Module-3

Forensic Detective Control using Digital Signature based Watermark for IP Core Protection

Dr Anirban Sengupta

Professor, CSE,

IIT Indore, India

Outline

- ❑ Introduction
- ❑ Threat Models of an IP Core
- ❑ Selected Contemporary Approaches
- ❑ Security Modules employed in Digital Signature based Watermark
- ❑ Forensic Detective Control using Digital Signature based Watermark
- ❑ Case study on 8-point DCT used in Image Compression
- ❑ Desirable properties of Digital Signature based Watermark
- ❑ Threat Scenarios and their Countermeasures using Digital Signature based Watermark
- ❑ Analysis on Case Studies

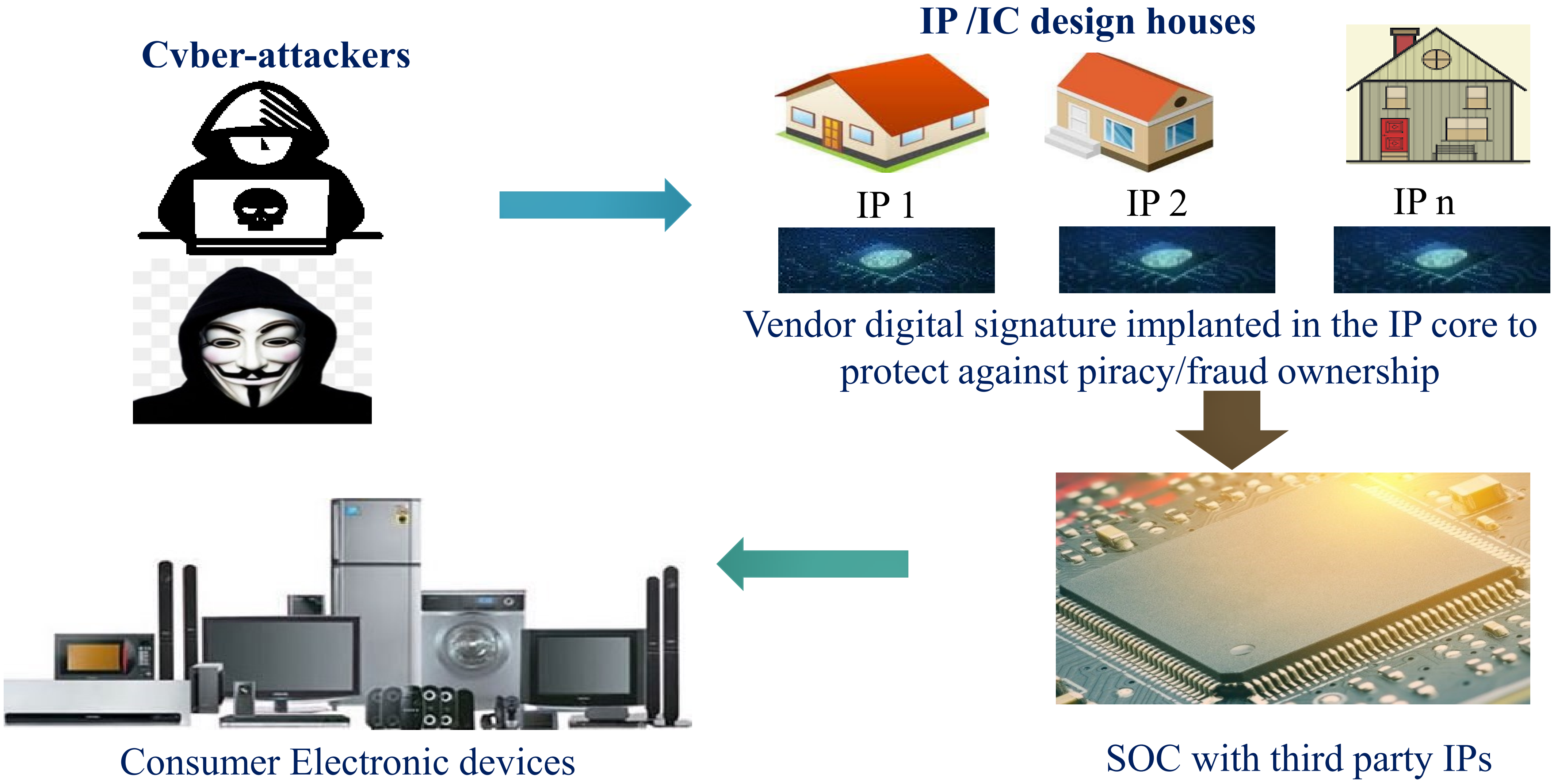
Introduction

- A single design house alone is not responsible for executing all the stages of an integrated circuit (IC) design flow .
- The primary reason behind the globalization of the IC design cycle is the exponential rise in the cost of manufacturing facilities and the pressure of ‘time to marketing’.
- However, because of time and economy constraints, it becomes impractical to realize their IP core into an end fabricated IC all by themselves. Thus they transfer it to production/manufacturing house which are referred as foundries.
- Further, the system-on-chip integrators also buy the IP cores from different fabless design houses/ third party IP (3PIP) vendor to generate a complex electronic system.
- If IP cores designs are unsecured then an adversary present in the remote foundries may exploit their vulnerabilities and can generate pirated/counterfeited/cloned copies of the design illegally and may also claim ownership fraudulently.
- Hence, robust protection during the design process is very crucial.

Cont.

- Limitations of hardware watermarking encourage the designer/owner to produce a more definite proof of signature through a digital signature based watermark, driven through cryptographic hashing and encryption.
- Cryptographic hashing is employed through secure hash algorithms (SHA-512) and private key encryption is performed through RSA.
- Thus signature leaked (compromised) to an adversary anyhow does not help as he/she is not able to meaningfully or scientifically prove his/her rights to the digital signature as he/she is unaware of the encoding rules, hash digest and encryption which are only known to the actual vendor or designer.
- In the consumer electronics (CE) products such as digital camera, television, tablets, laptops the DSP kernels are extensively used.

Cont.



Cvber-attackers

IP /IC design houses

IP 1

IP 2

IP n

Vendor digital signature implanted in the IP core to protect against piracy/fraud ownership

SOC with third party IPs

Consumer Electronic devices

Fig. *IP core protection using Digital Signature*

Threat Model of an IP core

❑ The IP core designs are susceptible to following potential threats which can be thwarted by a digital signature based watermarking:

(i) IP/IC piracy

(ii) IP/IC counterfeiting and cloning

(iii) Fraudulent claim of ownership

Selected Contemporary Approaches

1. Prior Work IP Core Protection using Watermarking

A) Hardware watermarking approaches for DSP. (Koushanfar et al., 2005), presented a behavioural synthesis technique for IP core protection using dynamic watermarking.

- It is based on the concept of embedding artificial design and timing constraints in the design to encode author's signature.
- The watermark presented by the authors successfully satisfies the following properties:
- (a) low overhead
- (b) strong tamper tolerance
- (c) high robustness (d) low signature detection time.

Selected Contemporary Approaches

B) (Sengupta et al., 2018), presented a triple phase watermarking methodology that leverages HLS framework for implanting vendor’s signature into DSP cores.

