

STTP on EMERGING TRENDS IN VLSI TECHNOLOGY

March 5, 2021

Hardware Cybersecurity for image processing and DSP based Accelerators

DR. ANIRBAN SENGUPTA, ASSOC. PROFESSOR

Fellow of IET, Fellow of British Computer Society (BCS), Senior Member of IEEE

IEEE Distinguished Lecturer (IEEE Consumer Electronics Society)

IEEE Distinguished Visitor (IEEE Computer Society)

Ex-Officio - Board of Governors, IEEE Consumer Electronics Society

Former Chairman, IEEE Computer Society Technical Committee on VLSI

Chairman & Founder, IEEE Consumer Electronics Society Bombay Chapter

Chairman, IEEE Consumer Electronics Society Technical Stream Committee - Security and Privacy

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

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

Associate Editor - 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

Former Editorial Board Member - IEEE Access, IEEE Consumer Electronics Magazine, IET Computers and Digital Techniques, 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

Email: asengupta@iiti.ac.in

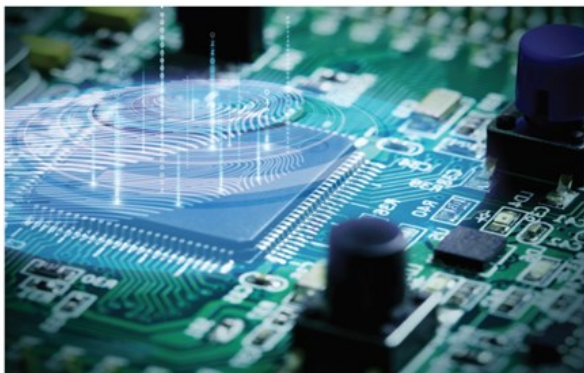
Web: <http://www.anirban-sengupta.com>

Computer Science and Engineering

Indian Institute of Technology Indore

Secured Hardware Accelerators for DSP and Image Processing Applications

Anirban Sengupta



Sengupta

IP Core Protection and Hardware-Assisted Security for Consumer Electronics

Anirban Sengupta and Saraju P. Mohanty



Sengupta and Mohanty

Frontiers in Securing IP Cores

Forensic detective control
and obfuscation techniques

Anirban Sengupta



Sengupta

Sengupta et al. (Eds.)

CCIS
1066

VLSI Design and Test

VDAT
2019Anirban Sengupta · Sudeb Dasgupta ·
Virendra Singh · Rohit Sharma ·
Santosh Kumar Vishvakarma (Eds.)

Communications in Computer and Information Science 1066

VLSI Design and Test

23rd International Symposium, VDAT 2019
Indore, India, July 4–6, 2019
Revised Selected Papers

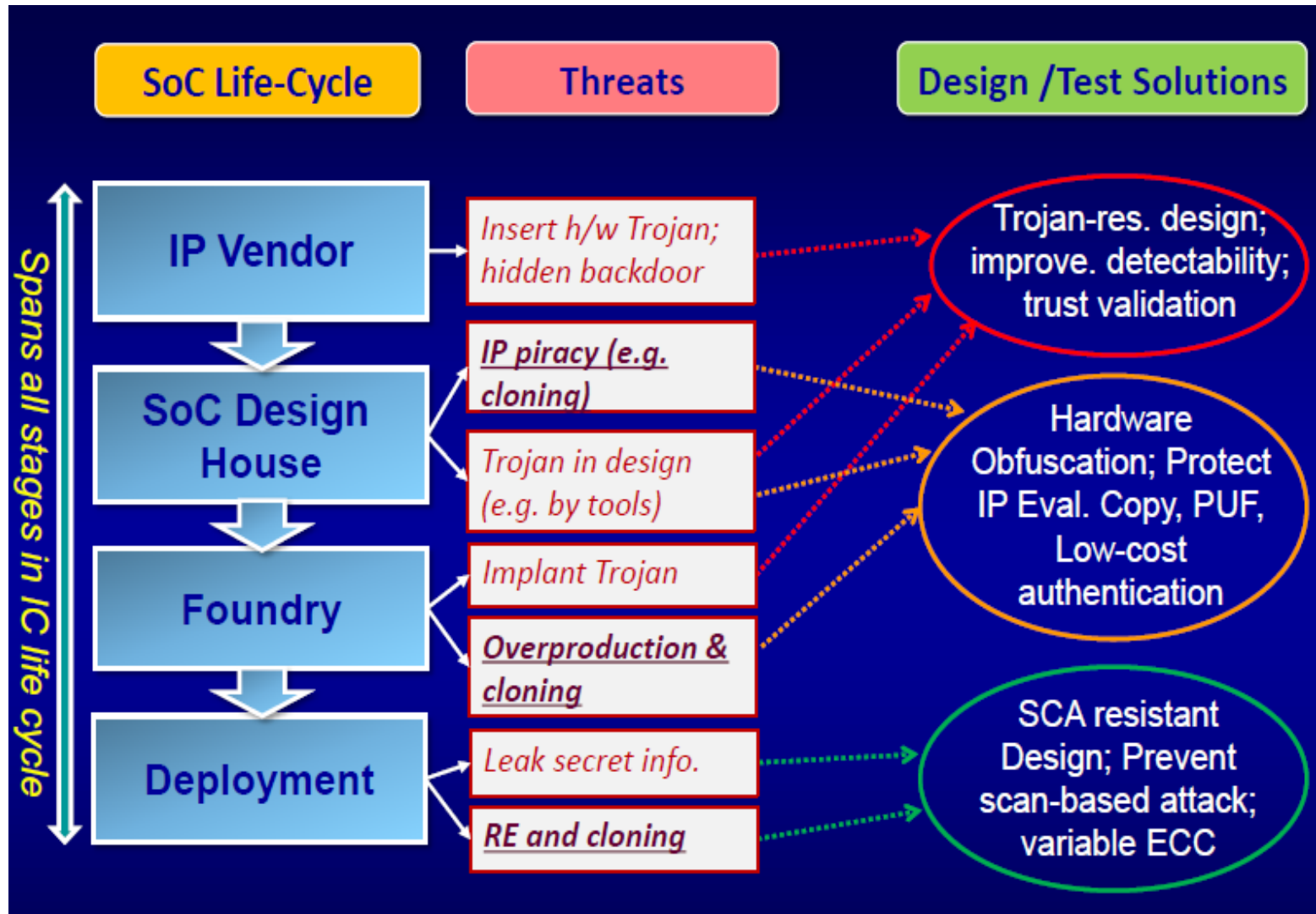
Introduction

- 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.

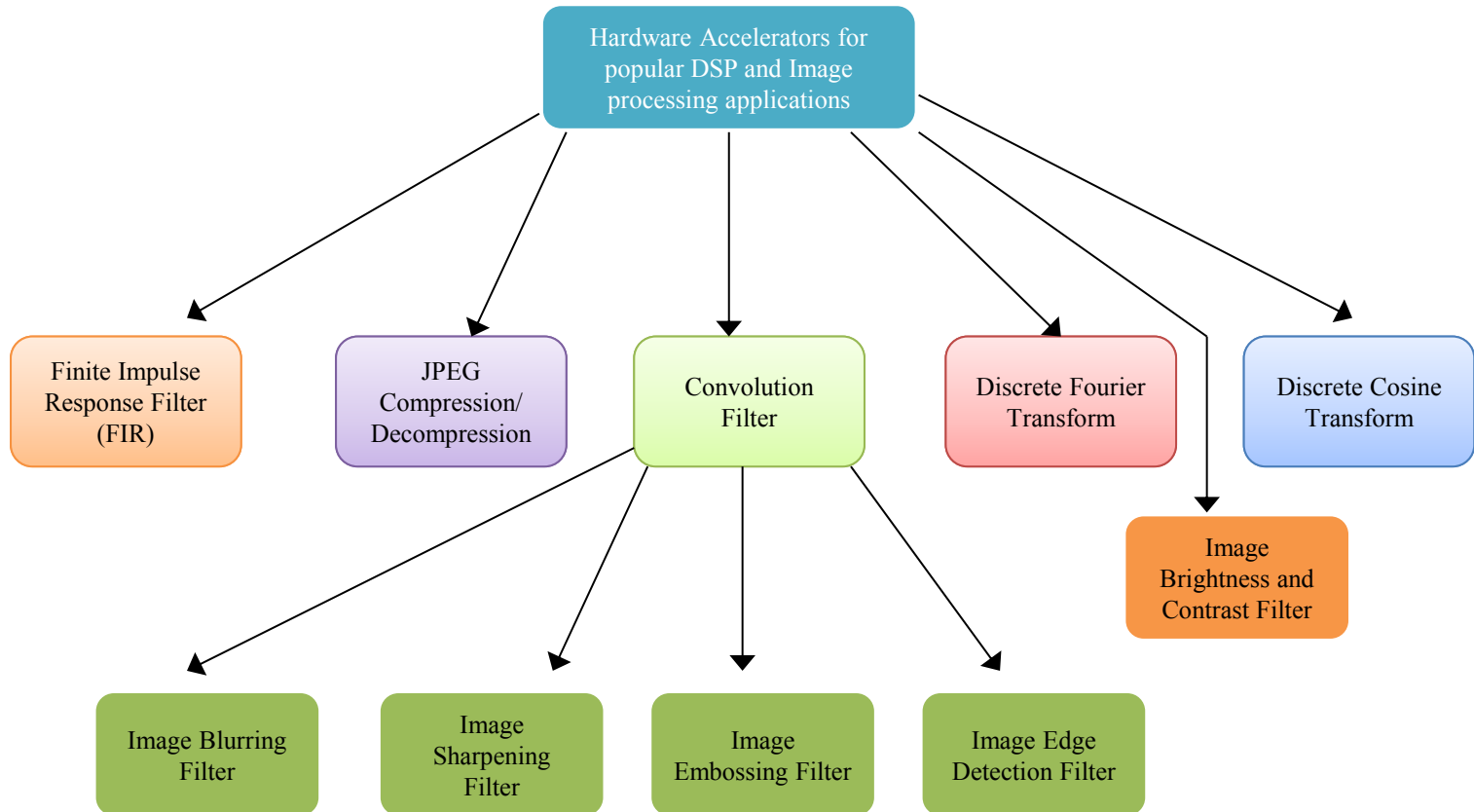
Anirban Sengupta "[Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques](#)", The Institute of Engineering and Technology (IET), 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

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

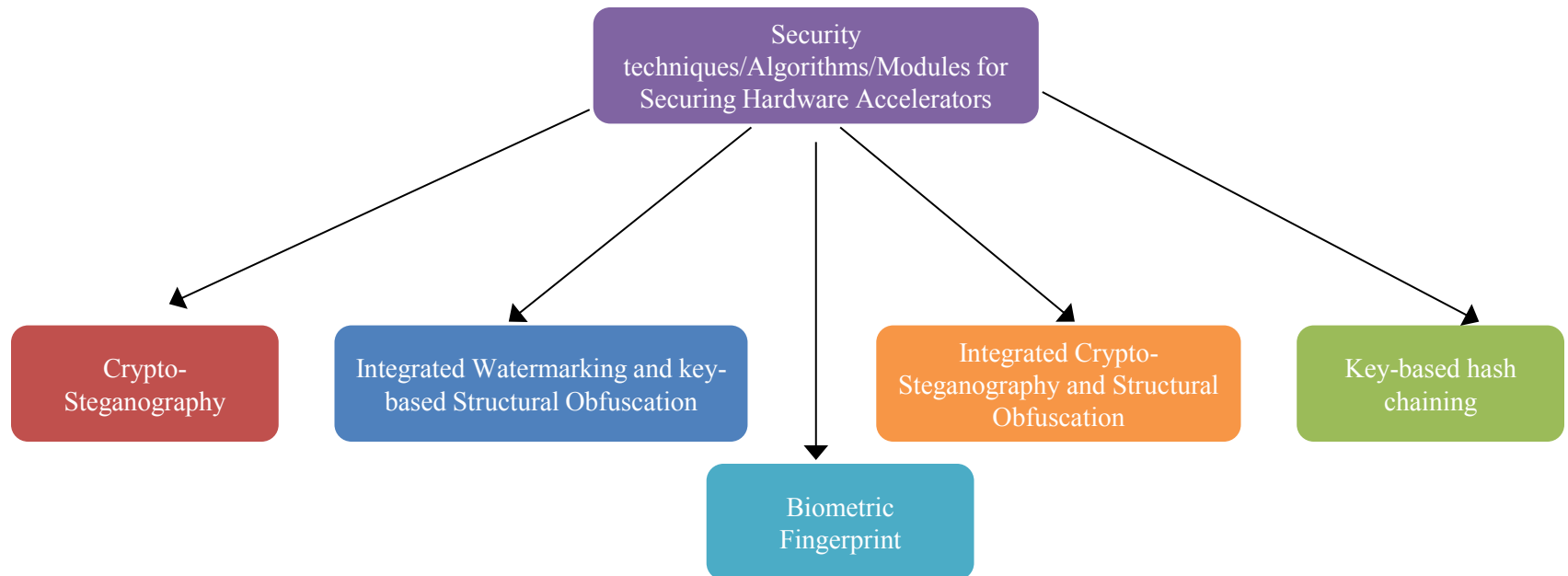
IP Core Protection and Hardware Security



Hardware accelerators: Example



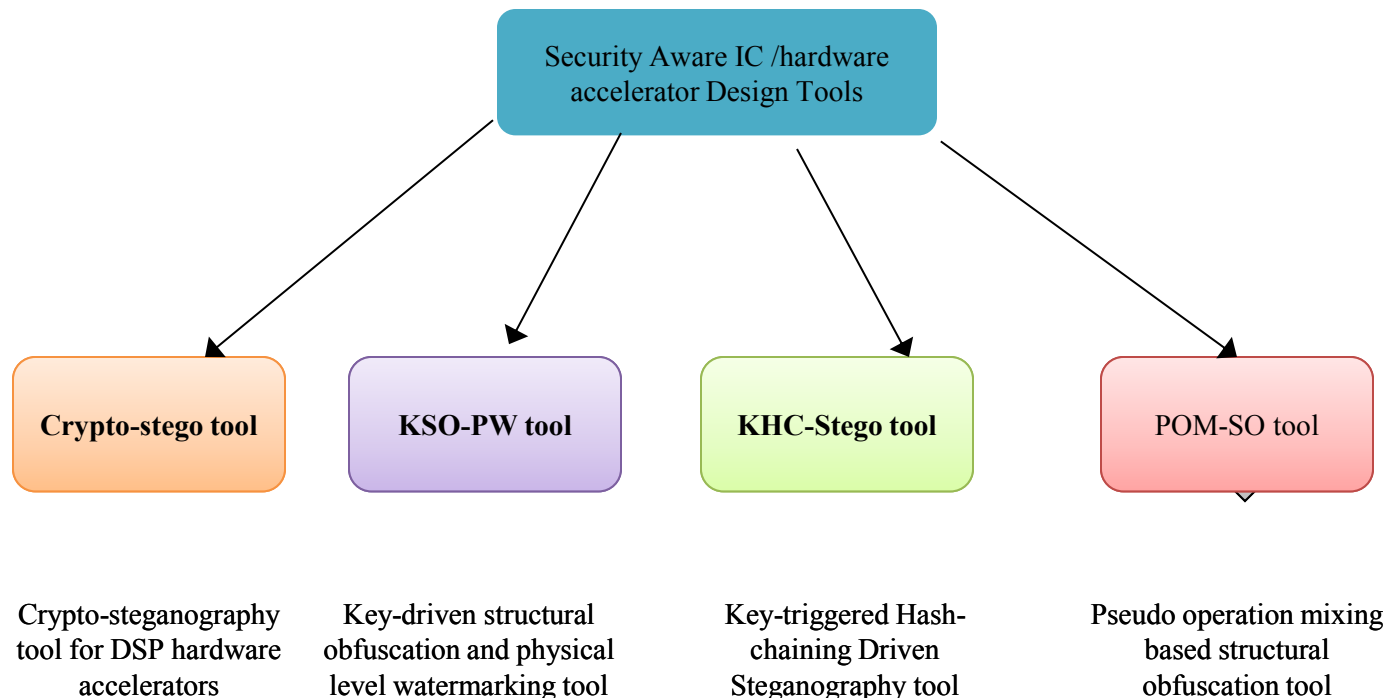
Hardware security techniques for securing hardware accelerators



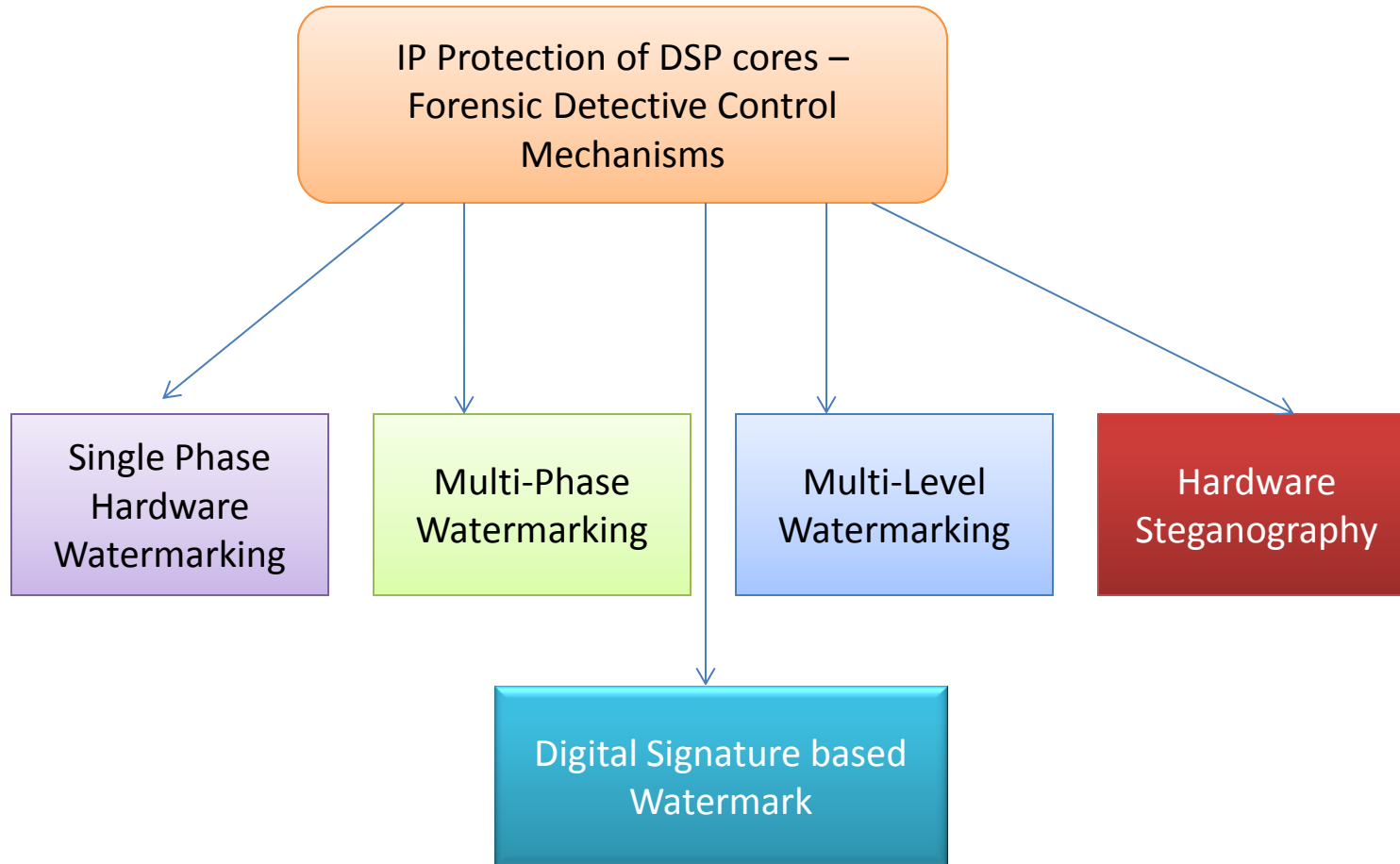
Our in-house hardware security tools for designing secured accelerators

Released publicly from our group in Sep 2020 !

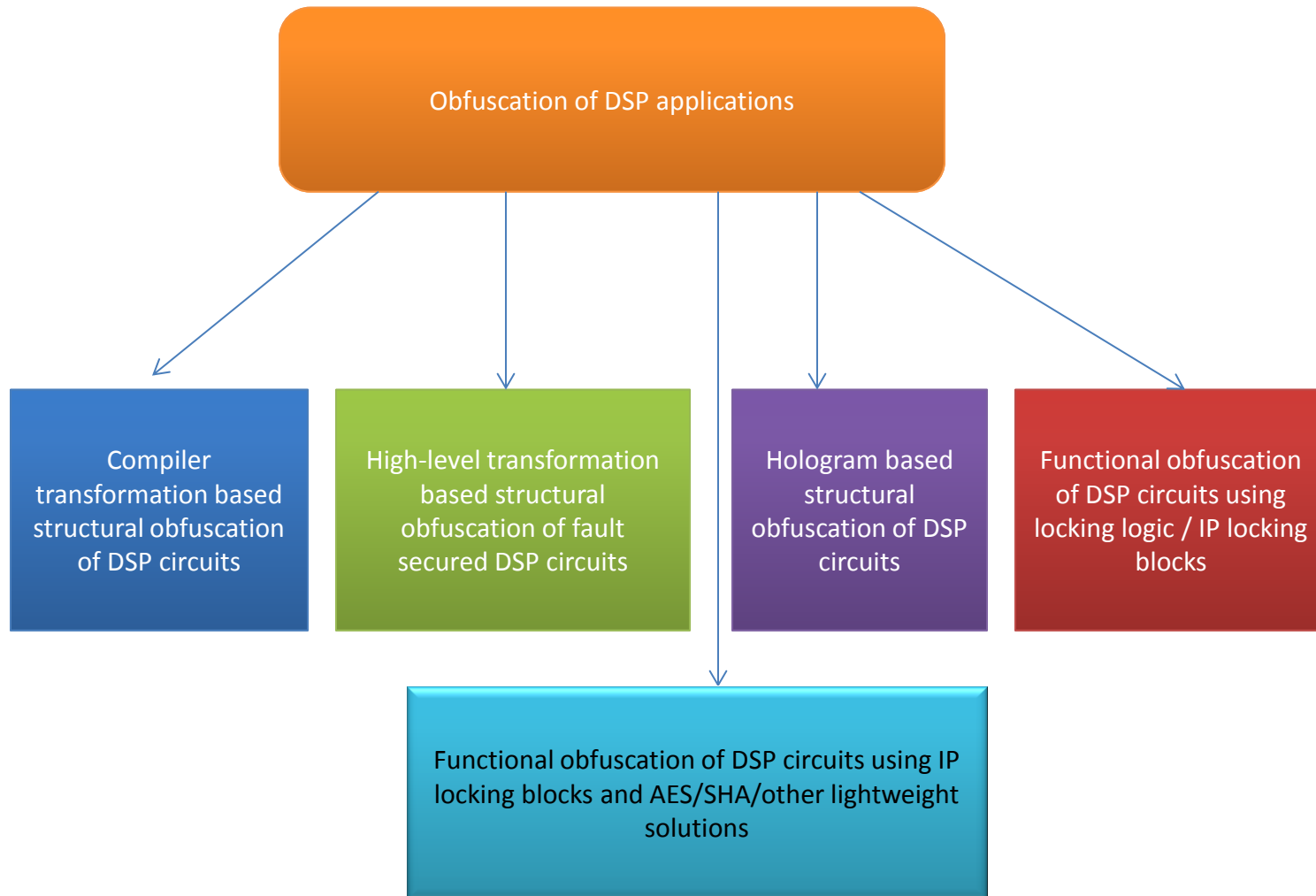
http://www.anirban-sengupta.com/Hardware_Security_Tools.php

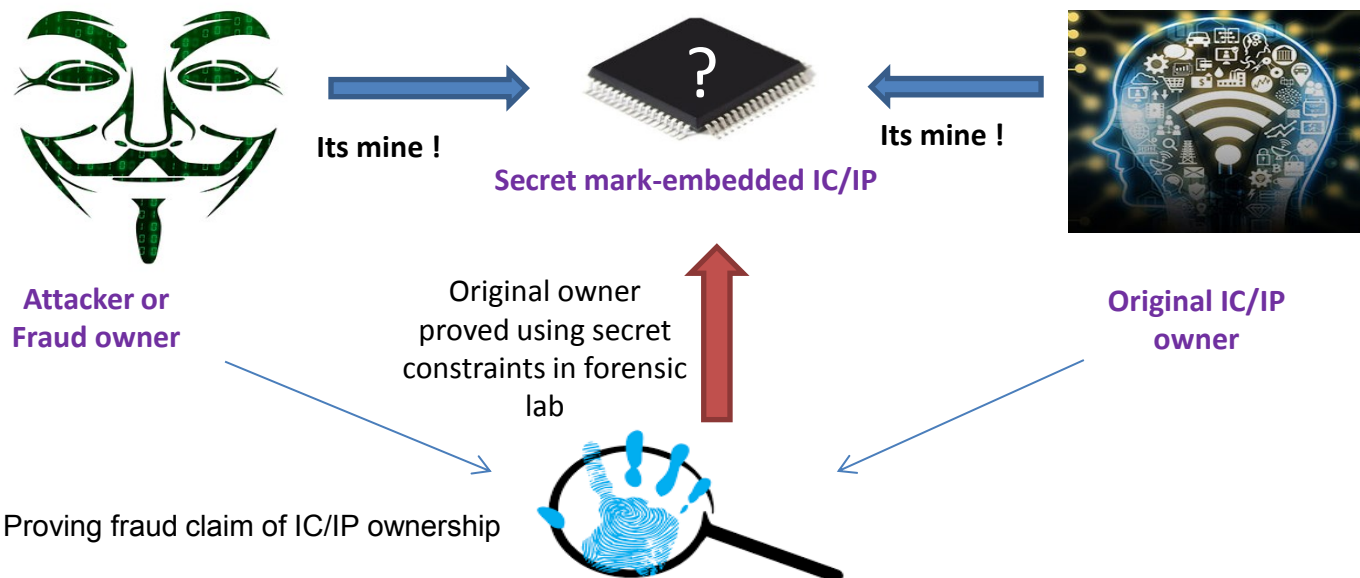
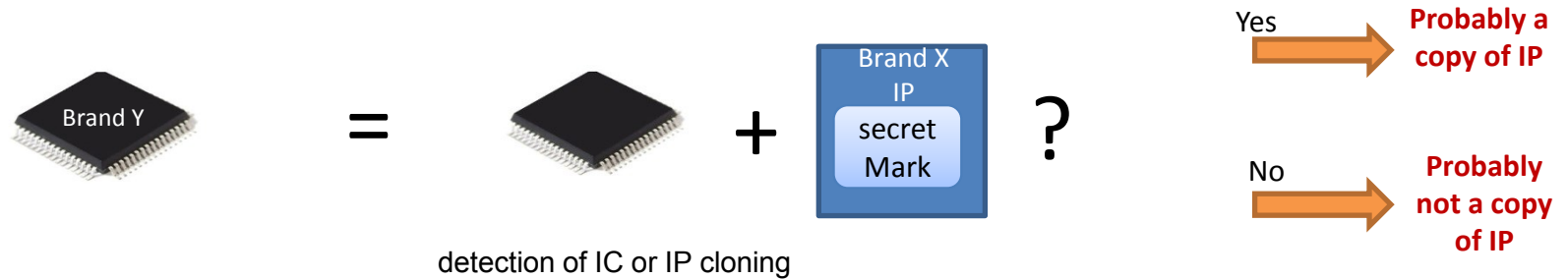
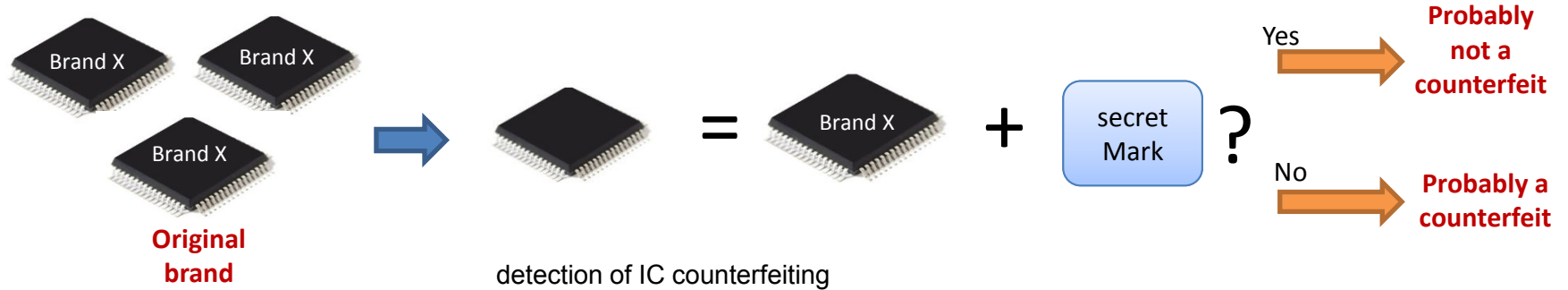


