IEEE-CS Executive Committee Meeting

June 14, 2021

Hardware Security and IP Core Protection

Dr. (Prof) Anirban Sengupta, FIET, FBCS
IEEE Computer Society Distinguished Visitor
Associate Editor, IEEE Transactions on VLSI Systems
Associate Editor, IEEE letters of Computer Society
Former Chair, IEEE-CS Technical Committee on VLSI
ExCom, IEEE-CS Technical Committee on VLSI
Former Editor-in-Chief, IEEE VLSI Circuits & Systems Letter (IEEE Computer Society TCVLSI)

Associate Professor, Indian Institute of Technology Indore
Homepage: https://www.anirban-sengupta.com/

Hardware Security and IP Core Protection

- 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.

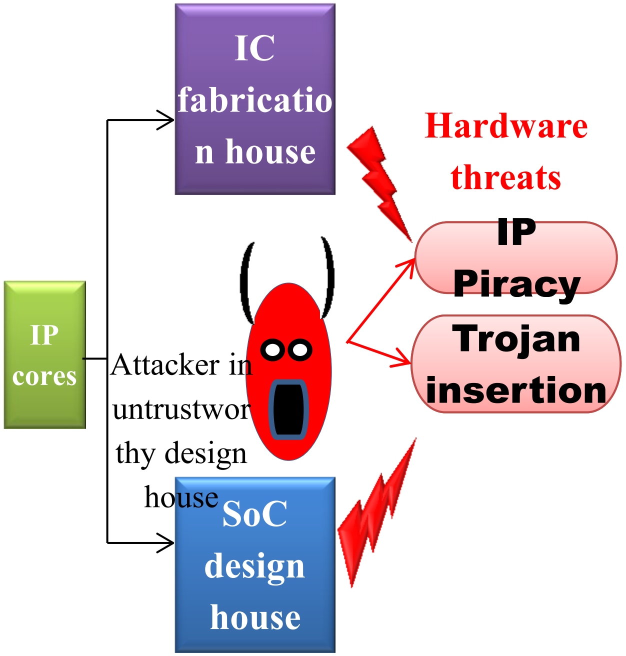
- Hardware security is broadly classified into two types: (a) authentication based approaches (b) obfuscation based approaches.

- 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 "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

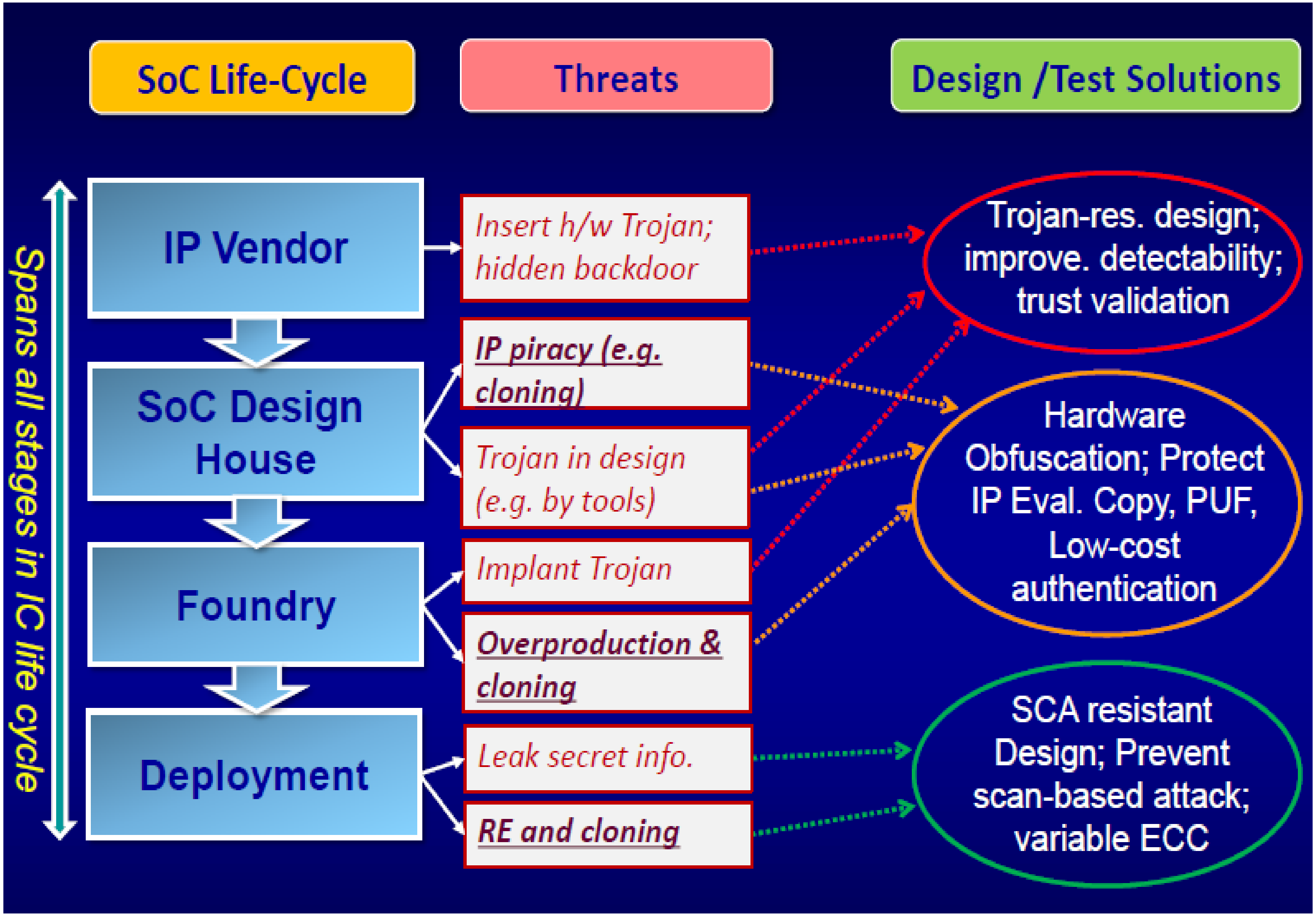
Affected Parties

- Distinct design houses involved in an IC design chain may not be trustworthy.
- Hence, due to globalization of IC design chain, the reusable **IP cores or ICs are susceptible** to various **hardware threats** such as:
  - ➢ Hardware Trojan insertion
  - ➢ IP piracy (Counterfeiting, Cloning, False claim of IP ownership)



"Potential hardware security threats in untrustworthy design houses"

Why is Hardware Security Important ?



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.

