Structural Obfuscation and Crypto-Steganography-Based Secured JPEG Compression Hardware for Medical Imaging Systems

Published in *IEEE Access*

A. Sengupta and M. Rathor, "Structural Obfuscation and Crypto-Steganography-Based Secured JPEG Compression Hardware for Medical Imaging Systems," in IEEE Access, vol. 8, pp. 6543-6565, 2020.

• Introduction

- The electronic integrated circuits (ICs) and internet technology have eased and fastened the diagnosis and treatment of critical diseases.
- The medical instruments such as CT scanner and MRI scanner generate large size of digital image data [1].
- Due to large, these images are required to be stored/ transmitted in the compressed form.

[1] D. A. Koff and H. Shulman, ``An overview of digital compression of medical images: Can we use lossy image compression in radiology?" Can. Assoc. Radiol. J., vol. 57, no. 4, pp. 211217, 2006.

• Threat Model

- Emerging hardware threats are increasingly corrupting compressed medical images from cameras and scanners, often by compromising the compression processor.

- Hardware threat like reverse engineering (causing Trojan insertion) [7] and piracy / counterfeiting [8]-[10].

[7] X. Zhang and M. Tehranipoor, ``Case study: Detecting hardware trojans in third-party digital IP cores," in Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust, San Diego CA, USA, Jun. 2011, pp. 6770.
[8] Maxim. Accessed: May. [Online]. Available: https://www.maxim integrated.com/en/app-notes/index.mvp/id/545
[9] SMT Corp. Counterfeit Detection. Accessed: May 2019. [Online]. Available: https://www.smtcorp.com/counterfeit-detection
[10] A. Sengupta, D. Roy, and S. P. Mohanty, ``Triplephase watermarking for reusable ip core protection during architecture synthesis," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 37, no. 4, pp. 742755,Apr. 2018..

• Related Work

Sr. No.	Existing Work	Technique Used	Remark
1.	F. Koushanfar et.al., [17] (2005) B. Le Gal et.al.,[22](2012)	employed watermarking technique to secure the designs against counterfeiting/cloning.	However, [17],[21] did not ensure the preventive security against RE
2.	A. Sengupta et.al., [11] (2017) A. Sengupta et.al., [20] (2005)	structural obfuscation has been applied on DCT	However, [11], [20] did not perform structural obfuscation on entire JPEG CODEC processor

