 to T30) executing through 8 registers (R1 to R8), the generated security constraints corresponding to the zeros are: <T0, T2>, <T0, T4>---<T16, T28>, the security constraints corresponding to ones are: <T1, T3>, -----<T27, T29> and corresponding to the binary points are: <T0, T1>, <T0, T3>, -- -, <T0, T11>.

TABLE I
REGISTER ALLOCATION OF A TARGET HARDWARE IP CORE POST IMPLANTATION



Registers	i0	i1	i2	i3	i4	i5	i6	i7	i8	i9
R1	T0	T8	T17	T24	T25	T26	T27	T28	T29	T30
R2	T1	T9	T16	--	--	--	--	--	--	--
R3	T2	T11	T18	T18	--	--	--	--	+	--
R4	T3	T10	T19	T19	T19	--	--	--	--	--
R5	T4	T4	T13	T20	T20	T20	--	--	--	--
R6	T5	T5	T12	T21	T21	T21	T21	--	--	--
R7	T6	T6	T15	T22	T22	T22	T22	T22	--	--
R8	T7	T7	T14	T23	T23	T23	T23	T23	T23	--
R9	--	T8	T19	T19	T19	--	--	--	--	--
R10	--	T9	--	T24	--	T26	--	T28	--	T30
R11	--	--	T18	T18	T25	--	--	--	--	--
R12	--	--	--	T20	T20	T20	T27	--	--	--
R13	--	--	--	T22	T22	T22	T22	T22	T29	--
R14	--	--	--	T21	T21	T21	T21	--	--	--
R15	--	--	--	T23	T23	T23	T23	T23	T23	--

Results and Discussion

- The proposed palmprint biometric approach is analyzed in terms of security and design overhead.

Security Analysis:

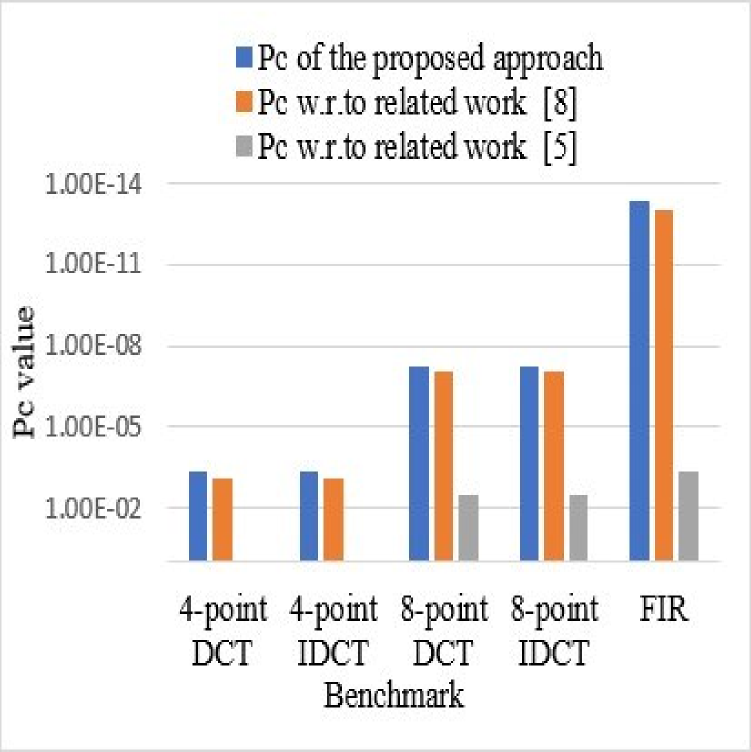
- The security of the proposed approach is analyzed in terms of probability of coincidence (Pc) and temper tolerance (TT) ability.
- The Pc metric is formulated as follows:

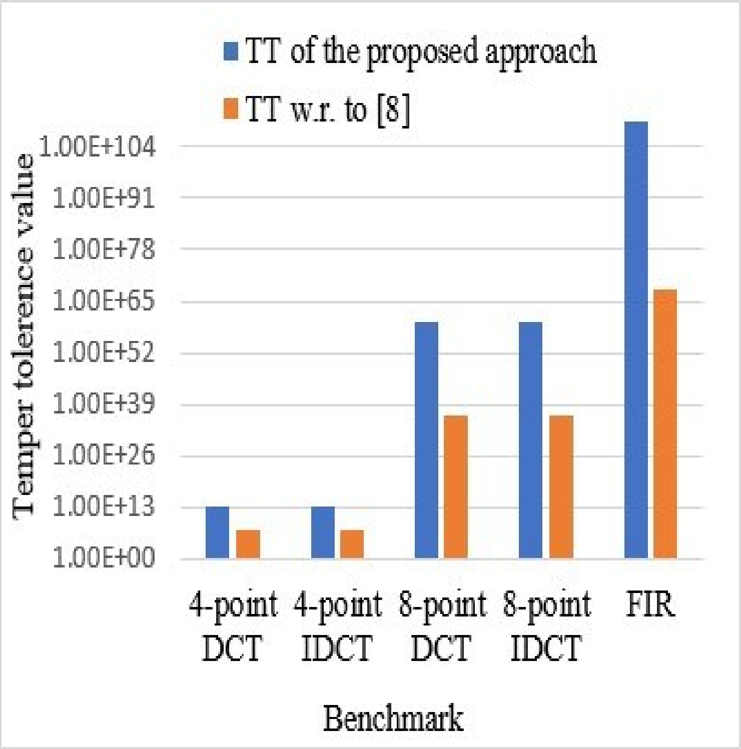
$$\text{Pc} = \left(1 - \frac{1}{\tau}\right)^{S} \quad (1)$$

- The TT metric is formulated as follows:

$$\text{TT} = P^{Q} \quad (2)$$

Comparison of Probability of Coincidence and Tamper Tolerance Ability with Previous Works





Design Cost Overhead Post Implanting the Palmprint Signature

Design cost Analysis:

Design cost can be measured using the following metric:

$$Z = h1\frac{\nabla t}{\nabla max} + h2\frac{\Delta t}{\Delta max}$$

(3)

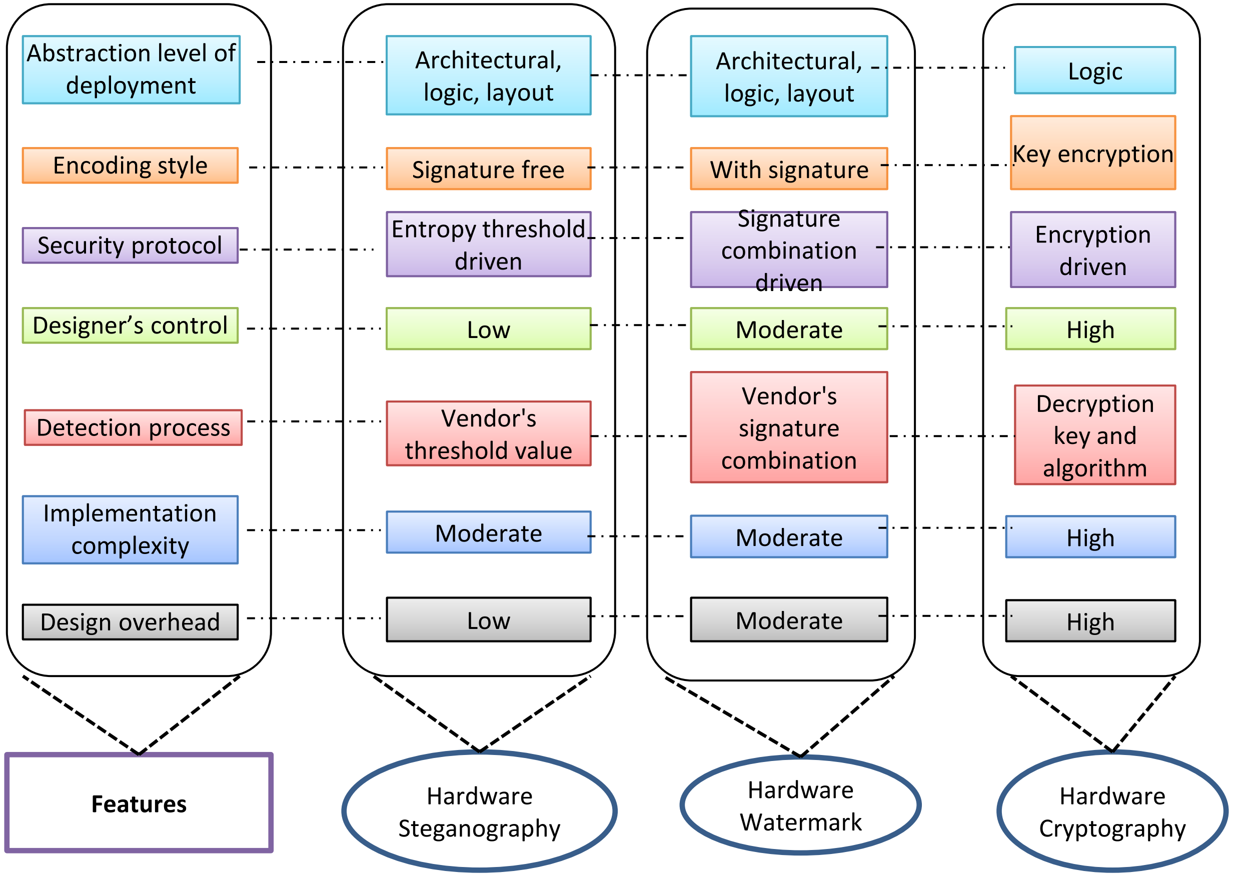
- Design cost overhead post implanting the palmprint signature into the design is minimal (0.2%-0.8%) as evident from Table II.