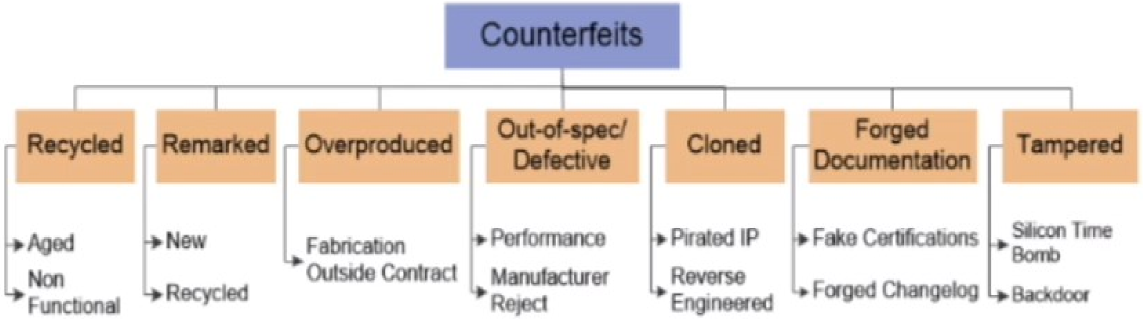
RE and cloning

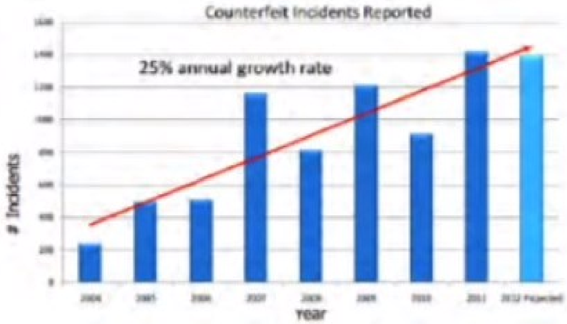
Trojan-res. design; improve. detectability; trust validation

Hardware Obfuscation; Protect IP Eval. Copy, PUF, Low-cost authentication

SCA resistant Design; Prevent scan-based attack; variable ECC

Why hardware Security is an important emerging need?



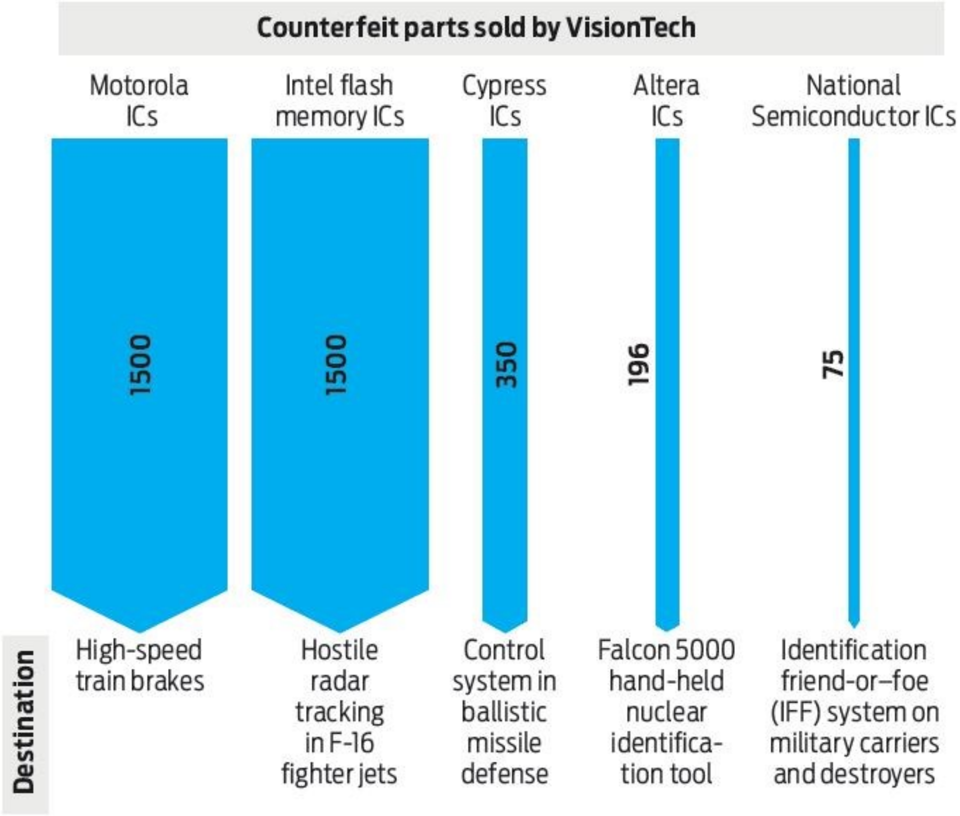


Reported counterfeit incidents are growing rapidly since 2009.

Electronics companies lose $100 billion dollar every year because of counterfeiting

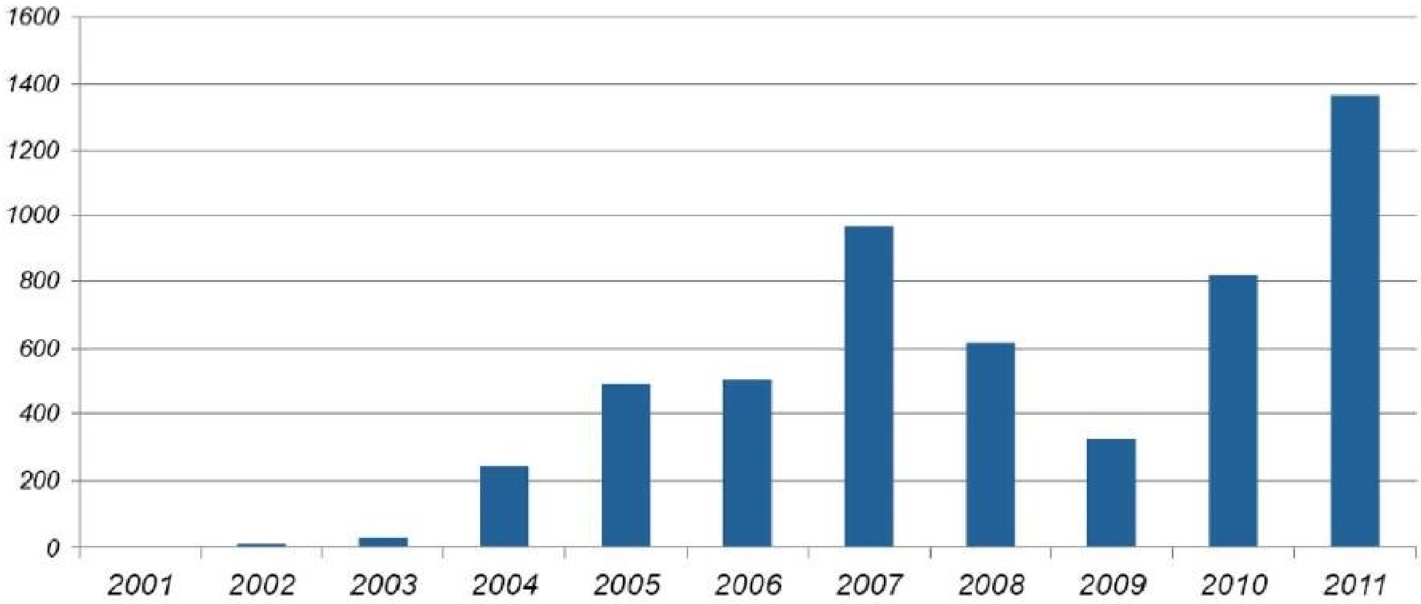
A Case Study in Fake Chips

In 2010 the United States prosecuted its first case against a counterfeit-chip broker. The company, VisionTech, sold thousands of fake chips, many of which were destined for military products.



Gorman, Celia. (2012). Counterfeit Chips on the Rise. IEEE Spectrum. 49. 16-17. 10.1109/MSPEC.2012.6203952.

- Data provided by IHS (Information Handling Services, Englewood, CO, USA), shown in the figure below, shows that reports of counterfeit parts have quadrupled since 2009.
- Legitimate electronics **companies miss out on about $100 billion of global revenue every year because of counterfeiting**.
- Around 1% of semiconductor sales are estimated to be those of counterfeited units



U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1207-1228, Aug. 2014.

