Triple-Phase Watermarking for Reusable IP Core Protection During Architecture Synthesis

Published in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)

A. Sengupta, D. Roy and S. P. Mohanty, "Triple-Phase Watermarking for Reusable IP Core Protection During Architecture Synthesis," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 37, no. 4, pp. 742-755, April 2018.

• Introduction

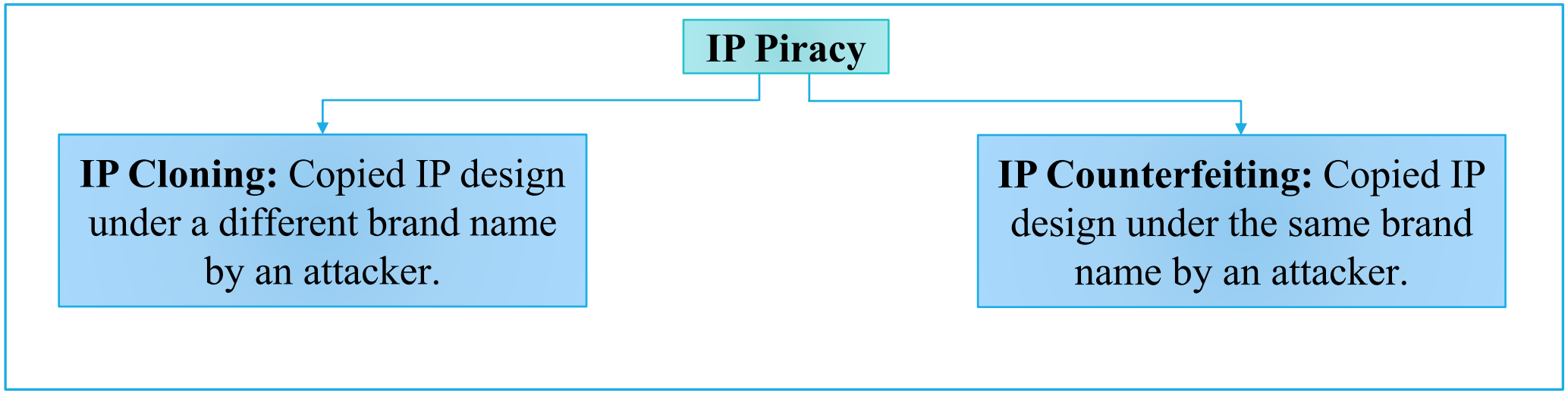
- Consumer electronics (CE) play a pivotal role in transforming the vision of emerging smart cities into reality.
- The current generation of CE design process is massively dependent on global IP supply chains.
- In such a CE-based framework, security and protection of its' intellectual property (IP) cores are considered as major challenges.
- Thus, the use of secured IPs is of paramount importance.

Fig. 1. IP protection of CE hardware

• Threat Model

➢ With the rise of globalization in hardware design and manufacturing, along with increasing competition among IP vendors, threats such as:

1. IP piracy
2. False claim of ownership.



• Novel contribution of this paper

➢ The novel contributions of this paper in terms of improving the state-of-art are as follows.

1) Proposes a novel triple-phase watermarking methodology to protect the reusable IP core during HLS.

2) Proposes a novel highly robust 7-variable signature encoding scheme for embedding watermark during consecutive phases of HLS.

3) Yields lower cost overhead in terms of hardware and latency compared to state of the art [4], [5].

➢ Motivation: Embedding Watermark at High Level [20]–[22].

[4] F. Koushanfar, I. Hong, and M. Potkonjak, "Behavioral synthesis techniques for intellectual property protection," *ACM Trans. Design Autom. Electron. Syst*., vol. 10, no. 3, pp. 523–545, 2005.
[5] A. Sengupta, S. Bhadauria, and S. P. Mohanty, "Embedding low cost optimal watermark during high level synthesis for reusable IP core protection," in *Proc. 48th IEEE Int. Symp. Circuits Syst. (ISCAS)*, Montreal, QC, Canada, 2016, pp. 974–977. [20] A. Sengupta, "Protection of IP-core designs for CE products," IEEE Consum. Electron. Mag., vol. 5, no. 1, pp. 83–89, Dec. 2015.
[21] A. Sengupta, "Hardware security of CE devices: Threat models and defence against IP trojans and IP piracy," IEEE Consum. Electron. Mag., vol. 6, no. 1, pp. 130–133, Jan. 2017.
[22] A. Sengupta and D. Roy, "Antipiracy-aware IP chipset design for CE devices: A Robust watermarking approach [hardware matters]," IEEE Consum. Electron. Mag., vol. 6, no. 2, pp. 118–124, Apr. 2017.