IP Protection of DSP cores – Forensic Detective Control Mechanisms

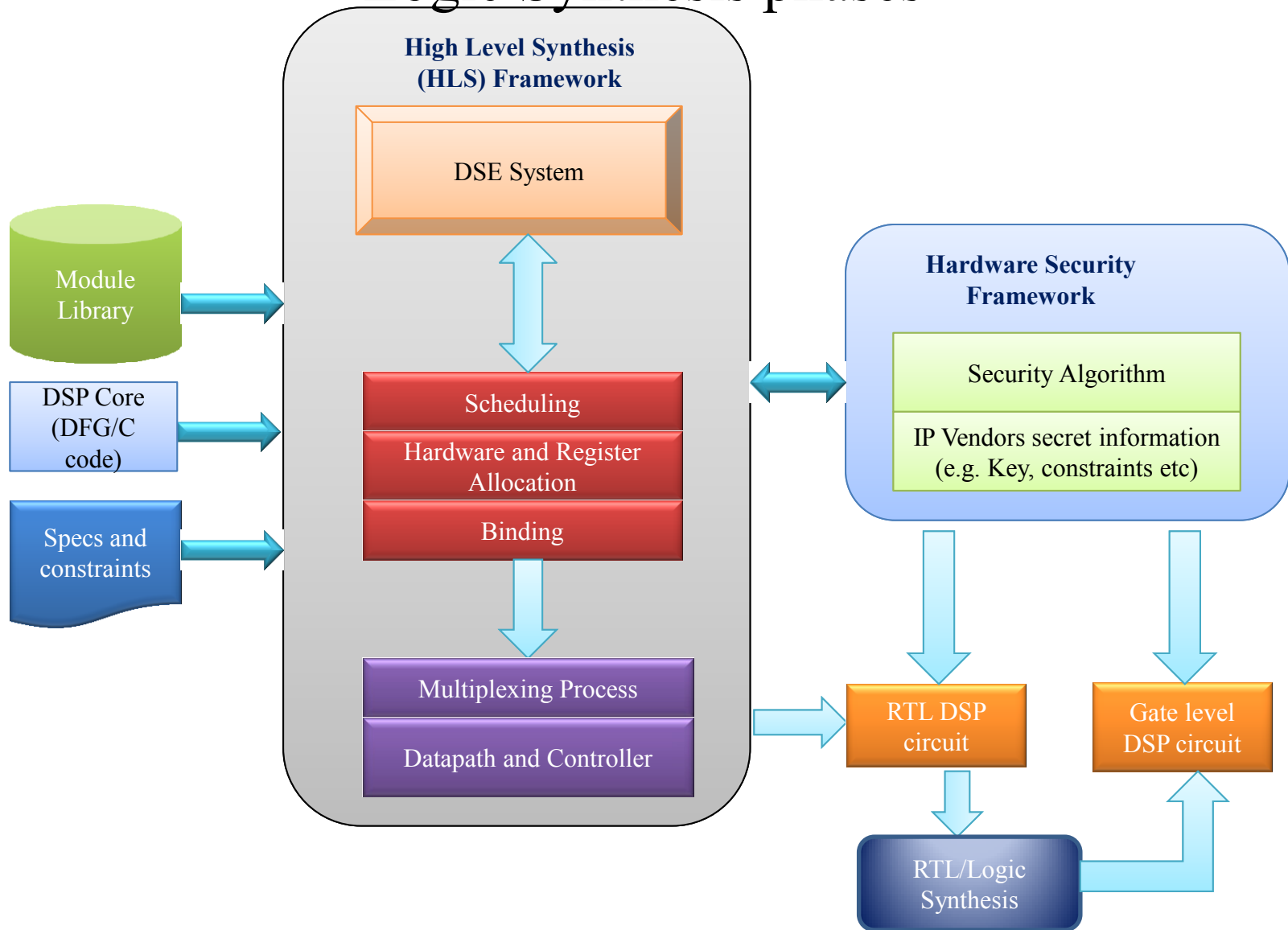


Hardware Security of DSP applications using Obfuscation

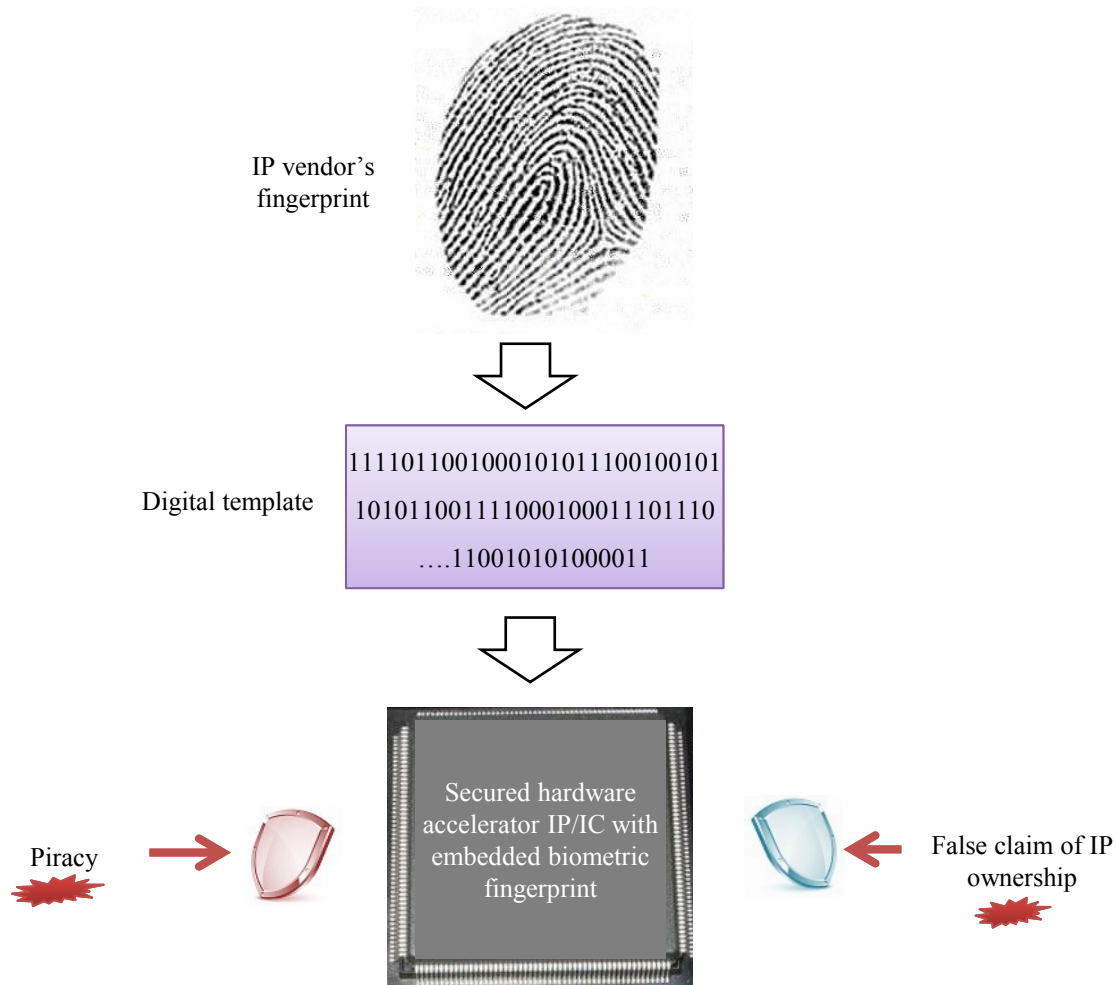




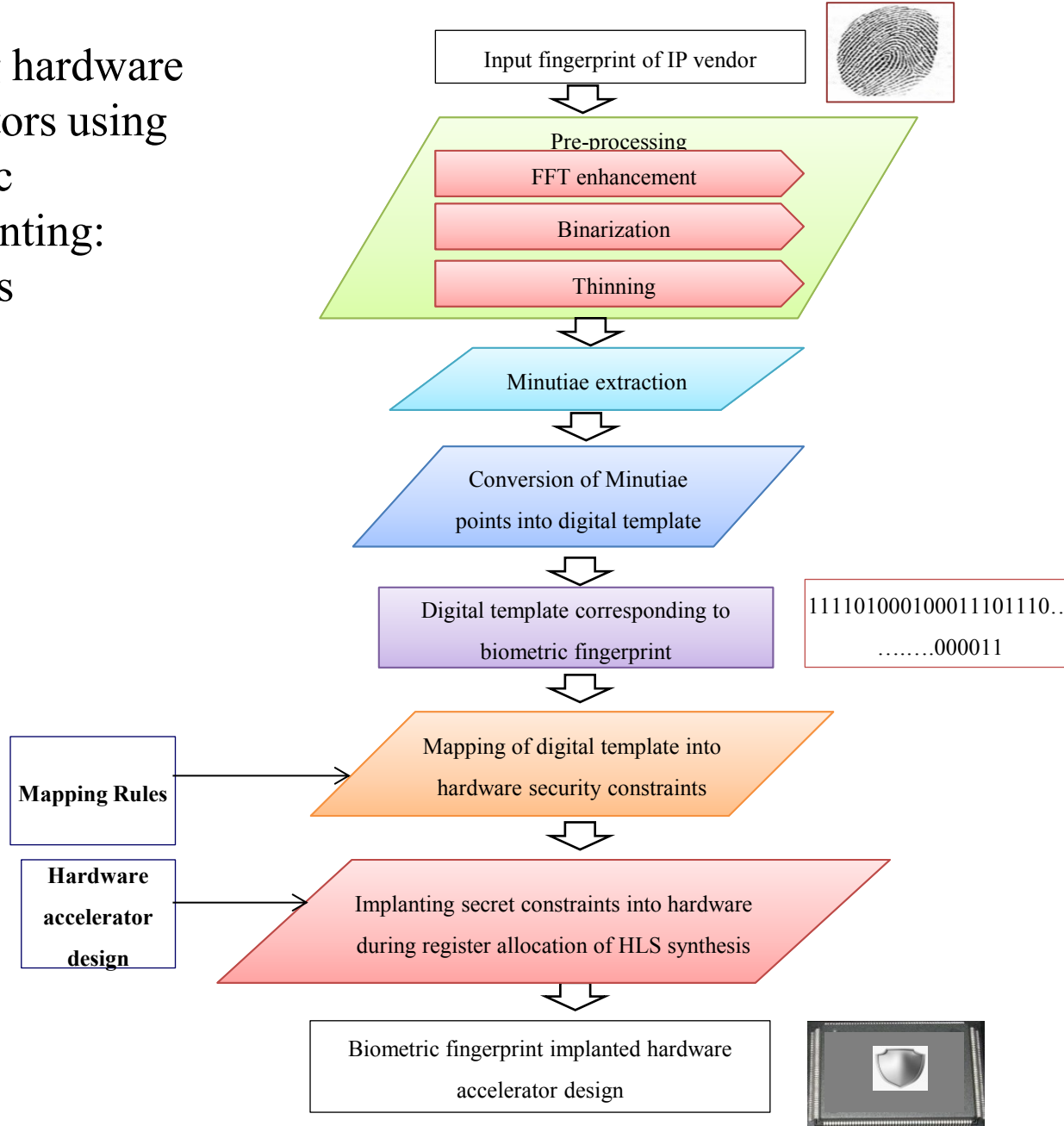
Hardware Security Algorithms integrated with HLS and Logic Synthesis phases

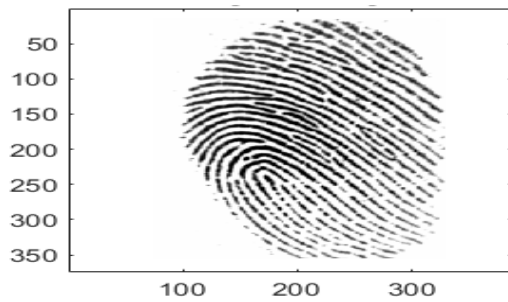


Securing hardware accelerators using biometric fingerprinting: Forensics

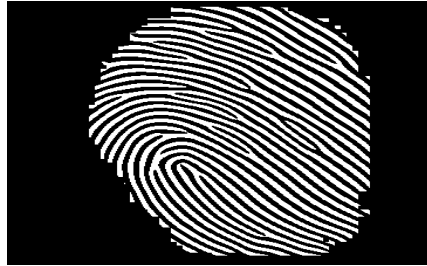


Securing hardware accelerators using biometric fingerprinting: Forensics





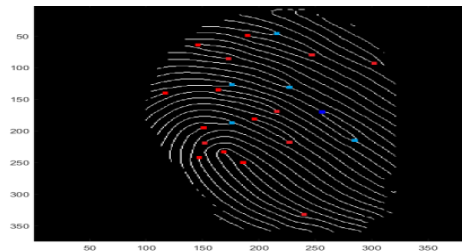
(a) Input fingerprint image (101_1)



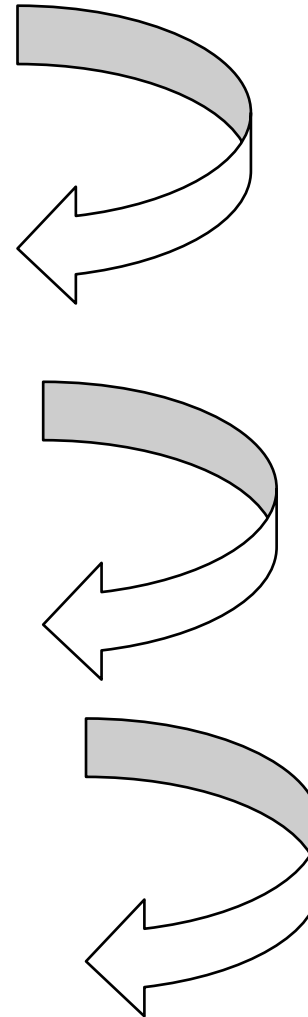
(b) Binary image



(c) Thinned image



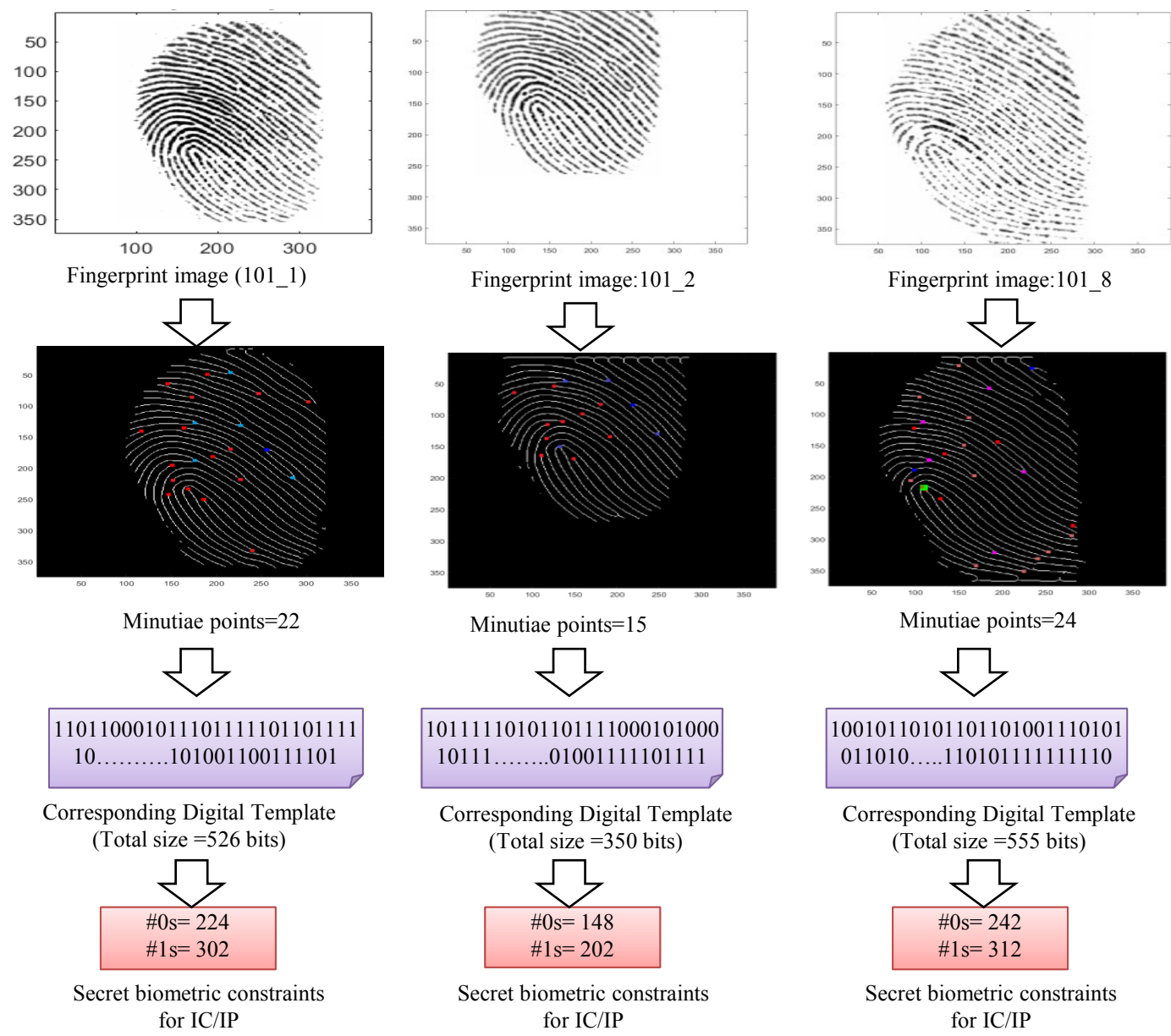
(d) Minutiae points



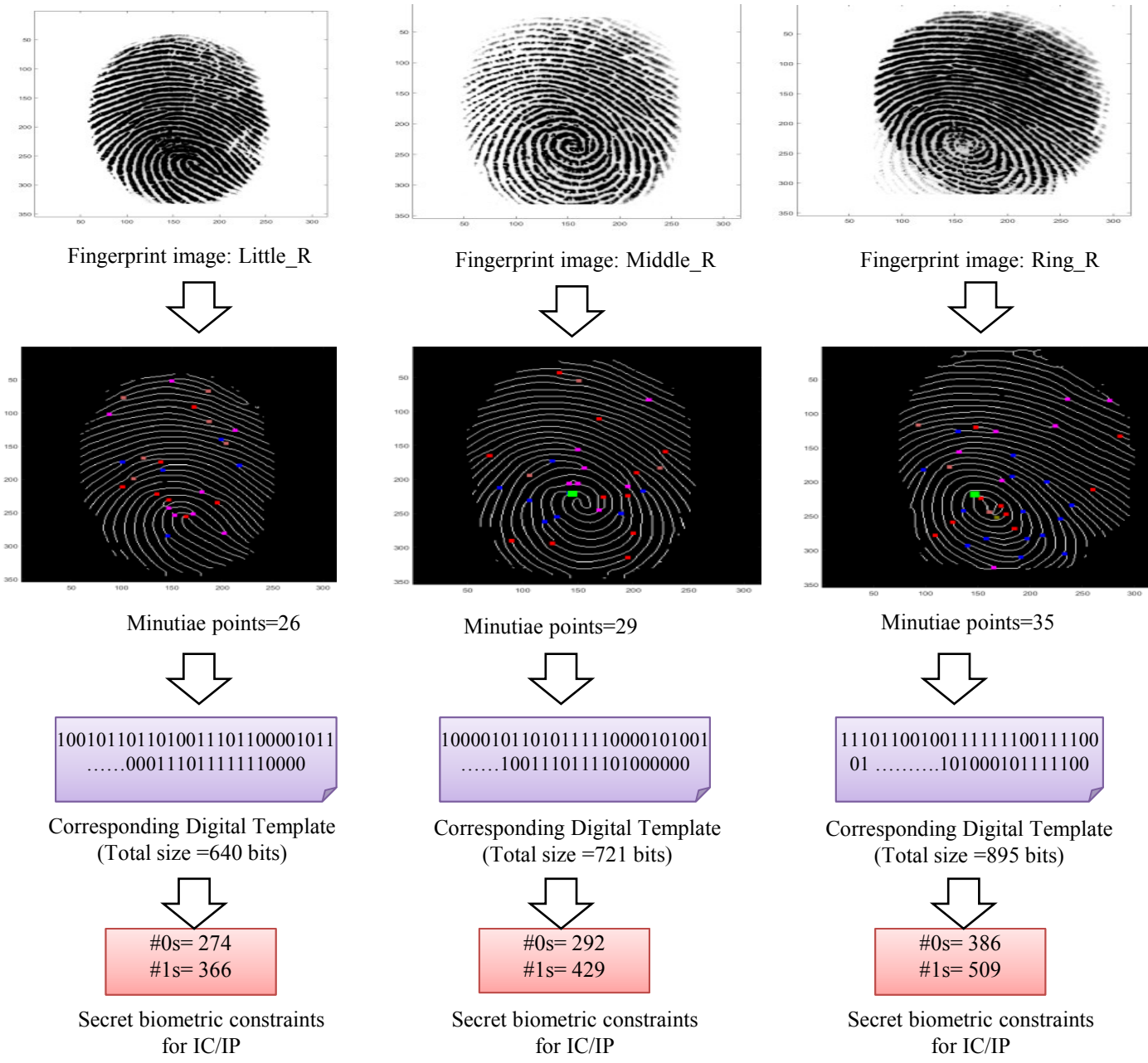
Securing hardware
accelerators using
biometric
fingerprinting:
Forensics: An
example

Minutiae points extraction flow (a) Captured fingerprint image (b) Binary fingerprint image post enhancement (c) Fingerprint image post applying thinning (d) Fingerprint image with minutiae points located

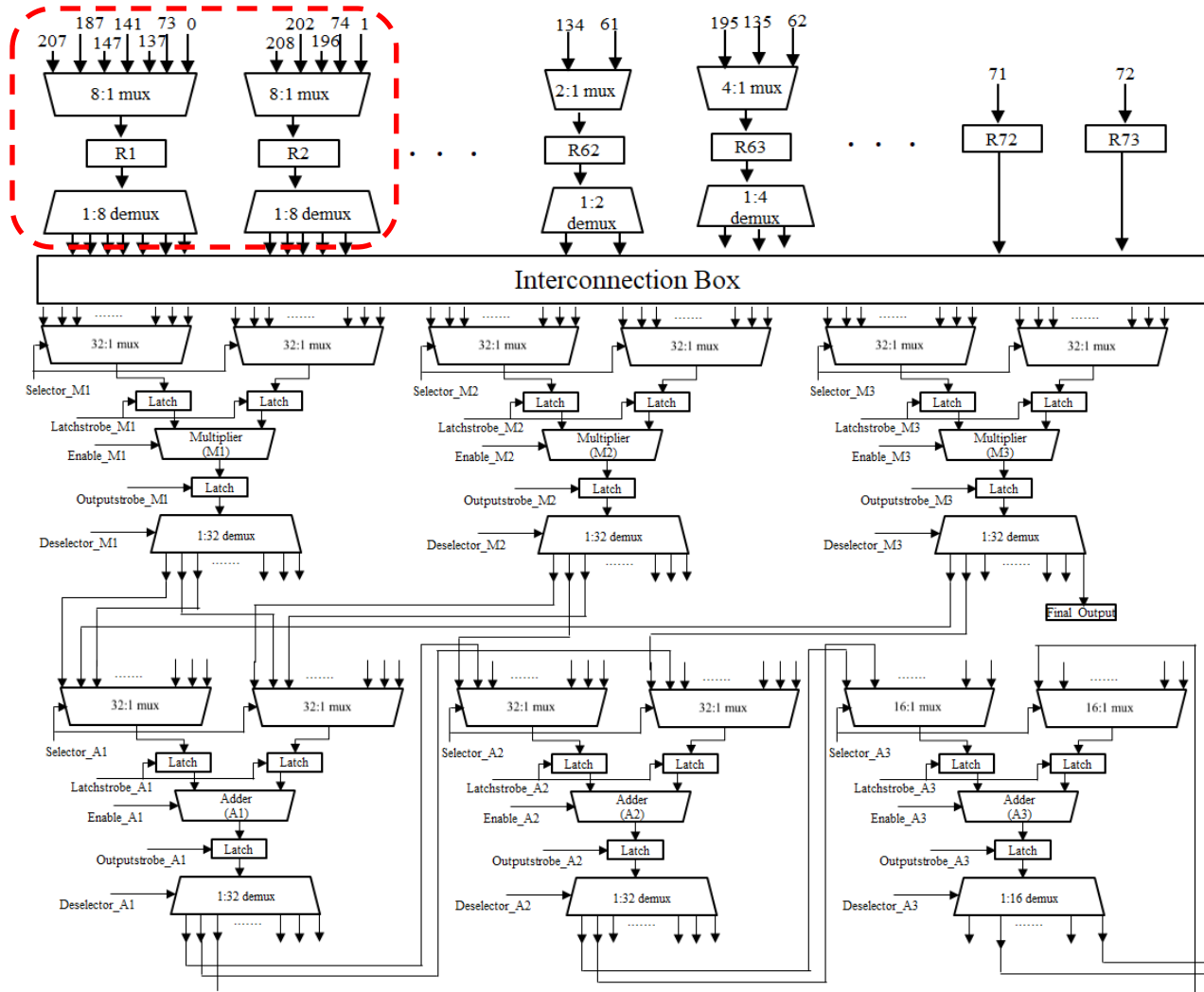
Secret biometric constraints for various fingerprint images



Secret biometric constraints for fingerprints of different fingers of an individual



Secured datapath of JPEG compression hardware accelerator implanted with biometric fingerprint