TABLE II

DESIGN COST PRE AND POST EMBEDDING PALMPRINT

Benchmarks	Design cost of baseline	Design cost of palmprint implanted design	% Cost overhead
4-pointDCT	0.5611	0.5623	0.2%
4-point IDCT	0.5611	0.5623	0.2%
8-pointDCT	.4721	.4740	0.4%
8-point IDCT	.4721	.4740	0.4%
FIR	.4443	.4479	0.8%

Comparison of hardware steganography with its contemporary approaches

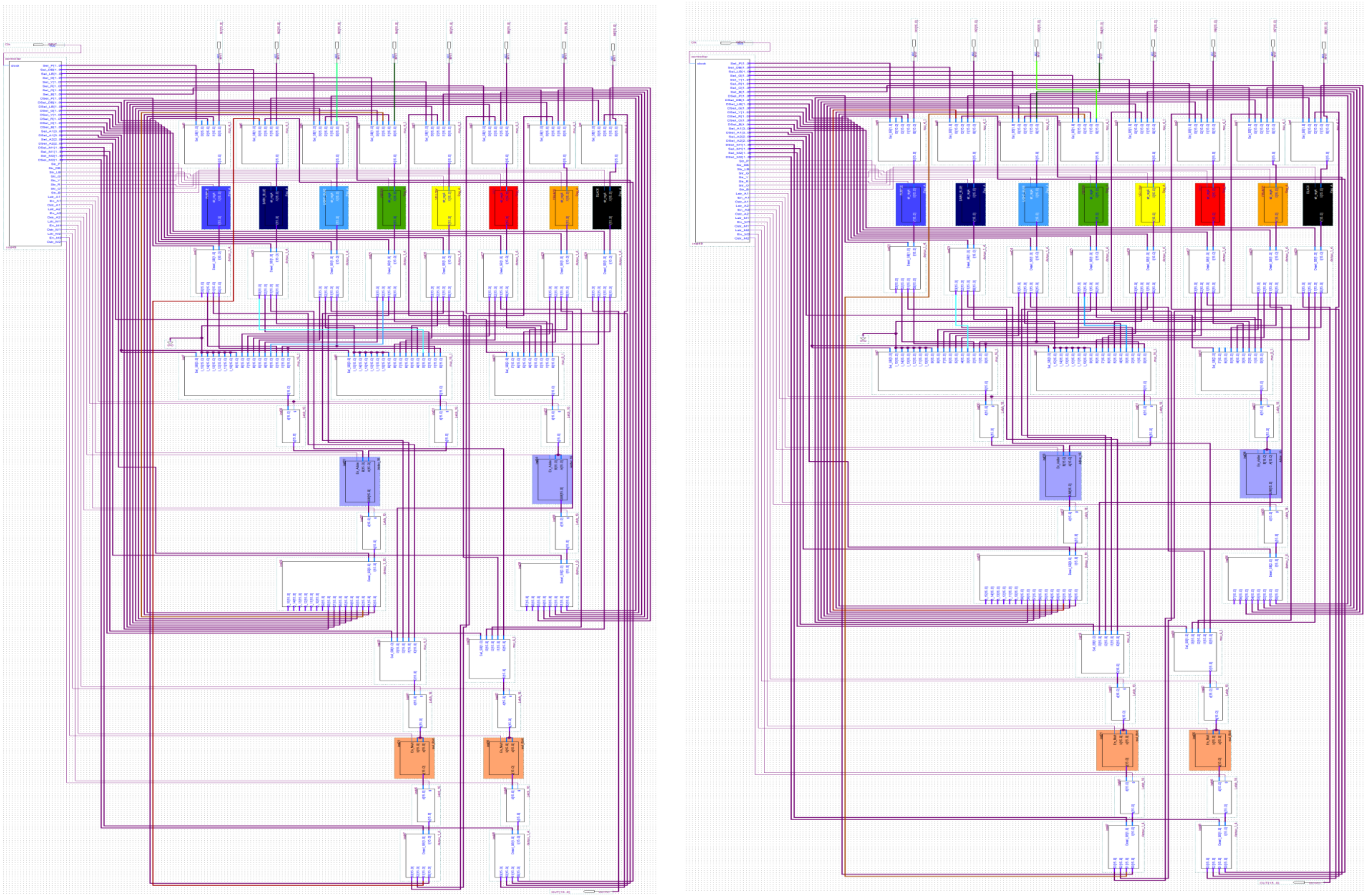


Features	Hardware Steganography	Hardware Watermark	Hardware Cryptography
Abstraction level of deployment	Architectural, logic, layout	Architectural, logic, layout	Logic
Encoding style	Signature free	With signature	Key encryption
Security protocol	Entropy threshold driven	Signature combination driven	Encryption driven
Designer’s control	Low	Moderate	High
Detection process	Vendor's threshold value	Vendor's signature combination	Decryption key and algorithm
Implementation complexity	Moderate	Moderate	High
Design overhead	Low	Moderate	High

Anirban Sengupta, Mahendra Rathor "IP Core Steganography for Protecting DSP Kernels used in CE Systems", **IEEE Transactions on Consumer Electronics (TCE)** , Volume: 65 , Issue: 4 , Nov. 2019, pp. 506 - 515

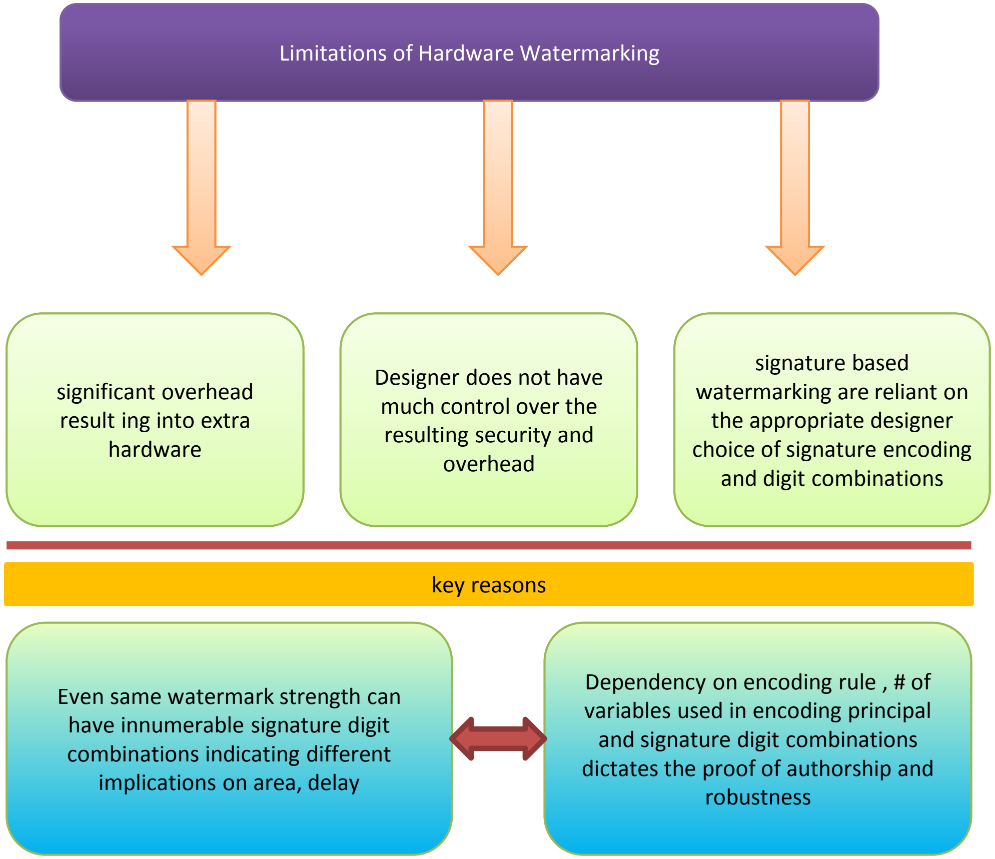
Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", **The Institute of Engineering and Technology (IET),** 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

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

Limitations of Hardware Watermarking



Limitations of Hardware Watermarking

significant overhead result ing into extra hardware

Designer does not have much control over the resulting security and overhead

signature based watermarking are reliant on the appropriate designer choice of signature encoding and digit combinations