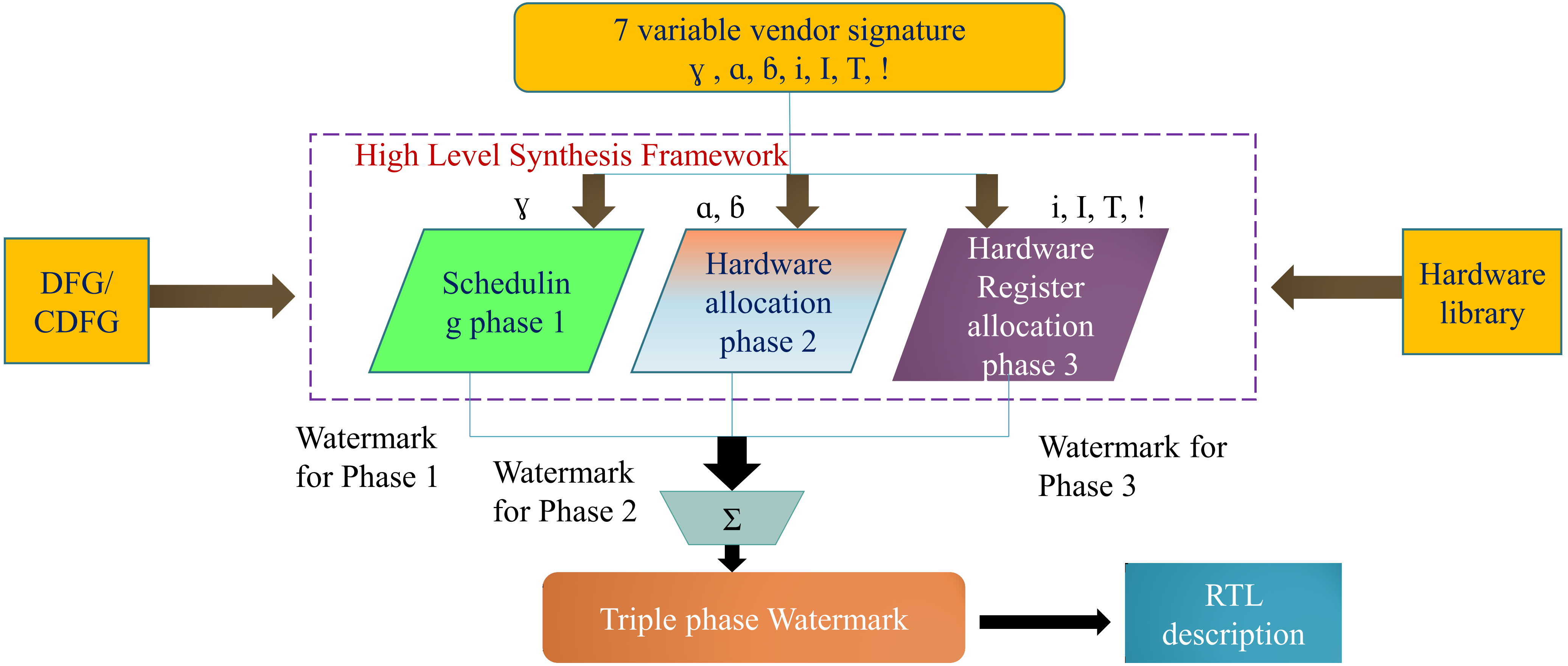
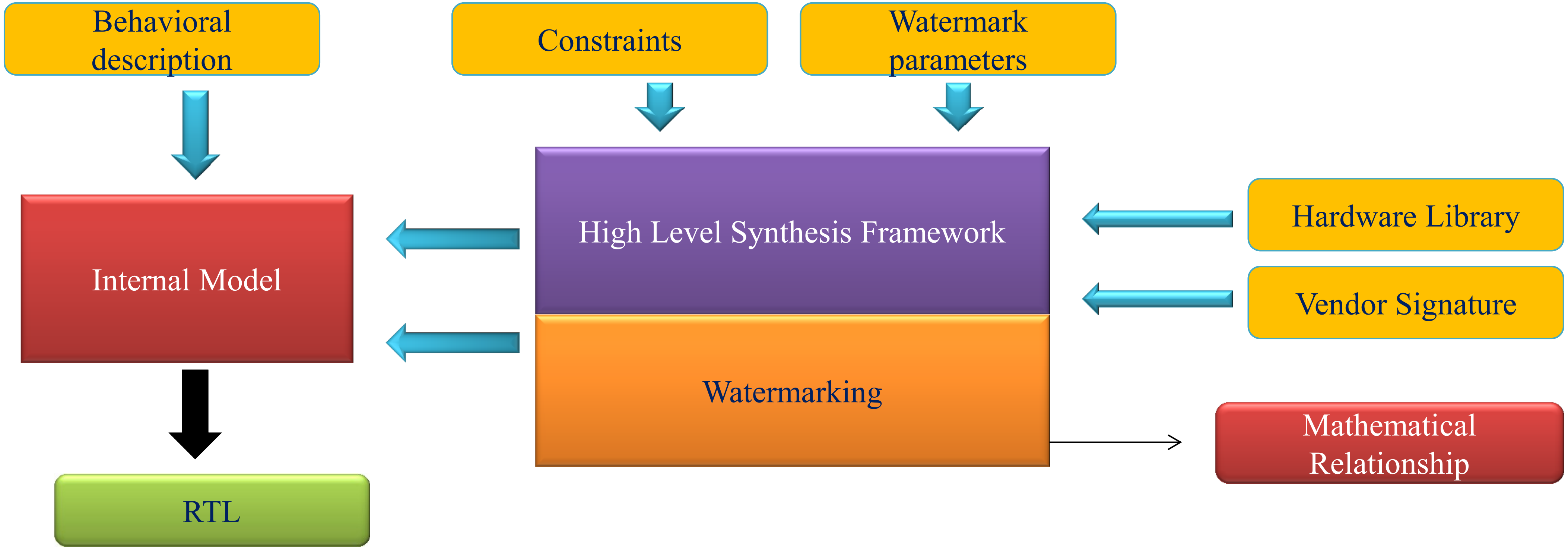


Fig. *High level overview of triple phase watermarking (Sengupta et al., 2018)*

Selected Contemporary Approaches

C) (Gal et al., 2012), presents a watermarking methodology that uses the concept of ‘temporally free slots’ of an IP core design execution cycle.

- The approach generates an IP watermark which is a set of mathematical relations between the IP input data, the initial values of the internal computation and the IP output.



Behavioral description

Constraints

Watermark parameters

High Level Synthesis Framework

Hardware Library

Vendor Signature

Internal Model

Watermarking

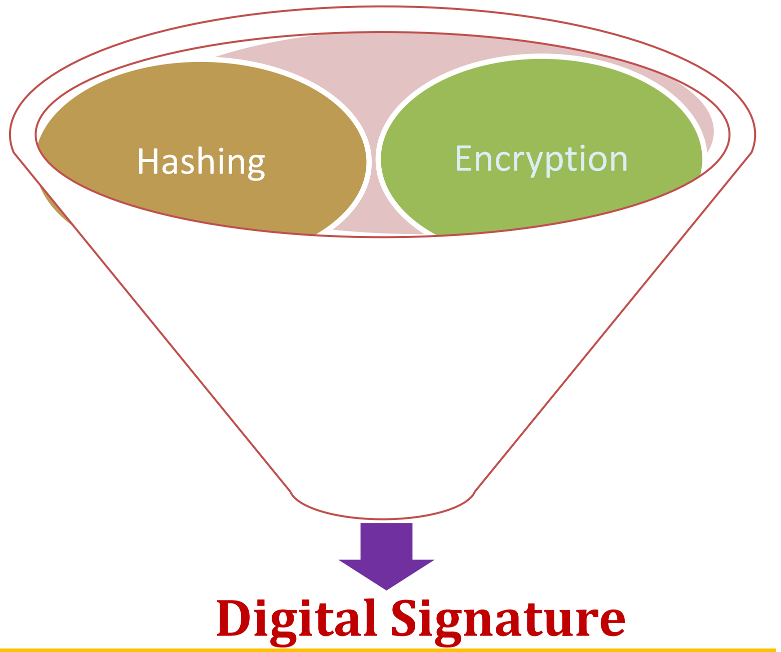
Mathematical Relationship

RTL

Fig. *High level overview of watermarking process of (Gal et al., 2012)*

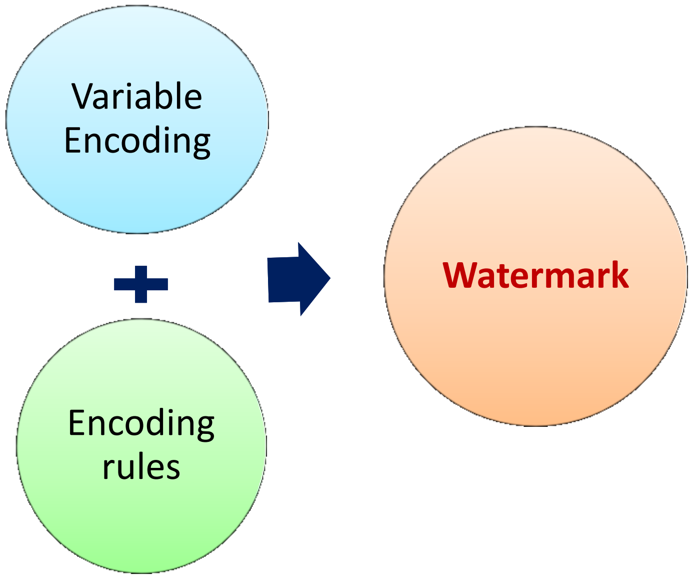
Hardware Watermarking approaches Vs Digital Signature based Watermarking

Digital Signature for Hardware Protection



- ✓ 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

Watermark for Hardware Protection



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

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

Security Modules employed in Digital Signature based Watermark

- ❑ In the process of creating digital signature based watermark, following two primary security modules are employed:

(a) ***crypto hash function- SHA-512***

(b) ***crypto encryption function- RSA.***

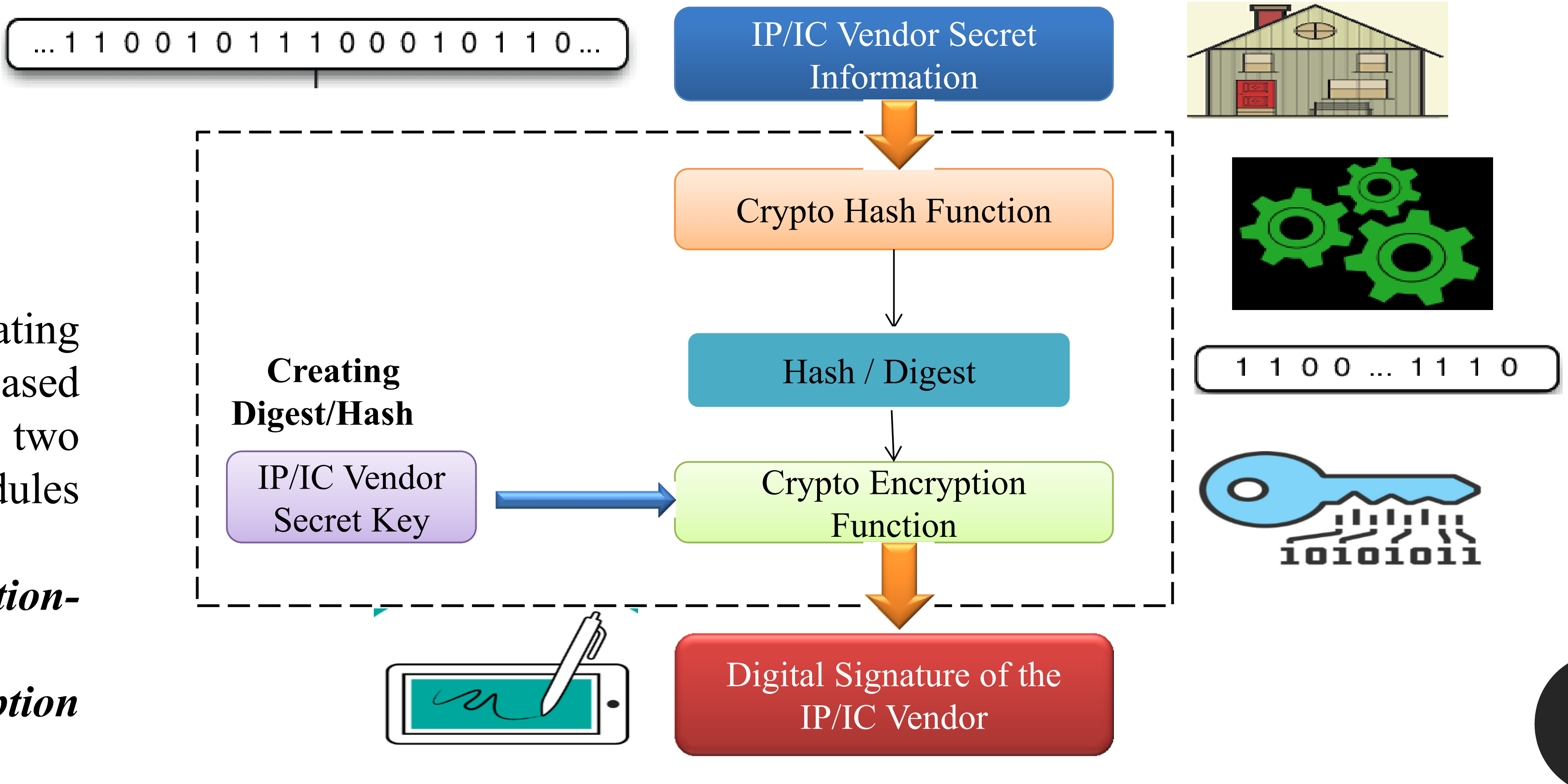
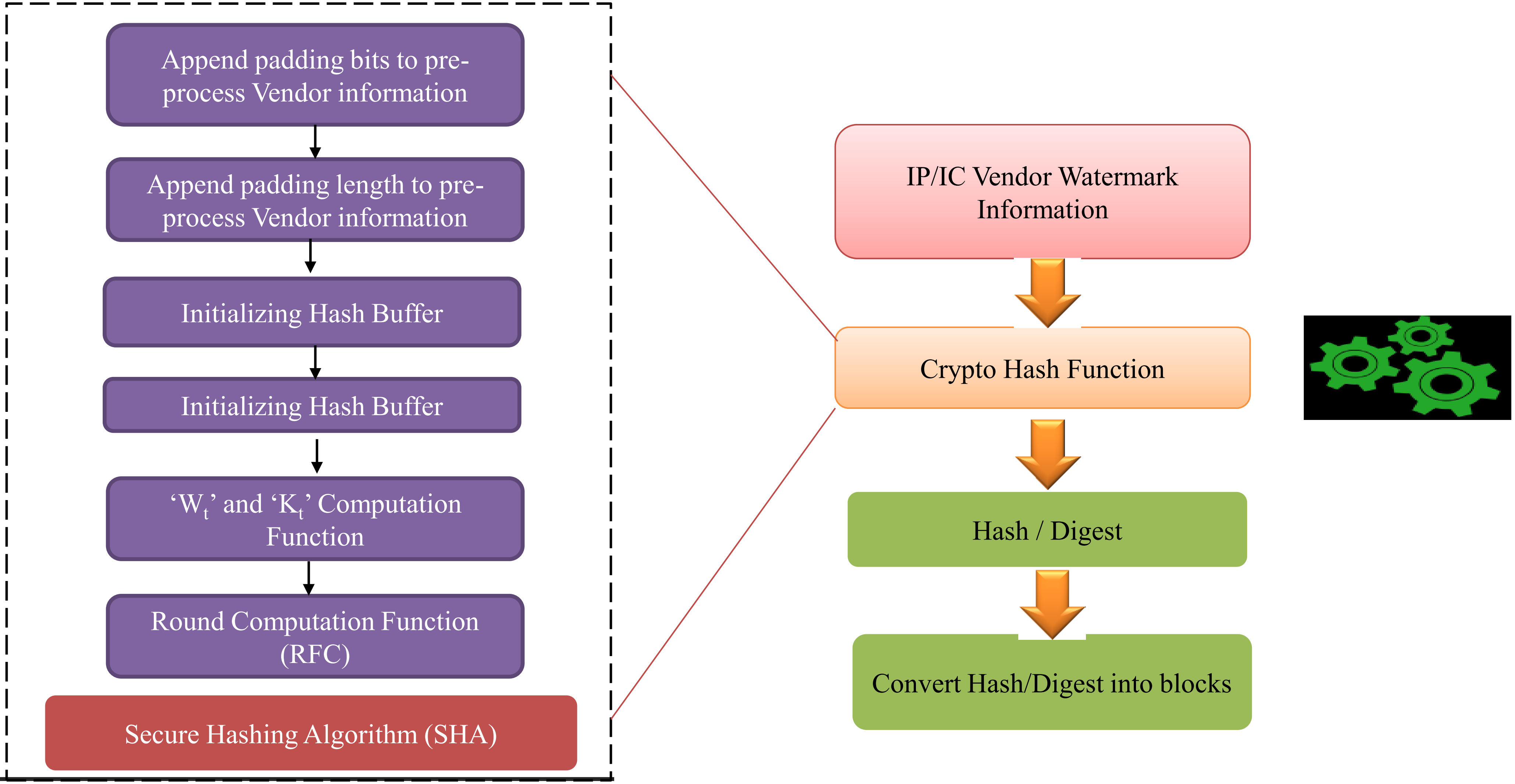


Fig. *High-level process of creating digital signature for IP cores*

(a)crypto hash function- SHA-512



Append padding bits to pre-process Vendor information

Append padding length to pre-process Vendor information

Initializing Hash Buffer

Initializing Hash Buffer

‘W_t’ and ‘K_t’ Computation Function

Round Computation Function (RFC)

Secure Hashing Algorithm (SHA)

IP/IC Vendor Watermark Information

Crypto Hash Function

Hash / Digest

Convert Hash/Digest into blocks

Fig. *Detailed Process of creating Hash/Digest of secret vendor mark*

Cont.

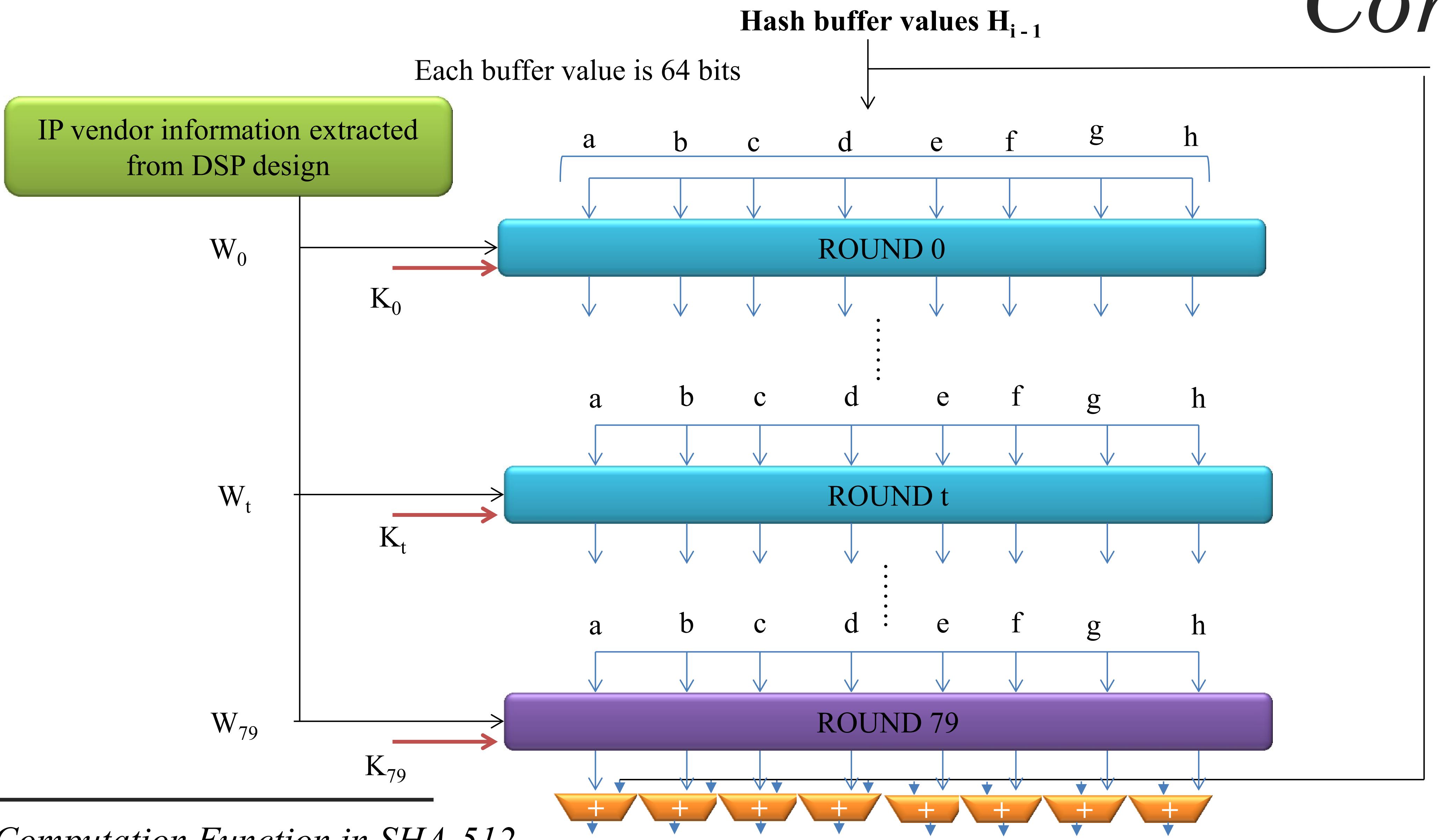
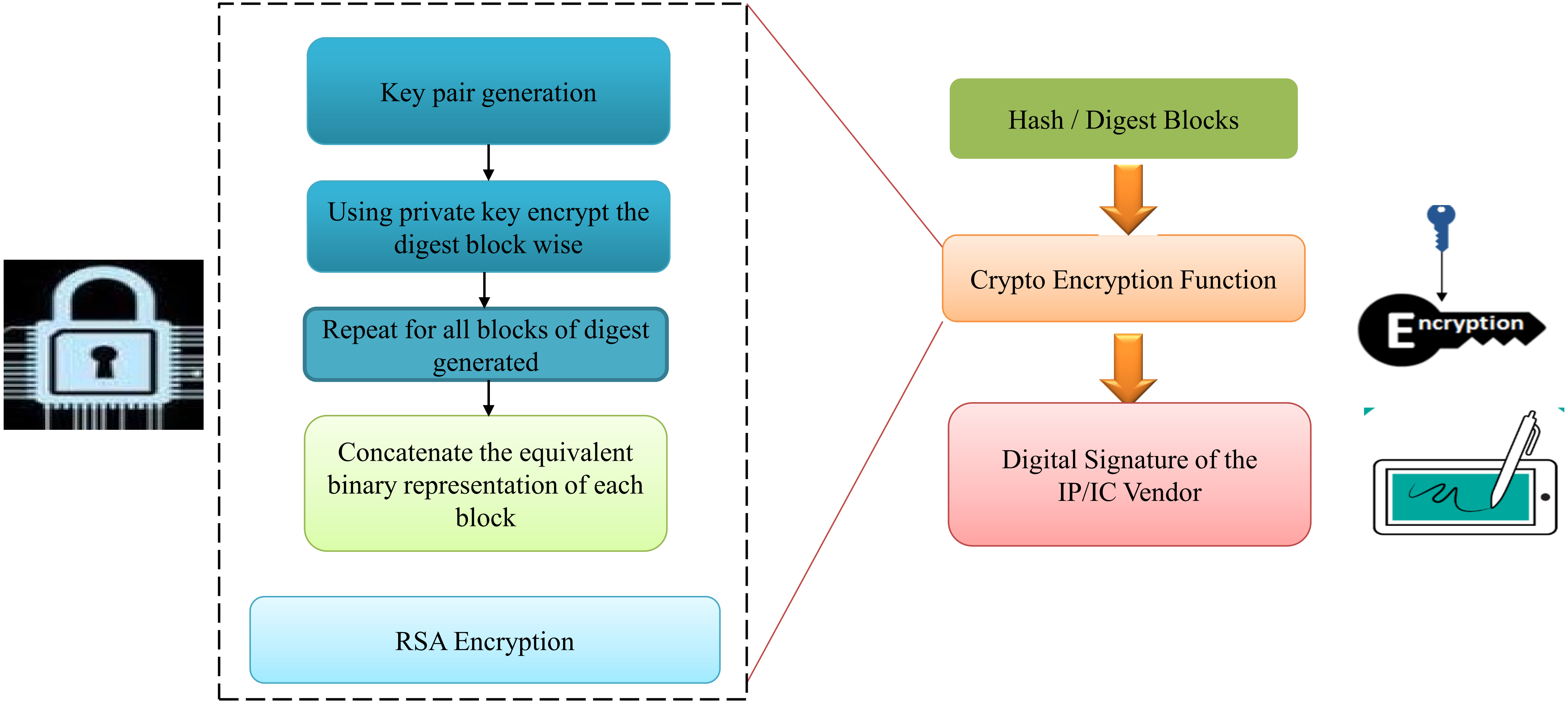