• Proposed Watermarking Methodology

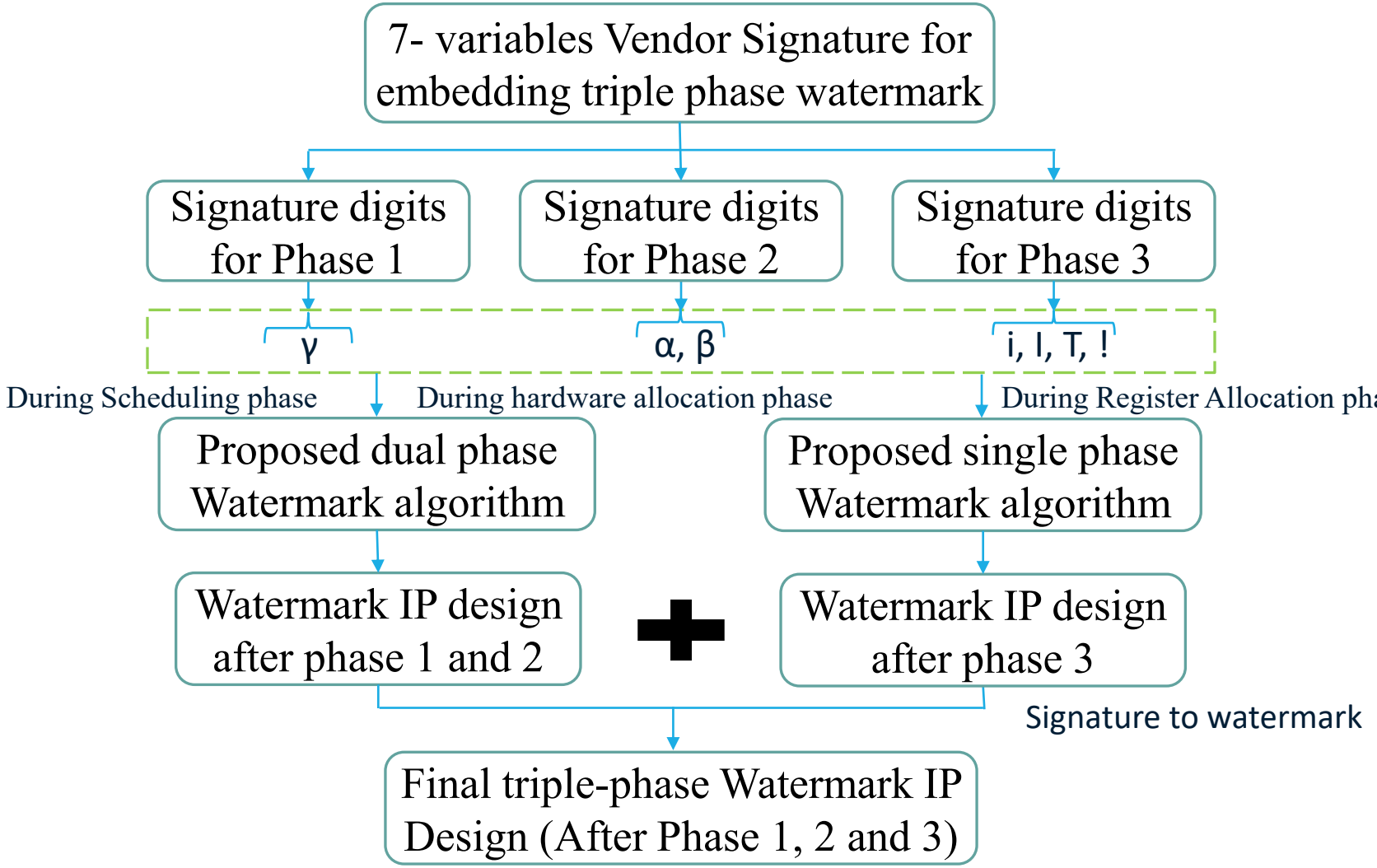


Fig. 3. Proposed triple-phase watermark at architecture level.

• Proposed Watermarking Methodology

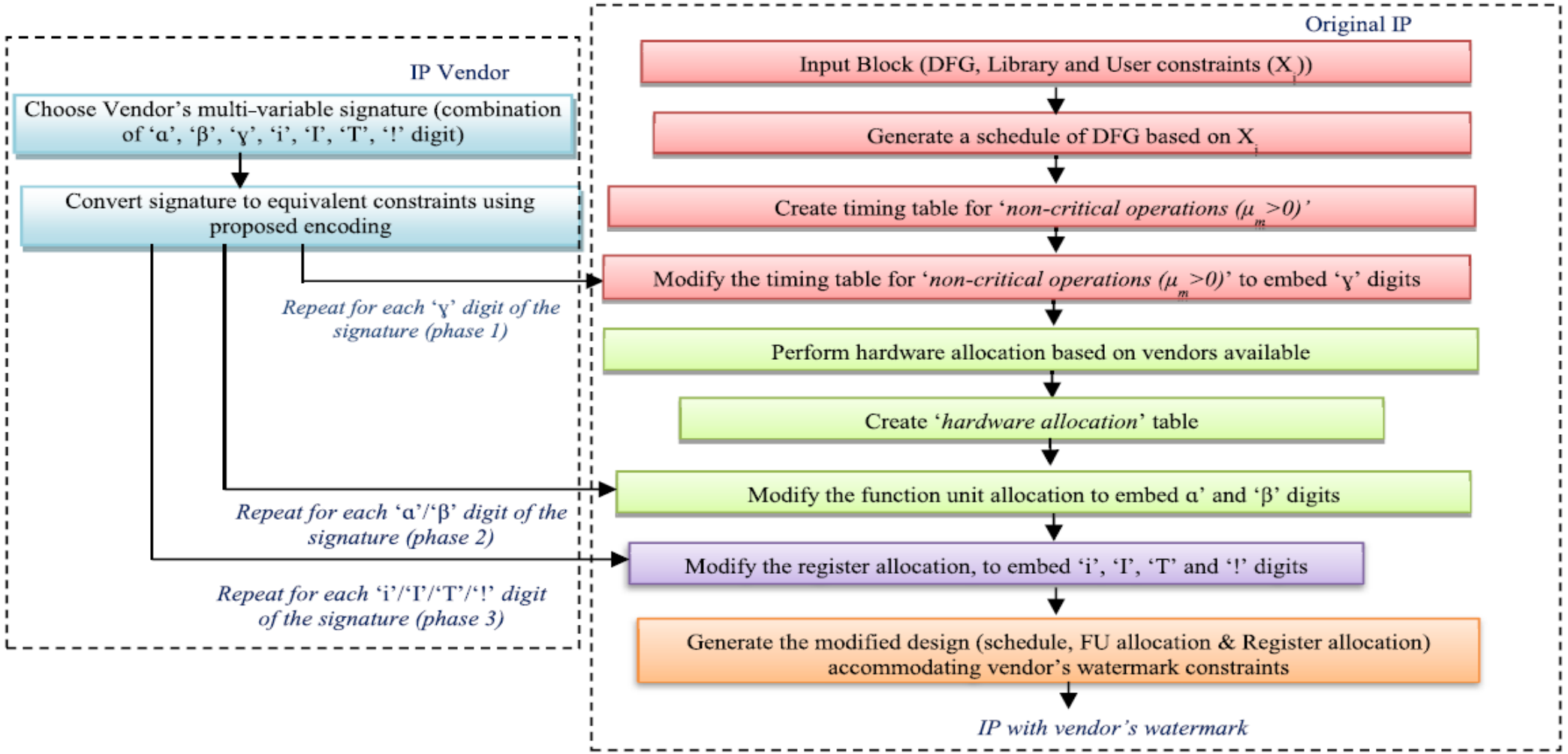


Fig. 4. Proposed HLS flow for reusable IP core protection using triple-phase watermark.