Hardware security is important for national security

- The deployment of hardware modules in consumer applications and life critical applications such as aerospace, military and healthcare entails securing them against potential hardware threats and ensuring trust.

- A failure of an electronic chip or generating erroneous output by a functional module in the chip during its operation may wreak havoc on people's life. For example, a Syrian radar failed to alert an incoming air strike in 2007.

- The possible cause was projected to be the presence of hardware Trojan (a malicious logic which is a backdoor entry in the design and remains stealthy in normal condition) in the chip.

- Additionally, a potential Trojan into the hardware design may leak secret information such as private keys; and, it may also cause excessive heat dissipation that may result in battery explosion.

- Counterfeit/pirated designs/IPs may contain such malicious Trojan logic as they are not obtained from a genuine or authentic and reliable source or IP vendor

What work has been done in this in IEEE-CS

- **Major IEEE-CS Publications has published few papers on this:**

1) IEEE Transactions on VLSI Systems (TVLSI) –periodical of IEEE-CS
2) IEEE Letters of Computer Society (LOCS) –periodical of IEEE-CS
3) IEEE-CS ISVLSI – Conference of IEEE-CS

Some examples:

Anirban Sengupta, Mahendra Rathor "Facial Biometric for Securing Hardware Accelerators", ***IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*** , Volume: 29, Issue: 1, Jan. 2021, pp. 112 – 123

Anirban Sengupta, Mahendra Rathor "Securing Hardware Accelerators for CE Systems using Biometric Fingerprinting", ***IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*** , Volume: 28, Issue: 9, Sep 2020, pp. 1979-1992

- **Special Issues on hardware security was commissioned in IEEE Transactions on VLSI Systems (TVLSI) –periodical of IEEE-CS**:

Anirban Sengupta, Sandip Kundu "Securing IoT Hardware: Threat models and Reliable, Low-power Design Solutions", ***IEEE Transactions on Very Large Scale Integration (VLSI) Systems***, Dec 2017, Volume: 25, Issue:12, pp. 3265 - 3267.

What more can be done in IEEE-CS ?

- **Other major IEEE-CS Publications / technical committee such as following needs to take initiative to involve/ recruit experts from this area as well as promote this area:**

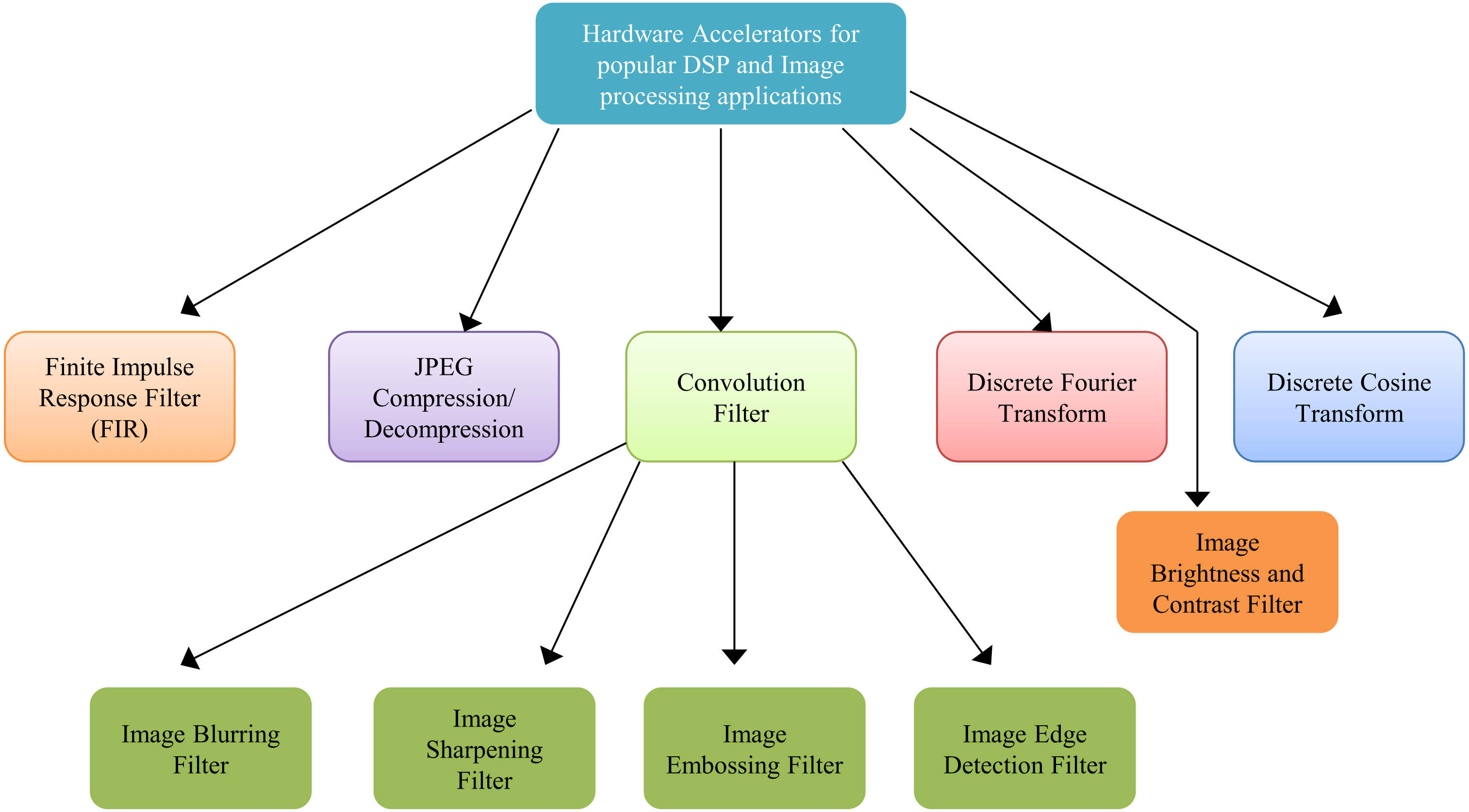
1) IEEE Symposium on Security and Privacy (S&P) – Still has no expert from hardware security
2) IEEE Security and Privacy (S&P) Journal - Still has no expert from hardware security
3) IEEE Computer Society's Technical Committee on Security and Privacy - Still has no expert from hardware security

I have expressed my interest - Sean Peisert, IEEE Security & Privacy Editor in Chief

4) IEEE-CS Conferences such as IEEE Symposium on High-Performance Computer Architecture (HPCA), IEEE Computer Society International Conference on Computers, Software, and Applications (COMPSAC) etc. needs to recruit experts at the organizing committee level.
5) Flagship Journal such IEEE Transactions on VLSI Systems (TVLSI) shoud emphasize more on publishing research work on hardware Security including from acknowledged experts in this area who are on the board.