Detecting Biometric Fingerprint in a hardware accelerator

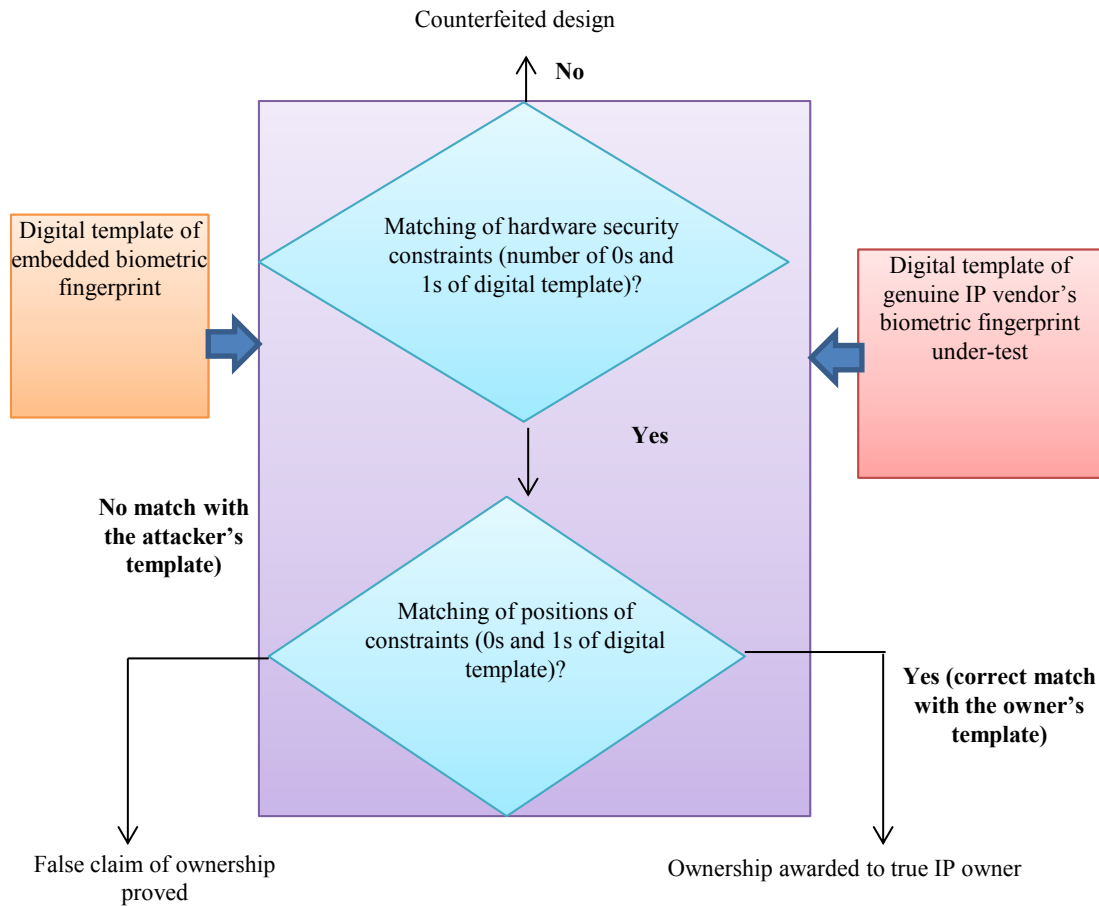
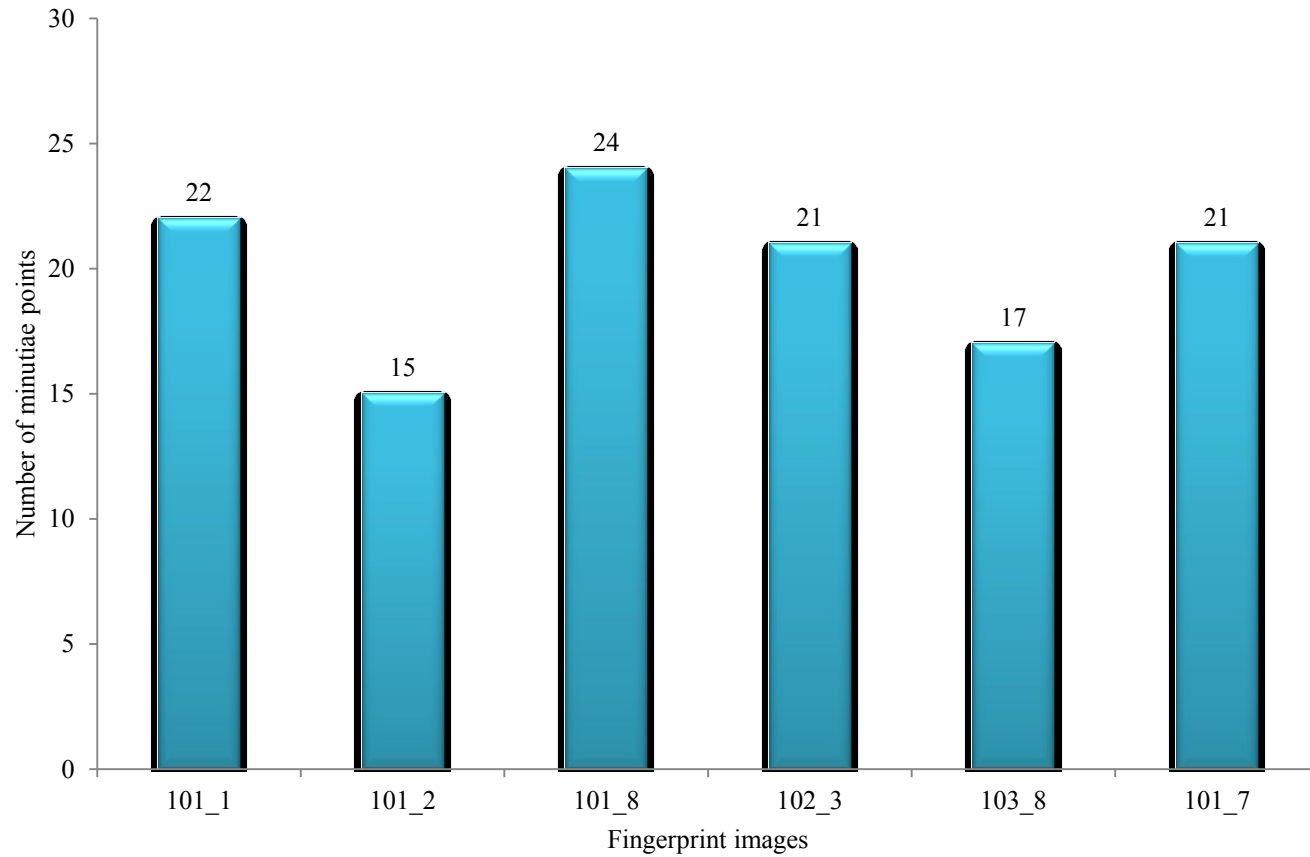
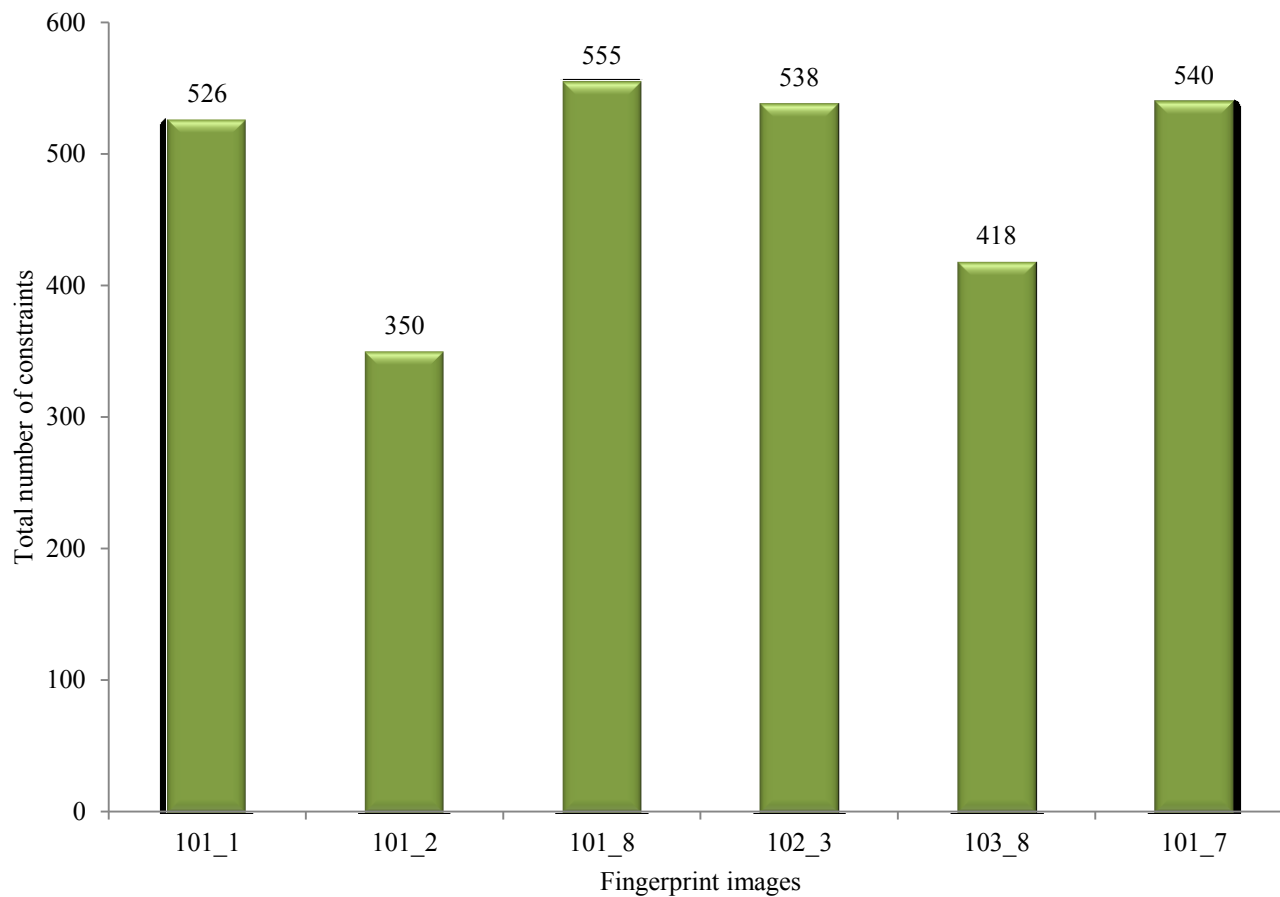


Fig. 9. Proving true IP ownership using proposed detection approach

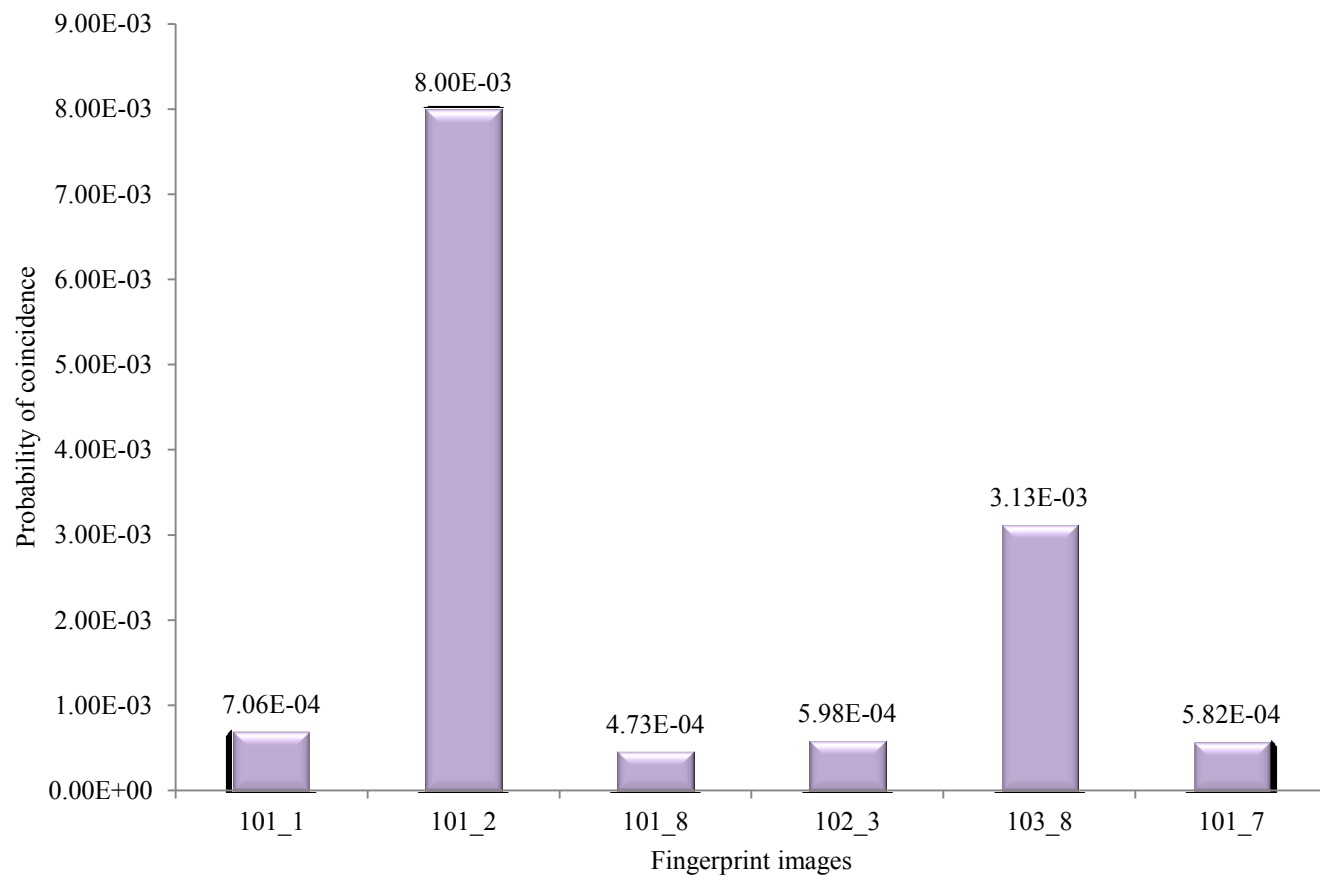
Variation in number of minutiae points for different fingerprint images



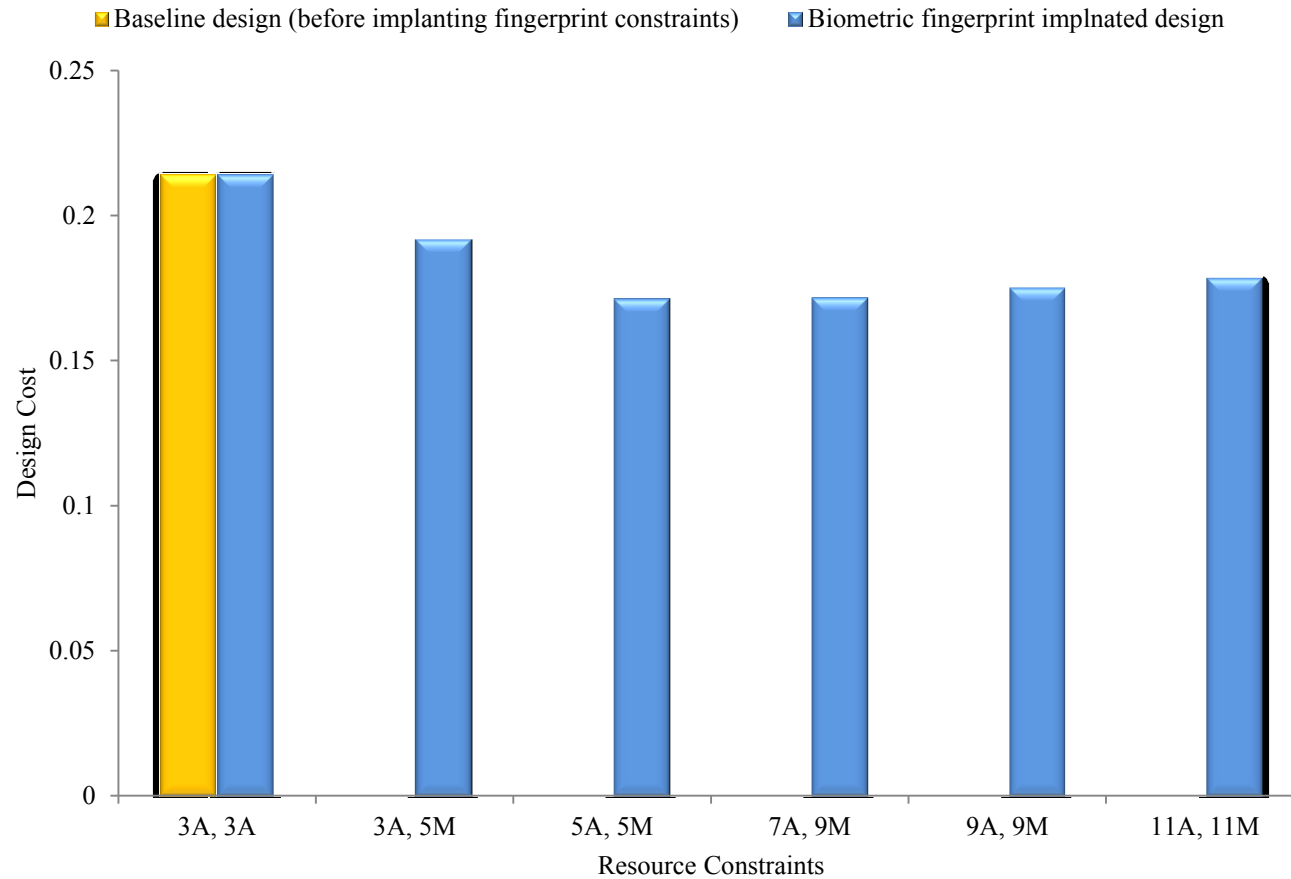
Variation in total number of constraints (k1) for different fingerprint images



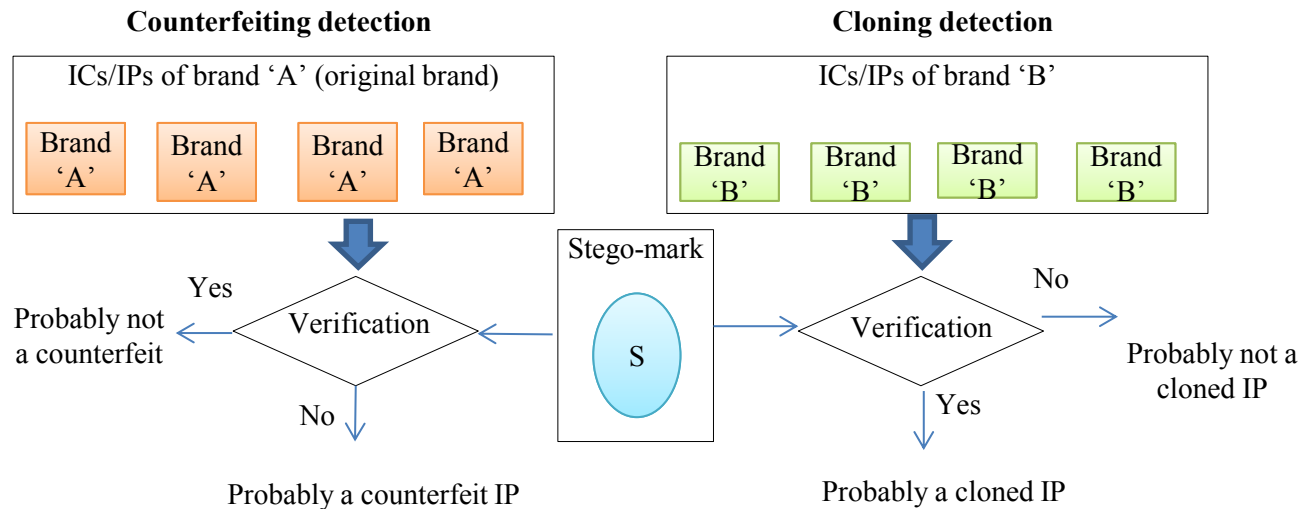
Variation in probability of coincidence for different fingerprint images



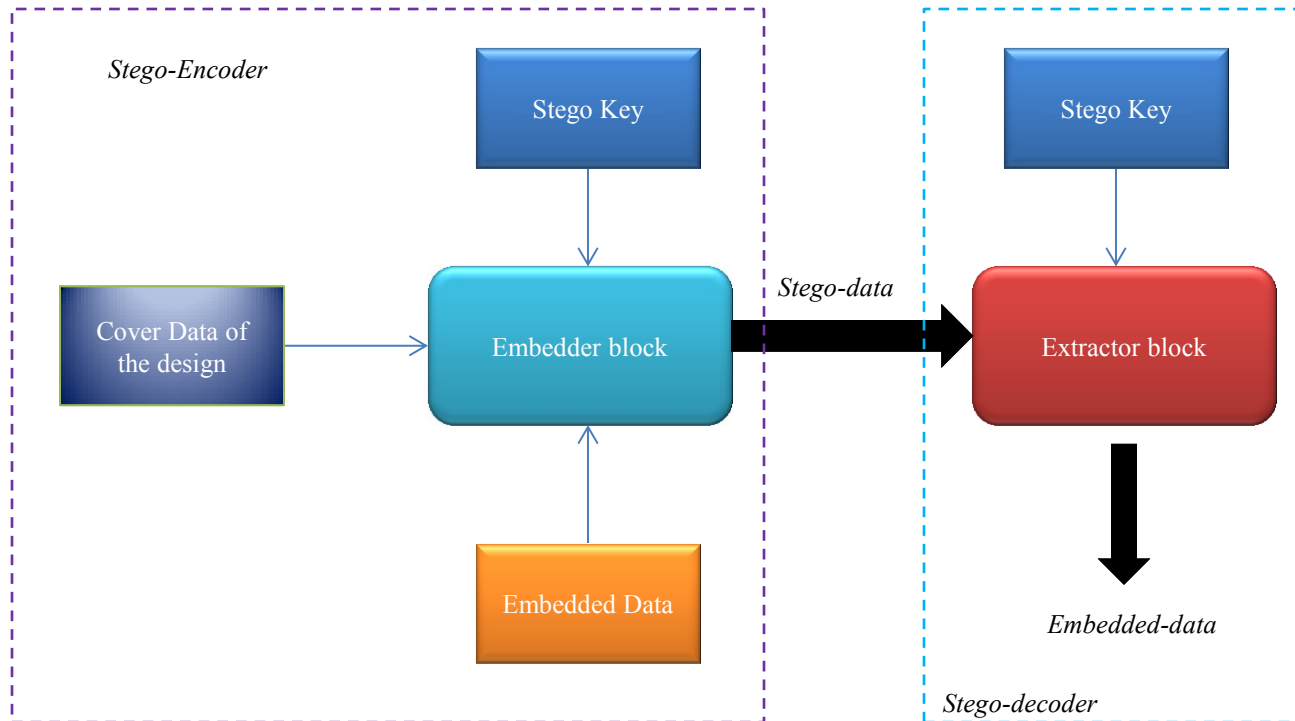
Comparison of design cost of JPEG compression hardware accelerator before and after implanting fingerprint constraints



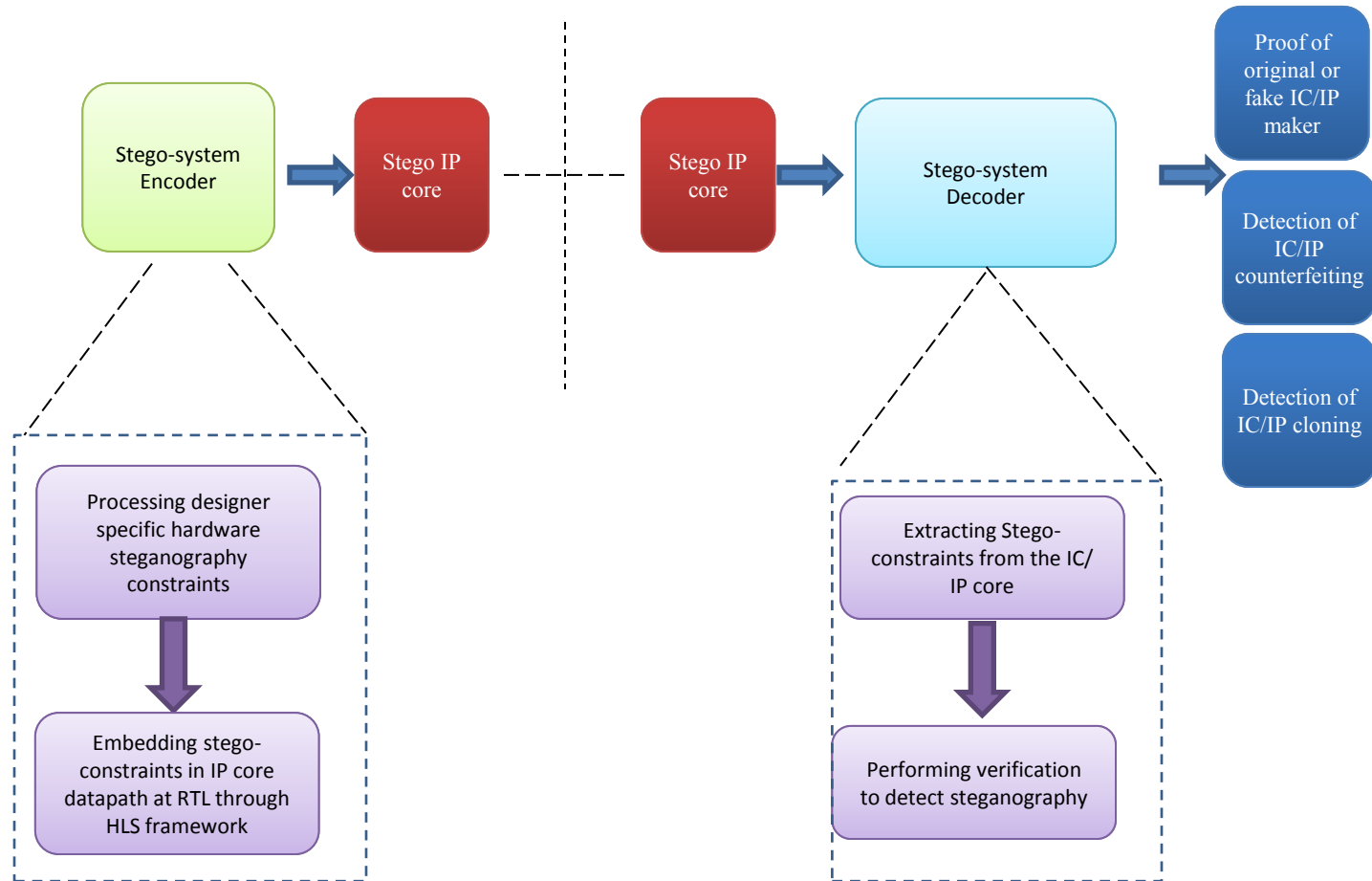
Counterfeiting/cloning detection using proposed steganography



Basic Steganography Model



Hardware Steganography Encoding-Decoding Process



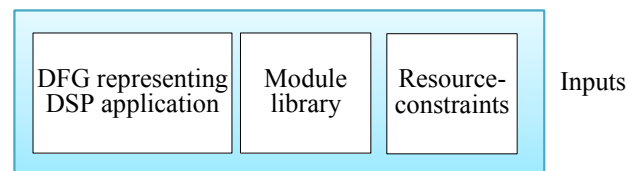
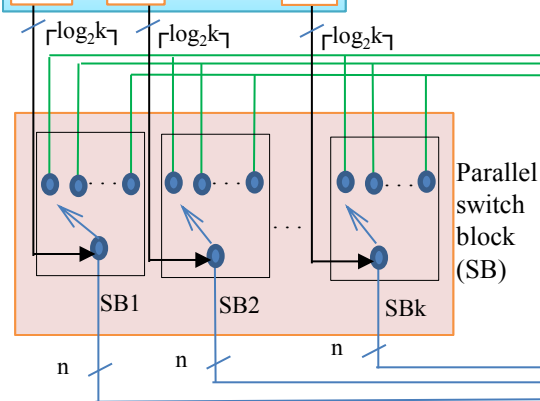
Anirban Sengupta "[Frontiers in Securing IP Cores - Forensic detective control and obfuscation techniques](#)", The Institute of Engineering and Technology (IET), 2020, ISBN-10: 1-83953-031-6, ISBN-13: 978-1-83953-031-9

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

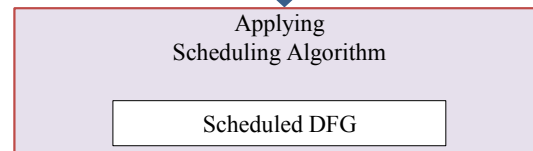
Securing DSP cores using key-triggered hash-chaining based steganography

The length of the bitstream is equal to the number of operations (m) present in the respective DSP application. Further, ' m ' bits of the encoded bitstream is converted into 1024 bits using following preprocessing rule:
(a) m -bit chunk is appended with '1' followed by sequence of '0' bits to generate 896 bits **(b) the 896-bit chunk is appended with 128-bit representation of the length ' m ' of encoded bitstream to obtain 1024 bits.** The 1024 bits are fed to first hash-block of hash-chaining.