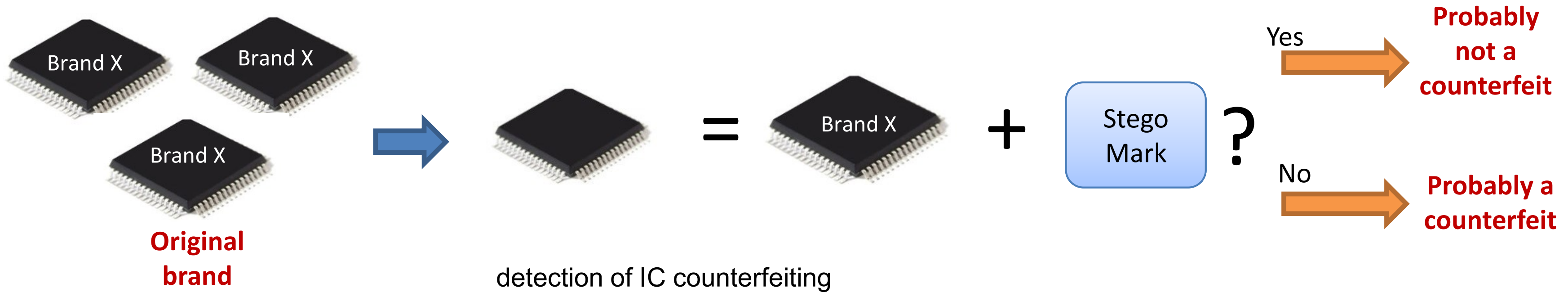
key reasons

Even same watermark strength can have innumerable signature digit combinations indicating different implications on area, delay

Dependency on encoding rule , # of variables used in encoding principal and signature digit combinations dictates the proof of authorship and robustness

Anirban Sengupta, Mahendra Rathor "IP Core Steganography for Protecting DSP Kernels used in CE Systems", **IEEE Transactions on Consumer Electronics (TCE)** , Volume: 65 , Issue: 4 , Nov. 2019, pp. 506 - 515

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



Brand X

Brand X

Brand X

Original brand

Brand X

Stego Mark

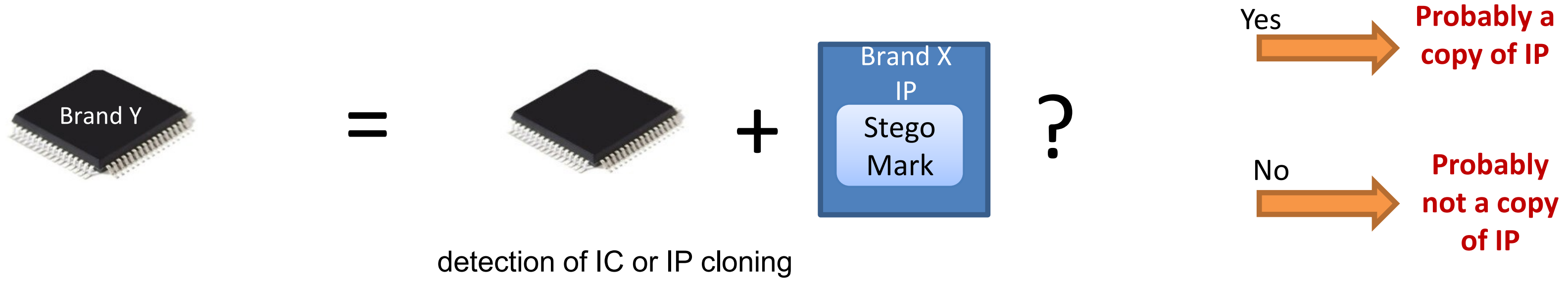
Yes

No

Probably not a counterfeit

Probably a counterfeit

detection of IC counterfeiting



Brand Y

Brand X IP

Stego Mark

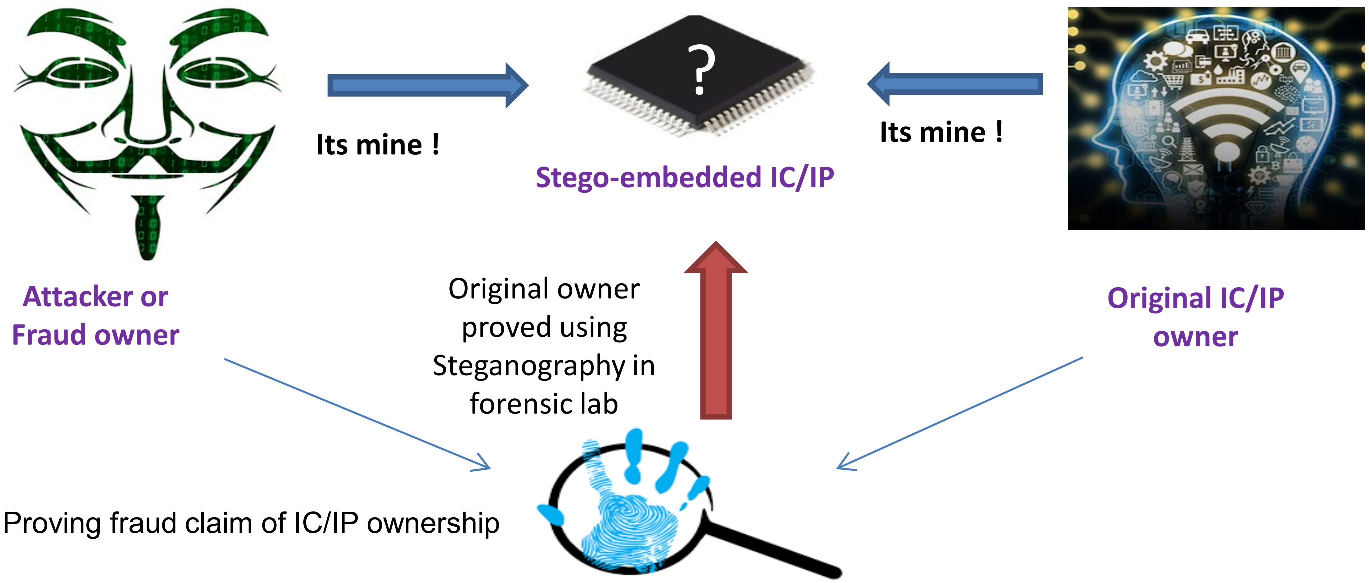
Yes

No

Probably a copy of IP

Probably not a copy of IP

detection of IC or IP cloning



Its mine !

Stego-embedded IC/IP

Its mine !