• Proposed Watermarking Methodology

➢ The encoding rules of all seven signature digits are defined as follows.

1) α = *For Odd Control Step:* Odd operation will be assigned to hardware of vendor type 1 (U1) and even operation will be assigned to hardware of vendor type 2 (U2).

2) β = *For Even Control Step:* Odd operation is assigned to hardware of vendor type 2 (U2) and even operation is assigned to hardware of vendor type 1 (U1).

3) γ = Move an operation of noncritical path with highest mobility into immediate next control step (cs).

4) i = encoded value of edge with node pair as (prime, prime).

5) I = encoded value of edge with node pair as (even, even).

6) T = encoded value of edge with node pair as (odd, even).

7) ! = encoded value of edge with node pair as (0, any integer).

• Proposed Watermarking Methodology

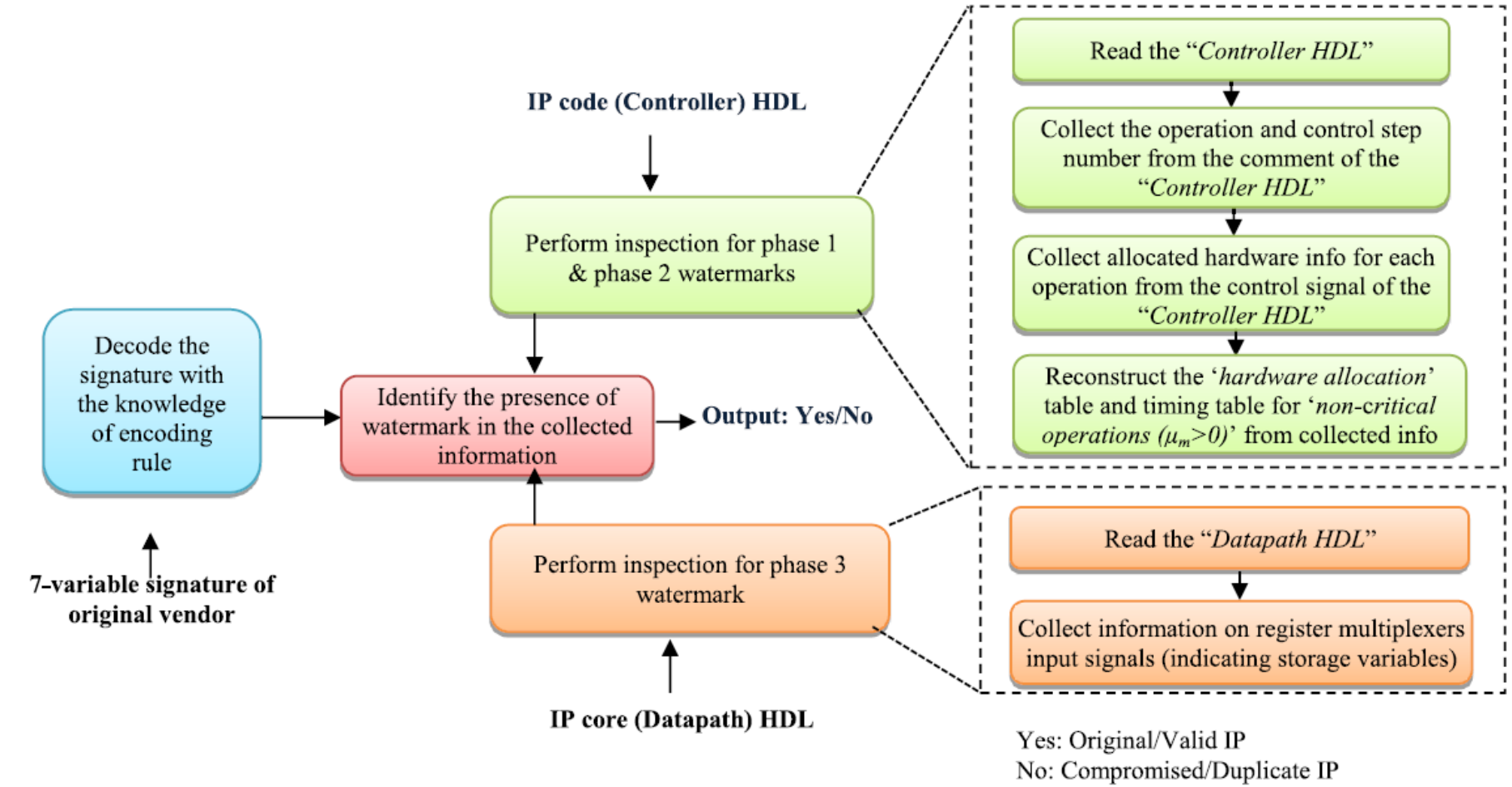


Fig. 5. Signature detection process.