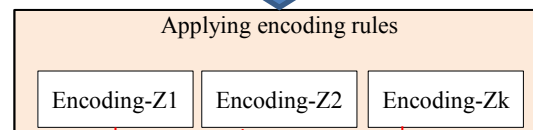
SK-1 SK-2 ... SK- k Stego-key (SK) block



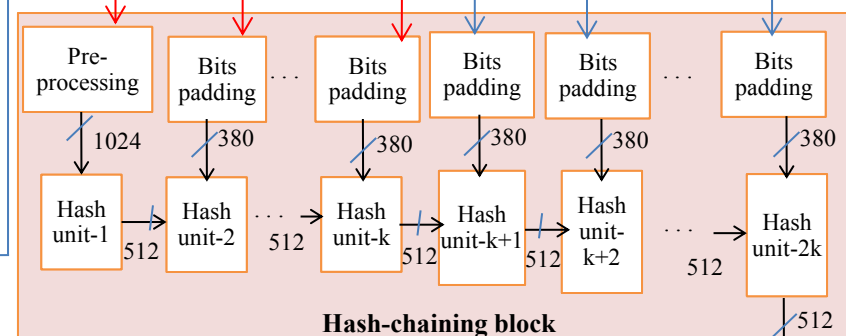
Inputs



HLS block



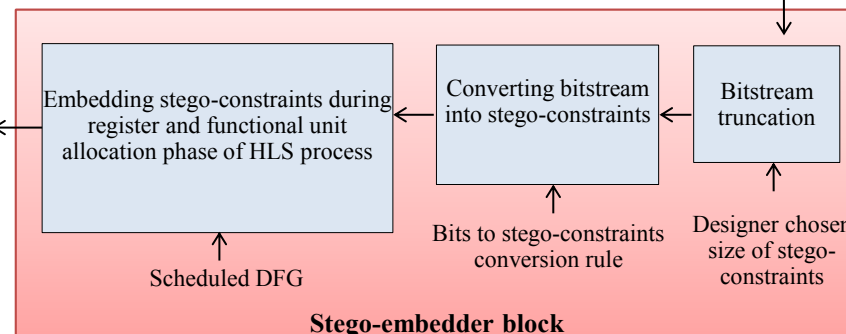
Parallel encoding block



For remaining hash-blocks, 1024-bit input is constructed using following proposed rule:
1024 bit = (512-bit output of previous hash-block) & "1000" & (380-bit output of bits-padding block) & (128-bit representation of the length '512 bits' of previous hash)

Stego-embedded DSP core

Output



Stego-embedder block

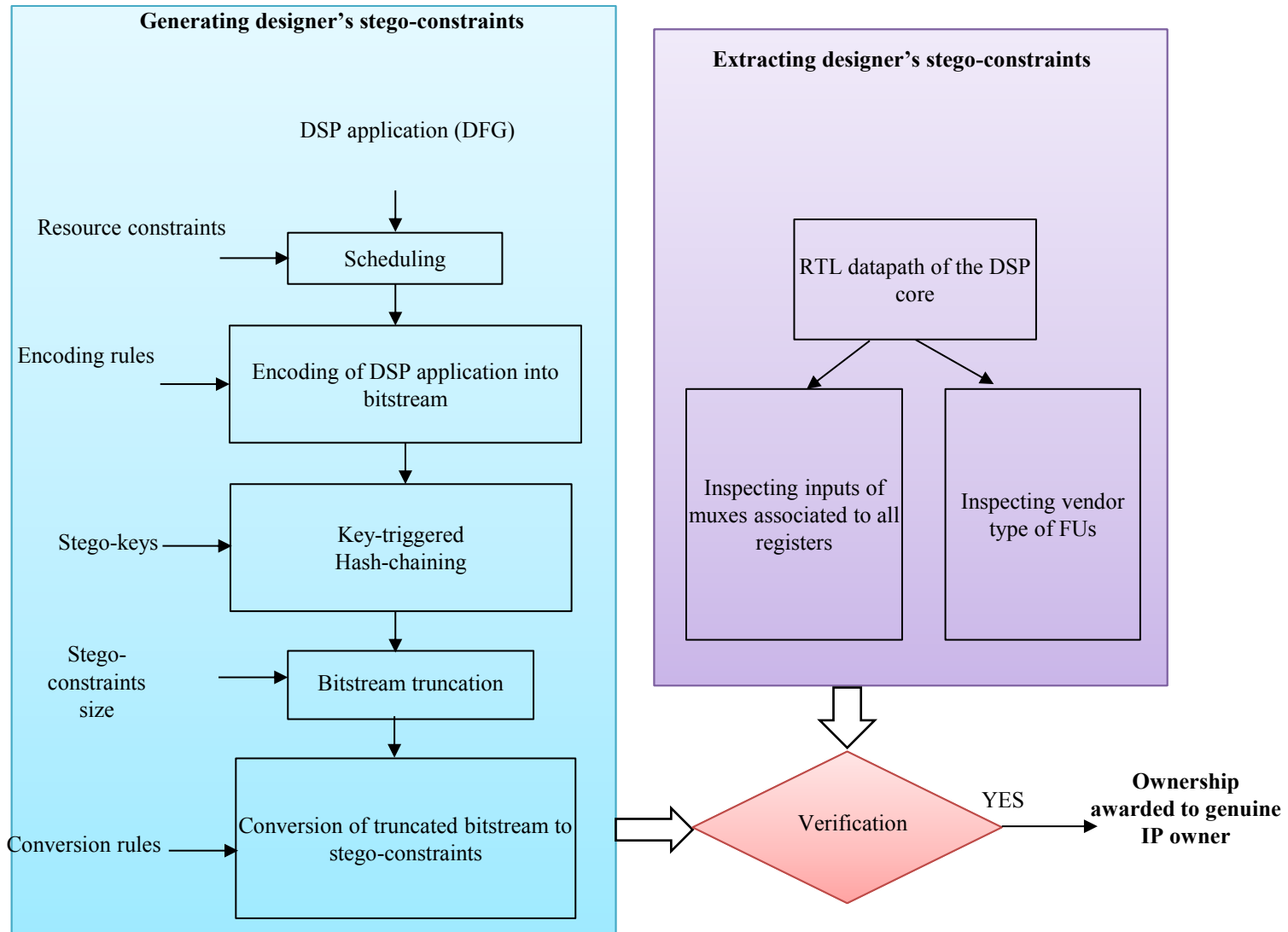
Anirban Sengupta,
 Mahendra Rathor, "IP Core
 Steganography using Switch
 based Key-driven Hash-
 chaining and Encoding for
 Securing DSP kernels used in
 CE Systems", **IEEE
 Transactions on Consumer
 Electronics (TCE)**, 2020

Encoding in steganography

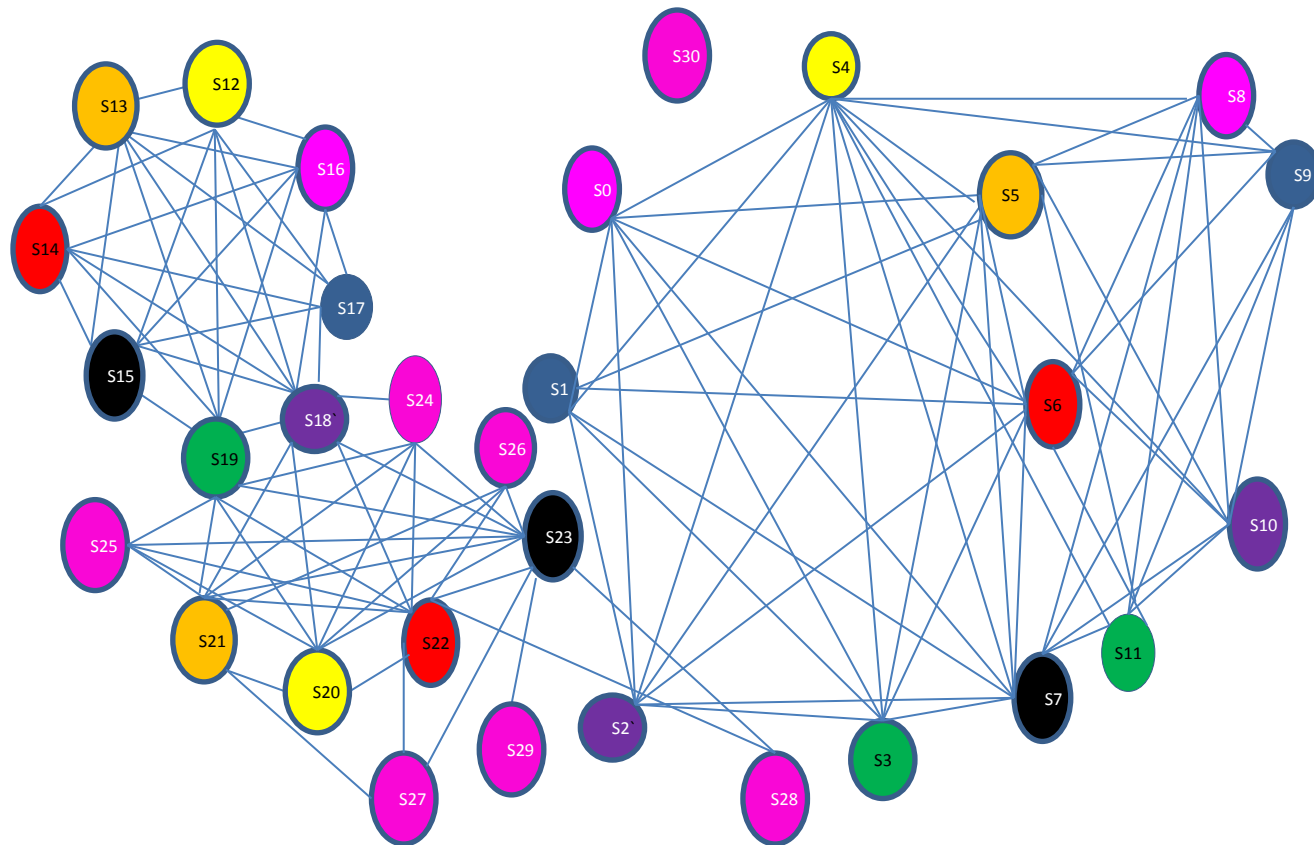
ENCODING RULES TO CONVERT DSP APPLICATION INTO BITSTREAM REPRESENTATIONS

Proposed encoding	Encoding rule (Condition and encoded bit)	
E1	If opn# and corresponding CS # are both even	0
	Otherwise	1
E2	If opn# and corresponding CS# are of same parity (both even or both odd parity)	0
	If opn# and corresponding CS# are of different parity	1
E3	If opn# and corresponding CS # are both odd	0
	Otherwise	1
E4	If opn# and corresponding CS# are of different parity	0
	If opn# and corresponding CS# are of same parity	1
E5	If opn# and corresponding CS# are both prime	0
	Otherwise	1
E6	If opn# and corresponding CS# are both prime	1
	Otherwise	0
E7	If GCD of opn# and corresponding CS# is 1	0
	If GCD of opn# and corresponding CS# is not 1	1
E8	If (opn#) mod (corresponding CS#) is 0	0
	If (opn#) mod (corresponding CS#) is not 0	1
E9	If CS# is equal to 2 nd odd sequence of opn#	0
	Otherwise	1

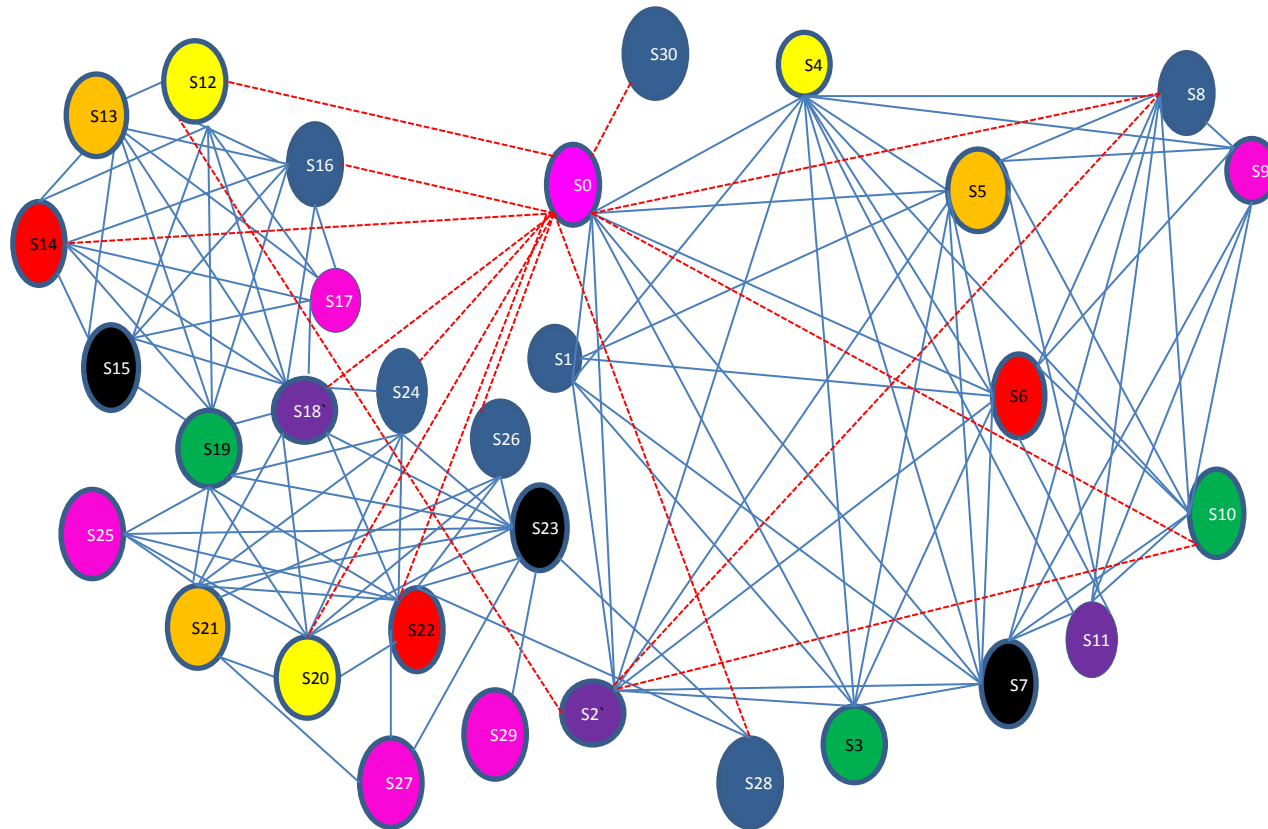
Detection process of steganography



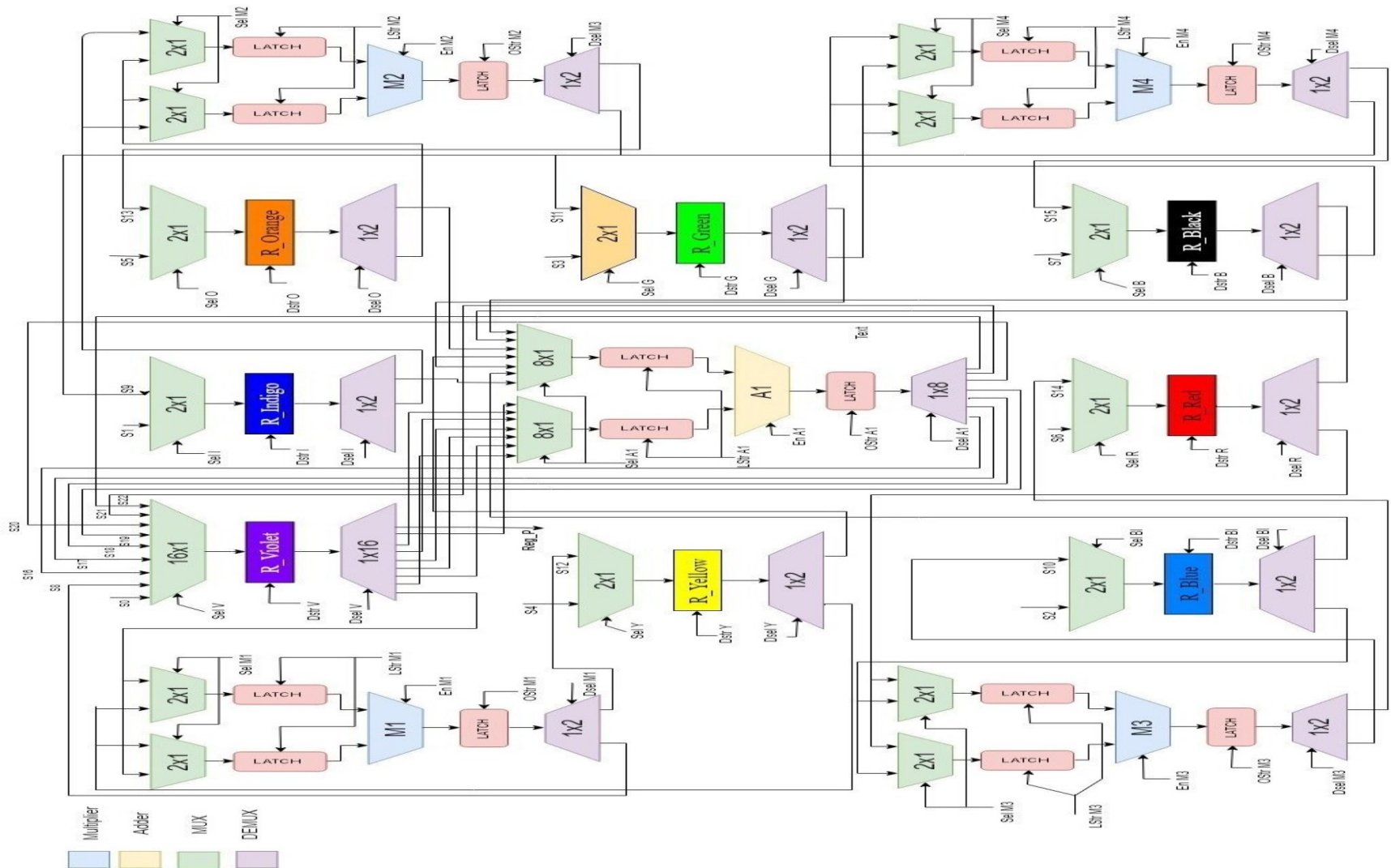
CIG of FIR filter hardware accelerator (IP core) before steganography



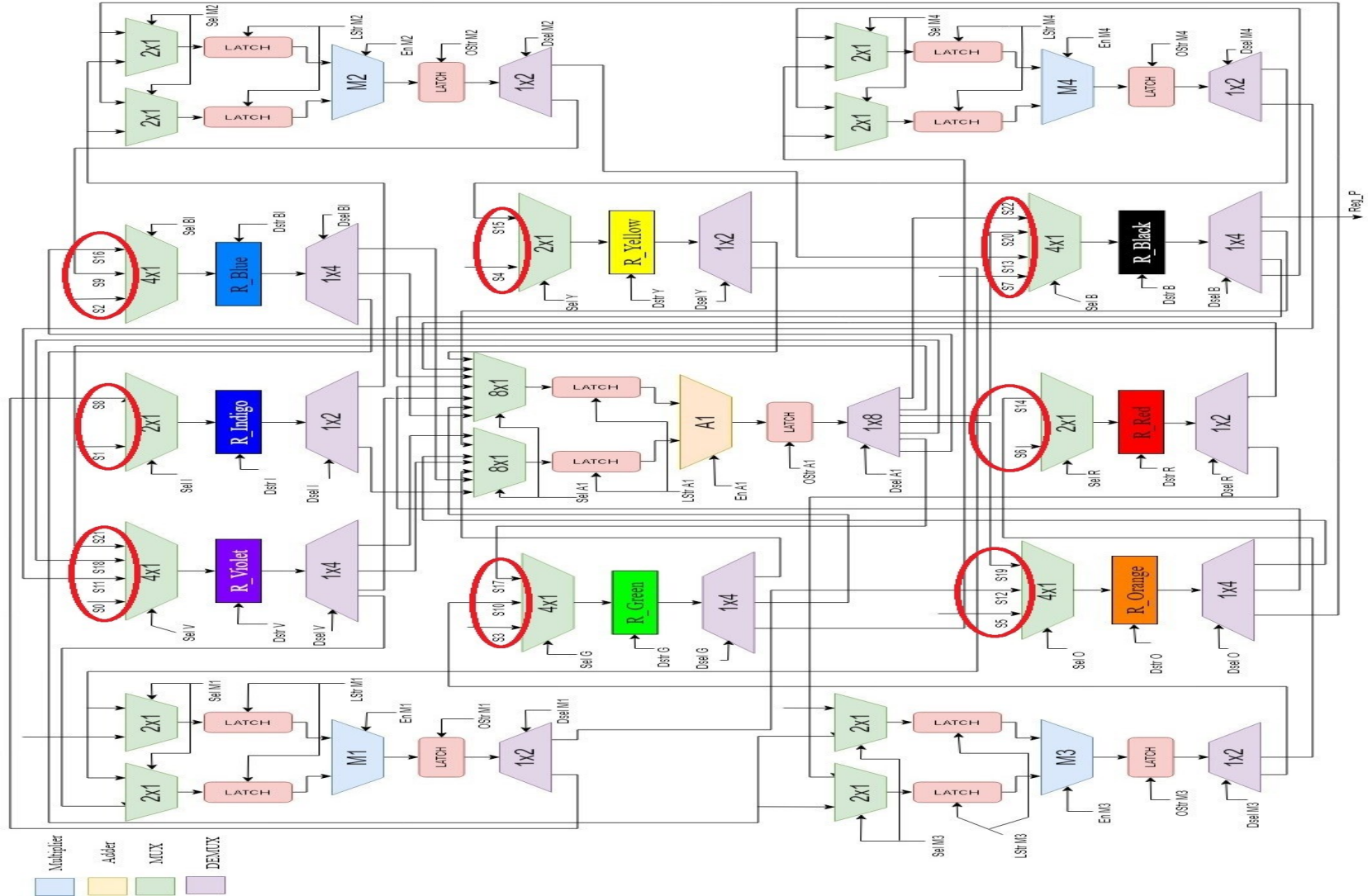
CIG of FIR filter hardware accelerator (IP core) after steganography



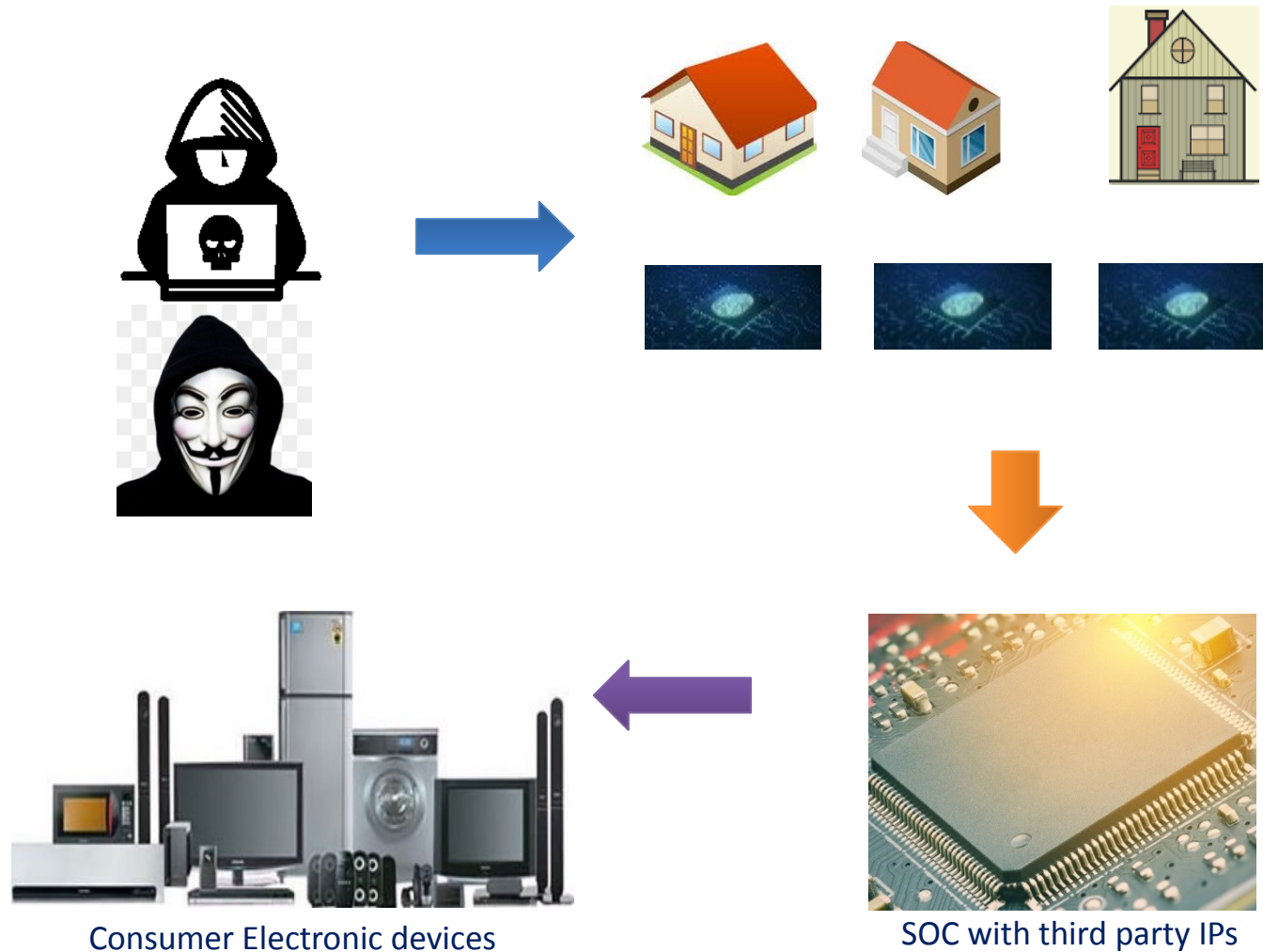
RTL datapath of 8-point DCT before



RTL datapath of 8-point DCT after Steganography



IP core protection using Digital Signature



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

IP core protection using Digital Signature

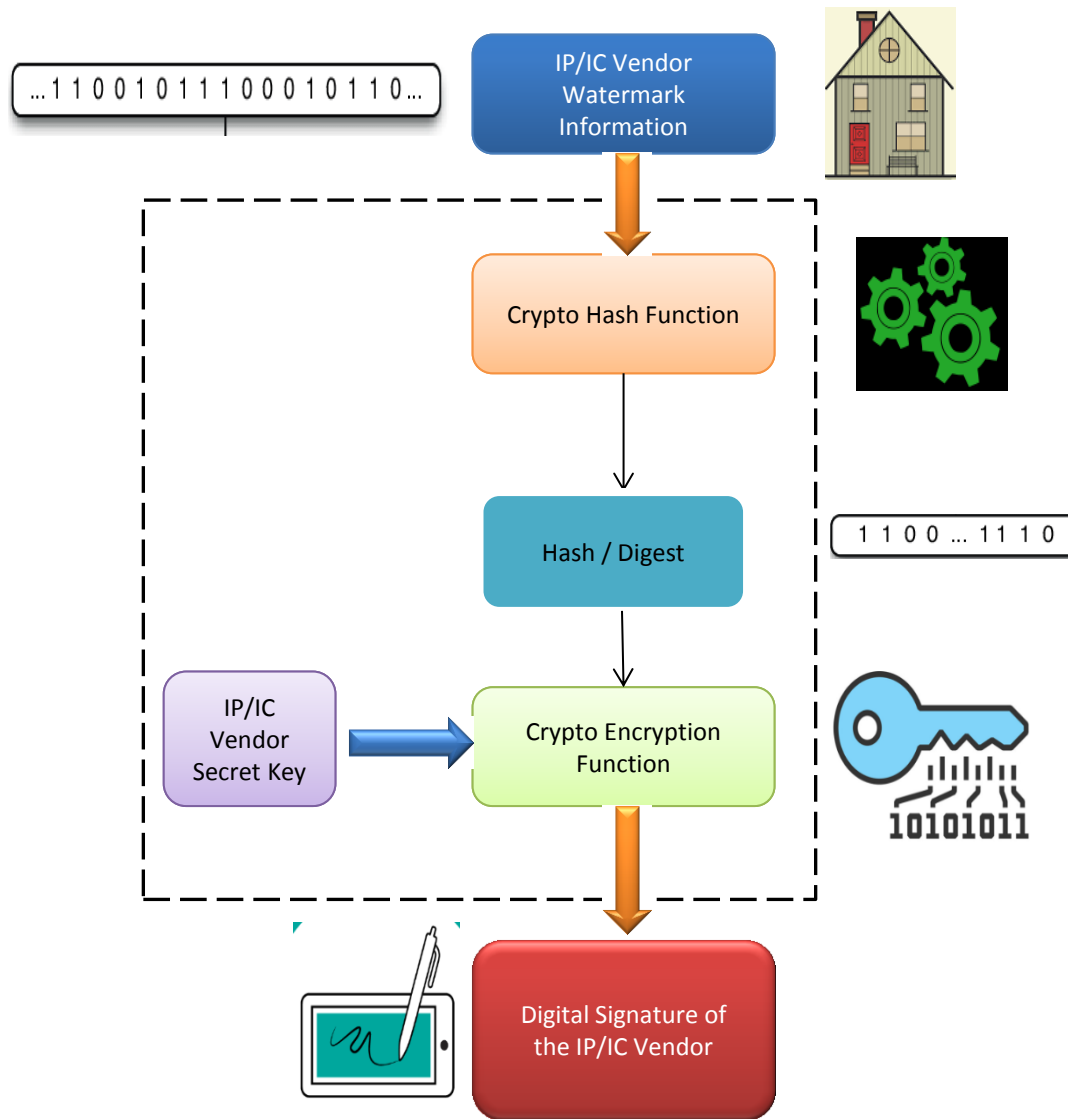
➤ **A novel crypto digital signature approach is presented which incorporates following security modules**