Attacker or Fraud owner

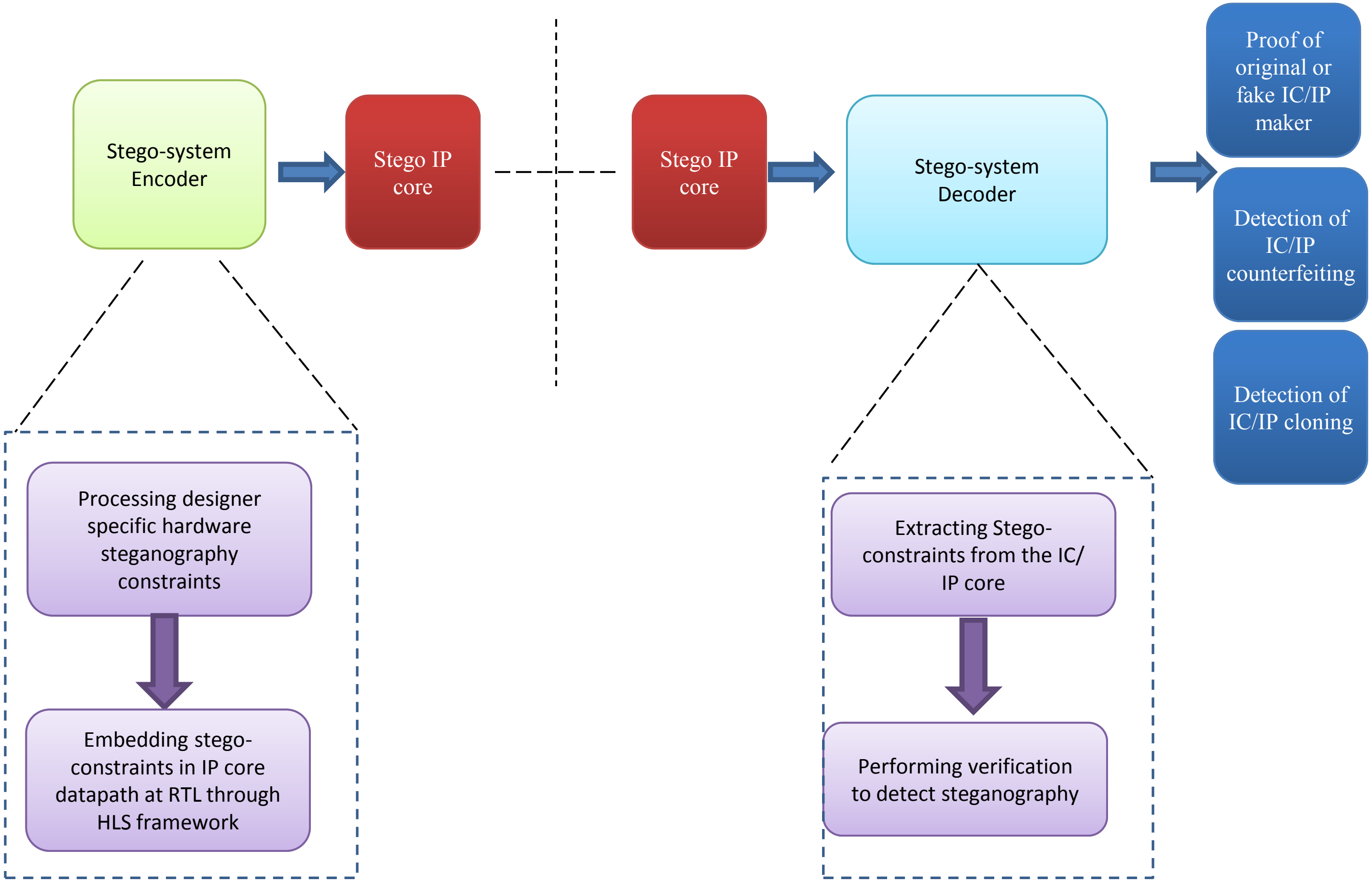
Original IC/IP owner

Original owner proved using Steganography in forensic lab

Proving fraud claim of IC/IP ownership

Anirban Sengupta, Mahendra Rathor "IP Core Steganography for Protecting DSP Kernels used in CE Systems", **IEEE Transactions on Consumer Electronics (TCE)** , Volume: 65 , Issue: 4 , Nov. 2019, pp. 506 - 515

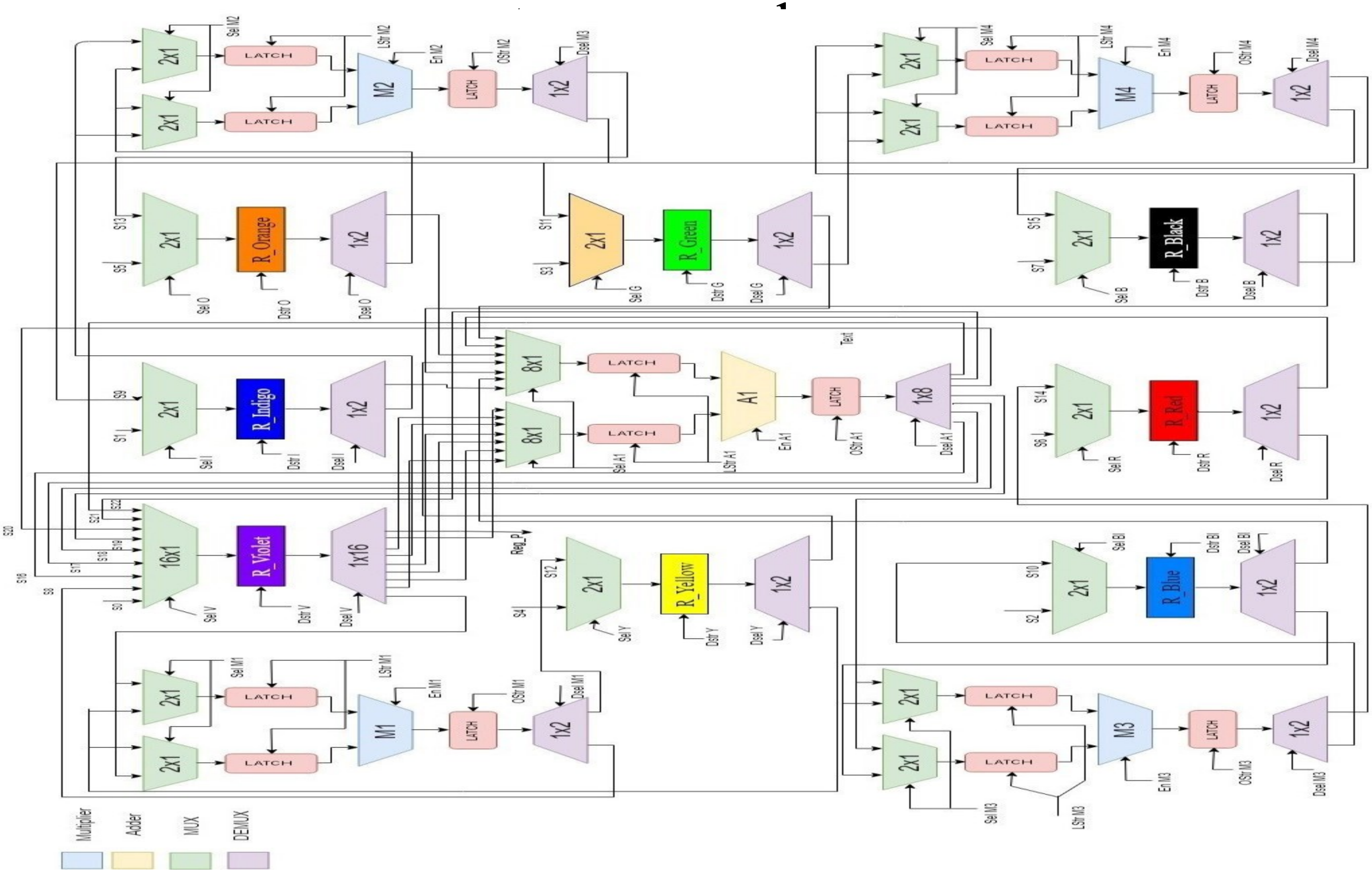
Hardware Steganography Encoding-Decoding Process


Stego-system Encoder
Stego IP core
Stego IP core
Stego-system Decoder
Proof of original or fake IC/IP maker
Detection of IC/IP counterfeiting
Detection of IC/IP cloning
Processing designer specific hardware steganography constraints
Embedding stego-constraints in IP core datapath at RTL through HLS framework
Extracting Stego-constraints from the IC/ IP core
Performing verification to detect steganography

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

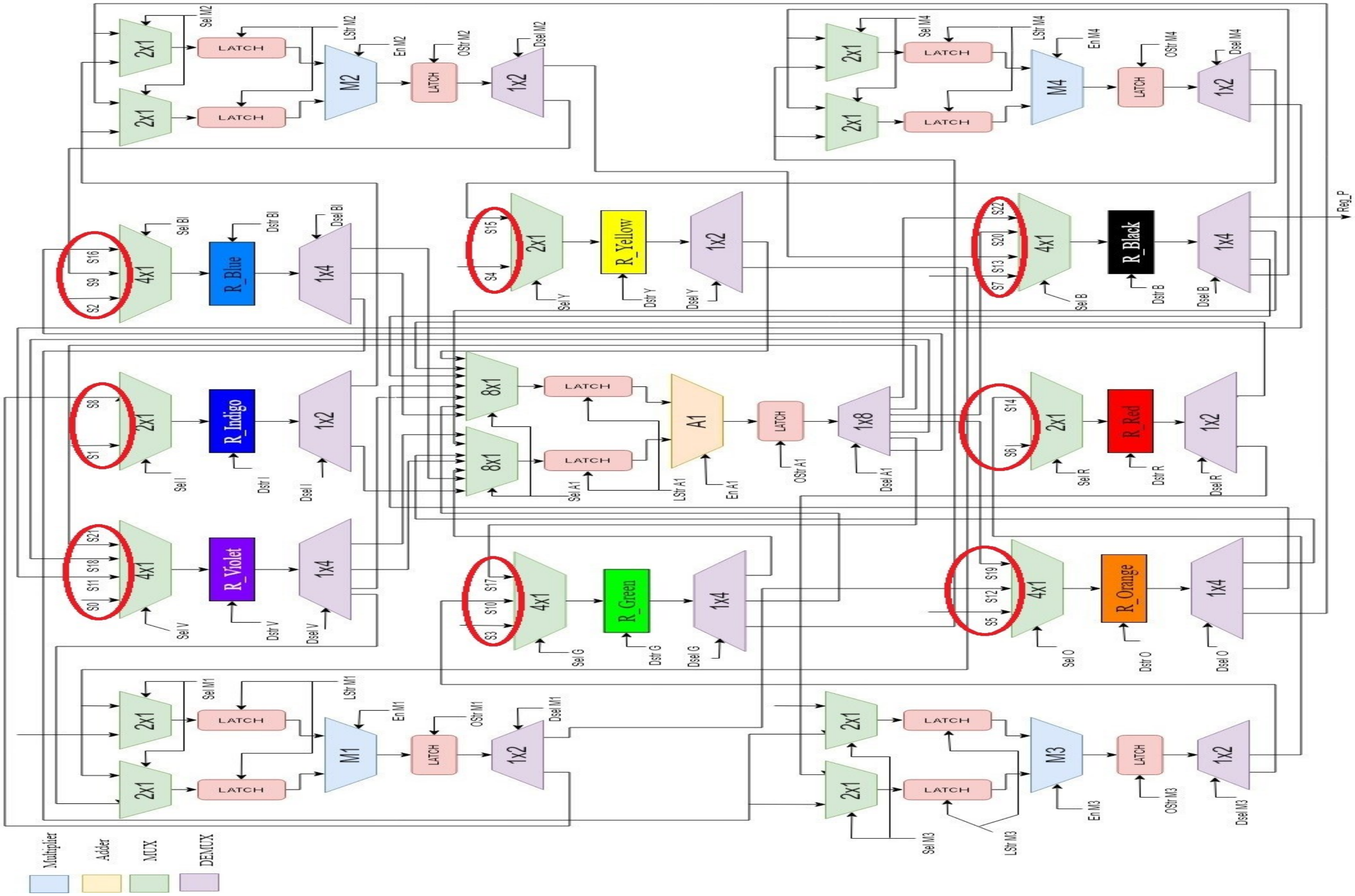
Anirban Sengupta, Mahendra Rathor "IP Core Steganography for Protecting DSP Kernels used in CE Systems", **IEEE Transactions on Consumer Electronics (TCE)** , Volume: 65 , Issue: 4 , Nov. 2019, pp. 506 - 515