• Proposed Watermarking Methodology

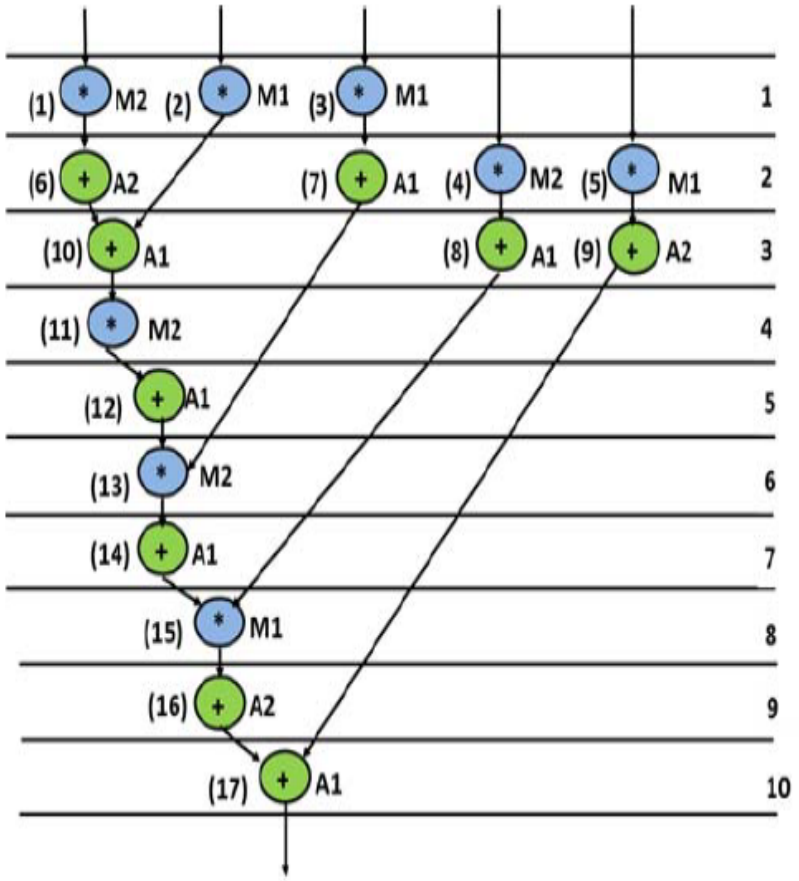


Fig. 6. Scheduled DFG (using three adders and three multipliers) of DWT with random FU allocation before embedding watermark.

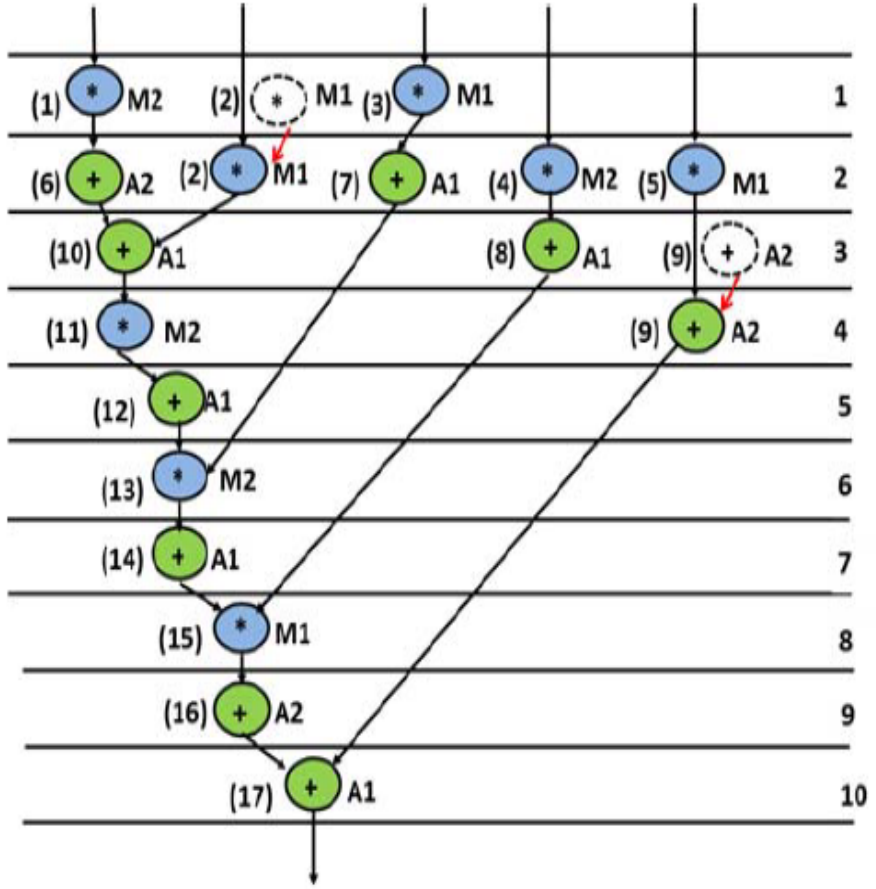


Fig. 7. Modified scheduled DFG after embedding phase 1 watermark (γ digits).

• Proposed Watermarking Methodology

TABLE I
VENDOR SIGNATURE AND ITS DECODED MEANING (WATERMARK CONSTRAINTS)

Desired Signature	Corresponding operation to shift (Phase 1)	Allocate FU type (Phase 2)	Additional edges to insert between nodes in the colored interval graph (Phase 3)	Observations
ɣ	opn 2 from c.s. 1 to 2	-----	—-	c.s. shift to be done
ɣ	opn 9 from c.s. 3 to 4	-----	—-	c.s. shift to be done
ɑ	——	opn 1 with vendor 1	—-	FU reallocation to be done
ɓ	——	opn 2 with vendor 1	—-	No change occurred
ɑ	——	opn 3 with vendor 1	—-	No change occurred
ɓ	——	opn 4 with vendor 1	—-	FU reallocation to be done
ɓ	——	opn 5 with vendor 2	—-	FU reallocation to be done
i	——	-----	(v2, v3)	Exists by default
I	——	-----	(v2, v4)	Exists by default
I	——	-----	(v2, v6)	New edge to be added
T	——	-----	(v1, v2)	Exists by default
!	——	-----	(v0, v1)	Exists by default