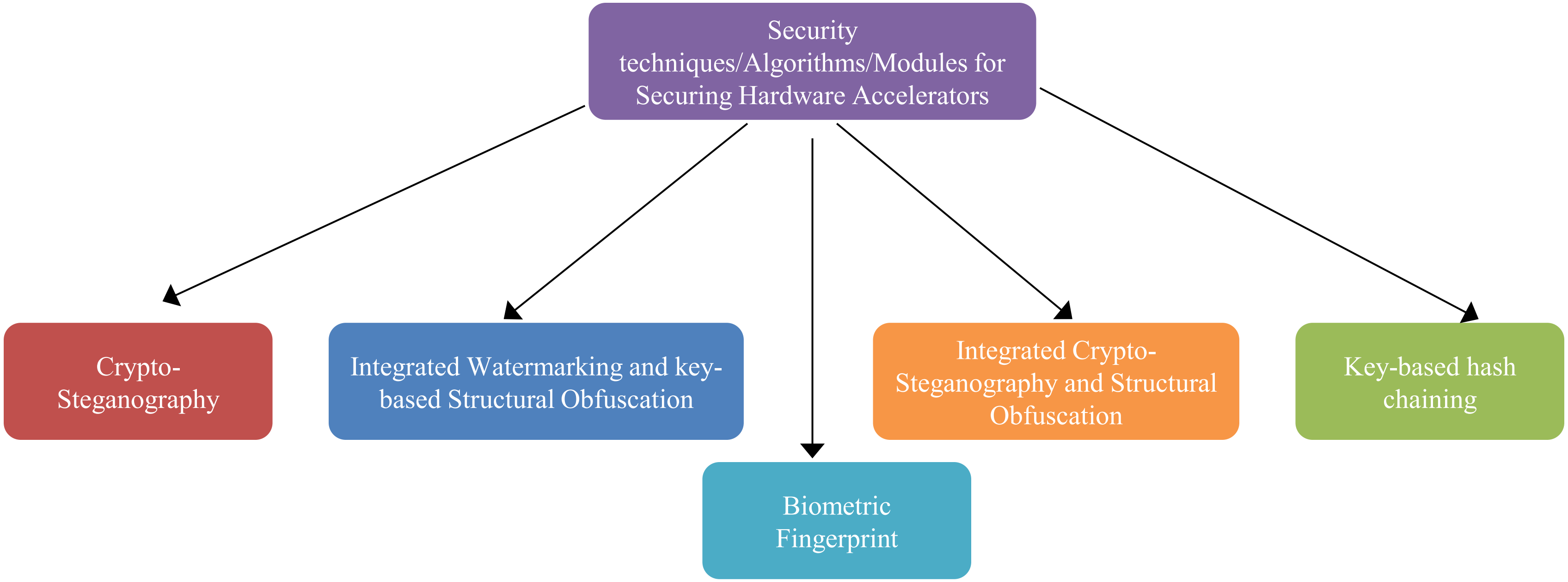
Thank you for your valuable time !

Hardware accelerators


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

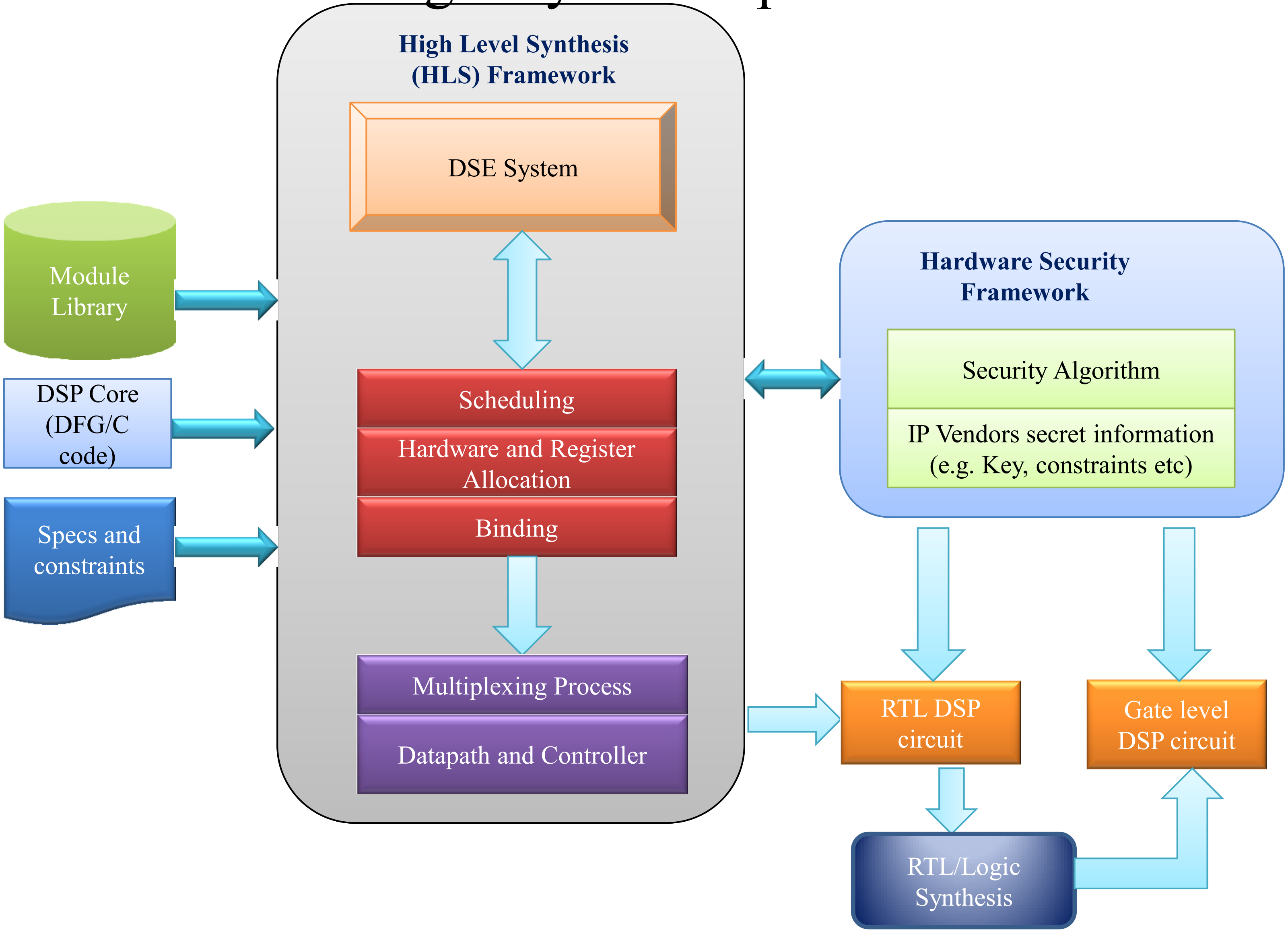
Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", The Institute of Engineering and Technology (IET), 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

Hardware security techniques for securing hardware accelerators


Security techniques/Algorithms/Modules for Securing Hardware Accelerators
Crypto-Steganography
Integrated Watermarking and key-based Structural Obfuscation
Biometric Fingerprint
Integrated Crypto-Steganography and Structural Obfuscation
Key-based hash chaining