• Proposed Methodology

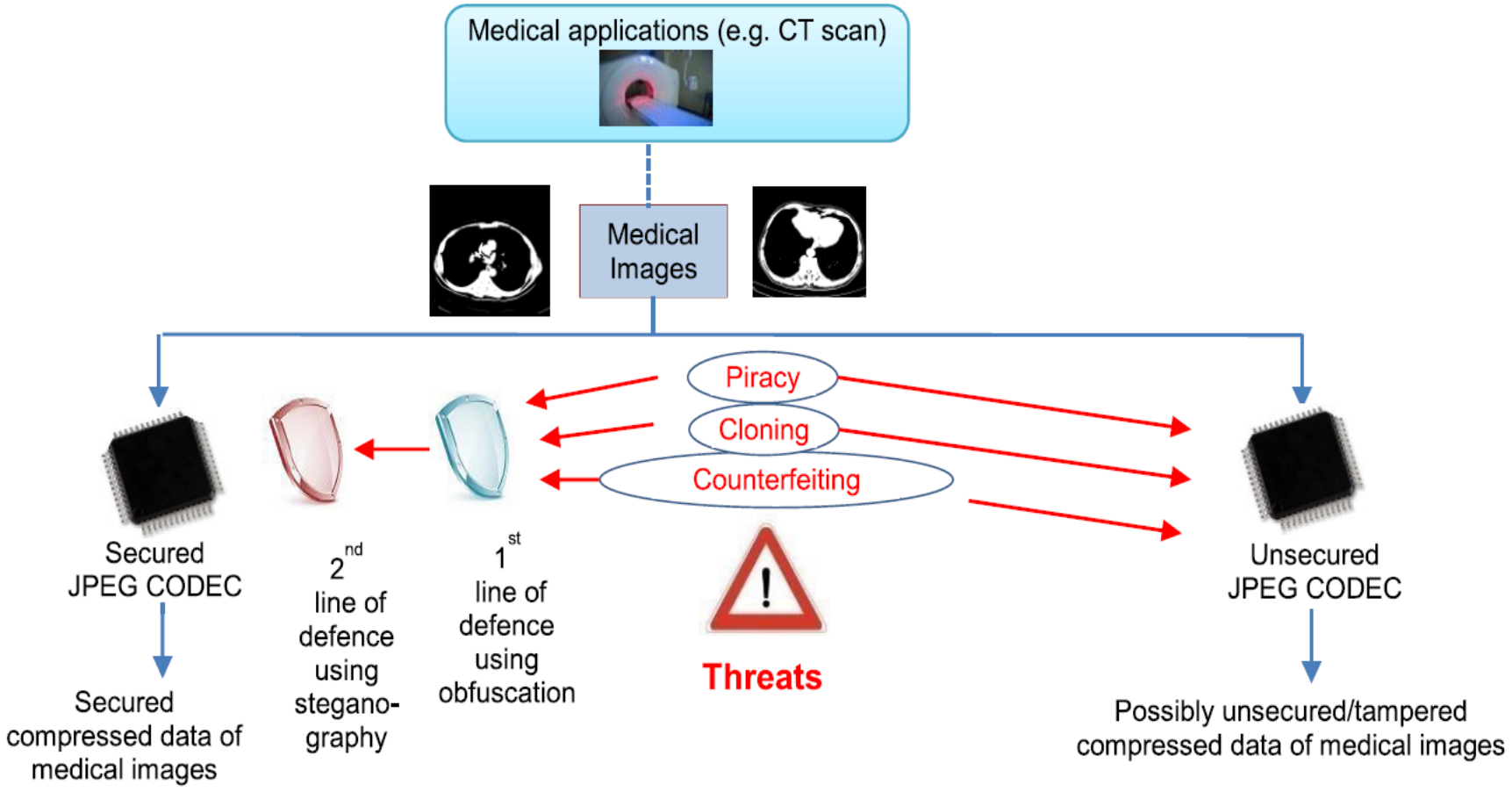


FIGURE 1. Thematic representation of securing medical images against external hardware threats.

• Proposed Methodology

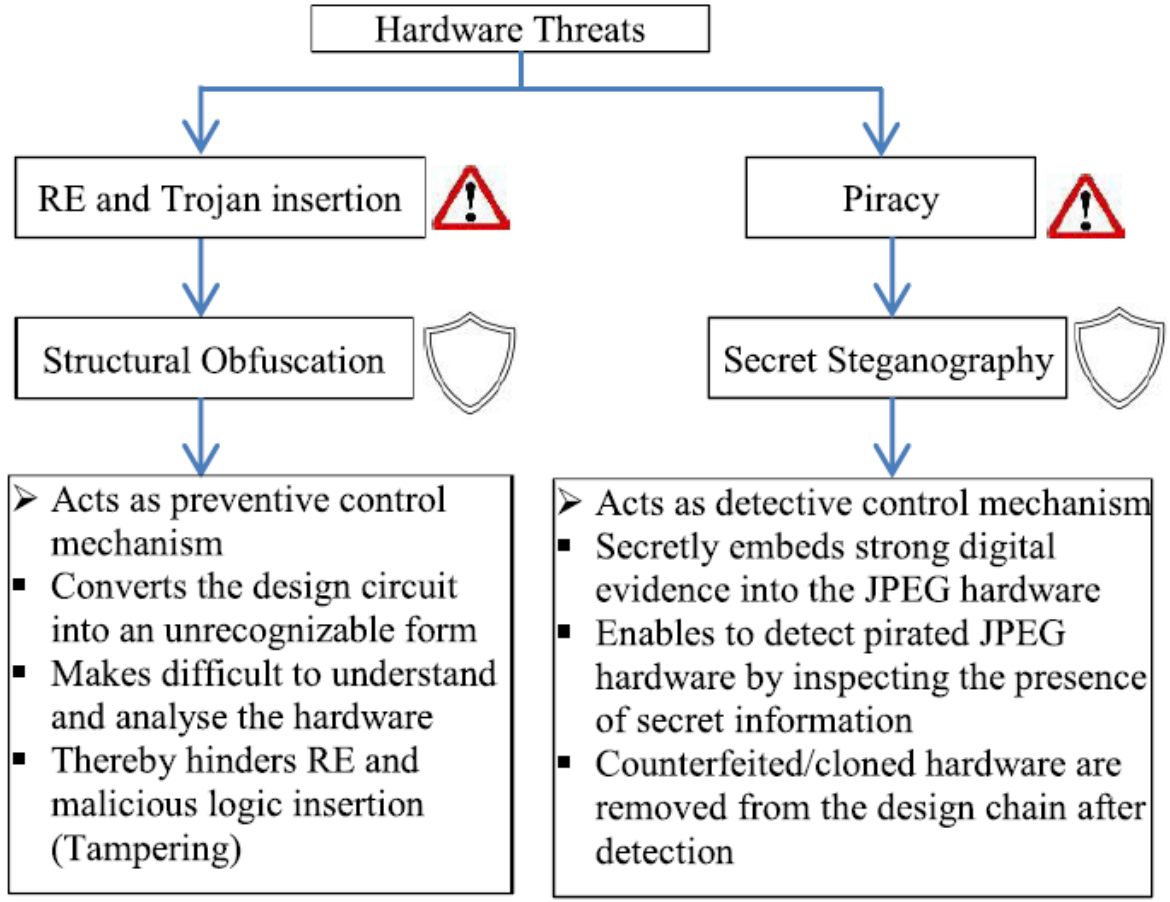


FIGURE 2. Overview of hardware threats and protection scenarios using proposed approach.