Fig. *Round Computation Function in SHA-512*

(b)Crypto-encryption function- RSA



Key pair generation

Using private key encrypt the digest block wise

Repeat for all blocks of digest generated

Concatenate the equivalent binary representation of each block

RSA Encryption

Hash / Digest Blocks

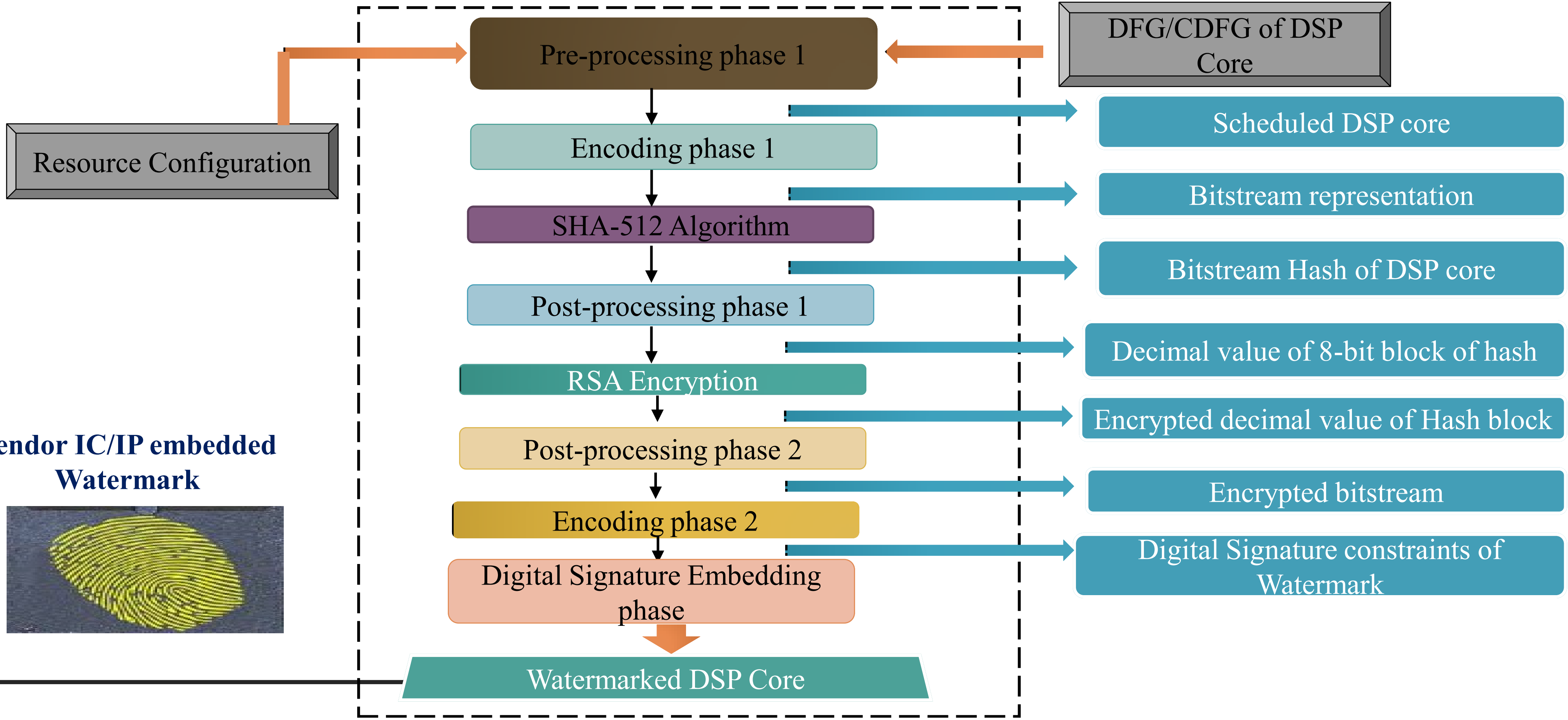
Crypto Encryption Function

Digital Signature of the IP/IC Vendor

Fig. *Detailed Process of creating Digital Signature of IP Vendor Watermark*

Forensic Detective Control using Digital Signature based Watermark

- ❑ This section describes the process of embedding digital signature as watermark into the IP core design followed by the signature detection process during forensic detection.



Resource Configuration

DFG/CDFG of DSP Core

Pre-processing phase 1

Encoding phase 1

SHA-512 Algorithm

Post-processing phase 1

RSA Encryption

Post-processing phase 2

Encoding phase 2

Digital Signature Embedding phase

Watermarked DSP Core

Scheduled DSP core

Bitstream representation

Bitstream Hash of DSP core

Decimal value of 8-bit block of hash

Encrypted decimal value of Hash block

Encrypted bitstream

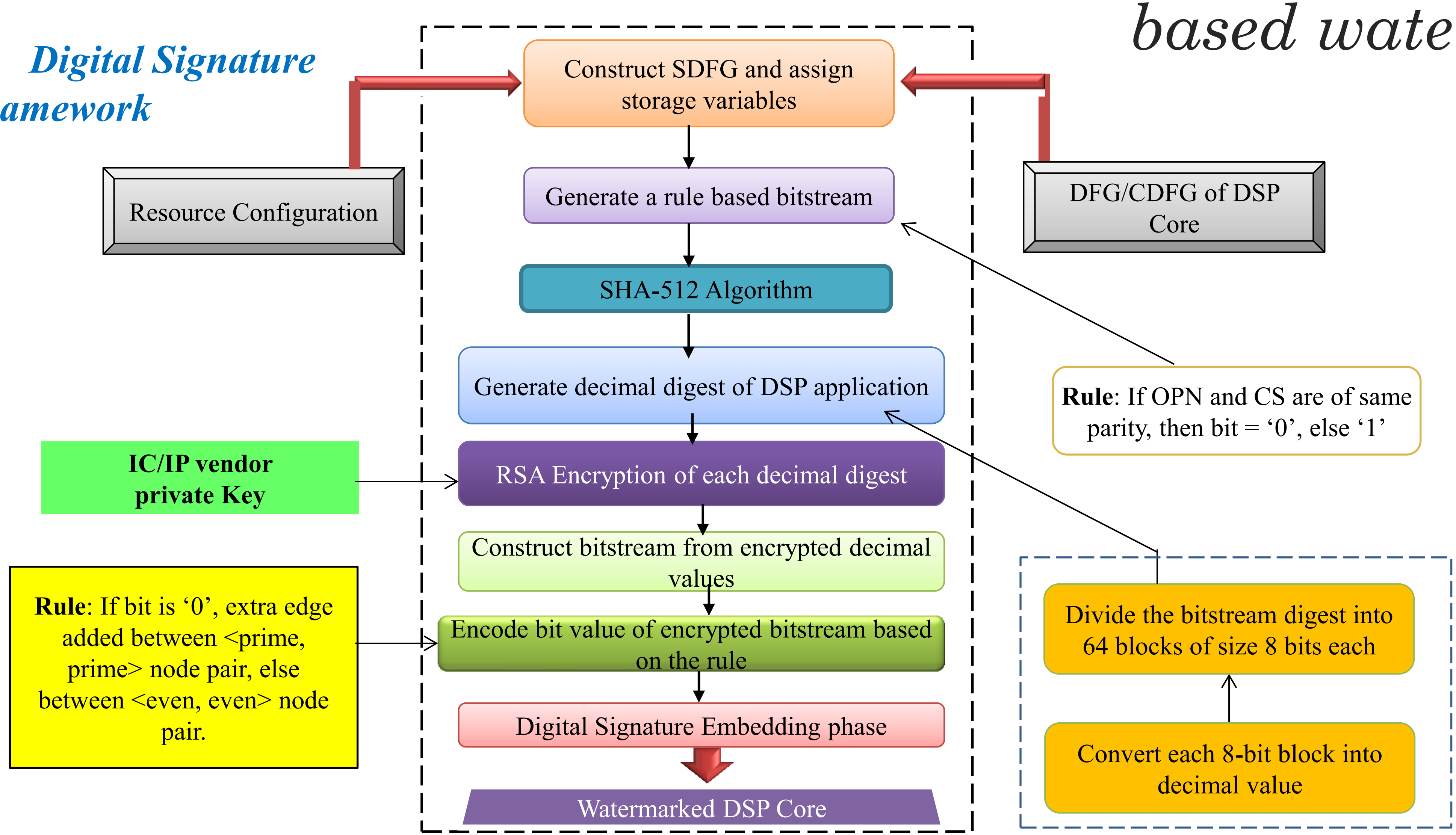
Digital Signature constraints of Watermark