RTL datapath of 8-point DCT before



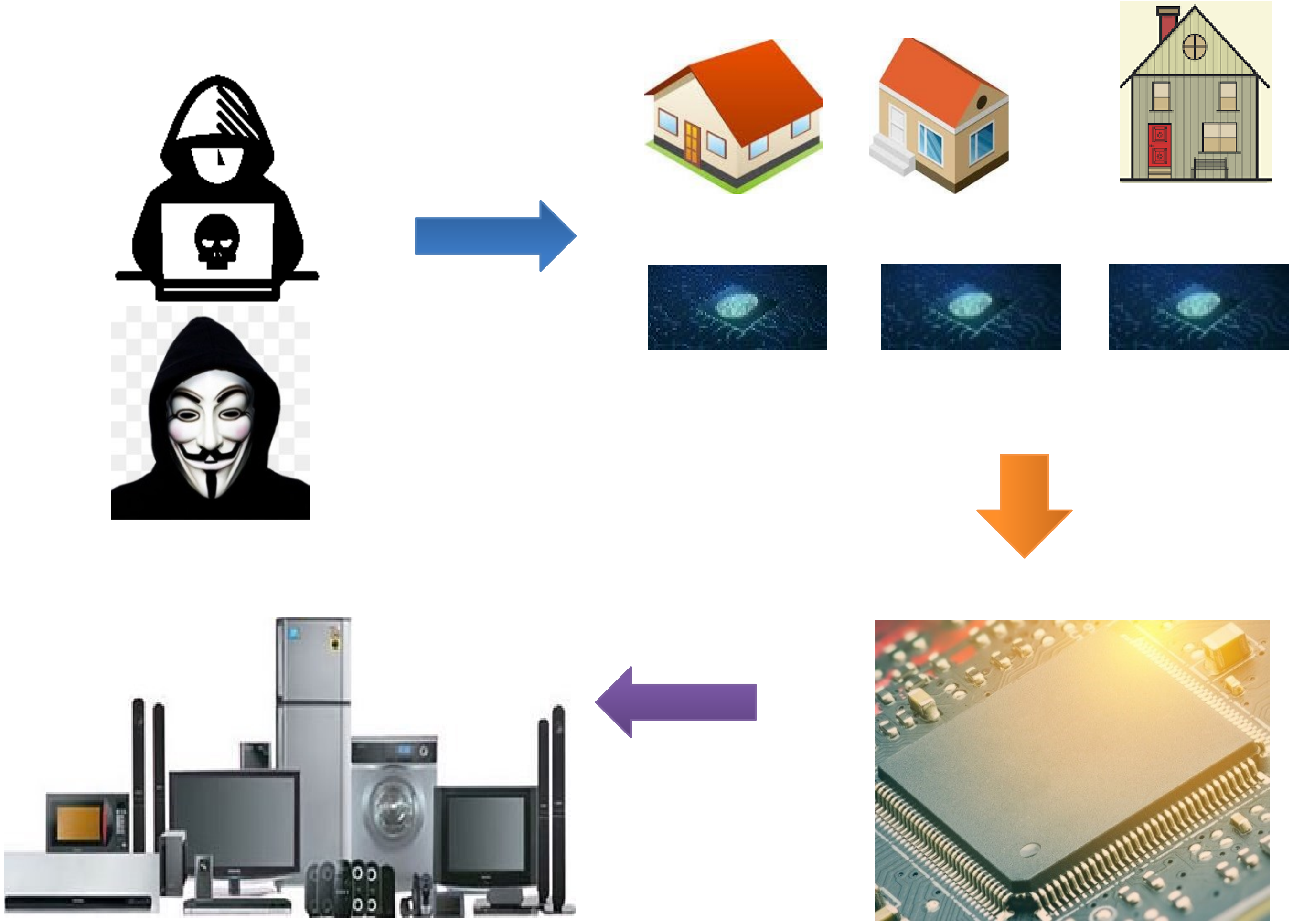
Anirban Sengupta, Mahendra Rathor "IP Core Steganography for Protecting DSP Kernels used in CE Systems", **IEEE Transactions on Consumer Electronics (TCE)** , Volume: 65 , Issue: 4 , Nov. 2019, pp. 506 - 515

RTL datapath of 8-point DCT **after** Steganography



Anirban Sengupta, Mahendra Rathor "IP Core Steganography for Protecting DSP Kernels used in CE Systems", **IEEE Transactions on Consumer Electronics (TCE)** , Volume: 65 , Issue: 4 , Nov. 2019, pp. 506 - 515