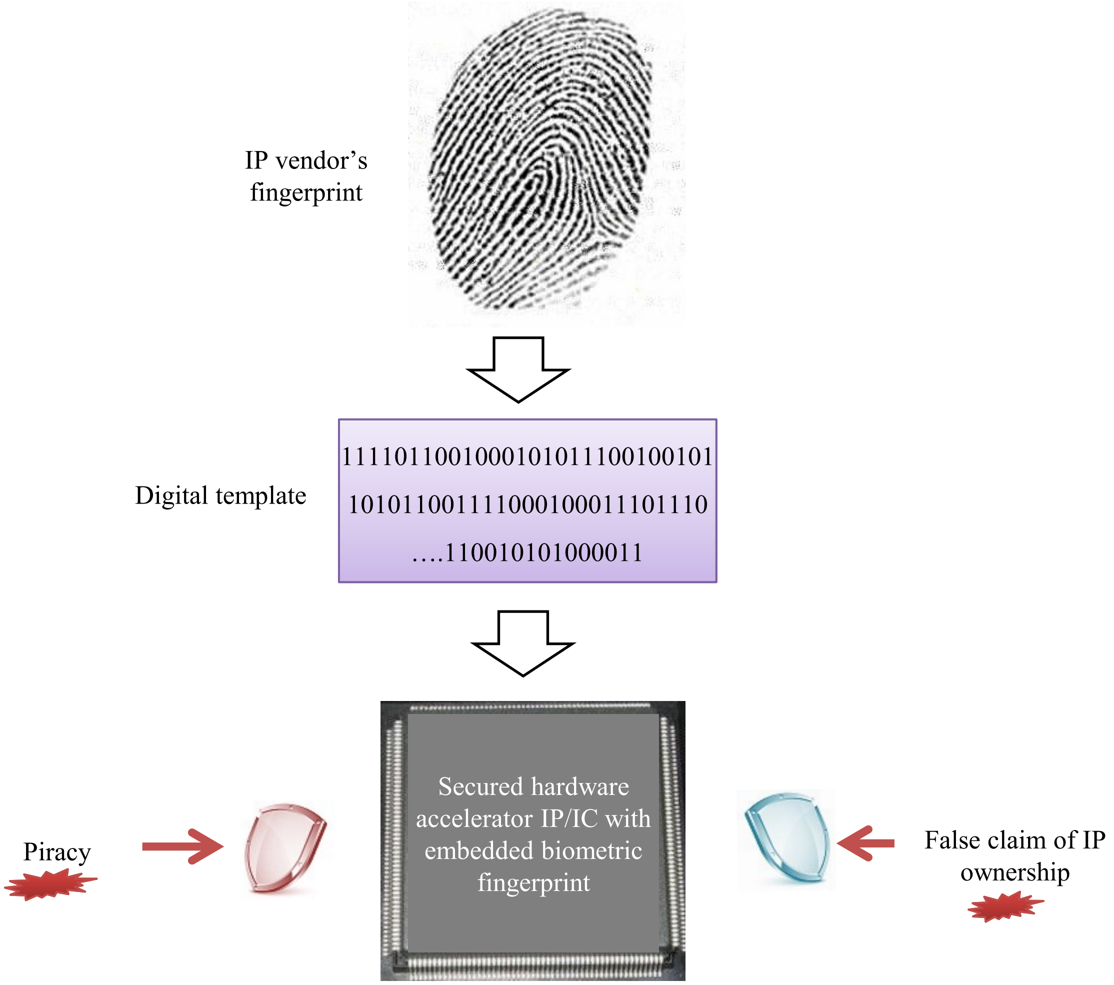
Anirban Sengupta "Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques", **The Institute of Engineering and Technology (IET),** 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

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

Securing hardware accelerators using biometric fingerprinting: Forensics



IP vendor's fingerprint

Digital template

1111011001000101011100100101

101011001111000100011101110

....110010101000011

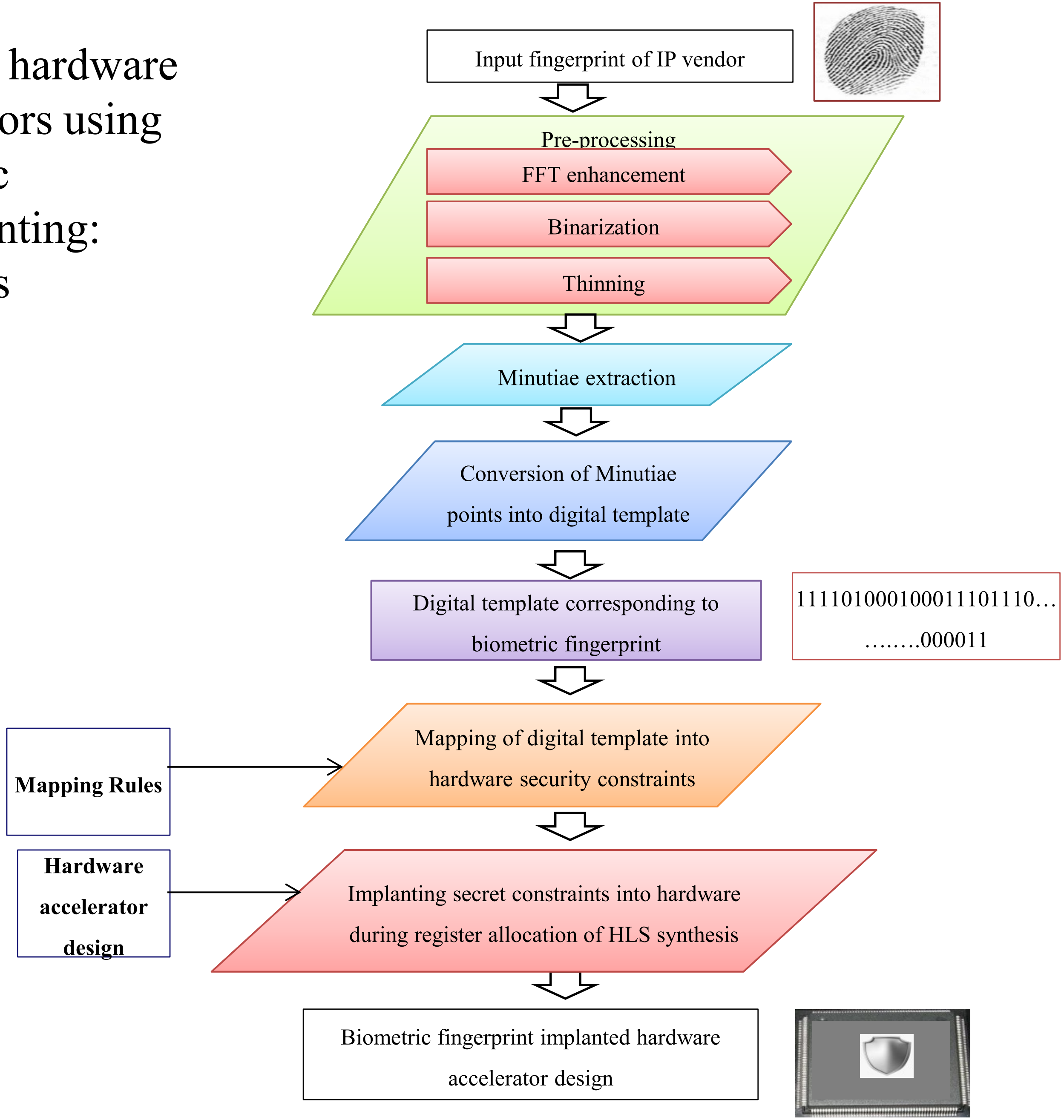
Secured hardware accelerator IP/IC with embedded biometric fingerprint