Vendor IC/IP embedded Watermark

Fig. *Digital Signature as Watermark Embedding Process in a DSP based IP Core*

The detailed process of embedding digital signature based watermark

1. Digital Signature Framework



Resource Configuration
Construct SDFG and assign storage variables
DFG/CDFG of DSP Core
Generate a rule based bitstream
SHA-512 Algorithm
Generate decimal digest of DSP application
Rule: If OPN and CS are of same parity, then bit = ‘0’, else ‘1’
IC/IP vendor private Key
RSA Encryption of each decimal digest
Construct bitstream from encrypted decimal values
Rule: If bit is ‘0’, extra edge added between <prime, prime> node pair, else between <even, even> node pair.
Encode bit value of encrypted bitstream based on the rule
Divide the bitstream digest into 64 blocks of size 8 bits each
Convert each 8-bit block into decimal value
Digital Signature Embedding phase
Watermarked DSP Core

Fig. *Detailed Digital Signature as Watermark Embedding Process using encoding (Sengupta et al. 2019a)*

Cont.

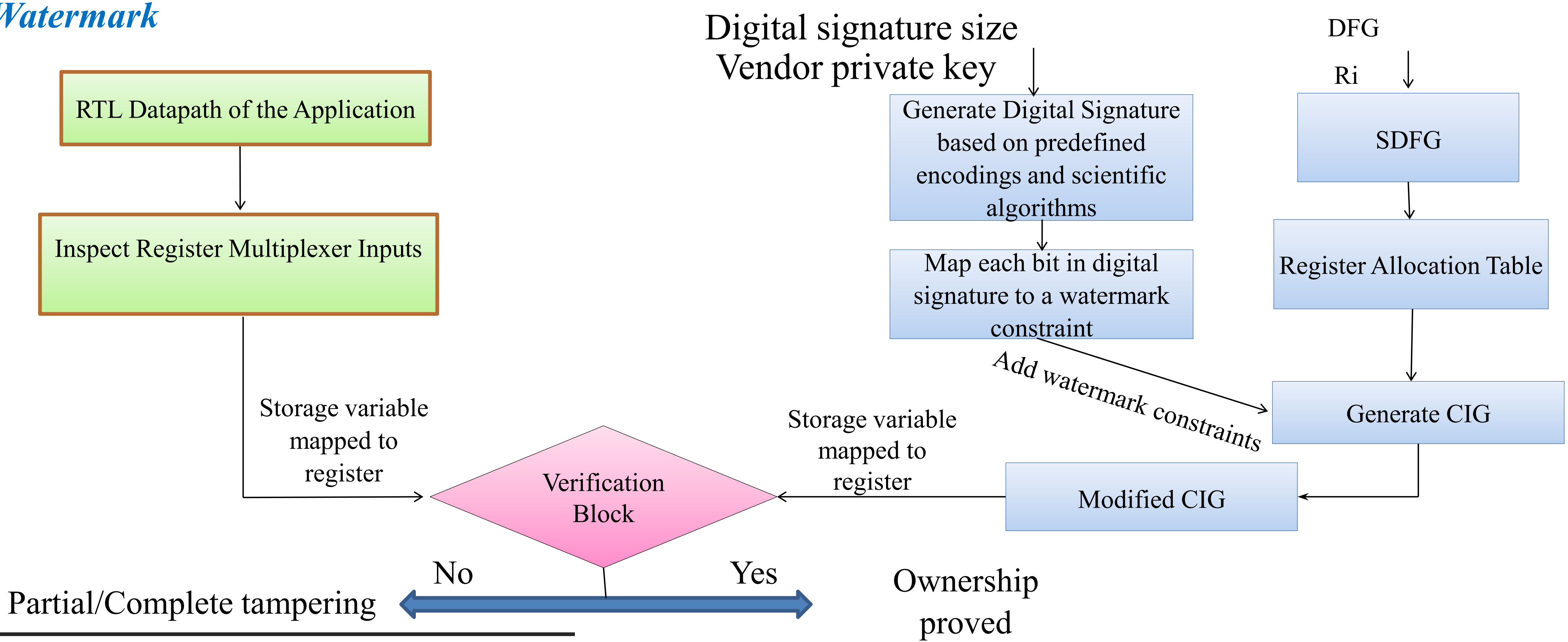
❑ The process of embedding digital signature based watermark can be summarized in following steps:

(1) The DFG of DSP IP core is scheduled based on user provided hardware resource configuration.
(2) In the scheduled DFG, storage variables are assigned to each primary and intermediate inputs/outputs.
(3) Representing all storage variables as nodes, a CIG is created to find the minimum number of registers required to accommodate all primary and intermediate inputs/outputs.
(4) A register allocation table is constructed to show the assignment of each storage variable to a particular register.
(5) Constraints-edges equivalent to each digit of digital signature (obtained through encoding rule presented in Table 3.2) are listed.
(6) All the constraints-edges representing secret vendor digital signature are added into the CIG representing watermark.
(7) The register allocation table is modified after embedding digital signature based watermark constraints into the CIG.

Cont.

2. Detection Process of Digital Signature based Watermark

Detection of digital signature is very crucial to resolve ownership conflict and as well as to detect IP/IC piracy, counterfeiting and cloning.



Digital signature size
Vendor private key

DFG

Ri

Generate Digital Signature based on predefined encodings and scientific algorithms

SDFG

Map each bit in digital signature to a watermark constraint

Register Allocation Table

Add watermark constraints

Generate CIG

Modified CIG

RTL Datapath of the Application

Inspect Register Multiplexer Inputs

Storage variable mapped to register

Verification Block

Storage variable mapped to register

No

Yes

Partial/Complete tampering

Ownership proved

Fig. *Digital signature detection process (Sengupta et al., 2019b)*

Case study on 8-point DCT used in Image Compression

- ❑ Embedding watermark during HLS is very crucial in the context of DSP/multimedia IP cores because of the following reasons:
- It protects the IP core design at higher abstraction level from IP infringements.
- Design remains secured at subsequent lower abstraction levels such as RTL, gate level, layout level etc from IP infringements.
- Highly complex electronic DSP kernels designs which are harder to describe directly at lower abstraction level can easily be secured through watermark at higher abstraction level (through HLS framework).
- Embedding watermark usually always adds extra cost/ overhead to the design. However, HLS framework enables designer to optimize design cost/overhead through design space exploration (DSE).
- Therefore, the design constraints such as area, delay and power can be optimized during watermark embedding process through HLS framework.

Demonstration Example

- ❑ The process of securing the 8-point DCT design using digital signature based watermark is illustrated in two sub-processes:

1. *Digital signature generation corresponding to an 8-point DCT core*
2. *Embedding of digital signature as watermark into the 8-point DCT core*

- ❖ The process of generating digital signature corresponding to an 8-point DCT design is carried out through following steps:

a) The DFG representing the 8-point DCT is transformed into scheduled DFG using LIST scheduling algorithm as shown below:

1.Digital signature generation corresponding to an 8-point DCT core

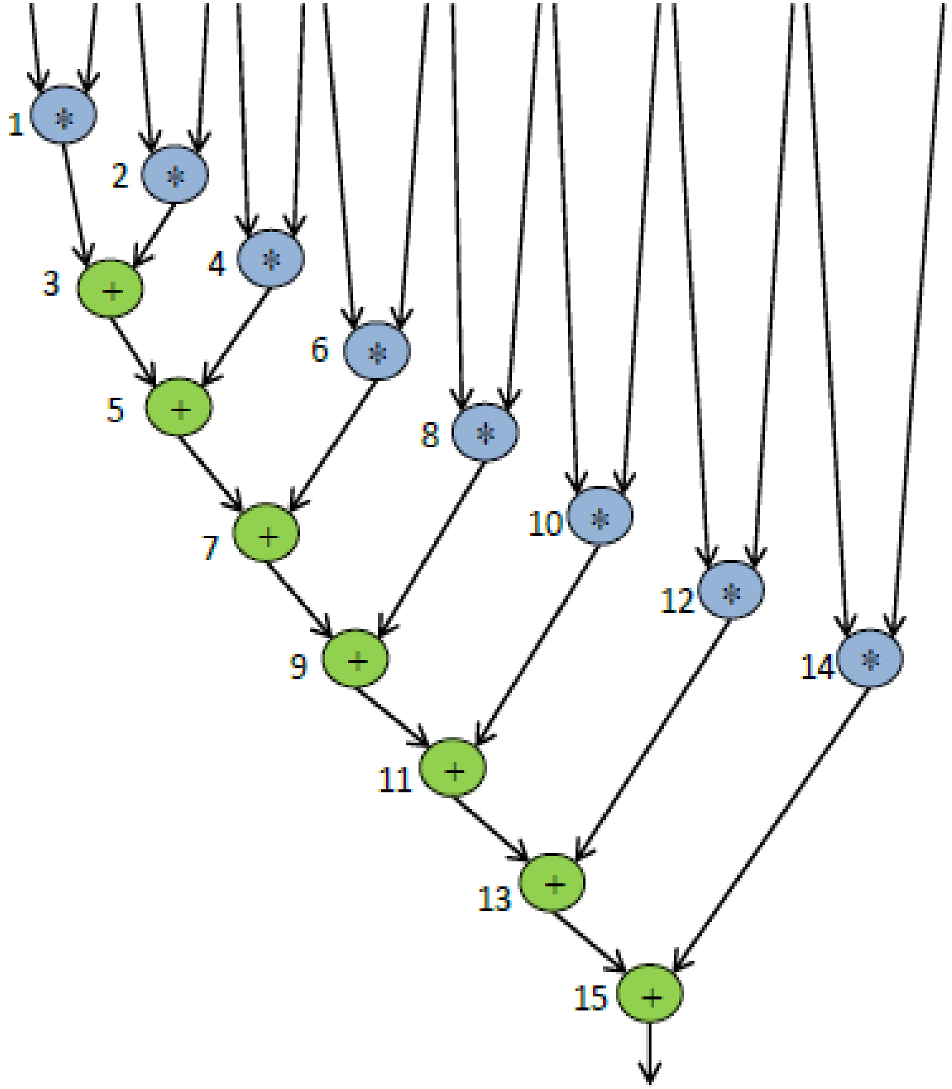


Fig. *Data Flow Graph of 8-point DCT core used in image compression*

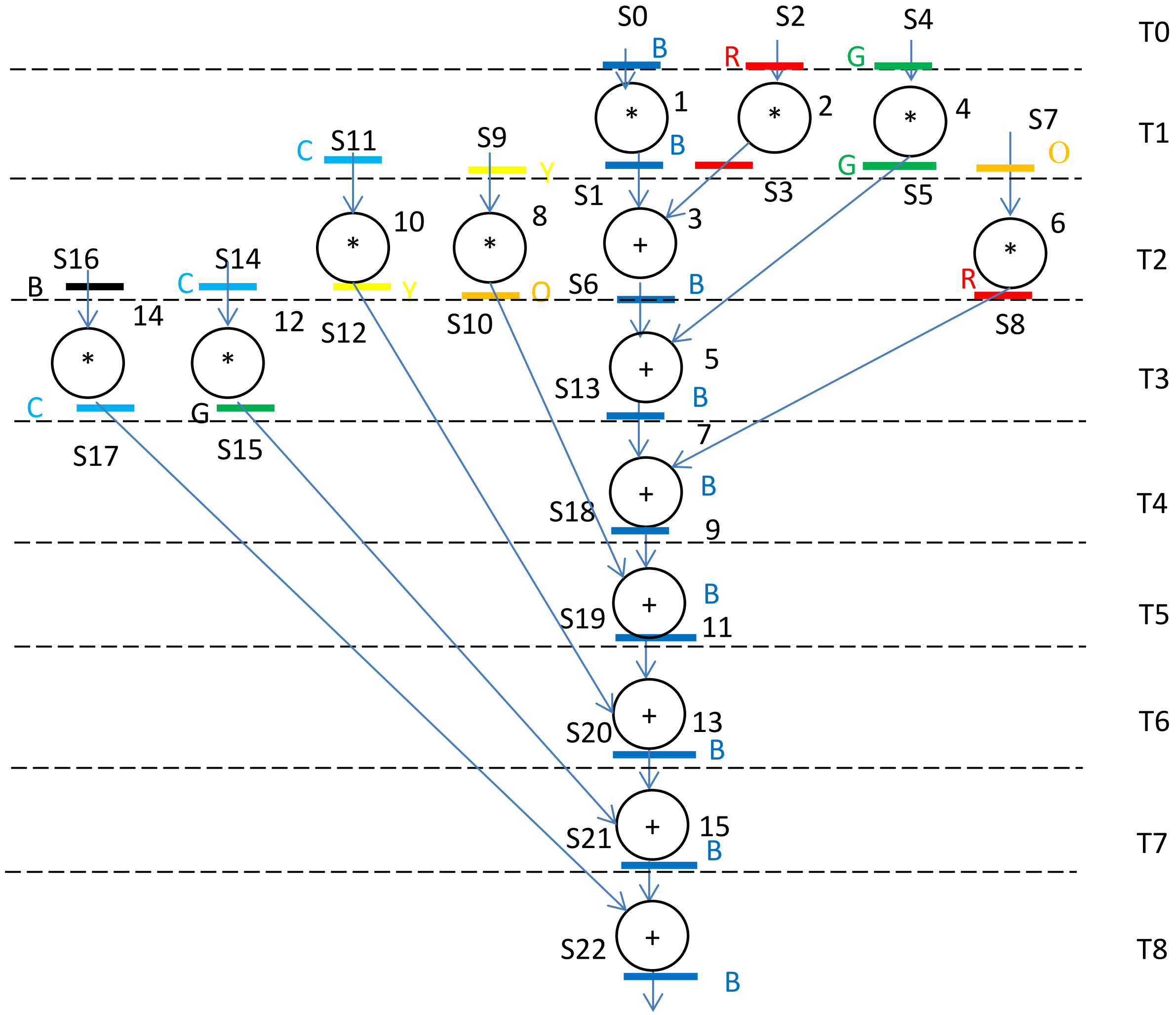


Fig. *Scheduled and hardware allocated 8-point DCT using 1 (+) and 3 (*) BEFORE implanting Digital signature*

Cont.

b) In the scheduled DFG based on the parity of operation number and its corresponding control step number, the 8-point DCT design is encoded into a bitstream (according to the IP vendor rule). The generated bitstream representing the initial vendor secret mark information is “011100100011011”.

c) The bitstream obtained from previous step is fed to SHA-512 algorithm which transforms it into a 512-bit hash digest.

❑ This transformation occurs in following sub- steps:

1. The bitstream is processed to generate 1024-bit block required as input for main hash algorithm - SHA-512. To do so, first the bitstream is padded with a fixed bit pattern (1 followed by sequence of 000…) to construct an 896-bit block. Thereafter, 128-bit binary representation of the initial bit-stream length is appended to construct a 1024-bit block which is as follows: 01110010 00110111 00000000…….. 00000000 00000000 00001111 (1024 bits)
2. All eight hash buffers are initialized with their fixed default values
3. A 64-bit word (W_t) is extracted/computed from 1024-bit block for each iteration of round function
4. 80 iterations of round function are executed using W_t, hash buffer values and constant (K_t)
5. The output of 80th round is added with the initial values of hash buffers (in the first round) to obtain the final hash-digest of 512-bit. In this way, the hash-bitstream is generated.

Cont.

d) The 512-bit hash-bitstream is partitioned into 64 blocks of eight bits each. Further, each block is translated into its equivalent decimal value.

e) The vendor private key (d) is computed to be 131 using RSA key generator.

f) Each decimal value of hash-bitstream is encrypted one by one using the private key (d=131) through RSA encryption algorithm.

g) All the encrypted binary values are concatenated to construct a single continuous bitstream.

h) A part of the encrypted hash-bitstream obtained from previous step is selected as digital signature. The respective digital signature size can be chosen by the vendor based on watermark strength required and design-cost trade-off.

First 16 decimal values of hash-bitstream and corresponding encrypted decimal and binary equivalent (for the sake of brevity).

RSA Decimal Input	Encrypted Decimal Output	Encrypted Binary Equivalent
247	304	100110000
59	70	1000110
175	74	1001010
18	18	10010
18	18	10010
113	56	111000
179	202	11001010
110	2	10
75	37	100101
137	188	10111100
15	230	11100110
137	188	10111100
230	32	100000
61	150	10010110

2. Embedding of digital signature as watermark into the 8-point DCT core

- The digital signature is processed to transform it into equivalent secret design watermark constraints.
- Thereafter, these digital signature constraints are embedded as watermark into the 8-point DCT design.

❑ The various steps of embedding digit signature as watermark are as follows:

a). The CIG of scheduled DFG corresponding 8-point DCT core and the corresponding register allocation for all storage variables (S0-S22) is created.

Cont.