IP core protection using Digital Signature

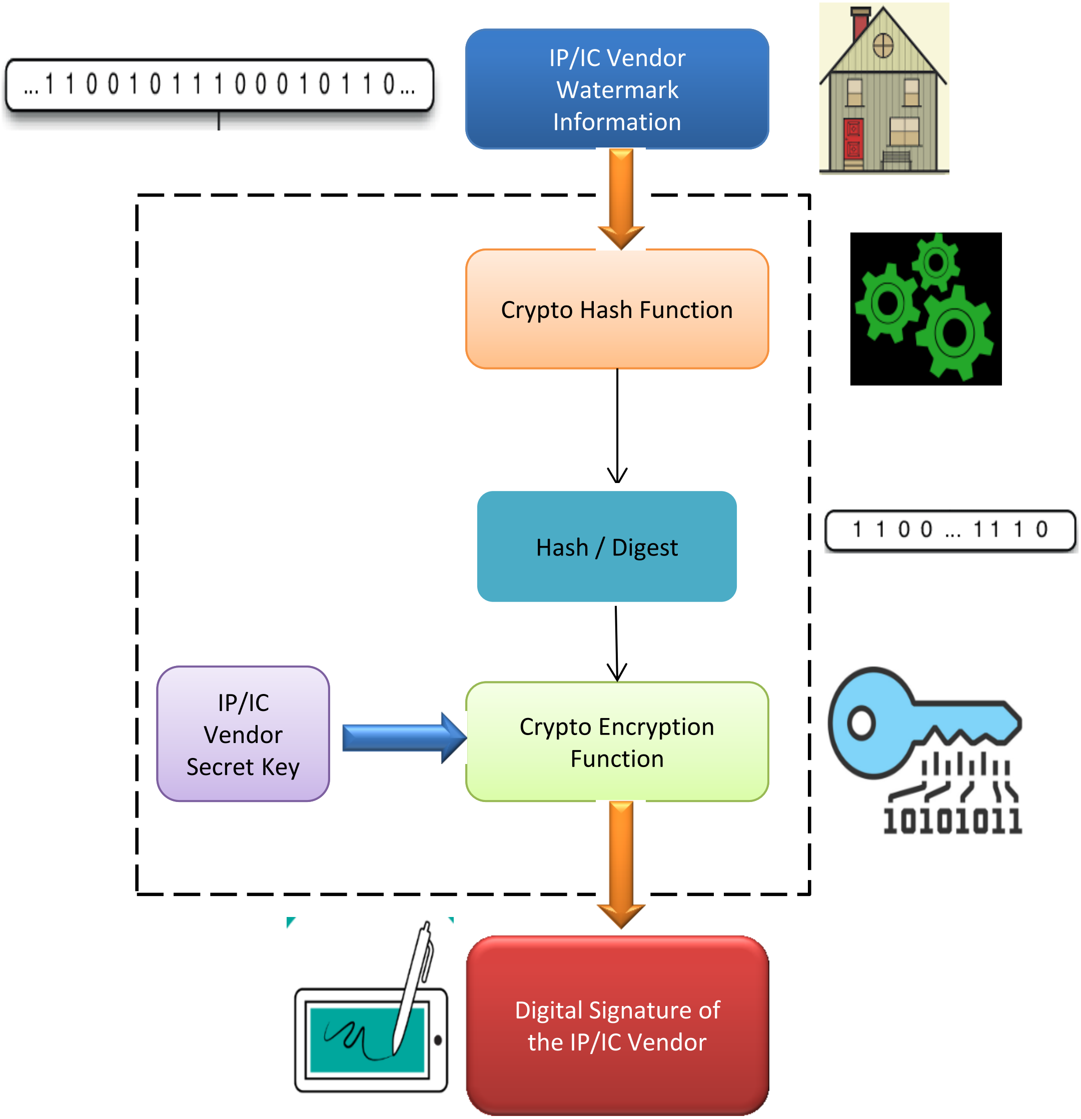


Consumer Electronic devices

SOC with third party IPs

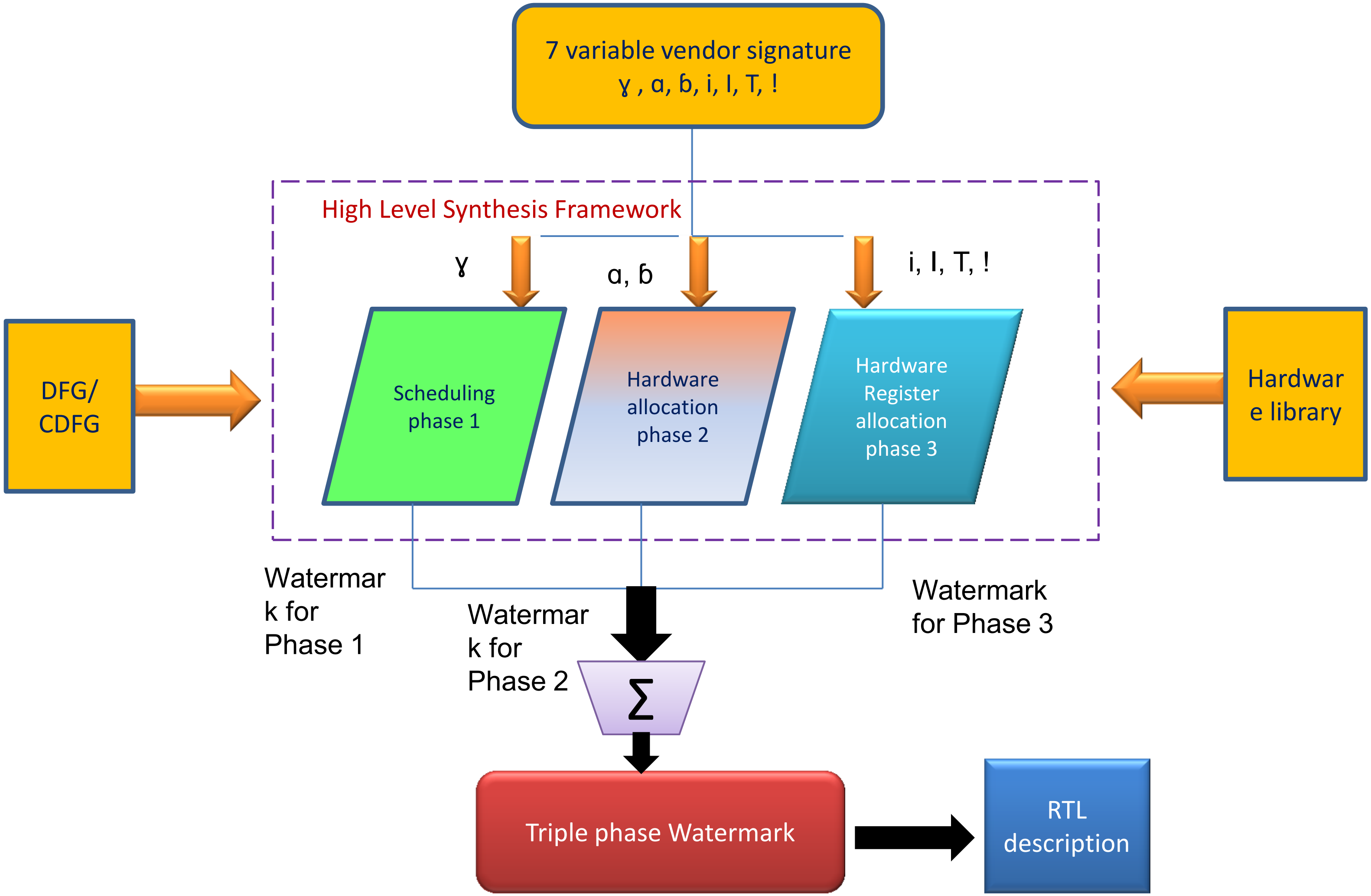
Anirban Sengupta, E. Ranjith Kumar, N. Prajwal Chandra "Embedding Digital Signature using Encrypted-Hashing for Protection of DSP cores in CE", **IEEE Transactions on Consumer Electronics (TCE)**, Volume: 65, Issue:3, Aug 2019, pp. 398 - 407

High-level process of creating digital signature for IP cores



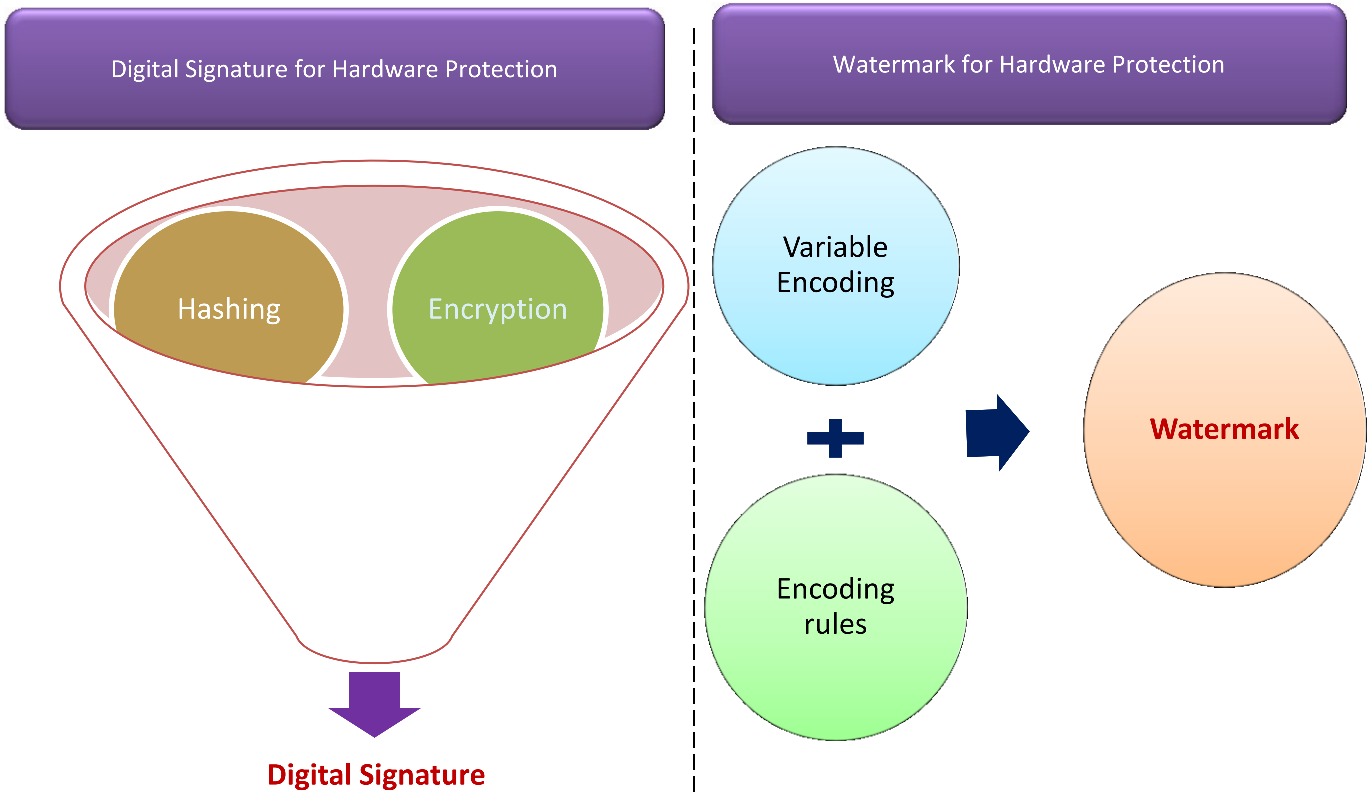
Anirban Sengupta, E. Ranjith Kumar, N. Prajwal Chandra "Embedding Digital Signature using Encrypted-Hashing for Protection of DSP cores in CE", **IEEE Transactions on Consumer Electronics (TCE)**, Volume: 65, Issue:3, Aug 2019, pp. 398 - 407

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

Hardware based Digital Signature Vs. Hardware Watermarking for IP Core Protection