Piracy

False claim of IP ownership

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



Input fingerprint of IP vendor

Pre-processing

FFT enhancement

Binarization

Thinning

Minutiae extraction

Conversion of Minutiae points into digital template

Digital template corresponding to biometric fingerprint

11110100010001110111 0…
……..000011

Mapping Rules

Mapping of digital template into hardware security constraints

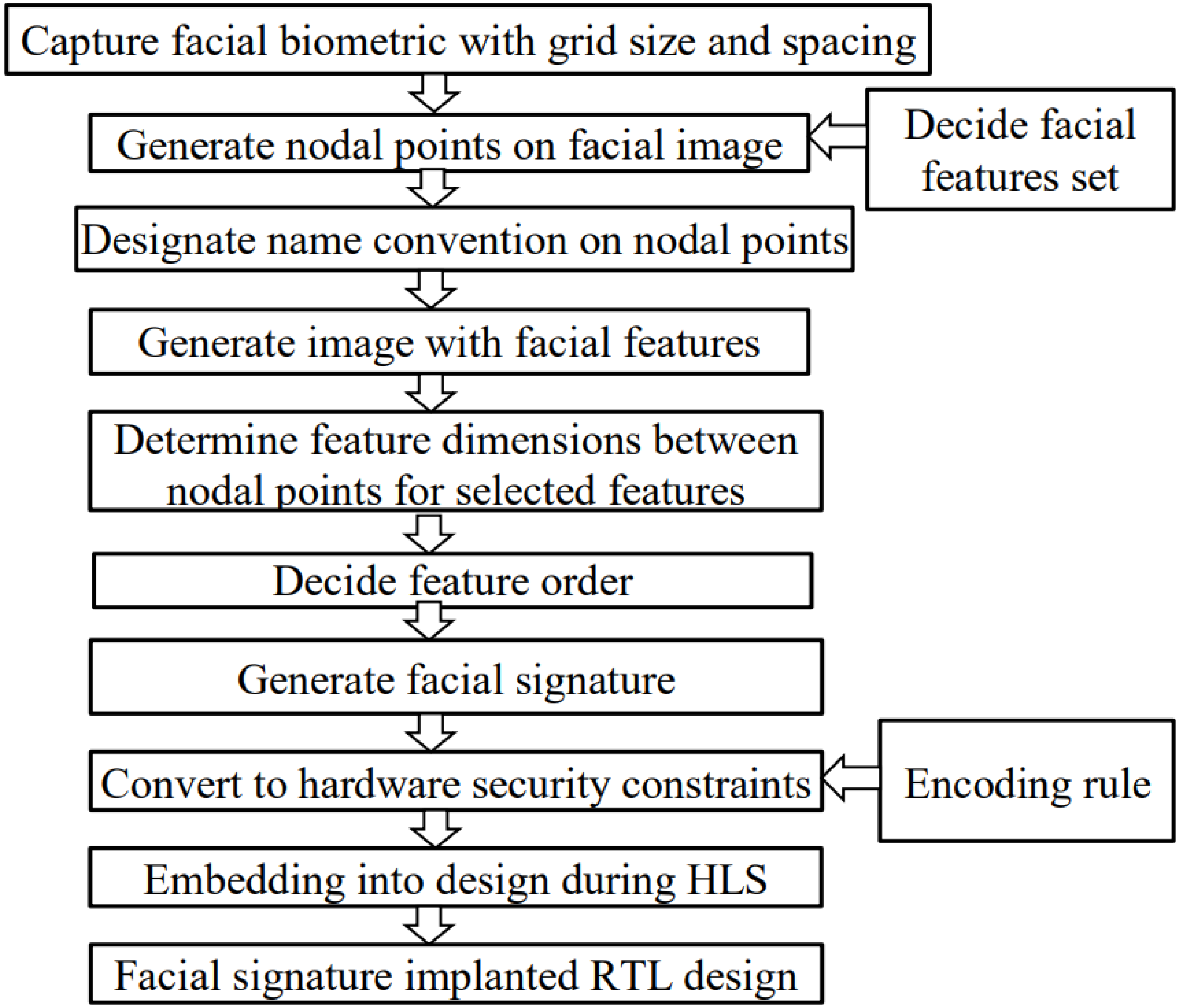
Hardware accelerator design

Implanting secret constraints into hardware during register allocation of HLS synthesis

Biometric fingerprint implanted hardware accelerator design

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

Flow of the proposed Face Biometric Approach


Capture facial biometric with grid size and spacing

Generate nodal points on facial image

Decide facial features set

Designate name convention on nodal points

Generate image with facial features

Determine feature dimensions between nodal points for selected features

Decide feature order

Generate facial signature

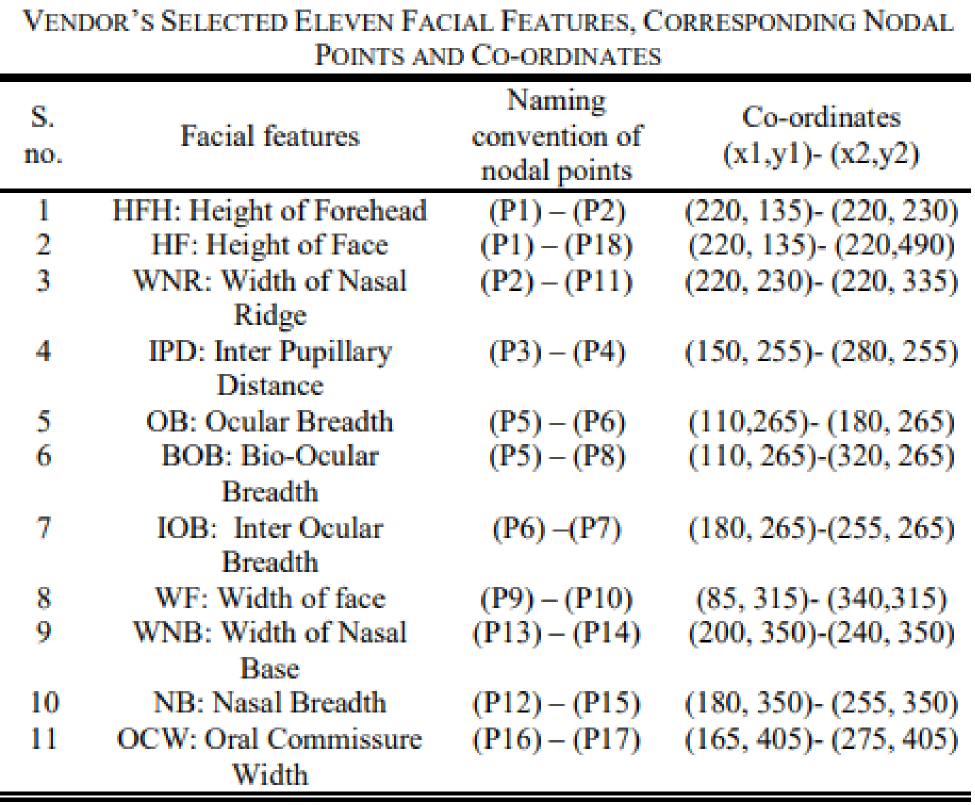
Convert to hardware security constraints