• Proposed Watermarking Methodology

TABLE II
TIMING TABLE FOR NONCRITICAL OPERATIONS ($\mu_m > 0$) SORTED IN INCREASING ORDER OF MOBILITY (BEFORE EMBEDDING WATERMARK)

Operation No.	3	2	5	4	7	9	8
Control Step	1		2			3	

TABLE III
TIMING TABLE FOR NONCRITICAL OPERATION ($\mu_m > 0$)
(AFTER EMBEDDING WATERMARK IN PHASE 1)

Operation	3	5	4	7	2	8	9
Control Step	1	2				3	4

• Proposed Watermarking Methodology

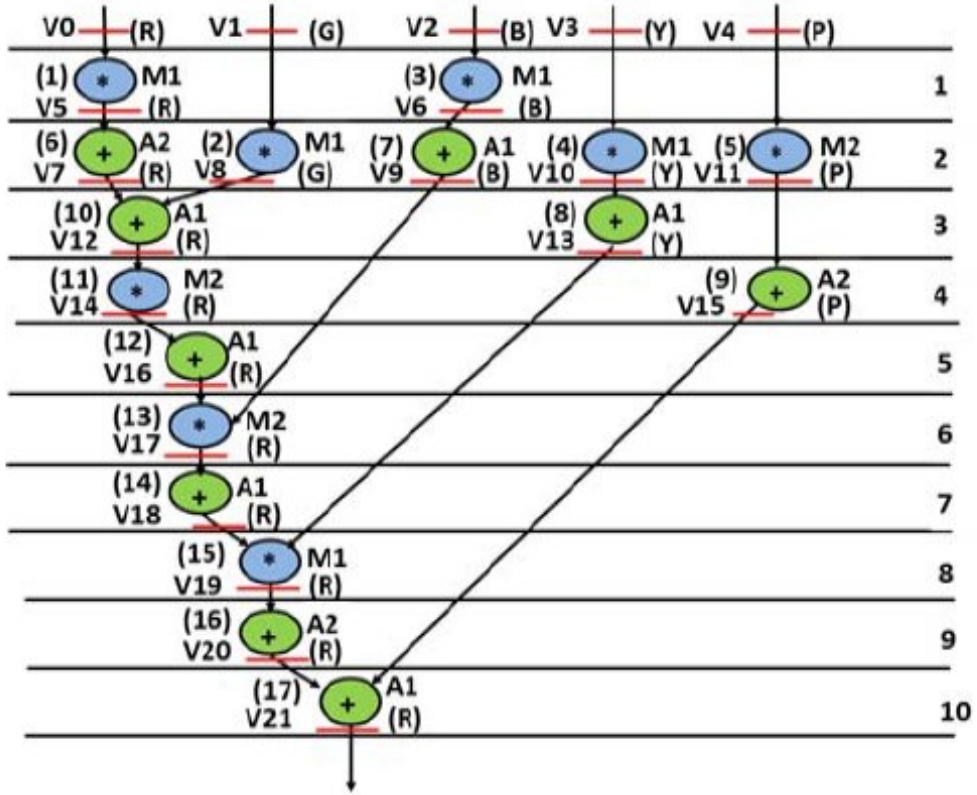


Fig. 8. Modified scheduled DFG after embedding phases 1 and 2 watermarks (α, β, and γ digits).

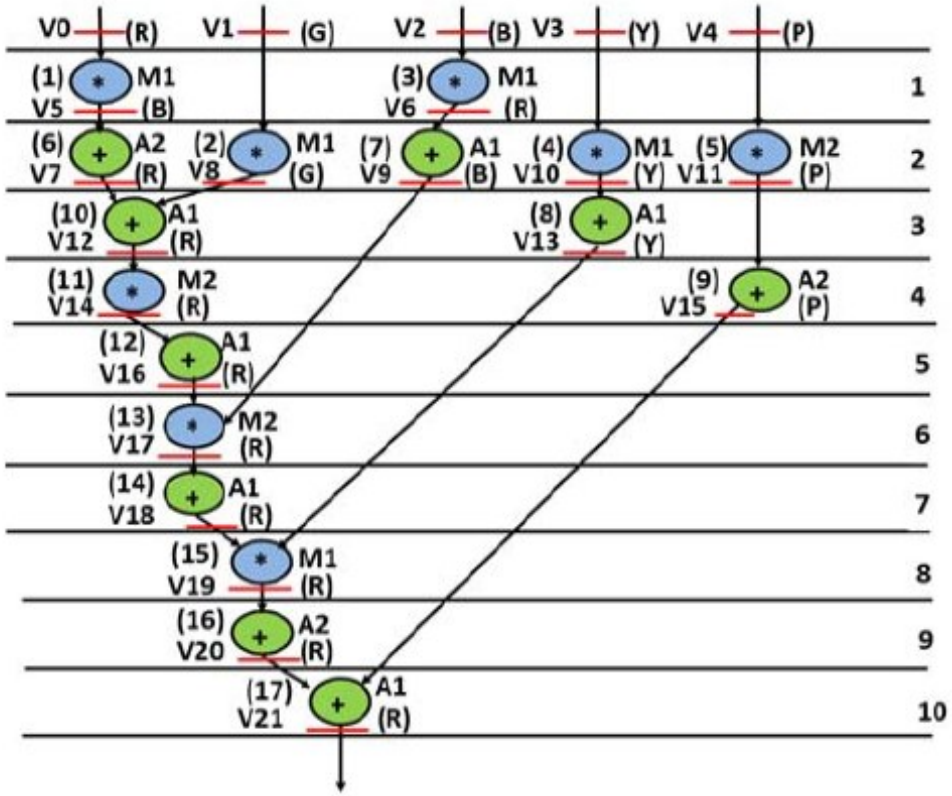


Fig. 9. Final scheduled DFG after embedding phases 1, 2, and 3 watermarks (α, β, γ, i, I, T, and ! digits).