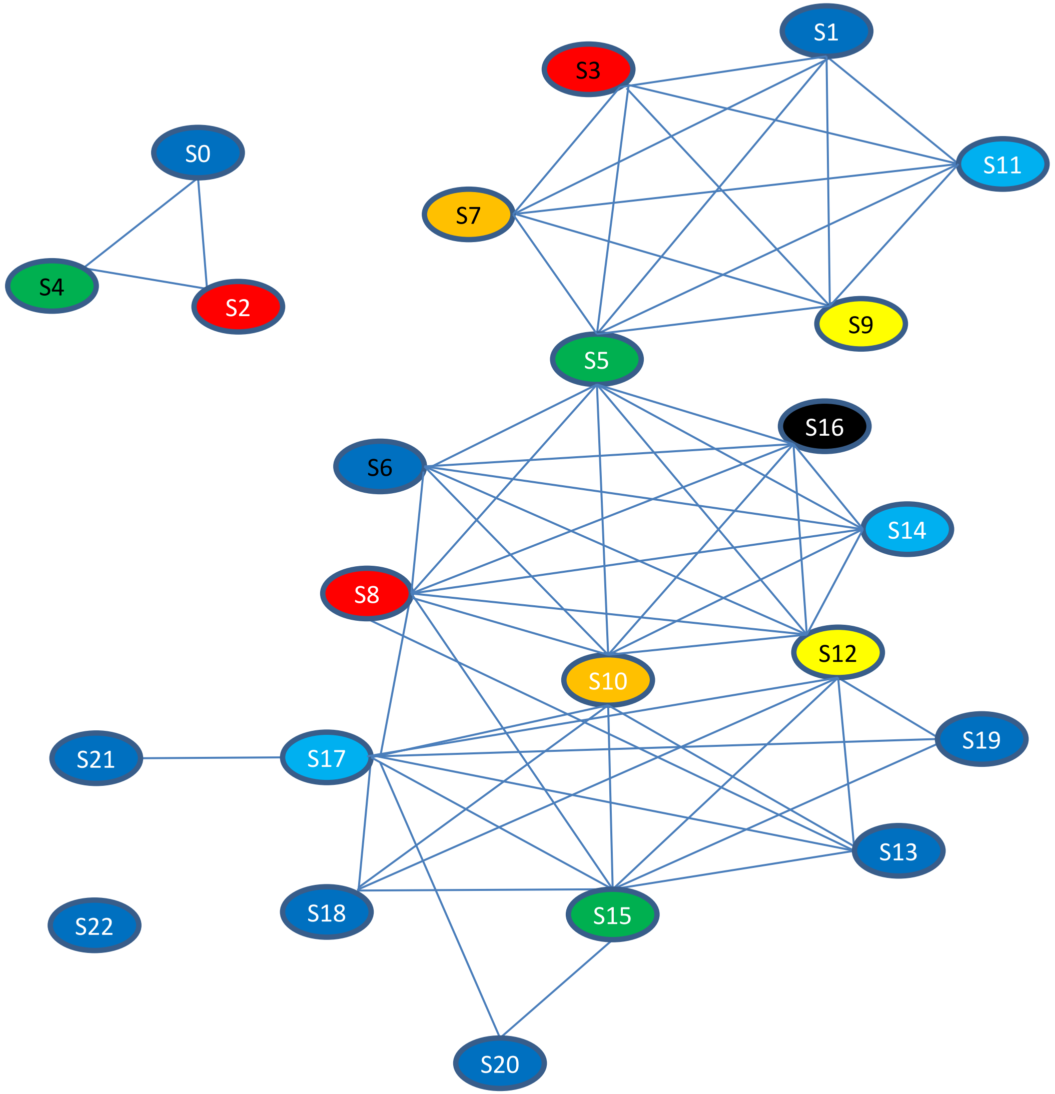


Fig. *A CIG of 8-point DCT before embedding Digital S*

Register allocation table of 8-point DCT **before** embedding digital signature

Control Step	B	R	G	O	Y	C	Bl
T0	S0	S2	S4	-	-	-	-
T1	S1	S3	S5	S7	S9	S11	-
T2	S6	S8	S5	S10	S12	S14	S16
T3	S13	S8	S15	S10	S12	S17	-
T4	S18	-	S15	S10	S12	S17	-
T5	S19	-	S15	-	S12	S17	-
T6	S20	-	S15	-	-	S17	-
T7	S21	-	-	-	-	S17	-
T8	S22	-	-	-	-	-	-

Cont.

b). Each digit of digital signature is encoded into watermarking constraints to be embedded into the design of 8-point DCT core.

- According to the encoding rules, the mapping of each signature bit to an extra edge, required for embedding into the CIG, is shown in Table

List of constraints edges corresponding to IP vendor digital signature

Bits in digital signature (Q=15)	Corresponding additional edges
1	<S2,S4>
0	<S2,S3>
0	<S2,S5>
1	<S2,S6>
1	<S2,S8>
0	<S2,S7>
0	<S2,S11>
0	<S2,S13>
0	<S2,S17>
1	<S2,S10>
0	<S2,S19>
0	<S3,S5>
0	<S3,S7>

Demonstration Example

c). All listed encoded edges <Si, Sj> are added into the CIG as additional secret edges.

- These inserted additional edges represent the covert watermark-constraints in the design.
- However, out of 15 only 12 potential edges viz. *(S2, S3), (S2, S5), (S2, S6), (S2, S8), (S2, S7), (S2, S11), (S2, S13), (S2, S17), (S2, S10), (S2, S19), (S2, S12), (S2, S14)* are newly added as watermark constraints and remaining three edges *<S2, S4>, <S3, S5>, <S3, S7>* need not be added into the CIG, as these three edges already exists into the CIG by default.

d). The register allocation of storage variables is modified after adding aforementioned 12 secret edges into the CIG.

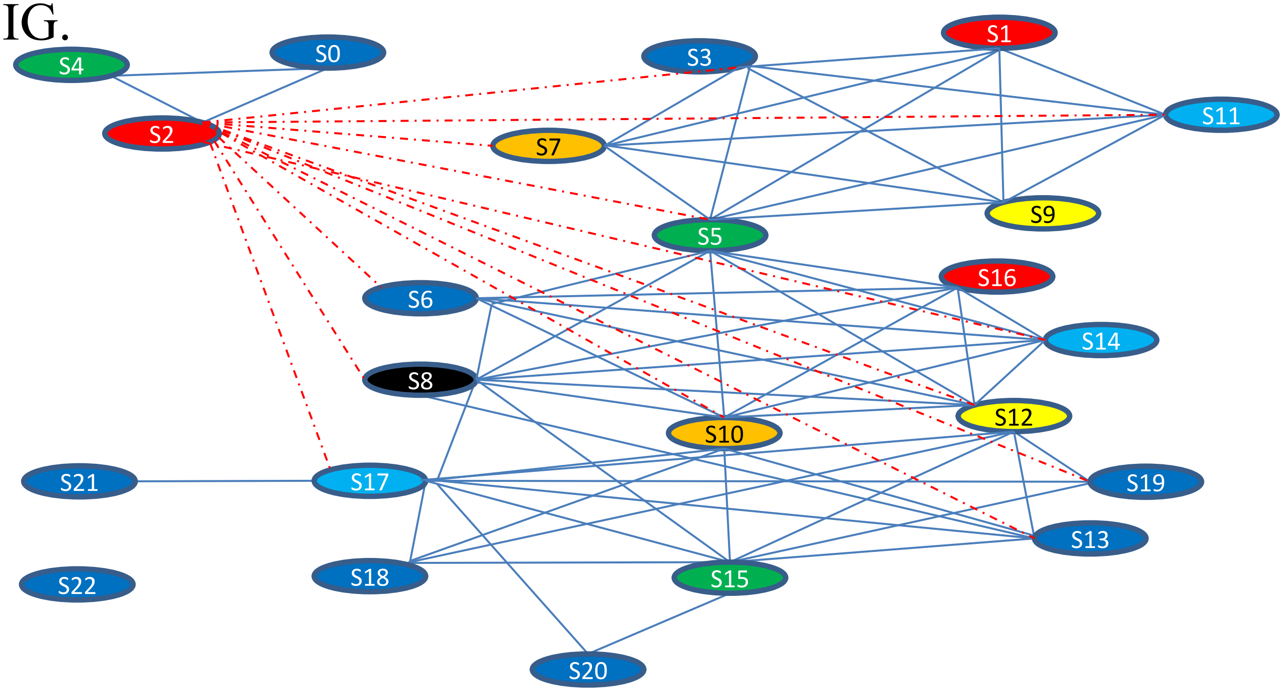


Fig. *A CIG of 8-point DCT* ***after*** *embedding Digital Signature*

Register allocation table of 8-point DCT **after** embedding digital signature (Q= 15)

Control Step	B	R	G	O	Y	C	Bl
T0	S0	S2	S4	-	-	-	-
T1	S3	S1	S5	S7	S9	S11	-
T2	S6	S16	S5	S10	S12	S14	S8
T3	S13	-	S15	S10	S12	S17	S8
T4	S18	-	S15	S10	S12	S17	-
T5	S19	-	S15	-	S12	S17	-
T6	S20	-	S15	-	-	S17	-
T7	S21	-	-	-	-	S17	-

Desirable properties of Digital Signature based Watermark

(a)High Resiliency

(b)Strong Tamper Tolerance

(c)Low Design Overhead

(d)Correct Functionality

(e)Low Signature Embedding and Detection Time

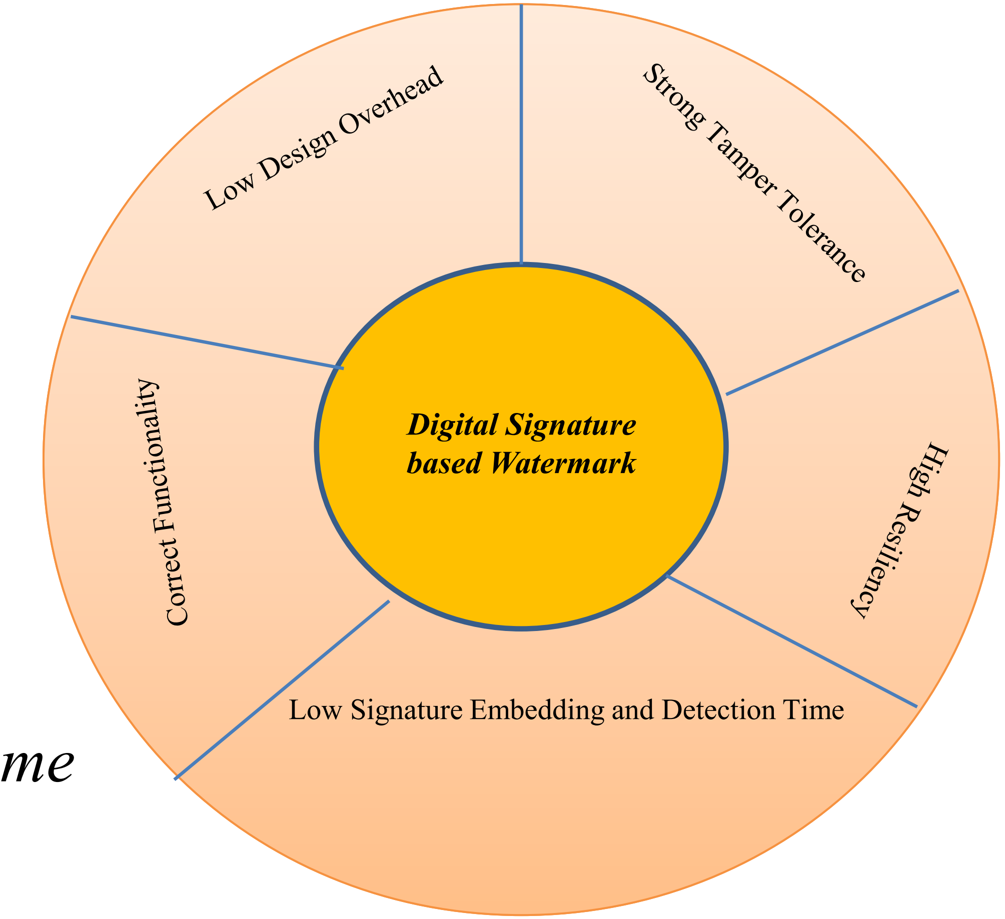


Fig. *Desirable properties of Digital Signature based watermark*

Threat Scenarios and their Countermeasures using Digital Signature based Watermark

- Consider a scenario in which two different parties ‘T’ and ‘F’ are involved where party ‘T’ represents the owner/vendor of the digital signature embedded IP core whereas party ‘F’ represents an adversary such as SoC integrator/IC manufacturer.
- The possible attacks and their countermeasures exploiting digital signature based watermark are discussed as follows:

1) *Unauthorized Signature-Constraints Insertion*

   - In this situation, if ‘F’ claims the ownership of the IP core, his/her claim can easily be nullified as the design contains the digital signature constraints of both parties ‘T’ and ‘F’; whereas the original digital signature embedded IP core of ‘T’ contains his/her signature constraints only.