- Crypto hash function- SHA-512
- Crypto encryption function- RSA
- Encoding

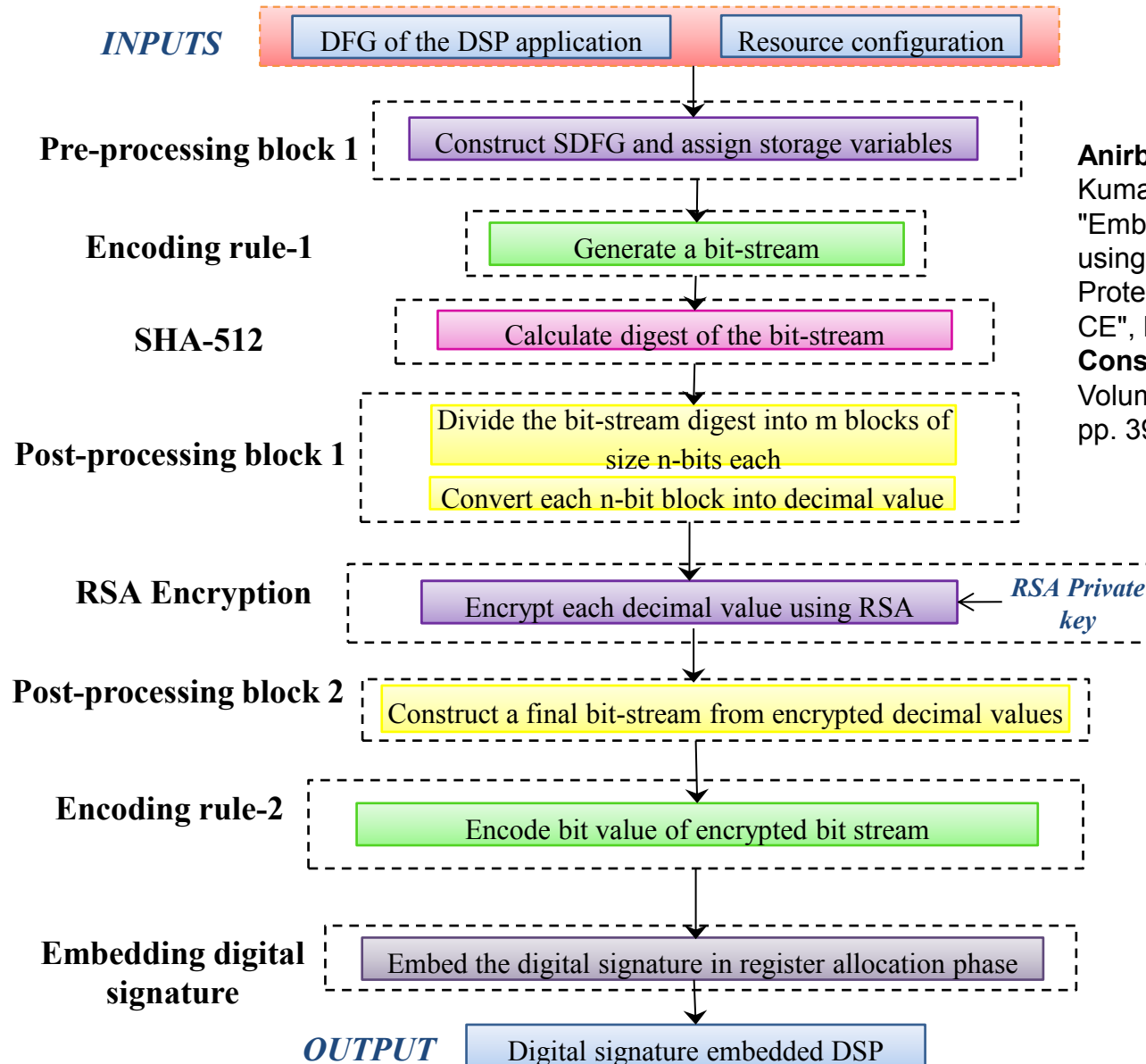
➤ **The generic steps of generating digital signature:**

- Generate a Bit-stream representation of DSP Core.
- Performing SHA-512
- Post-processing Step1
- RSA Encryption
- Post-processing Step 2

High-level process of creating digital signature for IP cores



Flow of the approach



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

Performing SHA-512 and Post Processing-1

➤ Performing SHA-512

- Generates decimal digest of DSP core
- The collision resistance and deterministic properties of SHA-512 ensures that the generated hash digest carrying vendor secret mark is unique for an IP core design.

➤ Post-Processing-1

- Divide the bitstream digest into m blocks of size n bits each
- Convert each n-bit block into decimal value

RSA Encryption

- RSA is an asymmetric key encryption algorithm in which two distinct keys (private key and public key) are involved in the cryptography.
- It is used to sign the hash digest of vendor secret mark information to ensure authentication of the genuine owner.

Inputs (128 bits) and outputs of RSA module

RSA Decimal Input	Encrypted Decimal Output	Encrypted Binary Equivalent
328629211327023509667307560 016780722176	259269232367594955022606516 388222677830	110000110000110.....011001 101000110
338967726051337675217876235 804913696768	103304422214721939828321919 365106451481	100110110110111.....100010 000011001
745080717249504132969595196 03599240546	246822478630224319655120426 30223003075	100101001000110.....111110 111000011
140476292891867587341382251 85020455483	289411796889479622387067677 582110256178	110110011011101.....110110 000110010

Post-processing Block 2

- The encrypted decimal values— output of RSA module— are provided as input to the post-processing block 2.
- Each decimal value is converted to binary and these individual binary streams are concatenated to form a single bit-stream.
- This encrypted-hashed bit-stream is referred to as **Digital Signature**. The digital signature size can be selected based on vendor's choice from the continuous bit-stream.
- For instance, if the vendor selects digital signature size as 15, then the first 15 bits of the bit-stream is the digital signature.

Embedding Digital Signature

Having created the digital signature, the next step is to embed it in the design. The steps to implant the digital signature are stated below:

- **Mapping the digital signature bits to watermarking constraints**

- Using the following encoding rule:
 - If bit = '0', then additional edge is added between node pair (prime, prime) in a colored interval graph.
 - If bit = '1', then additional edge is added between node pair (even, even) in a colored interval graph.

- **Embedding the watermarking constraints.**

- Watermark constraints are embedded in register allocation step during HLS (And it is performed through colored interval graph framework).
- These hidden constraints act as additional constraints to be imposed besides the regular design constraints of the design

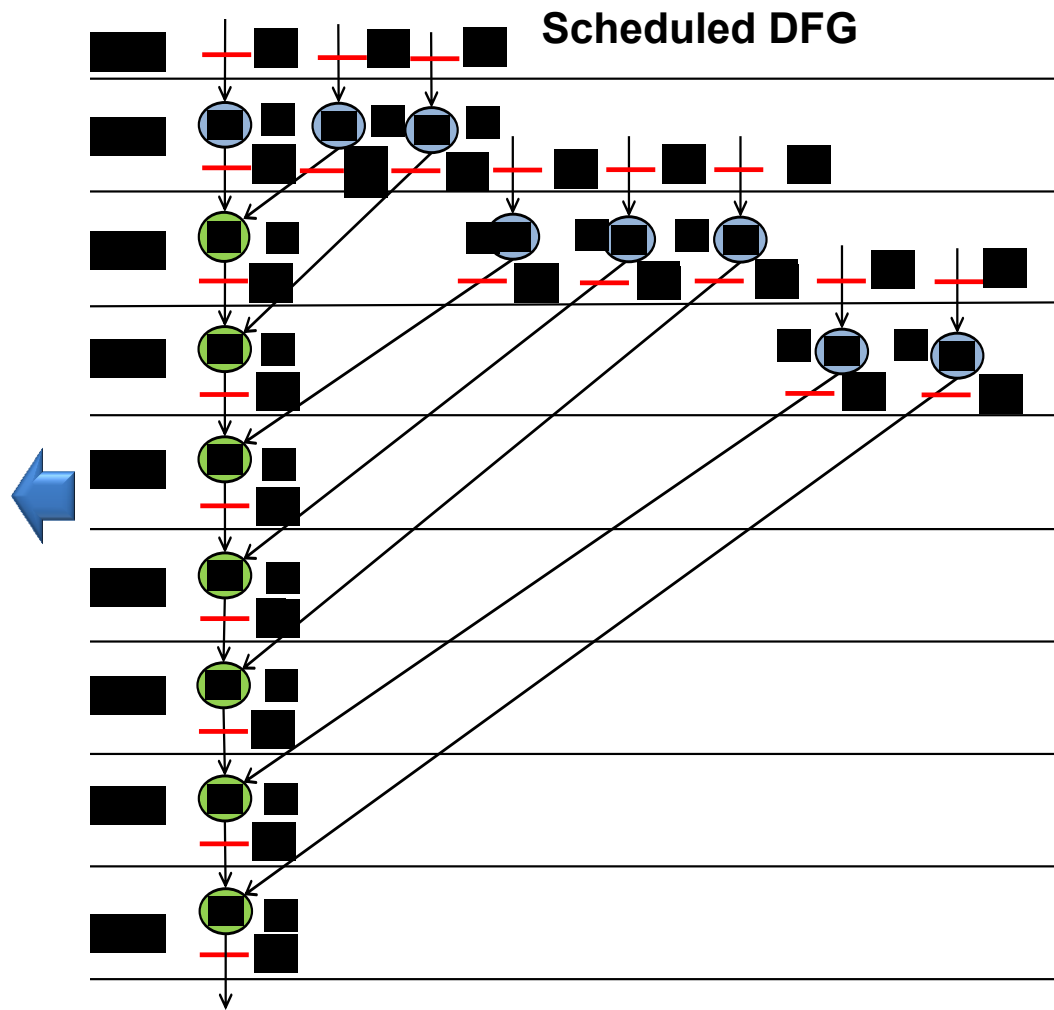
Bit stream Generation

➤ Based on encoding rule-1

Operation number (OPN)	Corresponding control step (CS) number	Encoded bit
Even	Even	0
Odd	Even	1
Even	Odd	1
Odd	Odd	0

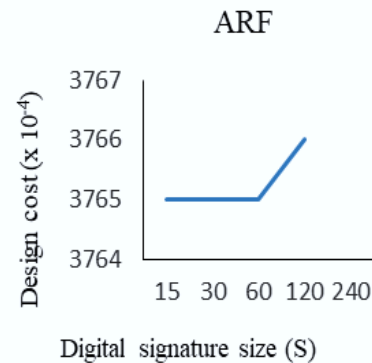
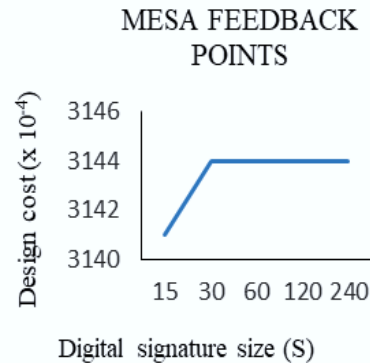
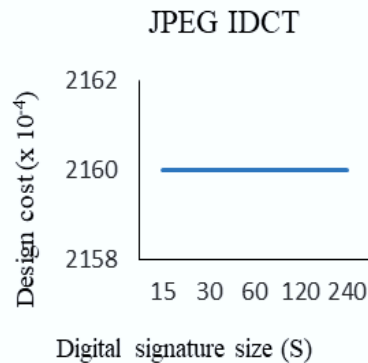
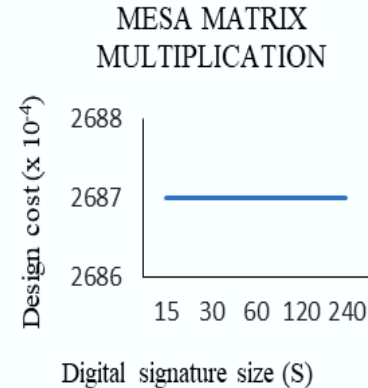
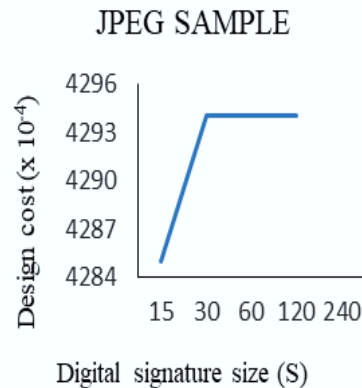
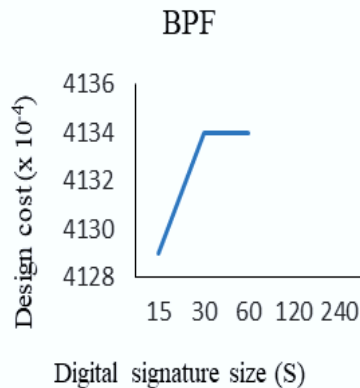
Generating the Bit-stream of DCT Core

Operation Number	Control Step Number	Bit generated
1	1	0
2	1	1
3	2	1
4	1	1
5	3	0
6	2	0
7	4	1
8	2	0
9	5	0
10	2	0
11	6	1
12	3	1
13	7	0
14	3	1
15	8	1



Experimental Results

➤ Graphical Representation of Design Cost for different benchmarks



Design cost

$$C_f(X_i) = \phi_1 \frac{L_T}{L_{max}} + \phi_2 \frac{A_T}{A_{max}}$$

L_T = design latency

A_T = hardware area

L_{max} = maximum execution latency

A_{max} = maximum hardware area.

ϕ_1, ϕ_2 represent the user specified weights both fixed at 0.5 to assign equal preference

Experimental Results

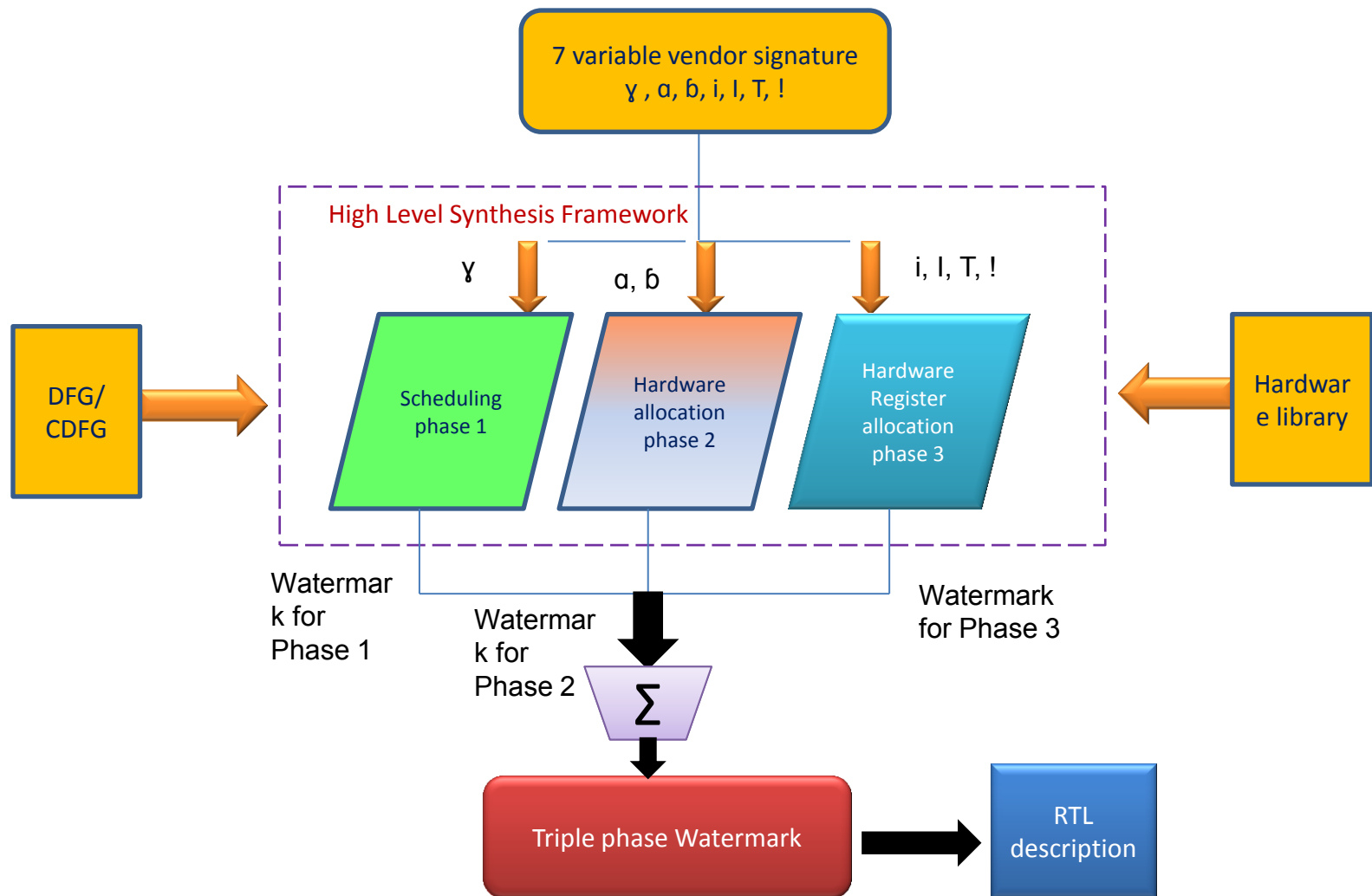
➤ Evaluation of Robustness Using Probability of Coincidence (P_c)

$$P_c = \left(1 - \frac{1}{c}\right)^S$$

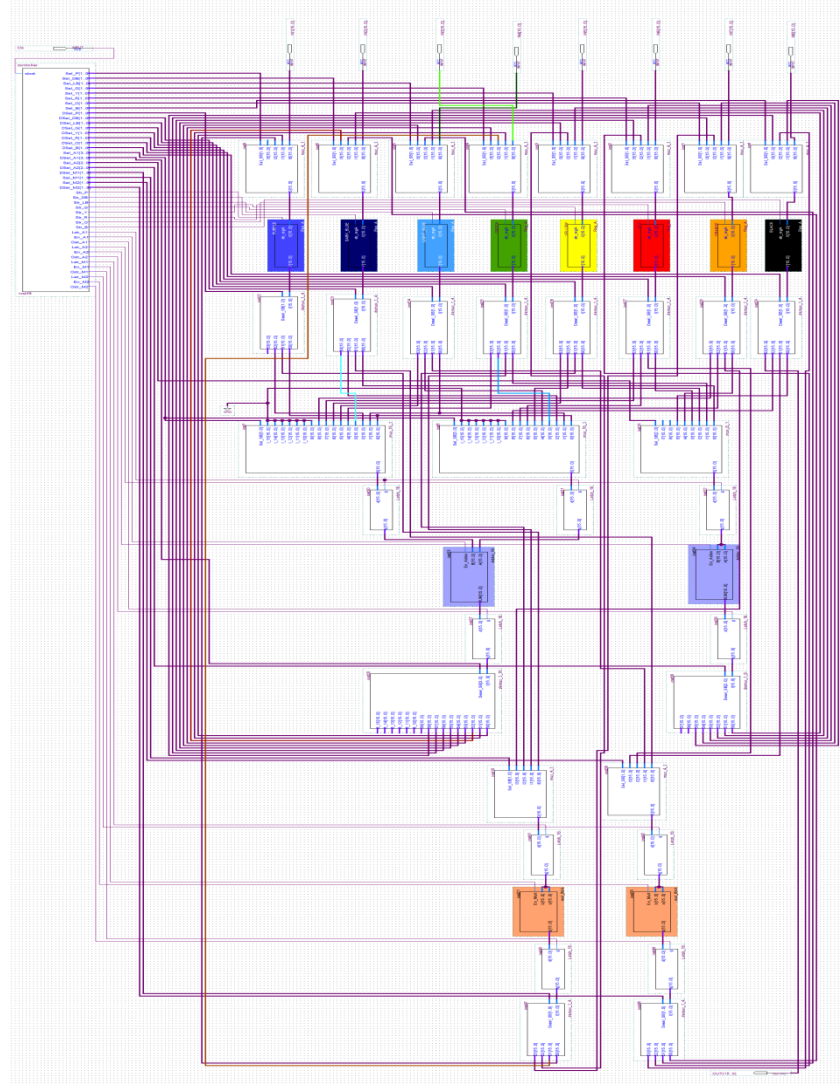
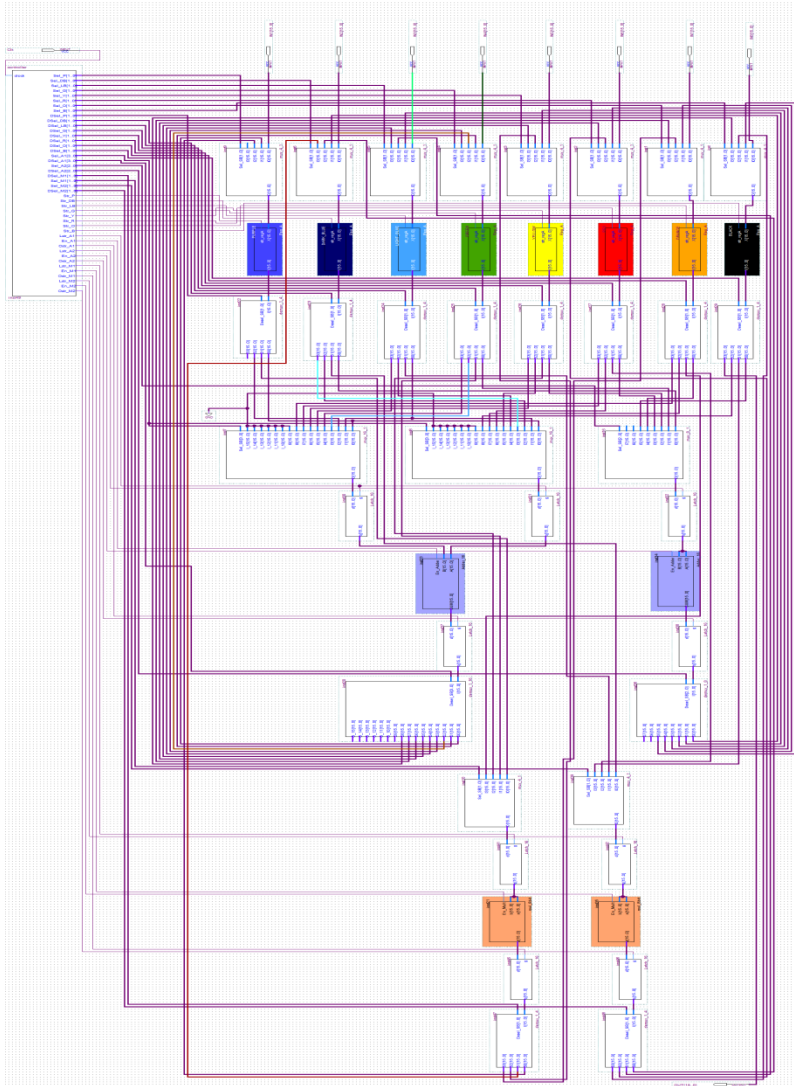
‘c’ denotes the number of colours used in the CIG and
‘S’ denotes the digital signature size

Benchmarks	c	Size of Digital signature (S)				
		S = 15	S = 30	S = 60	S = 120	S = 240
		P _c	P _c	P _c	P _c	P _c
BPF	6	0.0649	4.2127x10 ⁻³	1.7747x10 ⁻⁵	3.1496x10 ⁻¹⁰	9.9198x10 ⁻²⁰
JPEG SAMPLE	10	0.2059	0.0424	1.7970x10 ⁻³	3.2292x10 ⁻⁶	1.0428x10 ⁻¹¹
JPEG IDCT	29	0.5907	0.3490	0.1218	0.0148	2.1999x10 ⁻⁴
MESA FEEDBACK POINTS	17	0.4028	0.1622	0.0263	6.9267x10 ⁻⁴	4.7979x10 ⁻⁷
ARF	8	0.1349	0.0182	3.3150x10 ⁻⁴	1.0989x10 ⁻⁷	1.2076x10 ⁻¹⁴
MESA MATRIX MULTIPLICATION	23	0.5134	0.2635	0.0695	4.8237x10 ⁻³	2.3268x10 ⁻⁵

High level overview of triple phase watermarking

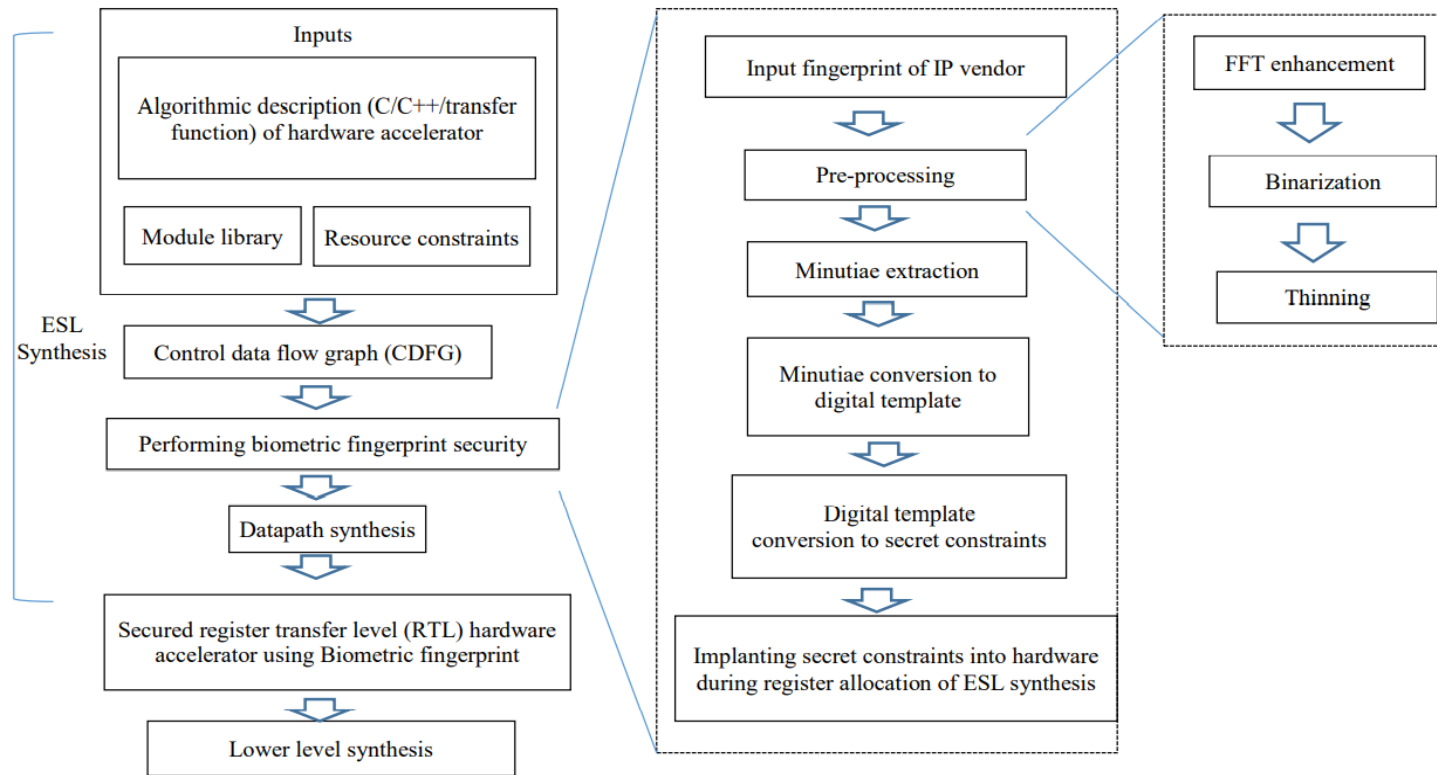


Watermarked FIR Vs Non-Watermarked FIR at RTL



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

Biometric Fingerprint for Hardware Security



- (i) *FFT enhancement:* The use of FFT on sets of pixels of the fingerprint image allows reconnection of broken ridges; finely separates the parallel ridges and also makes the ridges thick.
- (ii) *Binarization:* The image with only two intensity values is called as binary image. This image usually shows only black or white, where black is represented by 0 and white is represented by 255. The elementary principle of binarization is to compare the pixel intensities with the threshold, and setting the pixels whose intensities are less than threshold, to 0 and the other to 255.
- (iii) *Thinning:* In this process, the thickness of ridge lines is reduced to one pixel width by deleting pixels at the edge of ridge lines.