Encoding rule

Embedding into design during HLS

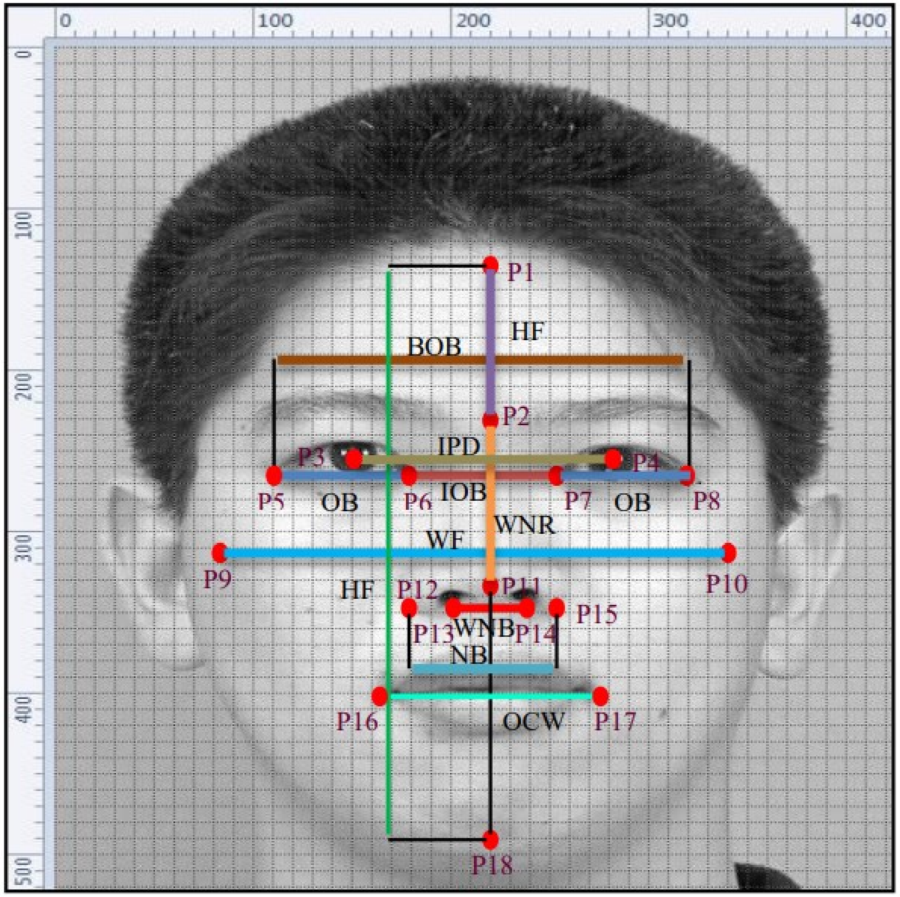
Facial signature implanted RTL design

Determining Facial Features



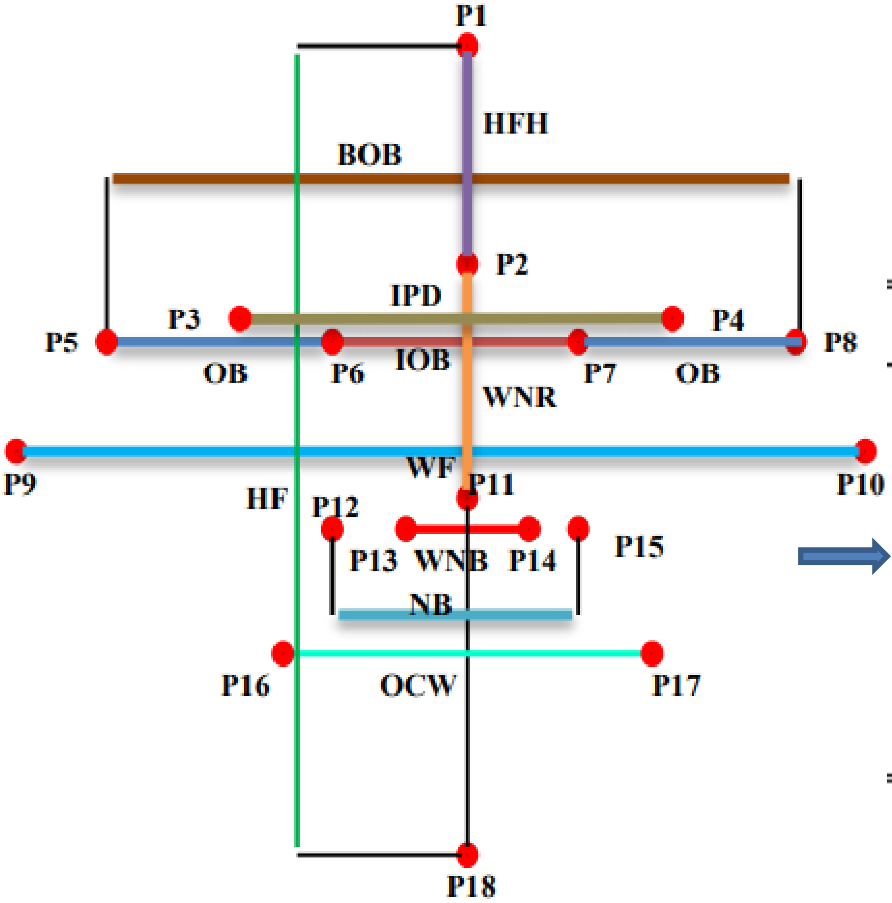
Vendor's Selected Eleven Facial Features, Corresponding Nodal Points and Co-ordinates

S. no.	Facial features	Naming convention of nodal points	Co-ordinates (x1,y1)- (x2,y2)
1	HFH: Height of Forehead	(P1) – (P2)	(220, 135)- (220, 230)
2	HF: Height of Face	(P1) – (P18)	(220, 135)- (220,490)
3	WNR: Width of Nasal Ridge	(P2) – (P11)	(220, 230)- (220, 335)
4	IPD: Inter Pupillary Distance	(P3) – (P4)	(150, 255)- (280, 255)
5	OB: Ocular Breadth	(P5) – (P6)	(110,265)- (180, 265)
6	BOB: Bio-Ocular Breadth	(P5) – (P8)	(110, 265)-(320, 265)
7	IOB: Inter Ocular Breadth	(P6) –(P7)	(180, 265)-(255, 265)
8	WF: Width of face	(P9) – (P10)	(85, 315)- (340,315)
9	WNB: Width of Nasal Base	(P13) – (P14)	(200, 350)-(240, 350)
10	NB: Nasal Breadth	(P12) – (P15)	(180, 350)- (255, 350)
11	OCW: Oral Commissure Width	(P16) – (P17)	(165, 405)- (275, 405)

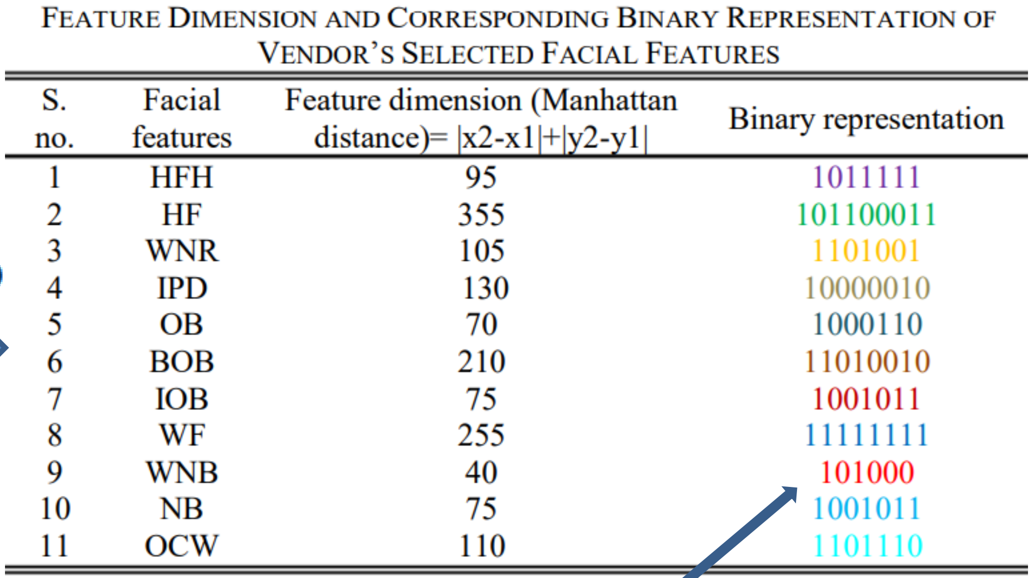


Plotting the selected features on the Facial Biometric.