• Proposed Watermarking Methodology

TABLE IV
FU ALLOCATION TABLE (BEFORE EMBEDDING WATERMARK)

ODD C.S.	Operation	1	2	3	8	9	10	12	14	16
	Allocated FU	M2	M1	M1	A1	A2	A1	A1	A1	A2
EVEN C.S.	Operation	4	5	6	7	11	13	15	17	–
	Allocated FU	M2	M1	A2	A1	M2	M2	M1	A1	–

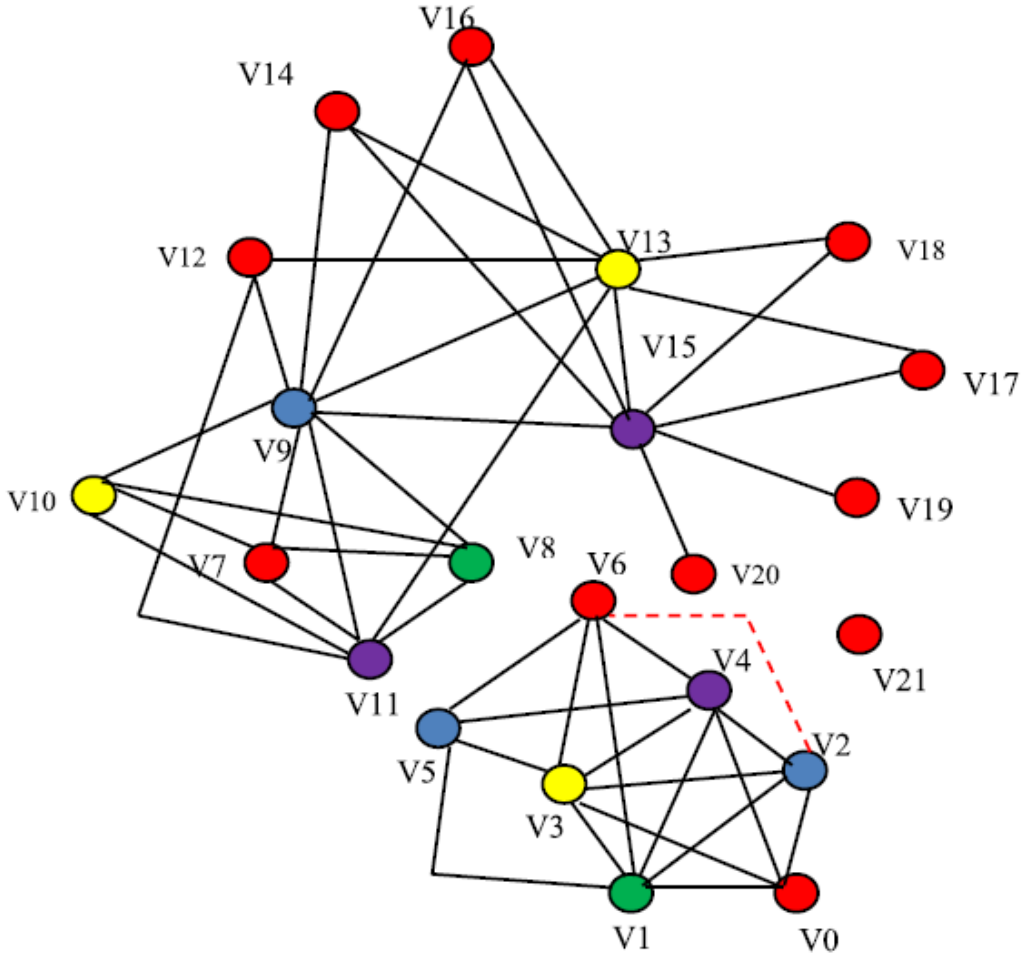


Fig. 10. Colored interval graph embedded with additional edges as per 3rd phase watermark.

• Proposed Watermarking Methodology

TABLE V
HARDWARE ALLOCATION TABLE (AFTER EMBEDDING WATERMARK IN PHASE 2 DURING FU ALLOCATION)

C.S. Count	Functional Unit Allocation						Register Allocation					
								R	G	B	Y	P
0	Operation	–	–	--	–	–	Storage Variable	V0	V1	V2	V3	V4
	Allocated Hardware	–	–	--	–	–						
1	Operation	1	3	--	–	–	Storage Variable	V5	V1	V6	V3	V4
	Allocated Hardware	M1	M1	--	–	–						
2	Operation	2	4	5	6	7	Storage Variable	V7	V8	V9	V10	V11
	Allocated Hardware	M1	M1	M2	A2	A1						
3	Operation	8	10	--	–	–	Storage Variable	V12	–	V9	V13	V11
	Allocated Hardware	A1	A1	--	–	–						
4	Operation	9	11	--	–	–	Storage Variable	V14	–	V9	V13	V15
	Allocated Hardware	A2	M2	--	–	–						
5	Operation	12	–	--	–	–	Storage Variable	V16	–	V9	V13	V15
	Allocated Hardware	A1	–	--	–	–						
6	Operation	13	–	--	–	–	Storage Variable	V17	–	--	V13	V15
	Allocated Hardware	M2	–	--	–	–						
7	Operation	14	–	--	–	–	Storage Variable	V18	–	--	V13	V15
	Allocated Hardware	A1	–	--	–	–						
8	Operation	15	–	--	–	–	Storage Variable	V19	–	--	--	V15
	Allocated Hardware	M1	–	--	–	–						
9	Operation	16	–	--	–	–	Storage Variable	V20	–	--	--	V15
	Allocated Hardware	A2	–	--	–	–						
10	Operation	17	–	--	–	–	Storage Variable	V21	–	--	--	--
	Allocated Hardware	A1	–	--	–	–						

• Proposed Watermarking Methodology

TABLE VI
FINAL HARDWARE ALLOCATION TABLE (AFTER EMBEDDING WATERMARK IN PHASES 1, 2, AND 3)