Processing the Biometric Fingerprint



Original Image

Binarization

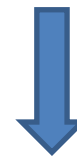


Setting pixel intensity to
0 or 1

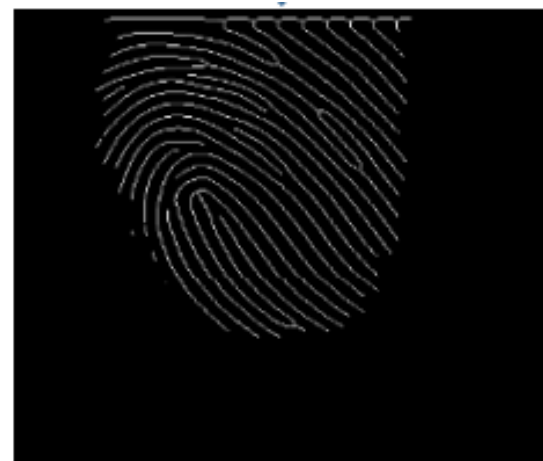


Binary Image

Thinning



Reducing ridge line
thickness to 1 pixel



Thinned Image

**Minutiae point
extraction**

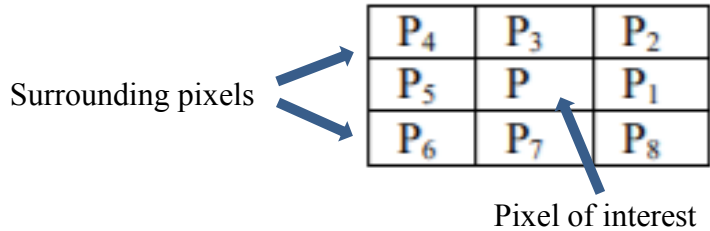


Applying CN algorithm to
obtain ridge endings and
bifurcations



Minutiae Points

Extracting Minutiae Points

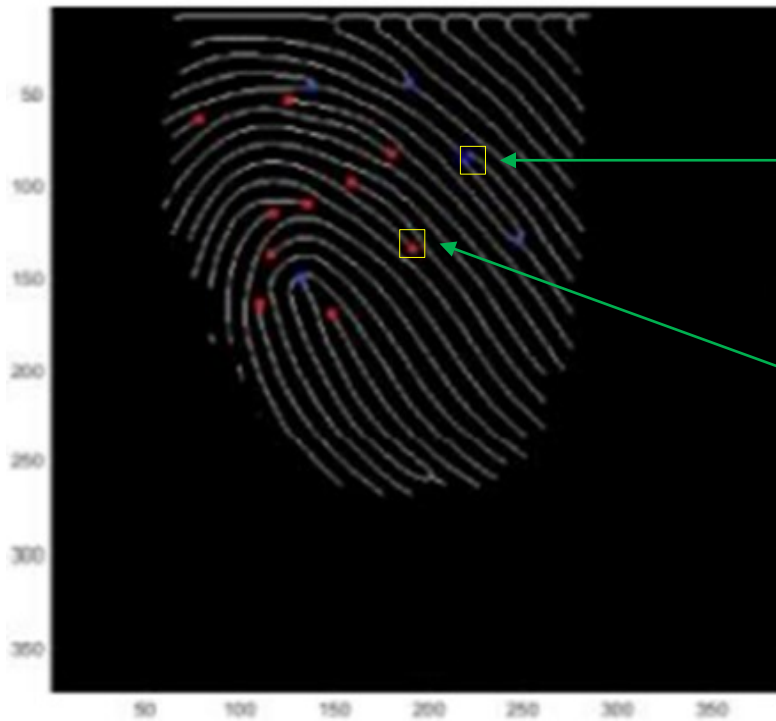


Crossing Number (CN)
algorithm

$$CN = 0.5 * \sum_{i=1}^8 |P_i - P_{i+1}|$$

P_i is the pixel value of the surrounding pixel.

$P_i = 0$ or 1 and $P_1 = P_9$

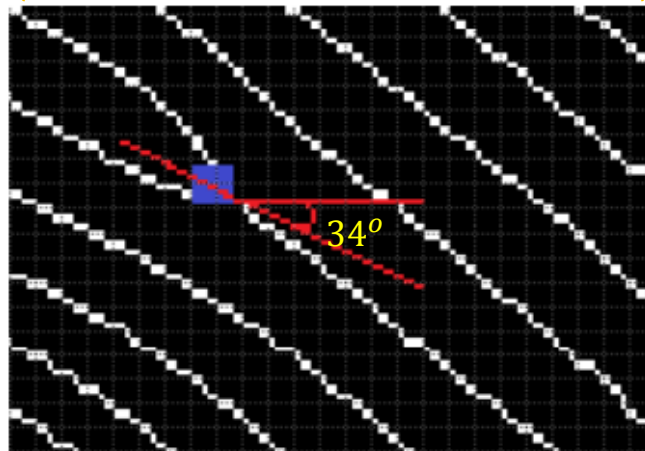
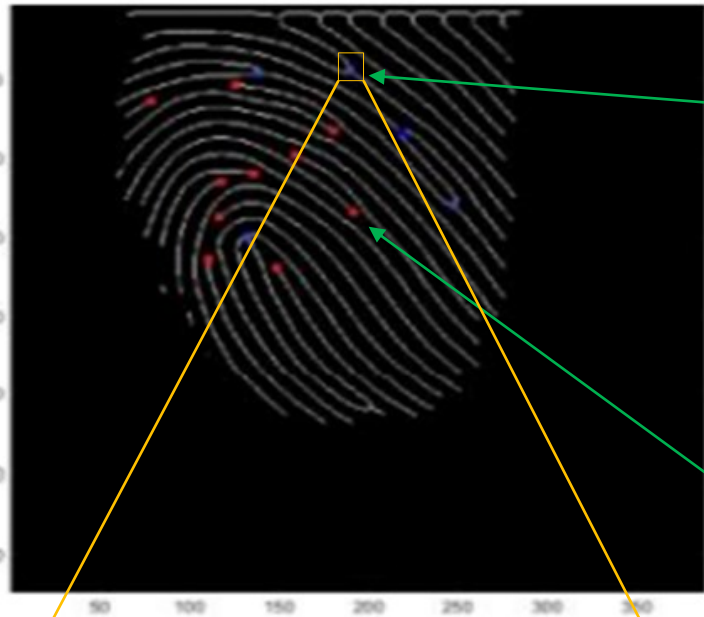


CN = 3 → Ridge Bifurcation

CN = 1 → Ridge Ending

Constructing the Digital Template

The ridge angle of first minutiae point has been measured clock-wise from the horizontal axis



DIGITAL TEMPLATE OF INDIVIDUAL MINUTIAE POINTS REPRESENTING
HARDWARE SECURITY CONSTRAINTS

x, y	m	Minutiae type name	d	Minutiae position in binary (digital template representing hardware constraints) $Z = (x \parallel y \parallel m \parallel d)$
190, 45	3	bifurcation	34	1011111010110111100010
139, 46	3	bifurcation	9	10001011101110111001
126, 54	1	ending	189	1111110110110110111101
79, 64	1	ending	327	10011111000000110100 0111
181, 83	1	ending	38	1011010110100111100110
219, 84	3	bifurcation	225	1101101110101001111100001
159, 98	1	ending	214	100111111100010111010110
136, 110	1	ending	15	10001000110111011111
118, 115	1	ending	334	111011011100111101001110
248, 130	3	bifurcation	50	111110001000001011110010
192, 134	1	ending	46	1100000010000110110 1110
117, 137	1	ending	135	111010110001001110000111
132, 150	3	bifurcation	138	10000100100101101110001010
111, 164	1	ending	267	11011111010 01001100001011
149, 169	1	ending	239	1001010110101001111101111

X co-ordinate(x)

Y co-ordinate(y)

Minutiae type(m)

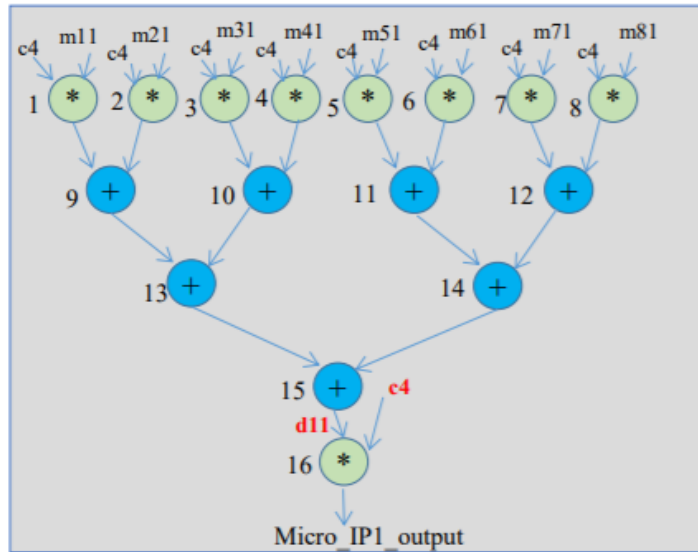
Angle(d)

Digital template obtained by concatenating templates of all 15 minutiae points

1011111010110111100010100010111011101110011111110110110111101100111110000001101
00011110110110101101001111001101101101110101001111100001100111111110001011101011010001
0001101110111111110110111001111010011101111100010000010111100101100000010000110110
11101110110001001110000111100001001001011011100010101101111101001001100001011100
1010110101001111101111

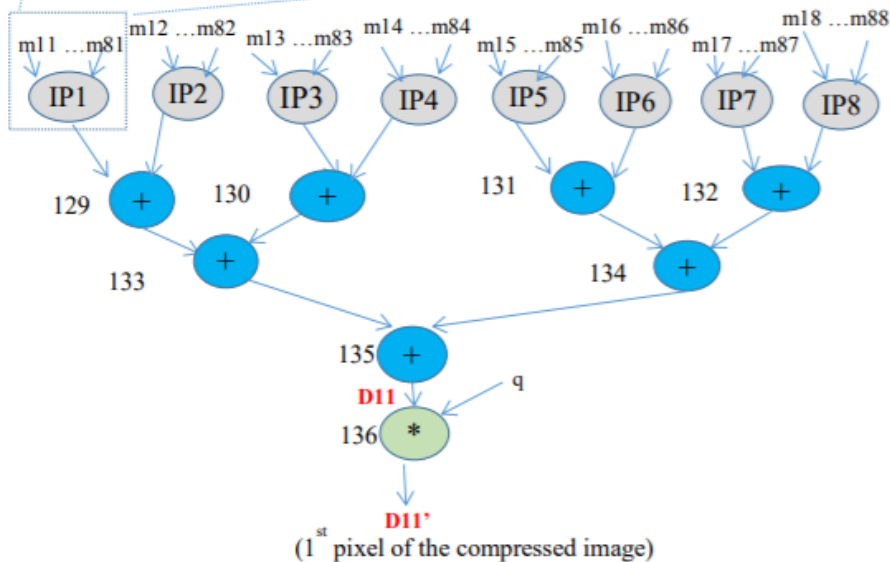
350 bits, 148 zeros and 202 ones

JPEG CODEC Compression Algorithm



$$\begin{bmatrix}
 C_4 & C_4 & C_4 & C_4 & C_4 & C_4 & C_4 & C_4 \\
 C_1 & C_3 & C_5 & C_7 & -C_7 & -C_5 & -C_3 & -C_1 \\
 C_2 & C_6 & -C_6 & -C_2 & -C_2 & -C_6 & -C_6 & C_2 \\
 C_3 & -C_7 & -C_1 & -C_5 & C_5 & C_1 & C_7 & -C_3 \\
 C_4 & -C_4 & -C_4 & C_4 & C_4 & -C_4 & -C_4 & C_4 \\
 C_5 & -C_1 & C_7 & C_3 & -C_3 & -C_7 & C_1 & -C_5 \\
 C_6 & -C_2 & C_2 & -C_6 & -C_6 & C_2 & -C_2 & C_6 \\
 C_7 & -C_5 & C_3 & -C_1 & C_1 & -C_3 & C_5 & -C_7
 \end{bmatrix}$$

2D- DCT coefficient matrix 'C'



- Post multiplying the 1st pixel (D11) of DCT transformed matrix with the quantization coefficient 'q', the 1st pixel (D11') of the compressed image is generated.
- Post quantization, the quantized image is converted to 1-D array using zigzag scanning and run length encoding is applied to obtain bit stream of the compressed image for storage purpose.
- In order to reconstruct the original image from the stored compressed image data, run length decoding followed by inverse zigzag scanning, inverse quantization and inverse DCT transformation are performed in the JPEG decompression process.
- The JPEG compression hardware comprises of 8 micro-IPs underneath. Each micro-IP performs 16 operations and total operations in the entire JPEG CODEC IP core are 136.

Embedding Security Constraints into JPEG CODEC

DIGITAL TEMPLATE TO HARDWARE SECURITY CONSTRAINTS MAPPING

RULES	
Bit	Mapping rules
0	Embed an edge between node pair (even, even) into the CIG (during register allocation of ESL synthesis)
1	Embed an edge between node pair (odd, odd) into the CIG (during register allocation of ESL synthesis)

148 zeroes → 148 even-even edges → (0,2), (0,4), . . . (0,208), (2,4), (2,6), (2,88), (2,90)

202 ones → 202 odd-odd edges → (1,3), (1,5), . . . (1,207), (3,5), (3,7), (3,199), (3,201)

RESOURCES IN THE RTL DATAPATH OF JPEG COMPRESSION HARDWARE (PRE AND POST EMBEDDING BIOMETRIC FINGERPRINT CONSTRAINTS)

Resources pre-embedding security constraints				Resources post-embedding security constraints			
FUs	# of registers	Multiplexers	Demultiplexers	FUs	# of registers	Multiplexers	Demultiplexers
3M, 3A	73	# 32x1 Muxes=10	# 1x32 Demuxes=5	3M, 3A	73	# 32x1 Muxes=10	# 1x32 Demuxes=5
		# 16x1 Muxes=3	# 1x16 Demuxes=2			# 16x1 Muxes=2	# 1x16 Demuxes=1
		# 8x1 Muxes =7	# 1x8 Demuxes=7			# 8x1 Muxes =9	# 1x8 Demuxes=9
		# 4x1 Muxes =24	# 1x4 Demuxes=24			# 4x1 Muxes =24	# 1x4 Demuxes=24
		# 2x1 Muxes =32	# 1x2 Demuxes=32			# 2x1 Muxes =31	# 1x2 Demuxes=31

As JPEG CODEC is a huge hardware accelerator, there is no overhead of registers.

Control steps (0-30)

[illegible]

CS	Pre-embedding		Post-embedding	
	R 1	R2	R 1	R 2
23	196	--	--	196
24	196	--	--	196
25	202	--	--	202
26	202	--	--	202
27	202	--	--	202
28	202	--	--	202
29	207	--	207	--
30	208	--	--	208

R: Register

Notice that storage variables 196, 202 and 208 had to be shifted from R1 to R2 to accommodate edges (0,196), (0,202) & (0,208).

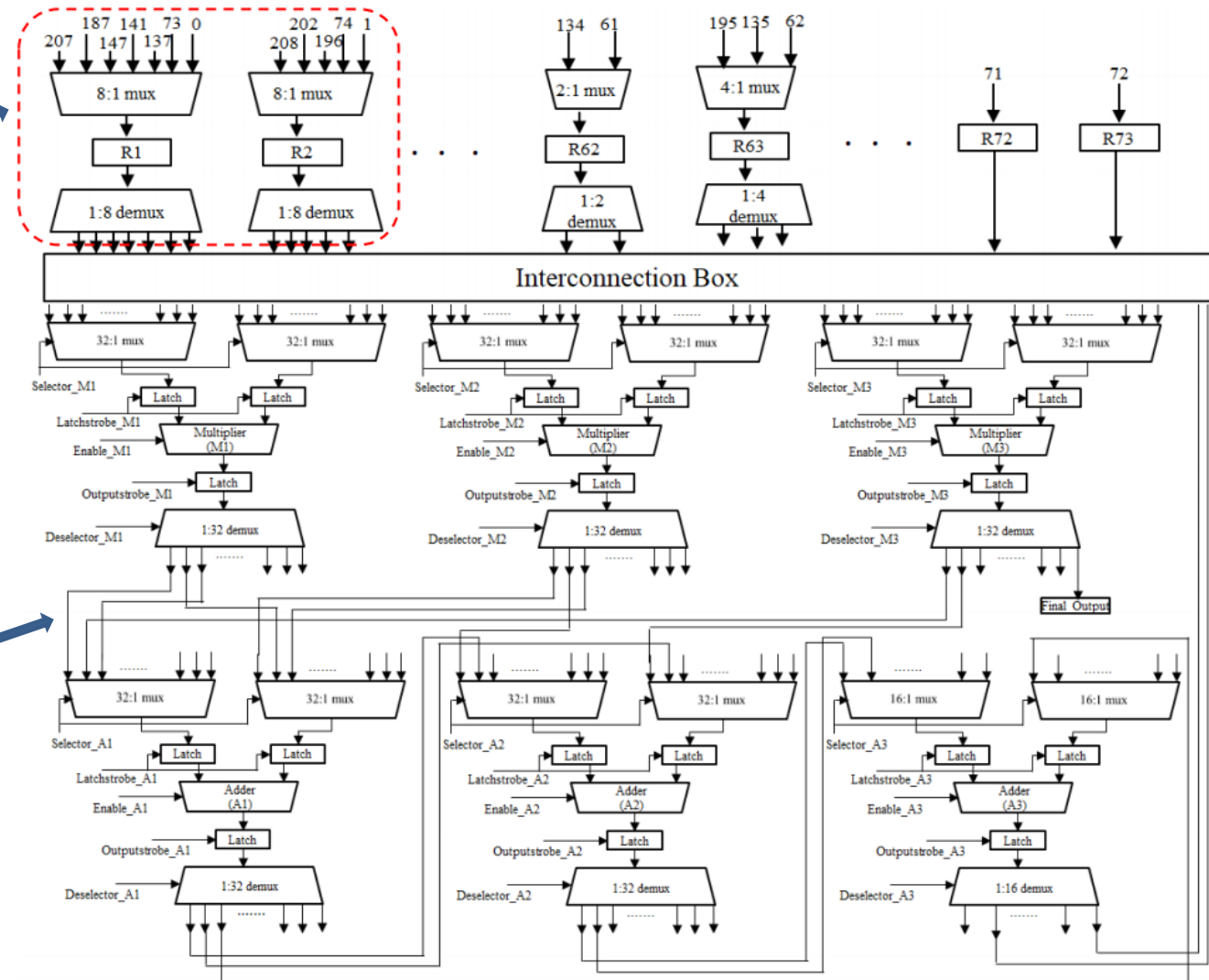
Since the design is very large, hence there isn't much change in register allocation and there is no design overhead.

- Register allocation of storage variables (0-208) post embedding during ESL synthesis of JPEG compression hardware accelerator

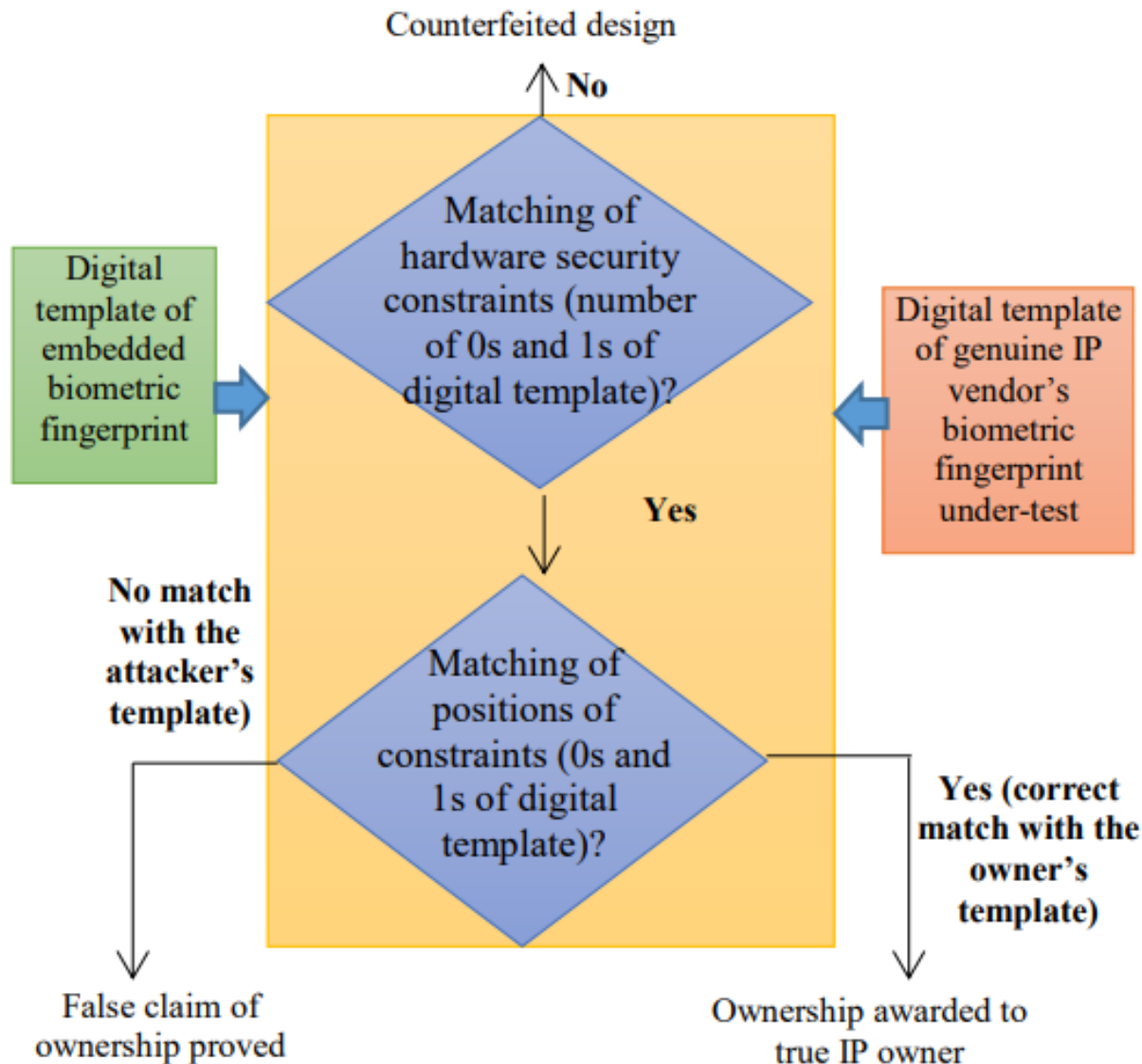
RTL Datapath of the Secured Design

The red box highlights the changes in register allocation amongst R1 and R2.

Notice how rest of the design hardware is unaffected. Further security constraints can be added by using much larger digital signature templates.