Digital Signature for Hardware Protection

Hashing

Encryption

Digital Signature

Watermark for Hardware Protection

Variable Encoding

Encoding rules

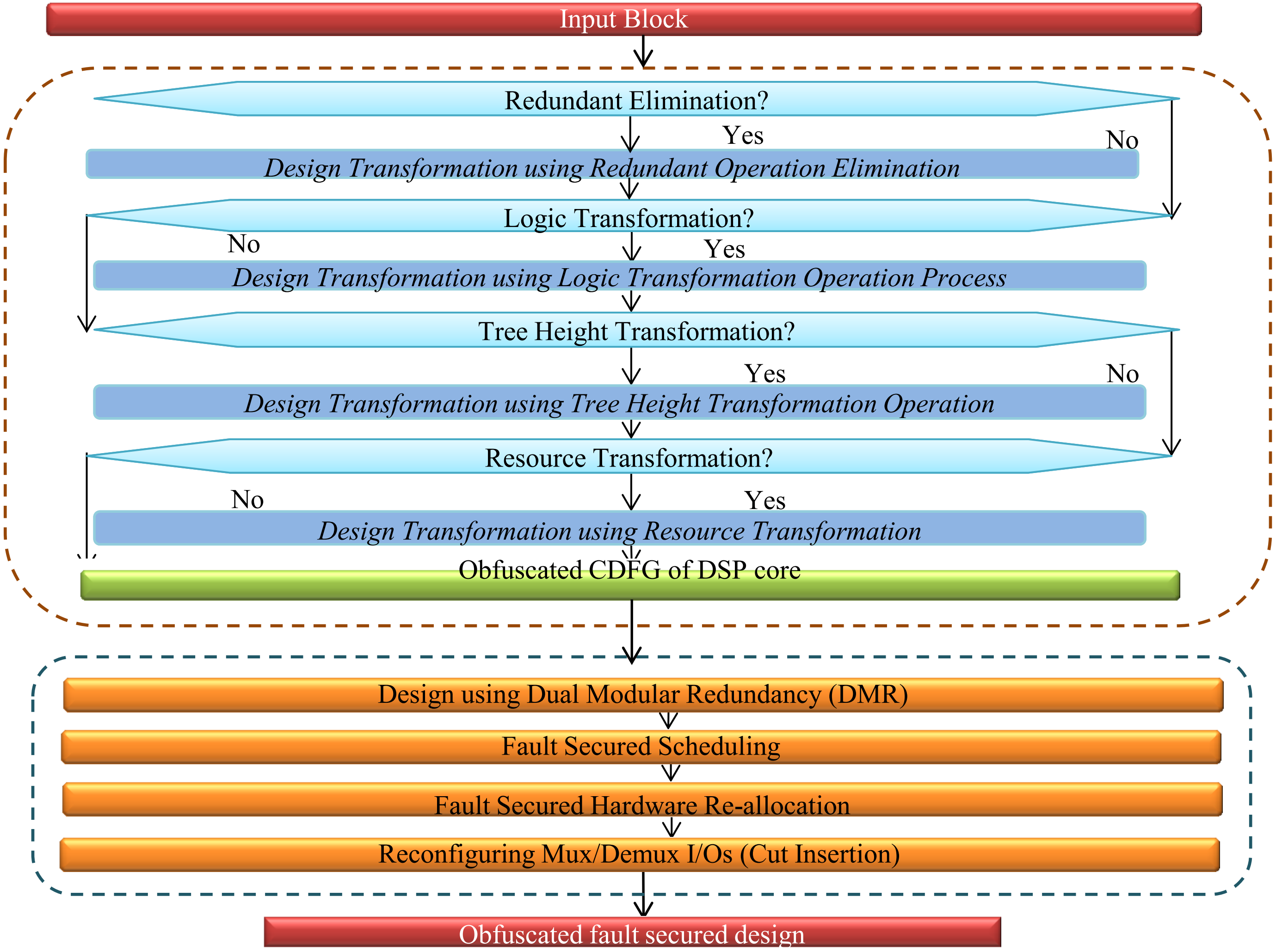
Watermark

- ✓ Provides stronger (more definite) proof of ownership than Watermark
- ✓ Stronger detection against IP/IC Counterfeiting
- ✓ Stronger detection against IP/IC Cloning
- ✓ Provides better control over design security and overhead

- ✓ Provides strong proof of ownership
- ✓ Detection against IP/IC Counterfeiting
- ✓ Detection against IP/IC Cloning
- ✓ High result into design overhead in many cases

Anirban Sengupta, E. Ranjith Kumar, N. Prajwal Chandra "Embedding Digital Signature using Encrypted-Hashing for Protection of DSP cores in CE", **IEEE Transactions on Consumer Electronics (TCE)**, Volume: 65, Issue:3, Aug 2019, pp. 398 - 407

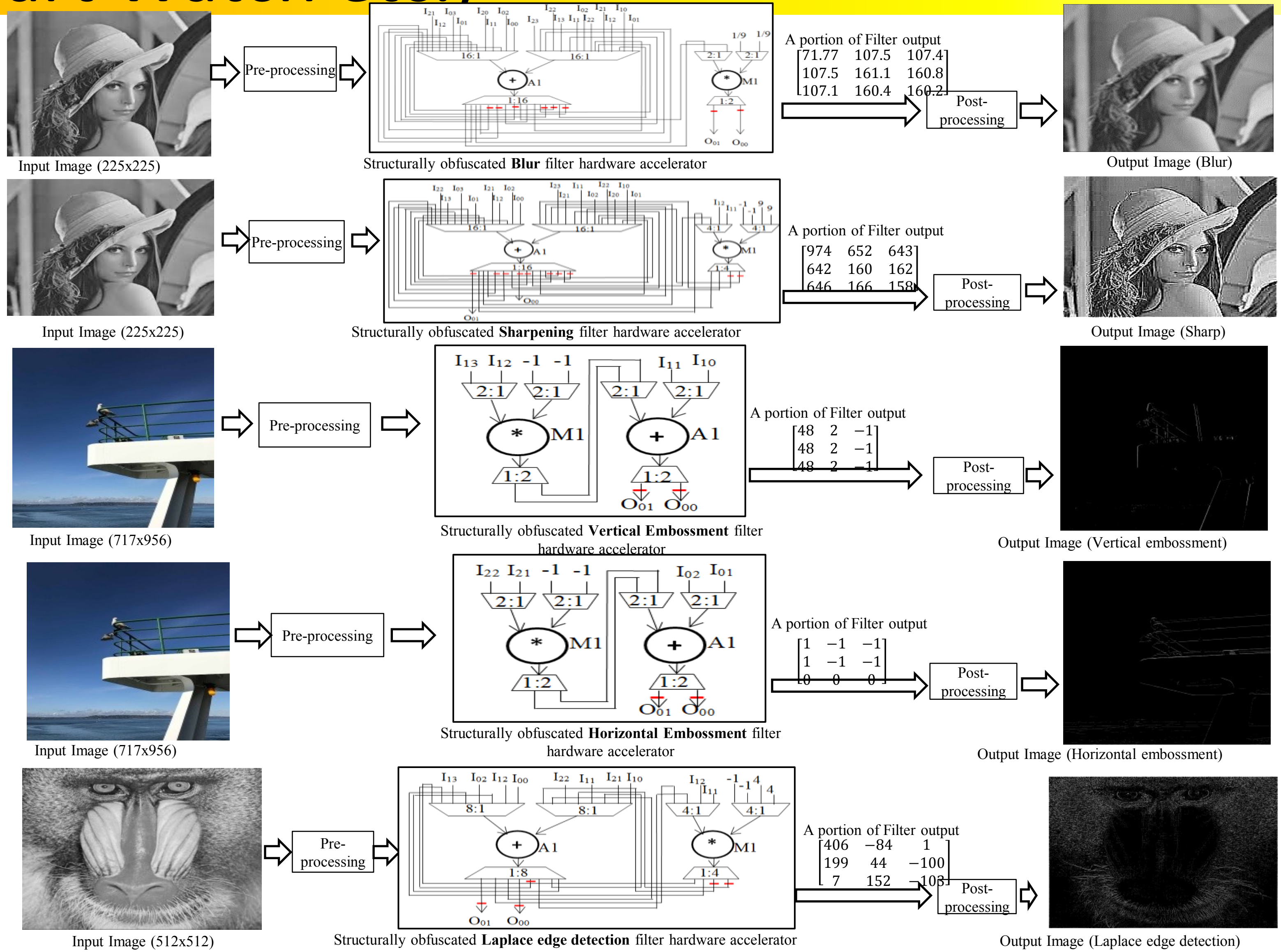
Generic Design Flow of the Obfuscation process


Input Block
Redundant Elimination?
Yes
No
Design Transformation using Redundant Operation Elimination
Logic Transformation?
No
Yes
Design Transformation using Logic Transformation Operation Process
Tree Height Transformation?
Yes
No
Design Transformation using Tree Height Transformation Operation
Resource Transformation?
No
Yes
Design Transformation using Resource Transformation
Obfuscated CDFG of DSP core
Design using Dual Modular Redundancy (DMR)
Fault Secured Scheduling
Fault Secured Hardware Re-allocation
Reconfiguring Mux/Demux I/Os (Cut Insertion)
Obfuscated fault secured design

Obfuscation for fault Secured DSP 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

Secured IPs for Image Processing (Camera, Smart Watch etc.)