1) *Original Signature Tampering*

   - Tampering with original digital signature is not easy because the distributed digital signature throughout the entire design upsets the attempt of modification in all signature constraints.
   - Further, it may alter the area overhead and latency of the original signature embedded IP core of ‘T

1) *Unintended Signature -Constraints Extraction*

   - In this scenario, ‘F’ performs the back engineering of embedding watermark in the IP core of ‘T’ with the intention of extracting his/her own signature-constraints.

Analysis on Case Studies

❑ The impact of different signature size on security and design cost has been assessed based on following criteria:

- Probability of coincidence (P^c)
- Extra register required after embedding digital signature as watermark
- Post-watermark embedded design cost

1. Security Analysis

Security achieved through digital signature based watermark is assessed in terms of the probability of coincidence:

$$(P^c) \text{ metric given as follows } P^c = \left(1 - \frac{1}{n}\right)^k \qquad (1)$$

- Where, $'P^{c}{}'$ denotes the probability of coincidence,
- 'n' denotes the number of colours used in the CIG before implanting digital signature and
- 'k' denotes the number of digits in digital signature i.e. the digital signature size (Q).

(Sengupta and Roy, 2017; Sengupta and Roy, 2018)

Cont.

- The impact of three different signature sizes (Q=60, 120, 240) on probability of coincidence has been shown in the table.

DSP applications	# of colours used in CIG (n)	Probability of coincidence (P^c)		
		Q = 60	Q= 120	Q = 240
IIR BUTTERWORTH	5	1.5325x10^{-6}	2.3485x10^{-12}	5.5157 x10^{-24}
BPF	6	1.7747x10^{-5}	3.1496x10^{-10}	9.9198x10^{-20}
JPEG SAMPLE	10	1.7970x10^{-3}	3.2292x10^{-6}	1.0428x10^{-11}
JPEG IDCT	29	0.1218	0.0148	2.1999x10^{-4}
MESA MATRIX MULTIPLICATION	23	0.0695	4.8237x10^{-3}	2.3268x10^{-5}

- Comparison with the contemporary watermarking approach for DSP cores:

DSP applications	Percentage reduction in P_c		
	S = 60	S = 120	S = 240
IIR BUTTERWORTH	0	0	0
BPF	81.55	96.60	99.88
JPEG SAMPLE	66.74	88.94	98.78
JPEG IDCT	6.88	13.45	24.84
MESA MATRIX MULTIPLICATION	10.9	20.31	36.5

(Sengupta and Bhadauria, 2016)

Cont.

❑ Design cost of the steganography embedded IP core is evaluated using following cost function:

$$C_d(R_i) = w_1 \frac{L_d}{L_{max}} + w_2 \frac{A_d}{A_{max}} \qquad (4)$$

- Where, $C_d(R_i)$ denotes the stego-embedded design cost with vendor specified resource configuration R_i.
- Here, design cost is evaluated in terms of the design latency and hardware area denoted by L_d and A_d respectively.
- Further, L_{max} and A_{max} denote the maximum execution latency and hardware area respectively and
- w_1, w_2 represent the user specified weights both fixed at 0.5 to assign equal preference.

Design Cost Analysis

- However, the digital signature based watermark approach does not affect the execution latency therefore, only the extra registers required (after embedding digital signature) affect the overall design cost.

Impact of variation in digital signature size (Q) on storage overhead

DSP applications	**# of storage variables**	**# of registers before applying proposed digital signature**	**# of edges added resulting into 'R^e' more registers**			
			$R^e = 0$	$R^e = 1$	$R^e = 2$	$R^e = 3$
IIR BUTTERWORTH	14	5	15	NA	NA	NA
BPF	36	6	15	30,60	NA	NA
JPEG SAMPLE	45	10	15	30,60,120	NA	NA
JPEG IDCT	136	29	15,30,60,120,240	-	-	-
MESA MATRIX MULTIPLICATION	108	23	15,30,60,120,240	-	-	-

Percentage decrement in # of registers required using digital signature based watermark in contrast to (Sengupta and Bhadauria, 2016)

DSP applications	**Percentage reduction in # of registers required**		
	S = 60	S = 120	S = 240
IIR BUTTERWORTH	0	0	0
BPF	22.22	0	0
JPEG SAMPLE	21.43	21.43	0
JPEG IDCT	3.33	6.45	6.45
MESA MATRIX MULTIPLICATION	8	11.54	11.54

Design Cost Analysis

Comparative study of digital signature based watermark and (Sengupta and Bhadauria, 2016) in terms of design cost

DSP applications	**Q = 30**		**Q = 60**		**Q = 120**		**Q = 240**	
	Design cost (digital signature based watermark)	Design cost (Sengupta and Bhadauria, 2016)	Design cost (digital signature based watermark)	Design cost (Sengupta and Bhadauria, 2016)	Design cost (digital signature based watermark)	Design cost (Sengupta and Bhadauria, 2016)	Design cost (digital signature based watermark)	Design cost (Sengupta and Bhadauria, 2016)
IIR BUTTERWORTH	NA	NA	NA	NA	NA	NA	NA	NA
BPF	0.4134	0.4145	0.4134	0.4143	NA	NA	NA	NA
JPEG SAMPLE	0.4294	0.4506	0.4294	0.4512	0.4294	0.4512	NA	NA
JPEG IDCT	0.2160	0.2333	0.2160	0.2333	0.2160	0.2335	0.2160	0.2335
MESA MATRIX MULTIPLICATION	0.2687	0.2790	0.2687	0.2792	0.2687	0.2795	0.2687	0.2795

A. Sengupta, S. Bhadauria (2016), ‘Exploring Low Cost Optimal Watermark for Reusable IP Cores During High Level Synthesis,

Conclusion

- ✓ A solution for ensuring the security of IP cores against various hardware threats such as IP piracy, counterfeiting, cloning and false claim of ownership, is presented using digital signature based watermarking approach.
- ✓ The digital signature based watermarking approach is capable to provide more definite and meaningful proof of signature.
- ✓ The standard secure hashing algorithm (SHA-512), RSA encryption and pre-defined encoding rules enable the digital signature based watermarking approach to produce more definite and meaningful signature.

References

1. B. Colombier, L. Bossuet (2015), ‘Survey of hardware protection of design data for integrated circuits and intellectual properties,’ *IET Computers & Digital Techniques*, vol. 8(6), pp. 274-287.
2. A. Sengupta (2016), ‘Intellectual Property Cores: Protection designs for CE products,’ *IEEE Consumer Electronics Mag*, vol. 5, no. 1, pp. 83-88.
3. A. Sengupta (2017), ‘Hardware Security of CE Devices [Hardware Matters],’ *IEEE Consumer Electronics Mag,* vol. 6(1), pp. 130-133.
4. A. Sengupta, S. Bhadauria (2016), ‘Exploring Low Cost Optimal Watermark for Reusable IP Cores During High Level Synthesis,’ *IEEE Access*, vol. 4, pp. 2198-2215,.
5. A. Sengupta, S. P. Mohanty (2019) 'Advanced encryption standard (AES) and its hardware watermarking for ownership protection', *Book: 'IP Core Protection and Hardware-Assisted Security for Consumer Electronics'*, e-ISBN: 9781785618000, pp. 317-335.
6. A. Sengupta, S. P. Mohanty (2019), 'IP core and integrated circuit protection using robust watermarking', *Book: 'IP Core Protection and Hardware-Assisted Security for Consumer Electronics*', e-ISBN: 9781785618000, pp. 123-170.
7. D. Ziener, J. Teich (2008), ‘Power signature watermarking of IP cores for FPGAs,’ *J. Signal Process. Syst*., vol. 51(1), pp. 123-136. A. Sengupta, E. R.Kumar, and N. P.Chandra (2019), " Embedding Digital Signature using Encrypted-Hashing for Protection of DSP cores in CE," in IEEE Transactions on consumer electronics. B. Le Gal, L. Bossuet (2012), ‘Automatic low-cost IP watermarking technique based on output mark insertions,’ *Design Autom. Embedded Syst*., vol. 16(2), pp. 71-92.
8. F. Koushanfar et al. (2005), “Behavioral synthesis techniques for intellectual property protection,” *ACM Trans. Des. Autom. Electron. Syst*., vol. 10(3), pp. 523-545.
9. A. Sengupta, D. Roy (2017), ‘Antipiracy-Aware IP Chipset Design for CE Devices: A Robust Watermarking Approach [Hardware Matters],’ *IEEE Consumer Electronics Mag*, vol. 6(2), pp. 118-124.
10. A. Sengupta, D. Roy (2018), ‘Multi-Phase Watermark for IP Core Protection,’ *Proc. 36th IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1-3.
11. A. Sengupta, D. Roy, S. P. Mohanty (2018), ‘Triple-Phase Watermarking for Reusable IP Core Protection During Architecture Synthesis,’ *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst*, vol. 37(4), pp. 742-755.
12. D. Roy, A. Sengupta (2019), ‘Multilevel Watermark for Protecting DSP Kernel in CE Systems [Hardware Matters],’ *IEEE Consumer Electronics Mag*, vol. 8(2), pp. 100-102.

Thank You