C.S. Count	Functional Unit Allocation						Register Allocation					
								R	G	B	Y	P
0	Operation	--	–	–	–	–	Storage Variable	V0	V1	V2	V3	V4
	Allocated Hardware	--	–	–	–	–						
1	Operation	1	3	–	–	–	Storage Variable	V6	V1	V5	V3	V4
	Allocated Hardware	M1	M1	–	–	–						
2	Operation	2	4	5	6	7	Storage Variable	V7	V8	V9	V10	V11
	Allocated Hardware	M1	M1	M2	A2	A1						
3	Operation	8	10	–	–	–	Storage Variable	V12	–	V9	V13	V11
	Allocated Hardware	A1	A1	–	–	–						
4	Operation	9	11	–	–	–	Storage Variable	V14	–	V9	V13	V15
	Allocated Hardware	A2	M2	–	–	–						
5	Operation	12	–	–	–	–	Storage Variable	V16	–	V9	V13	V15
	Allocated Hardware	A1	–	–	–	–						
6	Operation	13	–	–	–	–	Storage Variable	V17	–	–	V13	V15
	Allocated Hardware	M2	–	–	–	–						
7	Operation	14	–	–	–	–	Storage Variable	V18	–	–	V13	V15
	Allocated Hardware	A1	–	–	–	–						
8	Operation	15	–	–	–	–	Storage Variable	V19	–	–	–	V15
	Allocated Hardware	M1	–	–	–	–						
9	Operation	16	–	–	–	–	Storage Variable	V20	–	–	–	V15
	Allocated Hardware	A2	–	–	–	–						
10	Operation	17	–	–	–	–	Storage Variable	V21	–	–	–	–
	Allocated Hardware	A1	–	–	–	–						

• Threat Scenarios of False Claim of Ownership

A. Extracting Unintended Signature:

An attacker may claim "all operations of CS 1 should be allocated to Vendor 1" as his signature encoding rule, which may work for a single design, but will prove to be nonmeaningful for other watermarked designs.

B. Inserting Unauthorized Signature:

Entity B may insert his own signature into the original watermarked design of A and claim ownership. In such a conflict the actual owner A can prove his ownership as A's design only contains his watermark, however, B's design contains watermark of both A and B.

• Results and Analysis

TABLE VII
COMPARISON OF STRENGTH OF WATERMARK INDICATED THROUGH PROBABILITY OF COINCIDENCE (AS PROOF OF AUTHORSHIP) BETWEEN PROPOSED [4] AND [5] FOR SIGNATURE SIZE (80 DIGITS)

Benchmarks [4,5]	# of register before watermark	P_c			# of times lower P_c of proposed approach compared to [4] & [5]
		Proposed	[4]	[5]	
ARF	8	$3.3x10^{-27}$	$2.2x10^{-5}$	$2.2x10^{-5}$	$6.9x10^{21}$
DCT	8	$3.7x10^{-21}$	$2.2x10^{-5}$	$2.2x10^{-5}$	$6.1x10^{15}$
DWT	5	$8.3x10^{-35}$	$1.7x10^{-8}$	$1.7x10^{-8}$	$2.1x10^{26}$
EWF	4	$6.8x10^{-39}$	$1.0x10^{-10}$	$1.0x10^{-10}$	$1.5x10^{28}$
IDCT	8	$3.3x10^{-27}$	$2.2x10^{-5}$	$2.2x10^{-5}$	$6.9x10^{21}$
MPEG MV	14	$3.8x10^{-31}$	$2.6x10^{-3}$	$2.6x10^{-3}$	$6.9x10^{27}$
JPEG IDCT	12	$1.9x10^{-23}$	$9.4x10^{-4}$	$9.4x10^{-4}$	$5.0x10^{19}$

TABLE VIII
COMPARISON OF TAMPER TOLERANCE BETWEEN PROPOSED, [4] AND [5] FOR DIFFERENT SIGNATURE STRENGTH

Signature Size (digits)	# of possible signature combination			# of times higher tamper-tolerance of proposed approach compared to [4] & [5]	
	Proposed	[4]	[5]	[4]	[5]
15	$4.8*10^{12}$	32768	$10.7*10^{8}$	$14.5*10^{7}$	4421
30	$2.3*10^{25}$	$1.1*10^{9}$	$1.2*10^{18}$	$2.1*10^{16}$	$19.5*10^{6}$
45	$1.1*10^{38}$	$3.5*10^{13}$	$1.2*10^{27}$	$3.0*10^{24}$	$8.6*10^{10}$
60	$5.1*10^{50}$	$1.2*10^{18}$	$1.3*10^{36}$	$4.4*10^{32}$	$3.8*10^{14}$
80	$4.1*10^{67}$	$1.2*10^{24}$	$1.5*10^{48}$	$3.4*10^{43}$	$2.8*10^{19}$

• Results and Analysis

TABLE IX
COMPARISON OF PROPOSED APPROACH WITH BASELINE IN TERMS OF AREA, LATENCY, COST, AND COST OVERHEAD %

Benchmarks	Resource Configuration	Area (μm^2)		Latency (ns)		Cost		Cost Overhead %
		Baseline	Proposed	Baseline	Proposed	Baseline	Proposed	Proposed approach with respect to baseline
ARF	5(+), 3(*)	191.1	209.19	2.67	3.11	0.77	0.87	12.98
DCT	6(+), 3(*)	250.87	263.45	3.95	4.19	0.80	0.84	5.00
DWT	2(+), 4(*)	162.79	165.94	1.98	2.08	0.78	0.81	3.85
EWF	3(+), 2(*)	184.81	197.39	3.24	3.82	0.85	0.95	11.76
IDCT	5(+), 3(*)	246.15	253.23	3.77	4.16	0.78	0.83	6.41
MPEG	3(+), 8(*)	280.76	287.05	2.44	2.59	0.73	0.76	4.11
JPEG	5(+), 5(*)	747.9	756.55	14.9	15.92	0.72	0.76	5.56