Input Image (225x225)

Structurally obfuscated **Blur** filter hardware accelerator

$$\begin{bmatrix} 71.77 & 107.5 & 107.4 \\ 107.5 & 161.1 & 160.8 \\ 107.1 & 160.4 & 160.2 \end{bmatrix}$$

Output Image (Blur)

Input Image (225x225)

Structurally obfuscated **Sharpening** filter hardware accelerator

$$\begin{bmatrix} 974 & 652 & 643 \\ 642 & 160 & 162 \\ 646 & 166 & 158 \end{bmatrix}$$

Output Image (Sharp)

Input Image (717x956)

Structurally obfuscated **Vertical Embossment** filter hardware accelerator

$$\begin{bmatrix} 48 & 2 & -1 \\ 48 & 2 & -1 \\ 48 & 2 & -1 \end{bmatrix}$$

Output Image (Vertical embossment)

Input Image (717x956)

Structurally obfuscated **Horizontal Embossment** filter hardware accelerator

$$\begin{bmatrix} 1 & -1 & -1 \\ 1 & -1 & -1 \\ 0 & 0 & 0 \end{bmatrix}$$

Output Image (Horizontal embossment)

Input Image (512x512)

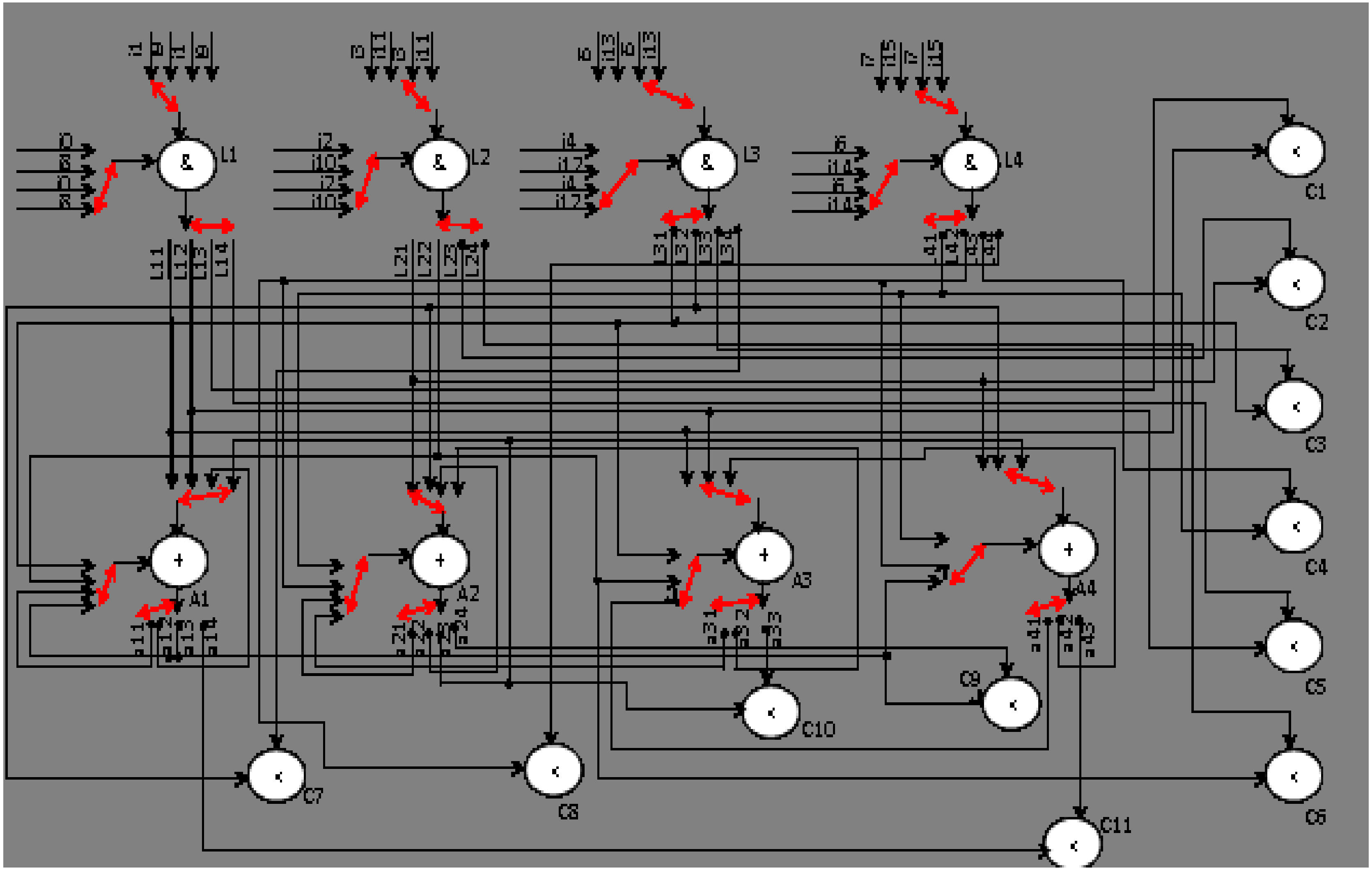
Structurally obfuscated **Laplace edge detection** filter hardware accelerator

$$\begin{bmatrix} 406 & -84 & 1 \\ 199 & 44 & -100 \\ 7 & 152 & -103 \end{bmatrix}$$

Output Image (Laplace edge detection)

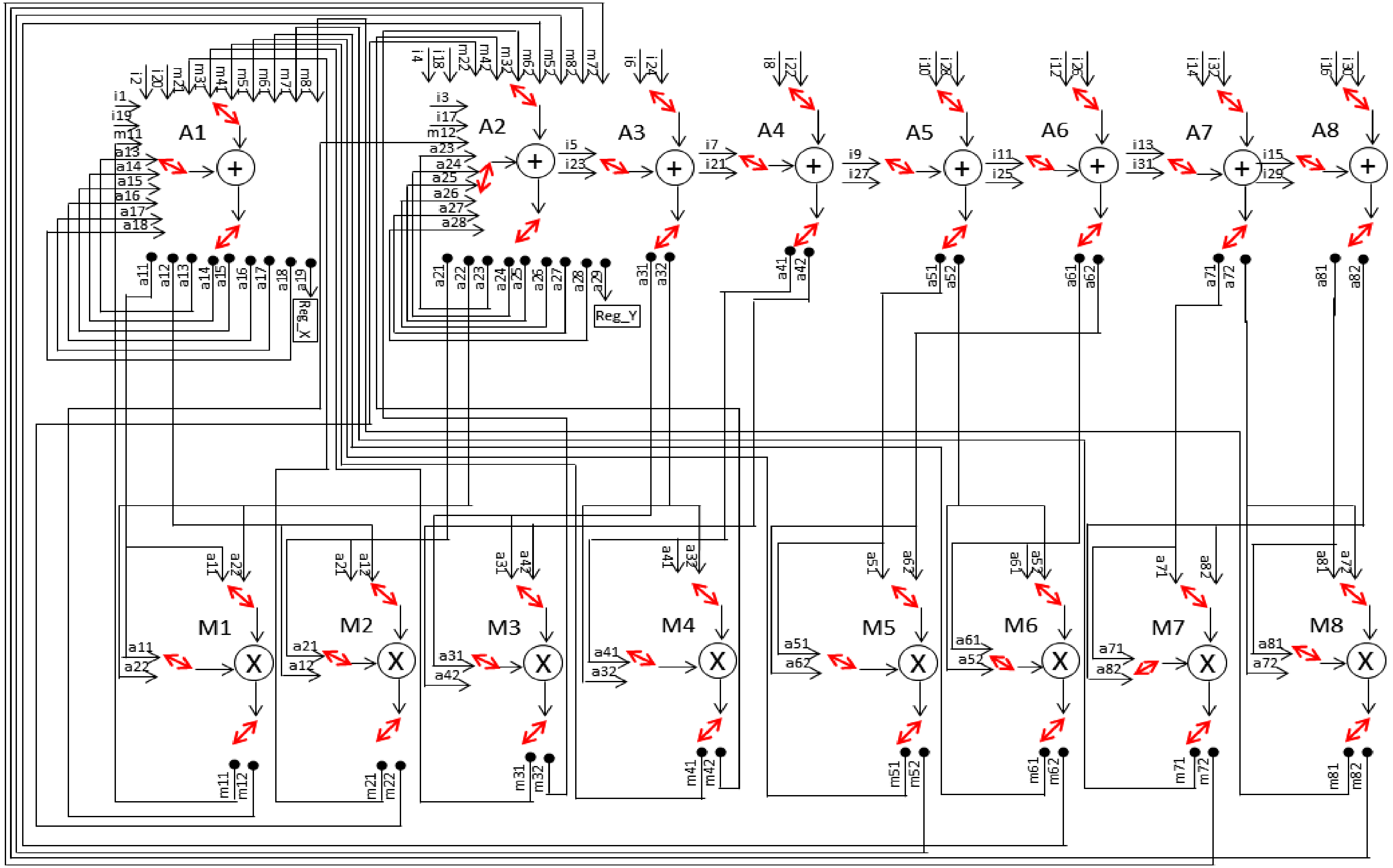
Five different 3×3 filter designs of image processing with end-to-end demonstration. Here, pre-processing includes conversion of RGB input image to gray-scale pixel matrix and zero padding. Post-processing includes conversion of filter output matrix from double data type to integer and then into an image form

Obfuscated Design of fault secured FIR filter



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

Non-obfuscated DSP circuit of a FIR filter with normal fault security



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

Conclusion

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

Thank You