Measuring Facial Feature Dimensions and Conversion into Binary Representation



Skeleton of the vendor’s selected eleven facial



Feature Dimension and Corresponding Binary Representation of Vendor’s Selected Facial Features

S. no.	Facial features	Feature dimension (Manhattan distance)= |x2-x1|+|y2-y1|	Binary representation
1	HFH	95	1011111
2	HF	355	101100011
3	WNR	105	1101001
4	IPD	130	10000010
5	OB	70	1000110
6	BOB	210	11010010
7	IOB	75	1001011
8	WF	255	11111111
9	WNB	40	101000
10	NB	75	1001011
11	OCW	110	1101110

Notice the varying lengths of feature dimensions in their binary representations. This lack of uniformity is an advantage as the adversary has no clue about the points of concatenation, making extraction of individual dimensions impossible.

Deciding Feature Order and Generating Digital Template

11 facial features

HFH & IPD & BOB & IOB & OB & WNR & WF & HF & WNB & NB & OC

↓

101111110000010110100101001011100011011010011111111110110001110100010010111101110

11 features, 81 bits (34 zeroes and 47 ones)

OB & HF & WNB & IPD & OC & NB & IOB & BOB & WF & HFH & WNR

↓

100011010110001110100010000010110111010010111001011110100101111111110111111101001

11 features, 81 bits (34 zeroes and 47 ones)

WNB & WNR & HFH & OC & HF & IOB

↓

1010001101001101111111011101011000111001011

6 features, 43 bits (17 zeroes and 26 ones), sufficient enough to secure small designs.

Embedding Security Constraints into the CIG

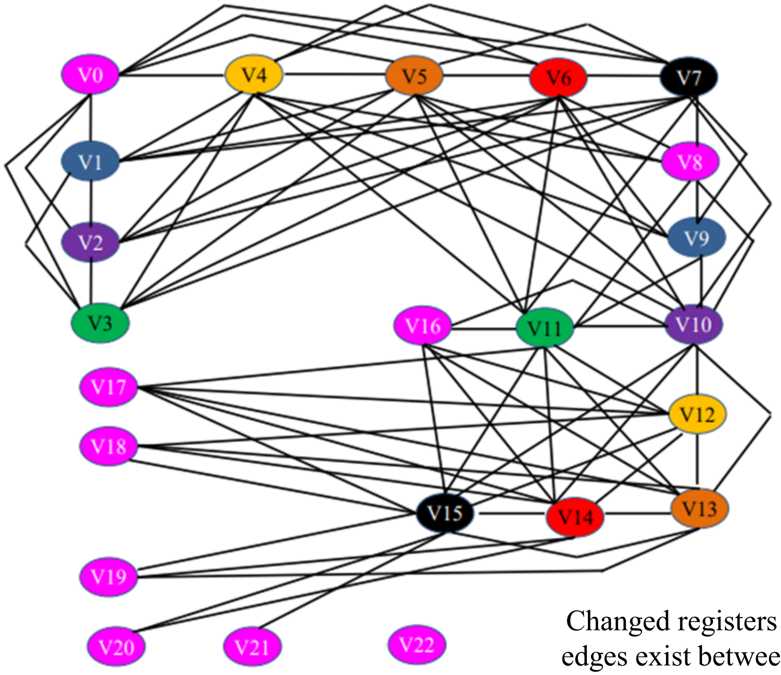
Encoding of Facial Signature into Hardware Security Constraints

Bit	Encoding rules
0	Encoded as an edge between node pair (even, even) into the CIG
1	Encoded as an edge between node pair (odd, odd) into the CIG

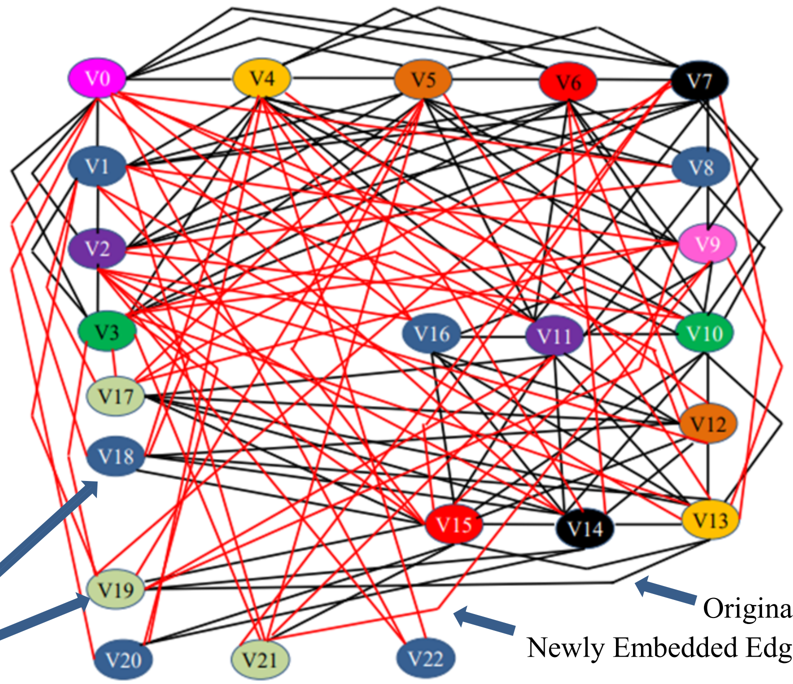
1011111100000101101001010010111000110110100111111111101100011101000100101111101110

34 zeroes → 34 even-even edges → (0,2), (0,4), . . . (0,22), (2,4), (2,6), ... (6,12), (6,14)

47 ones → 47 odd-odd edges → (1,3), (1,5), . . . (1,21), (3,5), (3,7), ... (13,15), (13,17)



Original CIG



Changed registers to ensure no edges exist between registers in the same time span

Original Edge

Newly Embedded Edge

CIG after embedding the above mentioned edges (shown in red)

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, Mahendra Rathor, "IP Core Steganography using Switch based Key-driven Hash-chaining and Encoding for Securing DSP kernels used in CE Systems", IEEE Transactions on Consumer Electronics (TCE), 2020

- 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

- https://cadforassurance.org/tools/ip-ic-protection/faciometric-hardware-security-tool

- Anirban Sengupta, Rahul Chaurasia, Tarun Reddy "Contact-less Palmprint Biometric for Securing DSP Coprocessors used in CE systems", IEEE Transactions on Consumer Electronics (TCE) , Volume: 67, Issue: 3, August 2021, pp. 202-213

- Rahul Chaurasia, Aditya Anshul, Anirban Sengupta "Palmprint Biometric vs Encrypted Hash based Digital Signature for Securing DSP Cores Used in CE systems", IEEE Consumer Electronics (CEM) , Volume: 11, Issue: 5, September 2022, pp. 73-80

- 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

- 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

- 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

- Anirban Sengupta, Saumya Bhadauria, "Exploring Low Cost Optimal Watermark for Reusable IP Cores during High Level Synthesis", IEEE Access, Invited paper, Volume:4, Issue: 99, pp. 2198 - 2215, May 2016 .