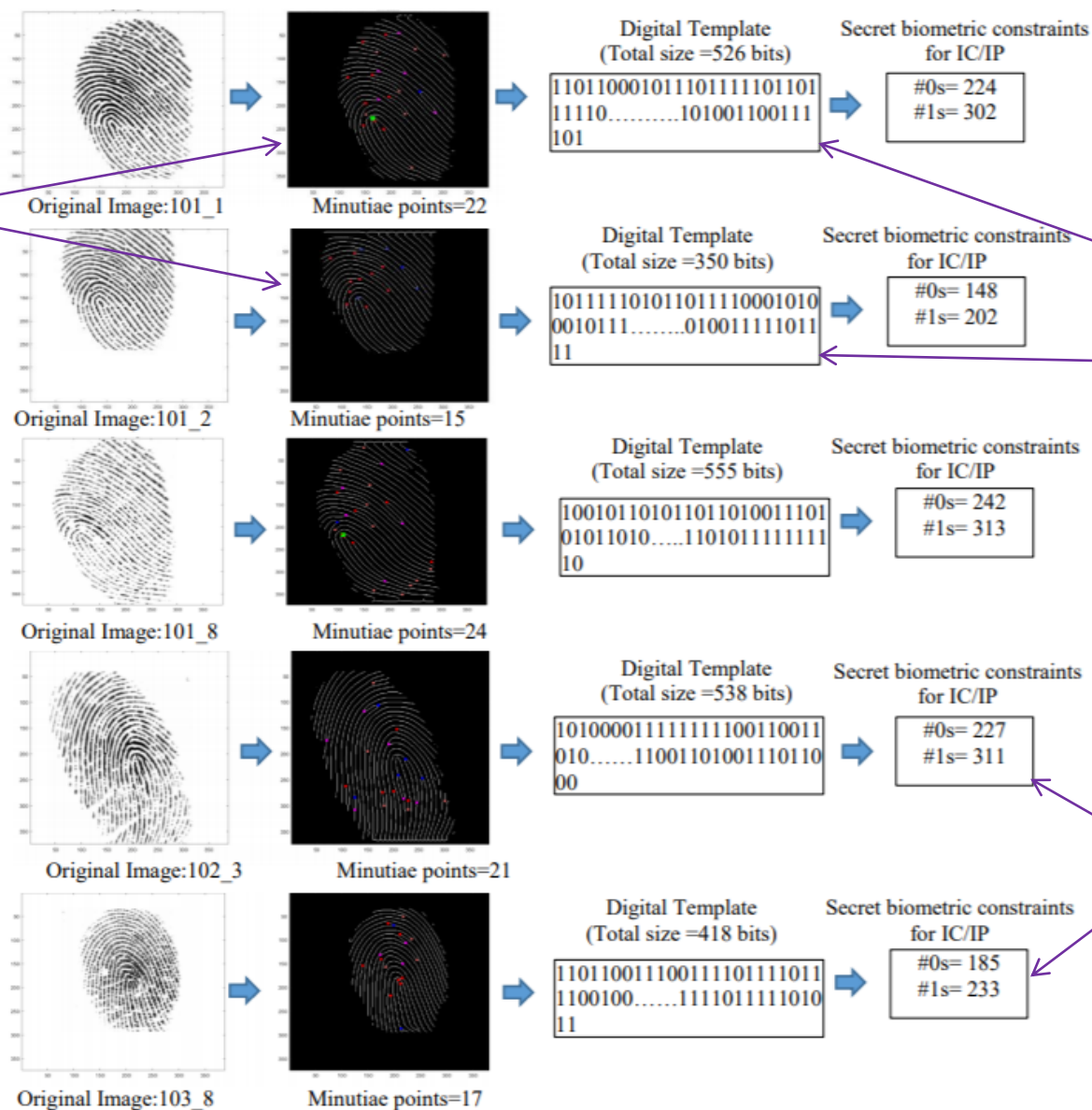
Detection of Biometric Fingerprint



Biometric Fingerprints of 5 different people

Notice how different fingerprints have different sets of minutiae points.

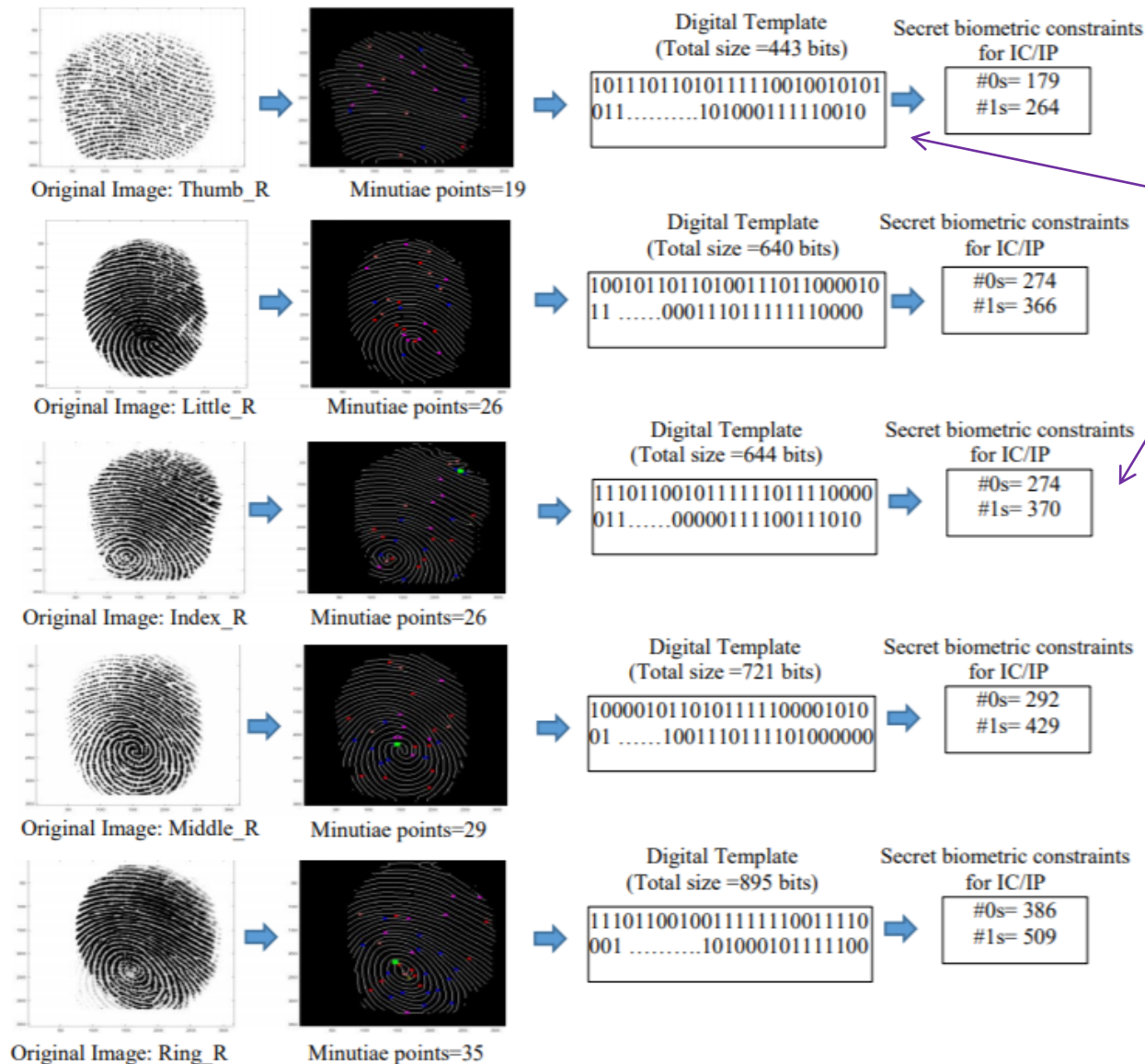
As fingerprints are naturally unique, there is bound to be at least one difference at some bit position in the digital template, thereby nullifying claims for IP ownership.



Notice the varying number of bits in the digital signatures.

Notice the varying number of 0s and 1s.

Biometric Fingerprints of 5 fingers of the same person



Notice how varied the fingerprints of different fingers of the same person are .

Notice that the Ring finger has the most minutiae points while the Thumb has the least. Hence, a design secured using the Ring finger is more secure.

Security Analysis

Probability of Coincidence,
$$Pc = \left(1 - \frac{1}{R}\right)^{f1} * \left(1 - \frac{1}{\pi_{i=1}^n N(Fi)}\right)^{f2}$$

R → number of colors/ registers in original CIG,

f1 → number of additional edges embedded into the CIG (in register allocation phase)

f2 → number of constraints embedded in the functional unit (FU) vendor allocation phase.

n → total types of FU

VARIAION IN PC OF PROPOSED APPROACH FOR DIFFERENT FINGERPRINTS

SELECTED FROM DATABASE			
Fingerprint image	# Minutiae points (M)	Total constraints (fl)	Probability of coincidence (Pc)
101_1	22	526	7.06E-4
101_2	15	350	8.00E-3
101_8	24	555	4.73E-4
102_3	21	538	5.98E-4
103_8	17	418	3.13E-3
101_7	21	540	5.82E-4

IMPACT OF FINGERPRINT OF DIFFERENT FINGERS OF SAME PERSON ON PC

Fingerprint image	# Minutiae points (M)	Total constraints (fl)	Pc
Thumb_R	19	443	2.22E-3
Little_R	26	640	1.46E-4
Index_R	26	644	1.38E-4
Middle_R	29	721	4.79E-5
Ring_R	35	895	4.35E-6

Comparison of proposed approach with Crypto-Steganography based approach [20]

Approaches	Total constraints	Pc	Approximate run time
Related work [20]	W=20	3.0e-1	~400 ms
	W=40	9.8e-2	
	W=60	1.9e-2	
	W=80	3.7e-3	
	W=100	1.7e-3	
Proposed work	M=35	4.35e-6	~185 ms

Note: The probability of coincidence represents the probability of coincidentally detecting hardware security constraints in an unsecured design. Since we don't want any coincidence between signatures of original IP vendor and adversary, it is desirable for Pc to be as low as possible.

Design Cost Analysis

$$\text{Design Cost, } C_d(F_i) = w_1 \frac{D_T}{D_{max}} + w_2 \frac{A_T}{A_{max}}$$

D_T & A_T $\rightarrow$ design delay and area respectively

A_{max} and D_{max} $\rightarrow$ maximum area and delay

w_1 and w_2 $\rightarrow$ user defined weights (both kept at 0.5 to assign equal preference).

DESIGN COST OF JPEG COMPRESSION HARDWARE PRE AND POST EMBEDDING BIOMETRIC FINGERPRINT CONSTRAINTS

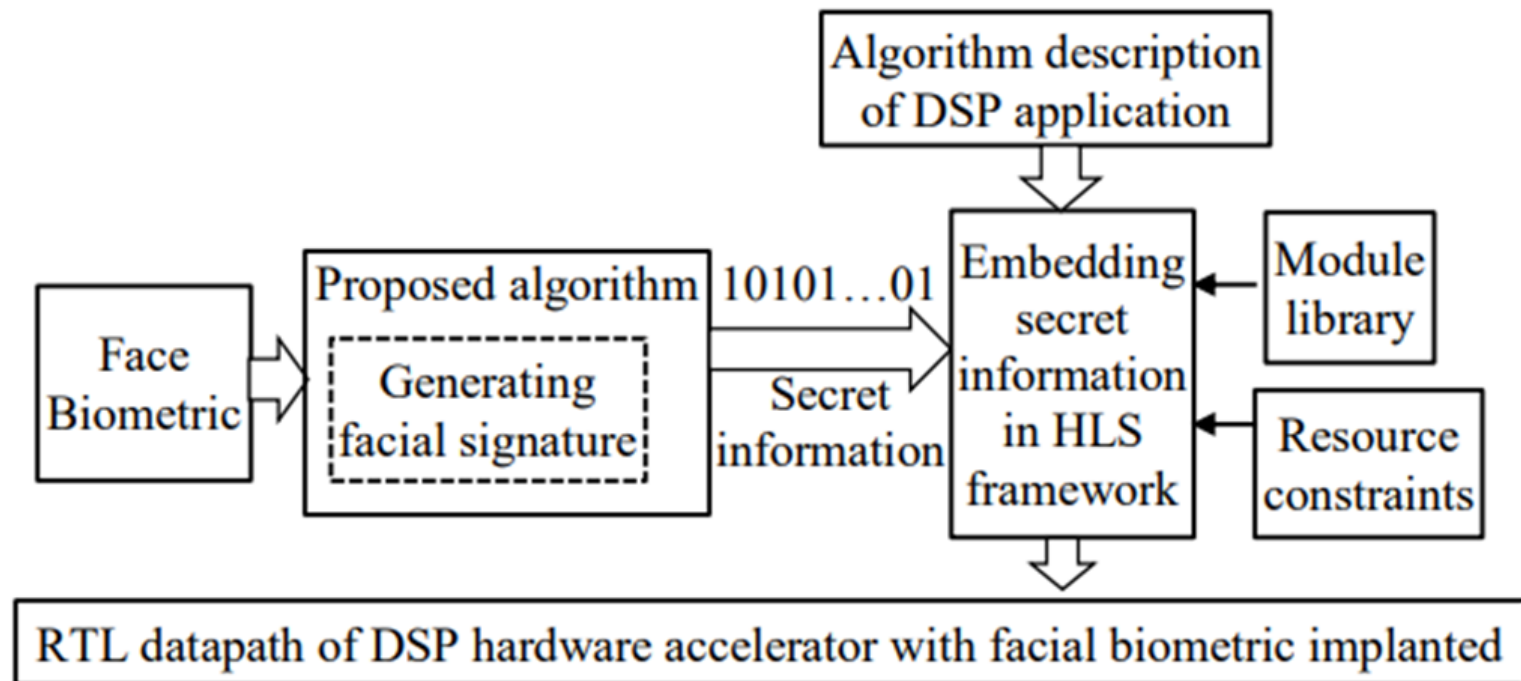
Resource constraints	# of registers in baseline JPEG	# of registers in fingerprint implanted JPEG	Design cost of baseline JPEG	Design cost of fingerprint implanted JPEG	Estimated % overhead
3A, 3A	73	73	0.214	0.214	0%
3A, 5M	73	73	0.1917	0.1917	0%
5A, 5M	73	73	0.1713	0.1713	0%
7A, 9M	73	73	0.1718	0.1718	0%
9A, 9M	73	73	0.1752	0.1752	0%
11A, 11M	73	73	0.1785	0.1785	0%

Notice how there is no design overhead for JPEG, implying that the proposed approach is apt for

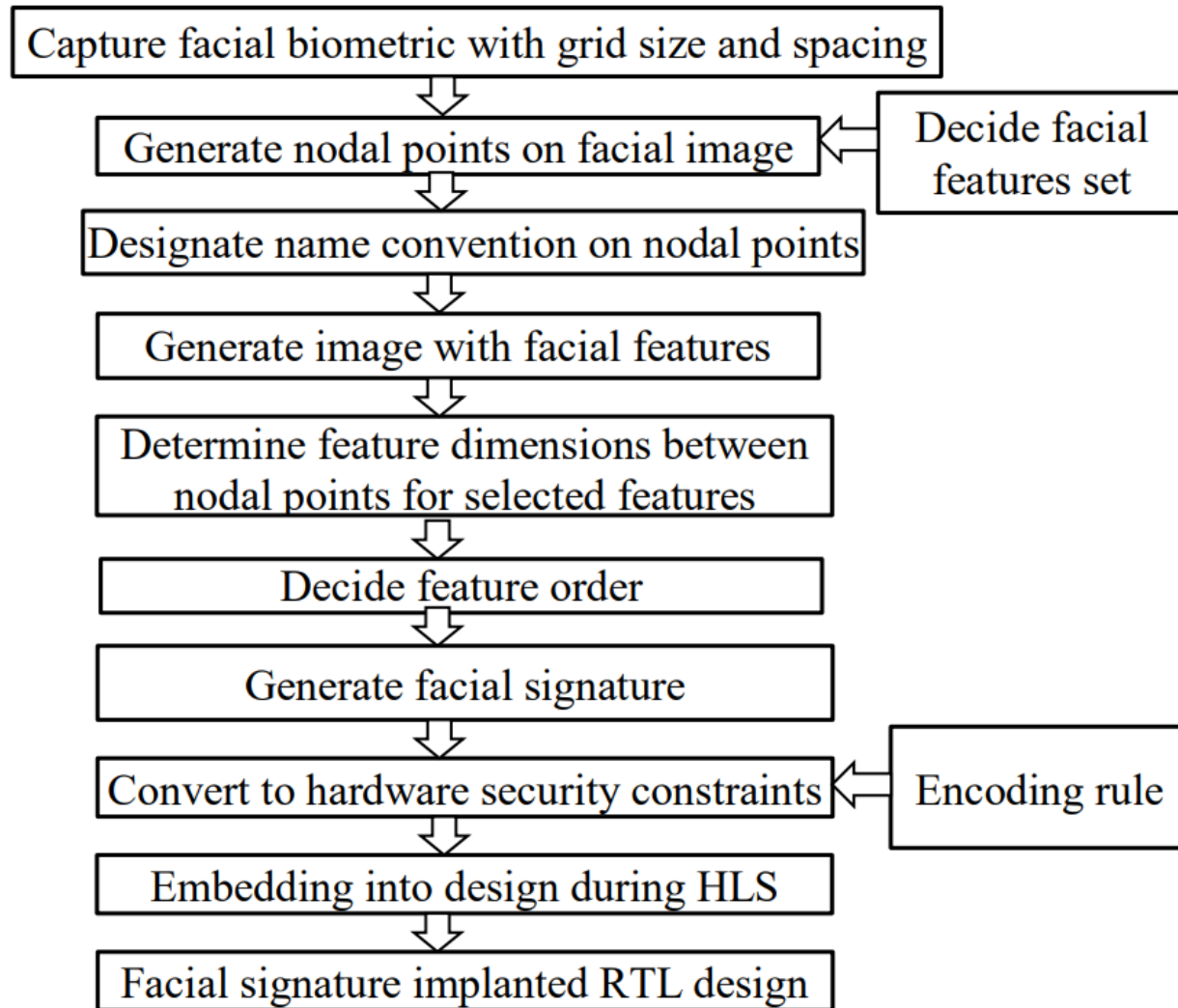
Facial Biometric for Hardware Security

- First approach in the literature that leverages unique facial biometric information to secure hardware accelerators.
- Contact-less mechanism for securing hardware accelerators.
- Low implementation complexity and higher robustness during authentication/verification process.
- Zero dependence on external factors.
- Non-vulnerable and non-replicable technique.

Overview of the Facial Biometric Approach

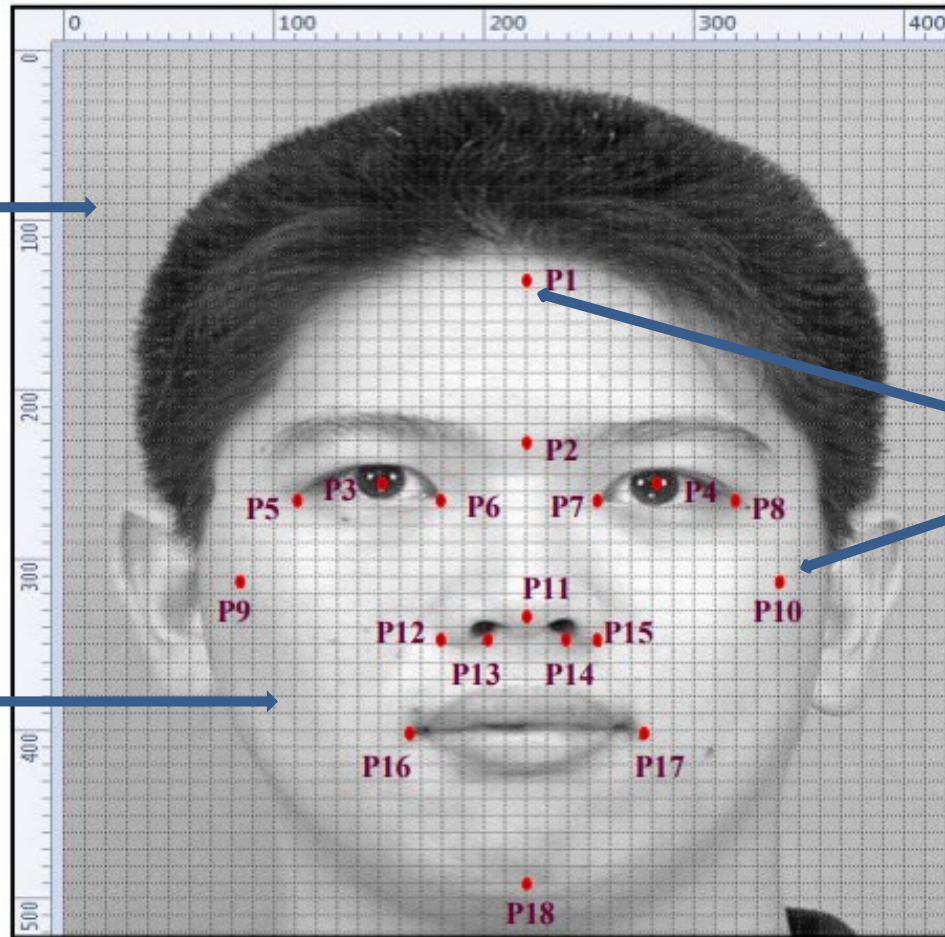


Flow of the proposed Face Biometric Approach



Generating Nodal Points

Grid
Spacing
(Used
to
calculat
e the
Facial
distance
Biometric
between
n
nodes)



Nodal
Points

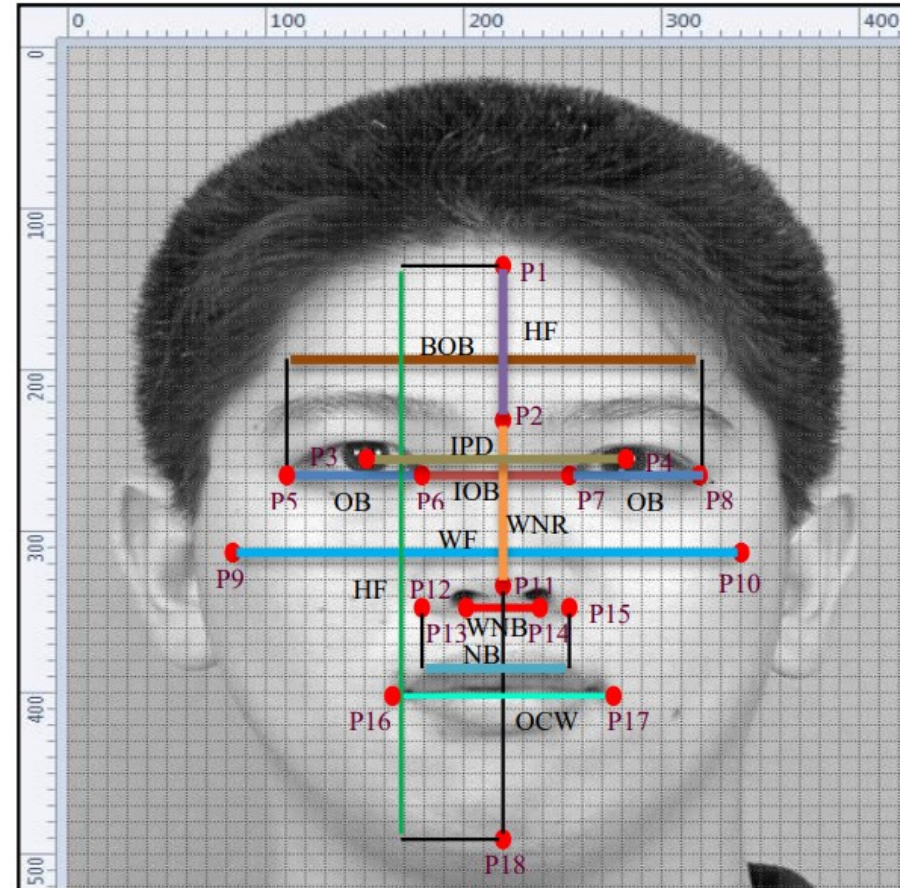
Naming the generated nodal points on
the facial biometric image according to

Determining Facial Features



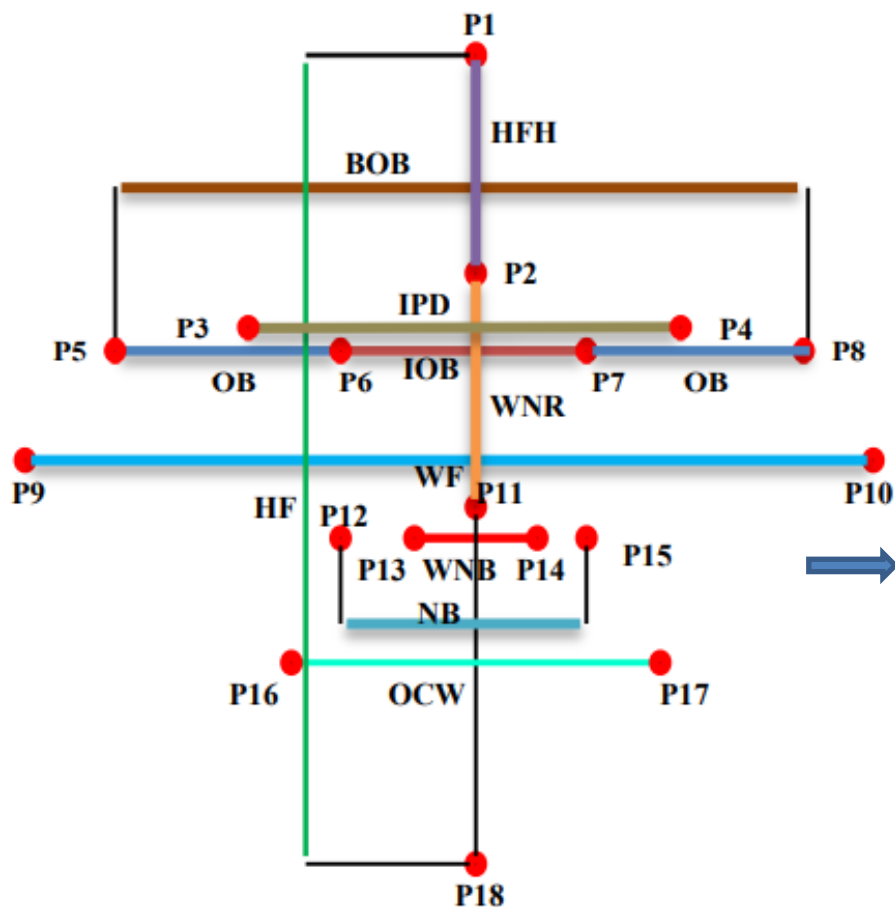
VENDOR'S SELECTED ELEVEN FACIAL FEATURES, CORRESPONDING NODAL POINTS AND CO-ORDINATES

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 Commis sure Width	(P16) – (P17)	(165, 405)- (275, 405)



Plotting the selected features
on the Facial Biometric.