• Results and Analysis

TABLE X
COMPARISON OF PROPOSED APPROACH WITH [4] AND [5] IN TERMS OF REDUCED WATERMARK DESIGN AREA, LATENCY, AND COST FOR SIGNATURE STRENGTH: 80

Benchmarks	Hardware configuration	Watermark Design Area (μm^2)			Watermark Design Latency (ns)			Watermark Design Cost		
		Proposed	[4]	[5]	Proposed	[4]	[5]	Proposed	[4]	[5]
ARF	5(+), 3(*)	209.19	225.71	223.35	3.11	3.11	3.11	0.87	0.92	0.90
DCT	6(+), 3(*)	263.45	290.98	288.62	4.19	4.51	4.51	0.84	0.94	0.92
DWT	2(+), 4(*)	165.94	182.37	180.01	2.08	2.43	2.43	0.81	0.93	0.92
EWF	3(+), 2(*)	197.39	209.19	204.47	3.82	3.89	3.89	0.95	0.99	0.98
IDCT	5(+), 3(*)	253.23	280.96	278.4	4.16	4.34	4.34	0.83	0.91	0.89
MPEG	3(+), 8(*)	287.05	309.85	309.85	2.59	2.77	2.77	0.76	0.81	0.81
JPEG	5(+), 5(*)	756.55	783.29	783.29	15.92	16.52	16.52	0.76	0.79	0.79

References

[1] S. P. Mohanty, U. Choppali, and E. Kougianos, “Everything you wanted to know about smart cities: The Internet of Things is the backbone,” IEEE Consum. Electron. Mag., vol. 5, no. 3, pp. 60–70, Jul. 2016.

[2] R. Maes, D. Schellekens, and I. Verbauwhede, “A pay-per-use licensing scheme for hardware IP cores in recent SRAM-based FPGAs,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 98–108, Feb. 2012.

[3] A. Cui, G. Qu, and Y. Zhang, “Ultra-low overhead dynamic watermarking on scan design for hard IP protection,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 11, pp. 2298–2313, Nov. 2015.

[4] F. Koushanfar, I. Hong, and M. Potkonjak, “Behavioral synthesis techniques for intellectual property protection,” ACM Trans. Design Autom. Electron. Syst., vol. 10, no. 3, pp. 523–545, 2005.

[5] A. Sengupta, S. Bhadauria, and S. P. Mohanty, “Embedding low cost optimal watermark during high level synthesis for reusable IP core protection,” in Proc. 48th IEEE Int. Symp. Circuits Syst. (ISCAS), Montreal, QC, Canada, 2016, pp. 974–977.

[6] Y. Alkabani, F. Koushanfar, and M. Potkonjak, “Remote activation of ICs for piracy prevention and digital right management,” in Proc. IEEE/ACM Int. Conf. Comput.-Aided Design, San Jose, CA, USA, 2007, pp. 674–677.

[7] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[8] L. M. Marvel, “Information hiding: Steganography and watermarking,” in Optical and Digital Techniques for Information Security (Advanced Sciences and Technologies for Security Applications), vol. 1, B. Javidi, Ed. New York, NY, USA: Springer, 2005, pp. 113–133.

[9] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. San Mateo, CA, USA: Morgan Kaufmann, 2007.

[10] Y.-T. Wu and F. Y. Shih, “Digital watermarking based on chaotic map and reference register,” Pattern Recognit., vol. 40, no. 12, pp. 3753–3763, 2007.

[11] E. Kougianos, S. P. Mohanty, and R. N. Mahapatra, “Hardware assisted watermarking for multimedia,” Comput. Elect. Eng., vol. 35, no. 2, pp. 339–358, 2009.

• Results and Analysis

[12] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York, NY, USA: Springer, 2009.
[13] J. A. Roy, F. Koushanfar, and I. L. Markov, "EPIC: Ending piracy of integrated circuits," in Proc. Design Autom. Test Europe (DATE), Munich, Germany, 2008, pp. 1069–1074.
[14] Y. Alkabani and F. Koushanfar, "Active control and digital rights management of integrated circuit IP cores," in Proc. Int. Conf. Compilers Archit. Synthesis Embedded Syst. (CASES), Atlanta, GA, USA, 2008, pp. 227–234.
[15] T. Nie, L. Zhou, and Y. Li, "Hierarchical watermarking method for FPGA IP protection," IETE Tech. Rev., vol. 30, no. 5, pp. 367–374, 2013.
[16] B. Le Gal and L. Bossuet, "Automatic low-cost IP watermarking technique based on output mark insertions," Design Autom. Embedded Syst., vol. 16, no. 2, pp. 71–92, 2012.
[17] Y. M. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," in Proc. 16th USENIX Security Symp., Boston, MA, USA, 2007, Art. no. 20.
[18] R. S. Chakraborty and S. Bhunia, "HARPOON: An obfuscationbased SoC design methodology for hardware protection," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 28, no. 10, pp. 1493–1502, Oct. 2009.
[19] (2016). NanGate 15 nm Library. [Online]. Available: http://www.nangate.com/?pageid=2328
[20] A. Sengupta, "Protection of IP-core designs for CE products," IEEE Consum. Electron. Mag., vol. 5, no. 1, pp. 83–89, Dec. 2015.
[21] A. Sengupta, "Hardware security of CE devices: Threat models and defence against IP trojans and IP piracy," IEEE Consum. Electron. Mag., vol. 6, no. 1, pp. 130–133, Jan. 2017.
[22] A. Sengupta and D. Roy, "Antipiracy-aware IP chipset design for CE devices: A Robust watermarking approach [hardware matters]," IEEE Consum. Electron. Mag., vol. 6, no. 2, pp. 118–124, Apr. 2017.

THANK YOU