Measuring Facial Feature Dimensions and Conversion into Binary Representation



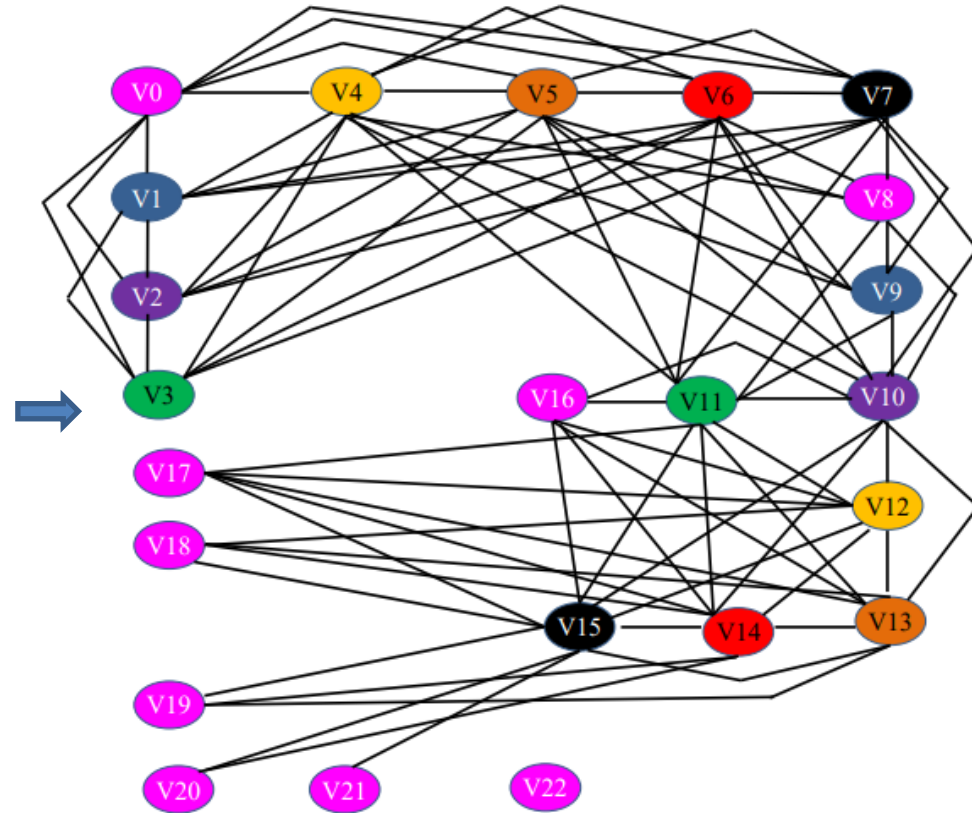
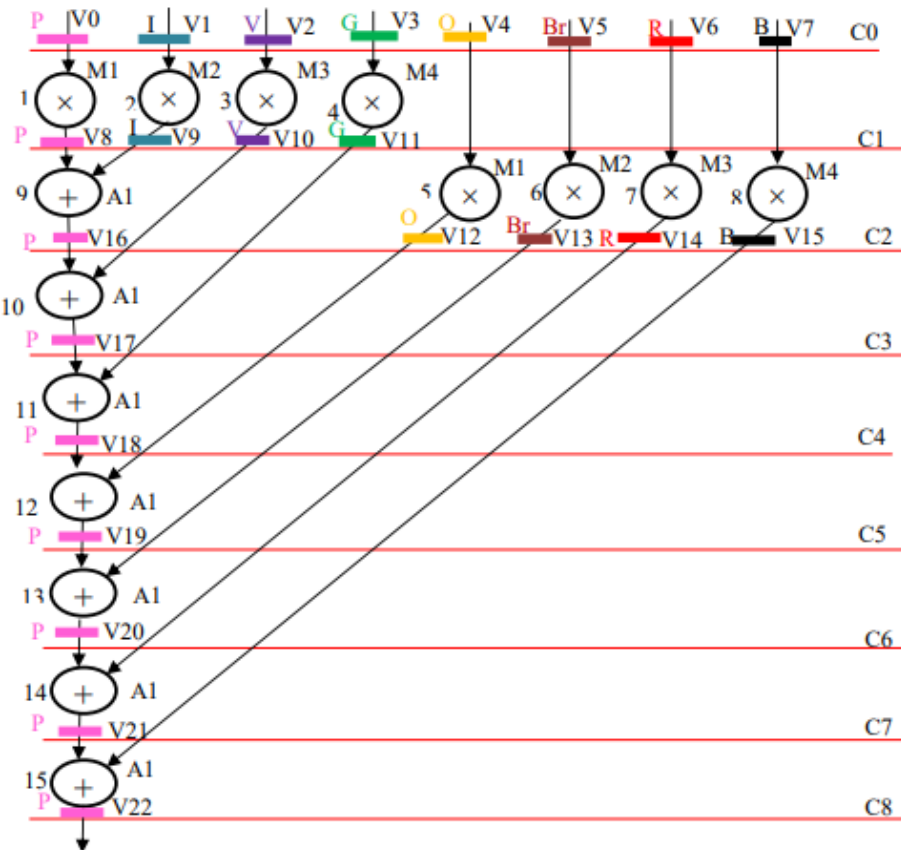
FEATURE DIMENSION AND CORRESPONDING BINARY REPRESENTATION OF VENDOR'S SELECTED FACIAL FEATURES

S. no.	Facial features	Feature dimension (Manhattan distance)= $ x_2-x_1 + y_2-y_1 $	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.

Skeleton of the vendor's selected eleven facial

Converting Scheduled Data Flow Graph to Coloured Interval Graph



CIG showing edges between storage

Notice 'V15' has most edges (10) as it shares time span with 10 storage variables and 'V22' has no edges because it doesn't share its time span with any other storage variable.

variables existing in the same time span.

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



100011010110001110100010000010110111010010111001011110100101111111111011111101001

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

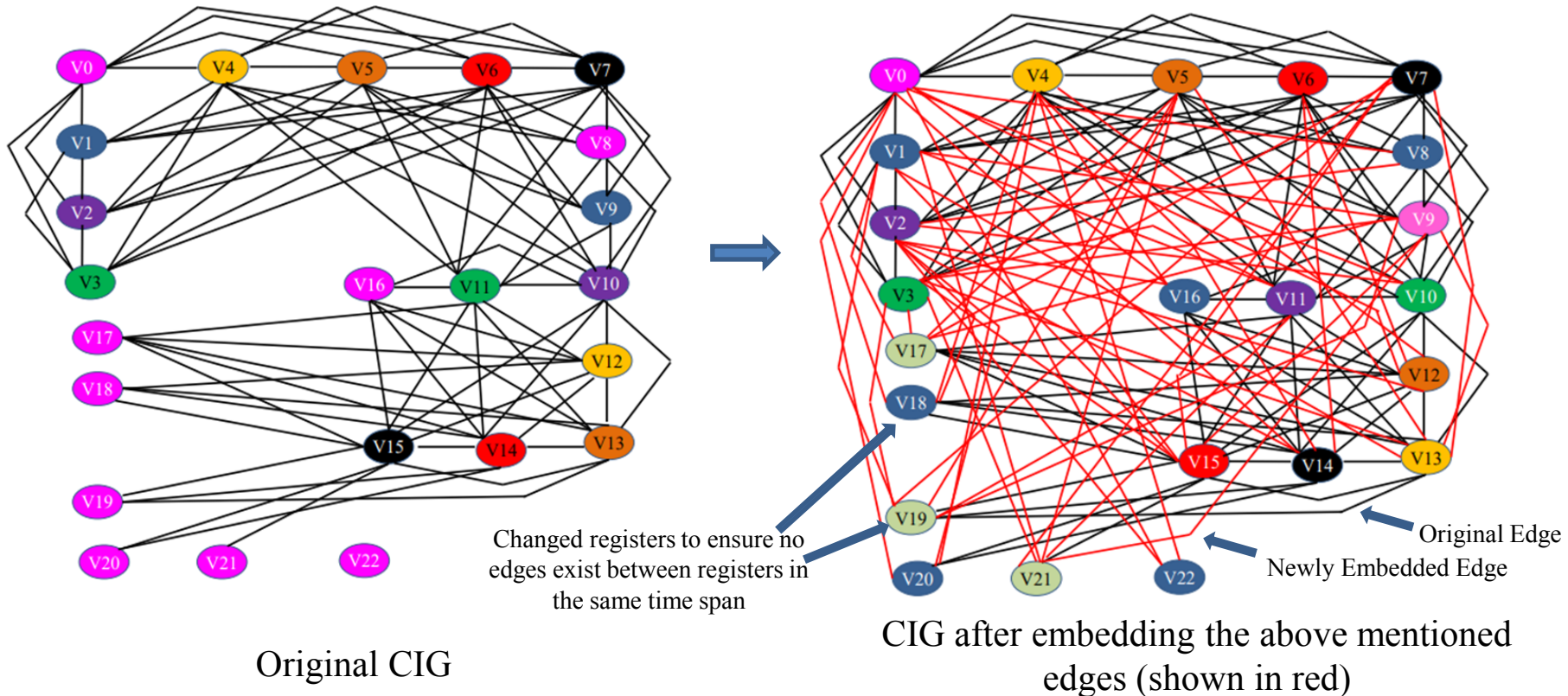
ENCODING OF FACIAL SIGNATURE INTO HARDWARE SECURITY CONSTRAINTS

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

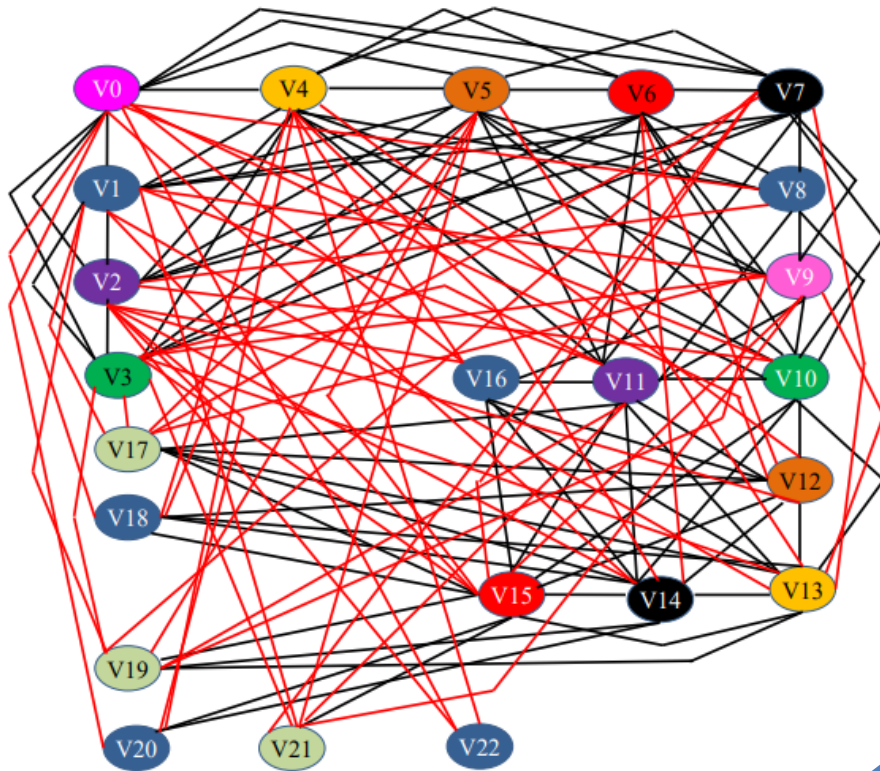
101111110000010110100101001011100011011010011111111110110001110100010010111101110

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

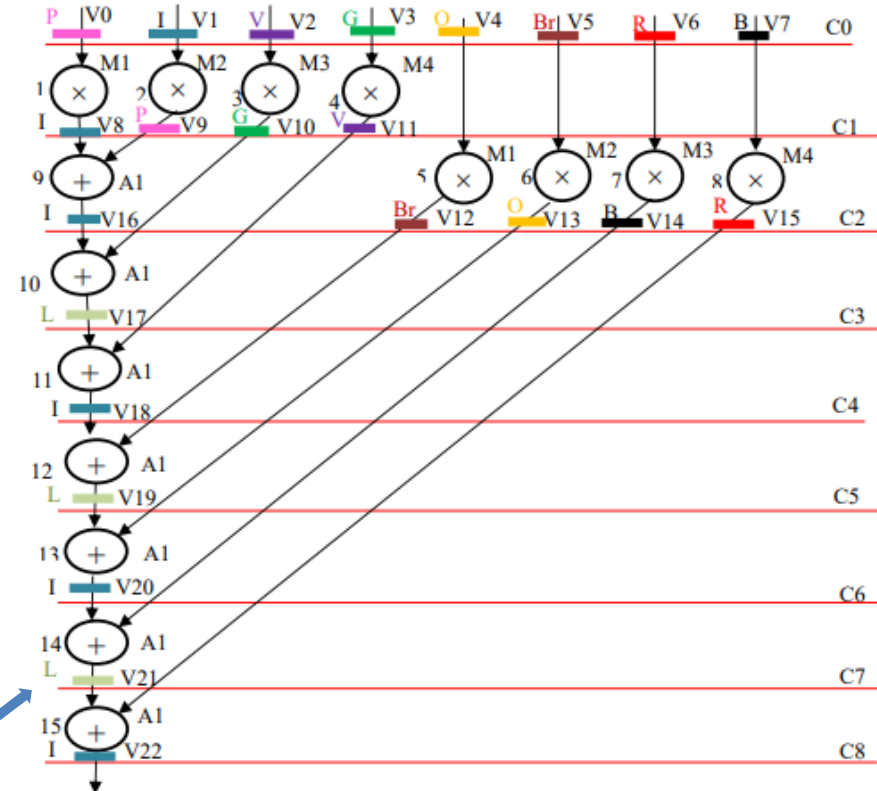
47 ones $\rightarrow$ 47 odd-odd edges $\rightarrow$ (1,3), (1,5), . . . (1,21), (3,5), (3,7), (13,15), (13,17)



Modifying the SDFG to Accommodate the Newly Embedded Edges

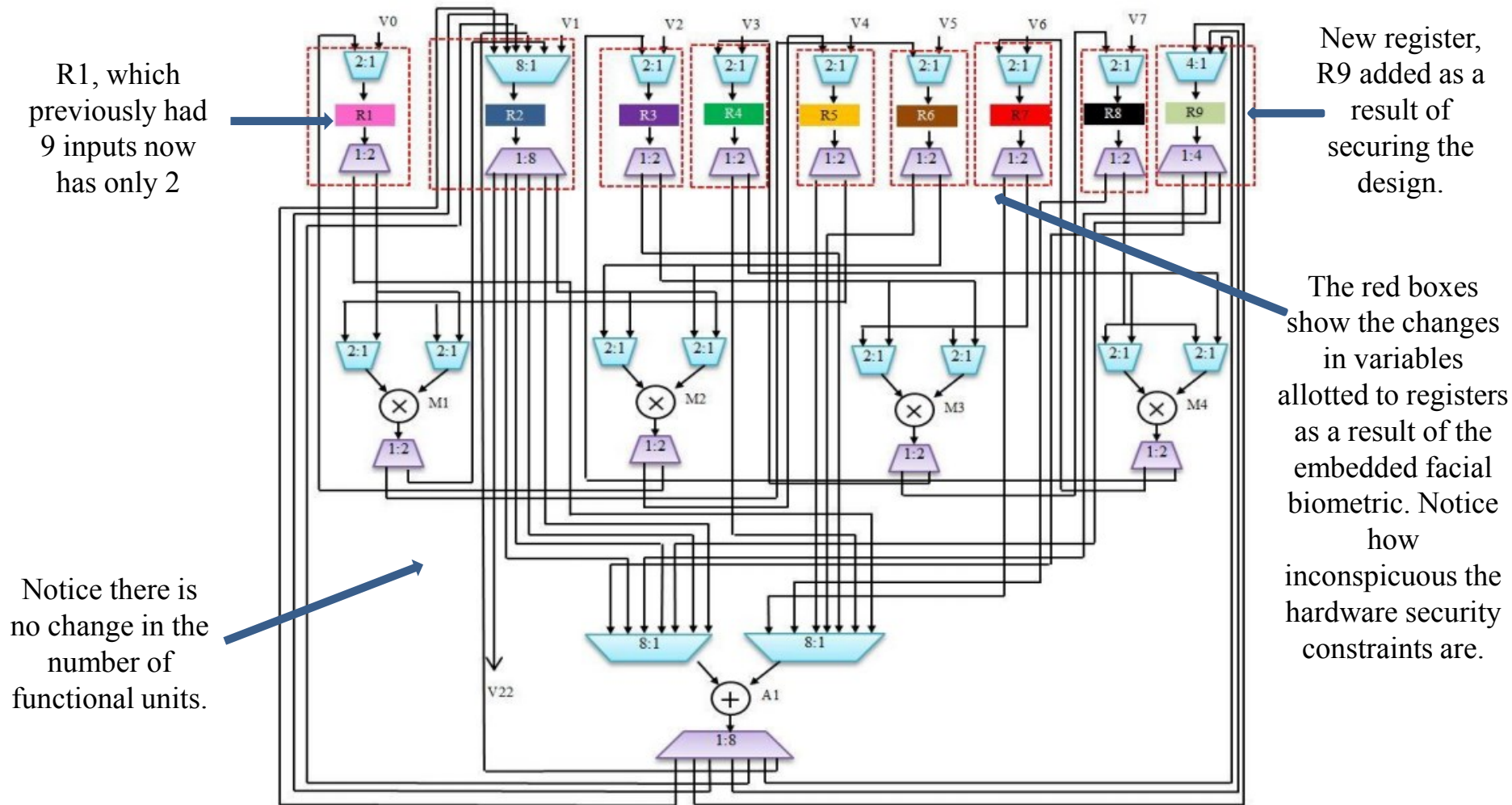


An extra register, 'Lime' (L) had to be incorporated and hence, an overhead of 1.



Scheduled Data Flow Graph constructed from the CIG after embedding secret hardware security constraints in the form of red edges.

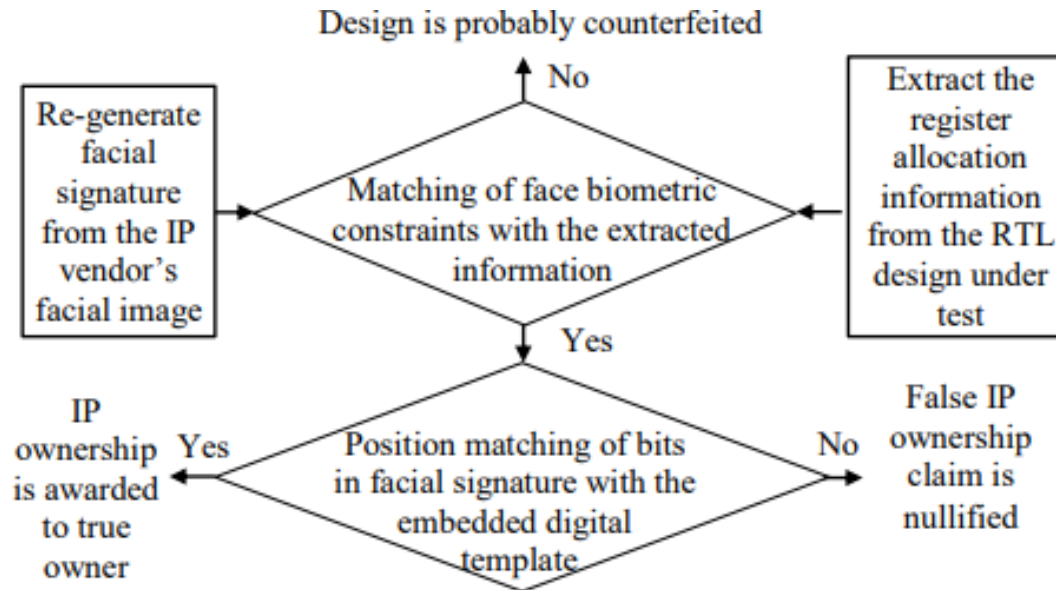
RTL Datapath of the Secured Design



RESOURCES IN THE RTL DATAPATH OF 8-POINT DCT (PRE AND POST EMBEDDING FACIAL BIOMETRIC CONSTRAINTS)

Resources pre-embedding security constraints				Resources post-embedding security constraints			
FUs	# of registers	Multiplexers	Demultiplexers	FUs	# of registers	Multiplexers	Demultiplexers
4M	8	# 16x1 Muxes=1	# 1x16 Demuxes=1	4M	9	# 8x1 Muxes=3	# 1x8 Demuxes=2
1A		# 8x1 Muxes=2	# 1x8 Demuxes=1	1A		# 4x1 Muxes=1	# 1x4 Demuxes=1
		# 2x1 Muxes=15	# 1x2 Demuxes=11			# 2x1 Muxes=15	# 1x2 Demuxes=11

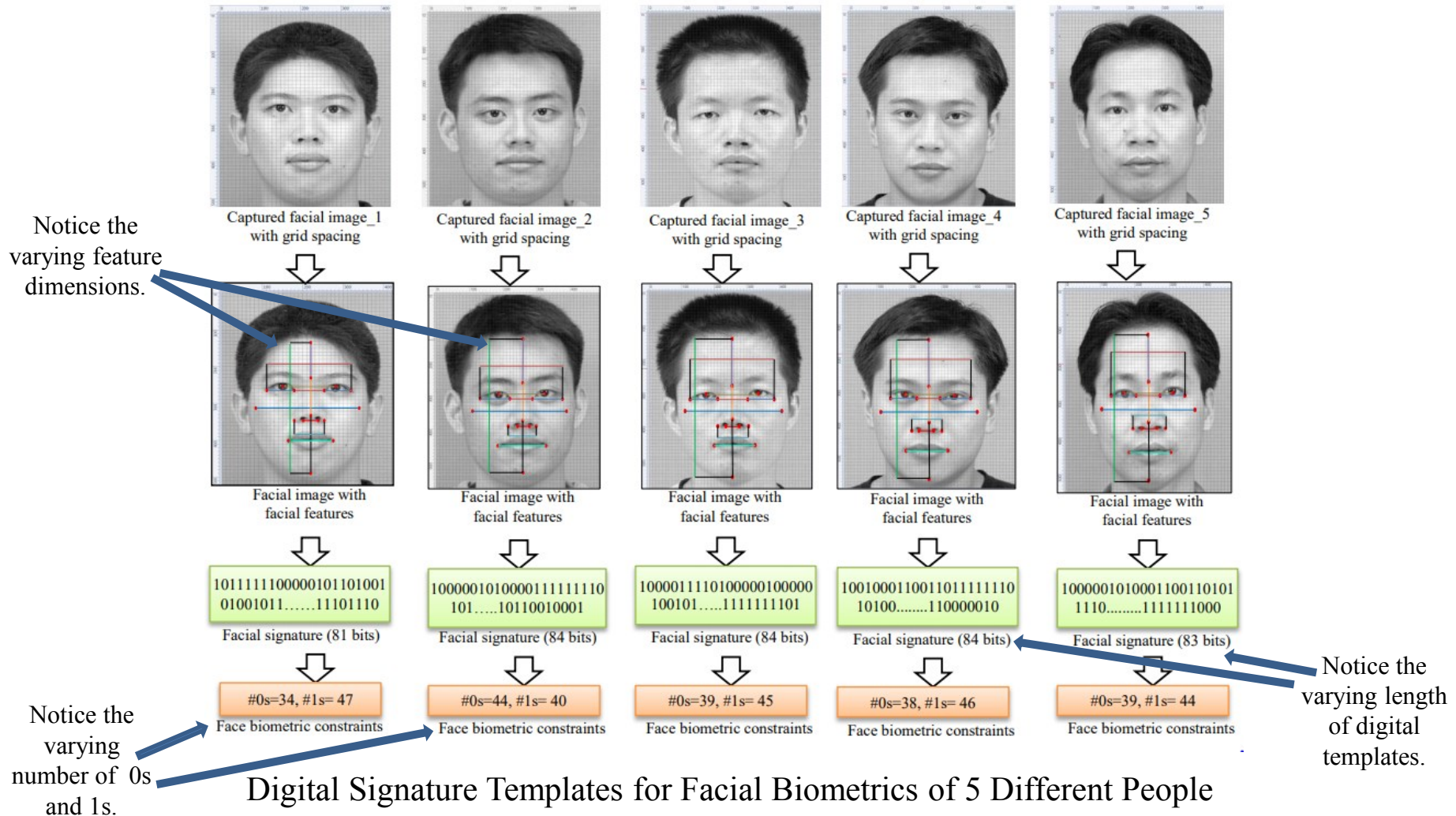
Detection of Face Biometric Embedded into Design



Too many details to be known to the adversary:

- Precise coordinates of the nodal points
- Type of features selected
- Ordering of the features
- Number of 0s and 1s
- Positions of 0s and 1s
- Grid size and spacing

Impact of Varying Facial Signature on Generated Hardware Security Constraints



More the number of features included, more likely the templates are bound to differ at atleast one bit position, thereby enhancing security.

Security Analysis

$$\text{Probability of Coincidence, } P_c = \left(1 - \frac{1}{h}\right)^g$$

$h \rightarrow$ number of registers in the CIG before implanting secret constraints

$g \rightarrow$ number of secret constraint edges added to the CIG

Variation in P_c for DCT for different facial images with same number of features

Bench-marks	Max. constraints	Pc	
		Proposed	[4]
8-point DCT	30	1.8E-2	1.8E-2
8-point IDCT	30	1.8E-2	1.8E-2
FIR	40	4.7E-3	4.7E-3
MPEG	54	1.8E-2	1.8E-2

Comparison of P_c w.r.t to Fingerprint Biometric Approach [4]

Facial images	# facial features	constraints (g)	Pc
Image_1	11	81	2.01E-5
Image_2	11	84	1.34E-5
Image_3	11	84	1.34E-5
Image_4	11	84	1.34E-5
Image_5	11	83	1.54E-5

Comparison of P_c w.r.t Hardware Steganography [18] for the facial Image 1 to Image 5

Bench-marks	# colors (registers)	Proposed work						Related work [18]	
		Image_1		Image_2, 3, and 4		Image_5		# stego-constraints	Pc
		(# biometric constraints)	Pc	(# biometric constraints)	Pc	(# biometric constraints)	Pc		
8-point DCT	8	81	2.01E-5	84	1.34E-5	83	1.54E-5	13	1.8E-1
								24	4.1E-2
								43	3.2E-3
8-point IDCT	8	81	2.01E-5	84	1.34E-5	83	1.54E-5	13	1.8E-1
								24	4.1E-2
								43	3.2E-3
FIR	8	81	2.01E-5	84	1.34E-5	83	1.54E-5	20	6.9E-2
								57	4.9E-4
								21	2.1E-1
MPEG	14	81	2.47E-3	84	1.98E-3	83	2.13E-3	52	2.1E-2
								59	1.3E-2

Notice how Pc decreases as number of constraints increase.

Note: The probability of coincidence represents the probability of coincidentally detecting hardware security constraints in an unsecured design. Since we don't want any coincidence between signatures of original IP vendor and adversary, it is desirable for P_c to be as low as possible.

Design Cost Analysis

$$\text{Design Cost, } C_f(Z_i) = \omega_1 \frac{L_d}{L_m} + \omega_2 \frac{A_d}{A_m}$$

Z_i → resource constraints

A_d and L_d → design area and latency respectively

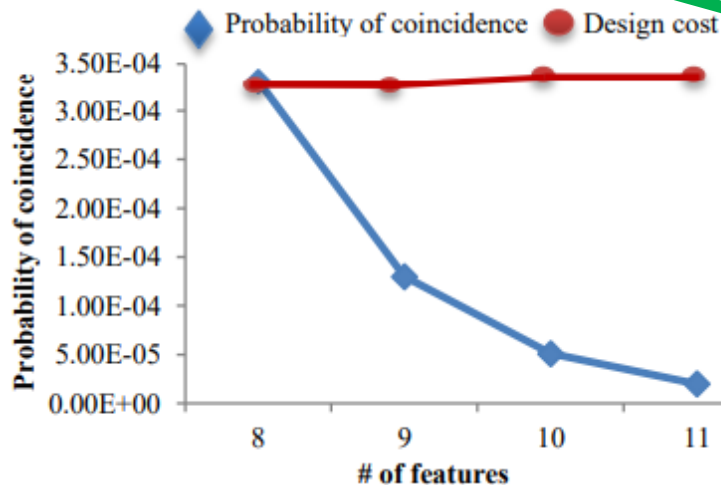
A_m and L_m → maximum area and latency of the design respectively

ω_1 and ω_2 → weights of latency and area in the cost function

Design Cost Comparison of Facial Biometric Approach [4] with Fingerprint Biometric Approach and Baseline

Benchmarks	Design cost of pre-embedded design (baseline)	Design cost of fingerprint biometric approach [4]	Design cost of proposed facial biometric approach
8-point DCT	0.4721	0.5327	0.4727
8-point IDCT	0.4721	0.5327	0.4727
FIR	0.4443	0.4939	0.4443
MPEG	0.37046	0.37080	0.37080

A 15nm NanGate library is used to calculate the latency and area of the design.



Notice that the design cost is comparable to the baseline as there is almost no design overhead involved.

Notice how Design Cost remains almost constant while P_c drops exponentially.

Our CAD tools

Some CAD tools designed by us and hosted @
University of Florida – Cybersecurity Center, USA:

<https://cadforassurance.org/tools/ip-ic-protection/crypto-steganography-tool/>

<https://cadforassurance.org/tools/ip-ic-protection/khc-stego/>

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

Conclusion

The future of VLSI is Energy-Security Tradeoff..

Thank you