• Proposed Methodology

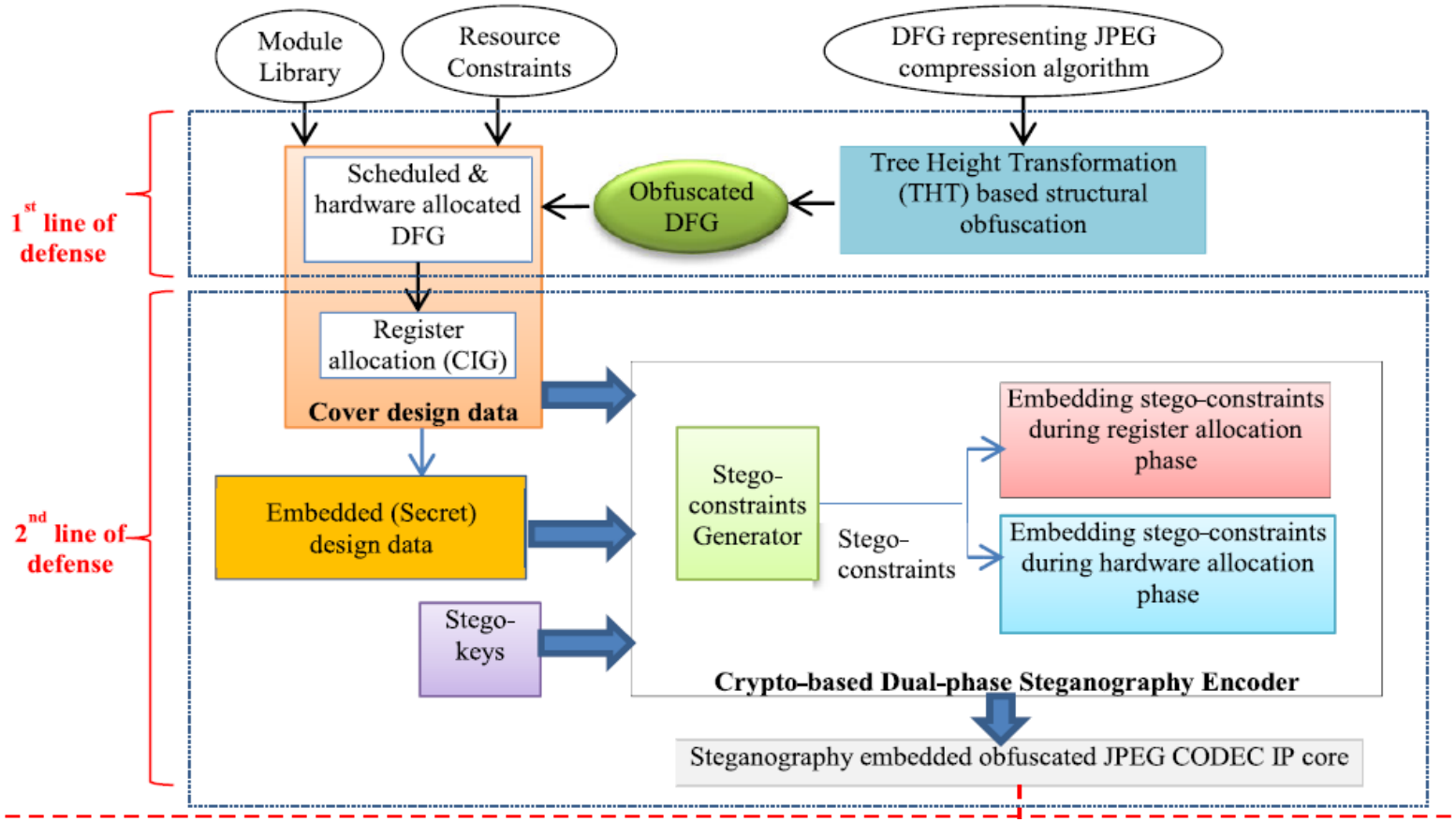


FIGURE 3(a). Proposed double line defense using structural obfuscation and crypto-based dual-phase steganography to secure JPEG CODEC processor used for compression of medical images.

• Proposed Methodology

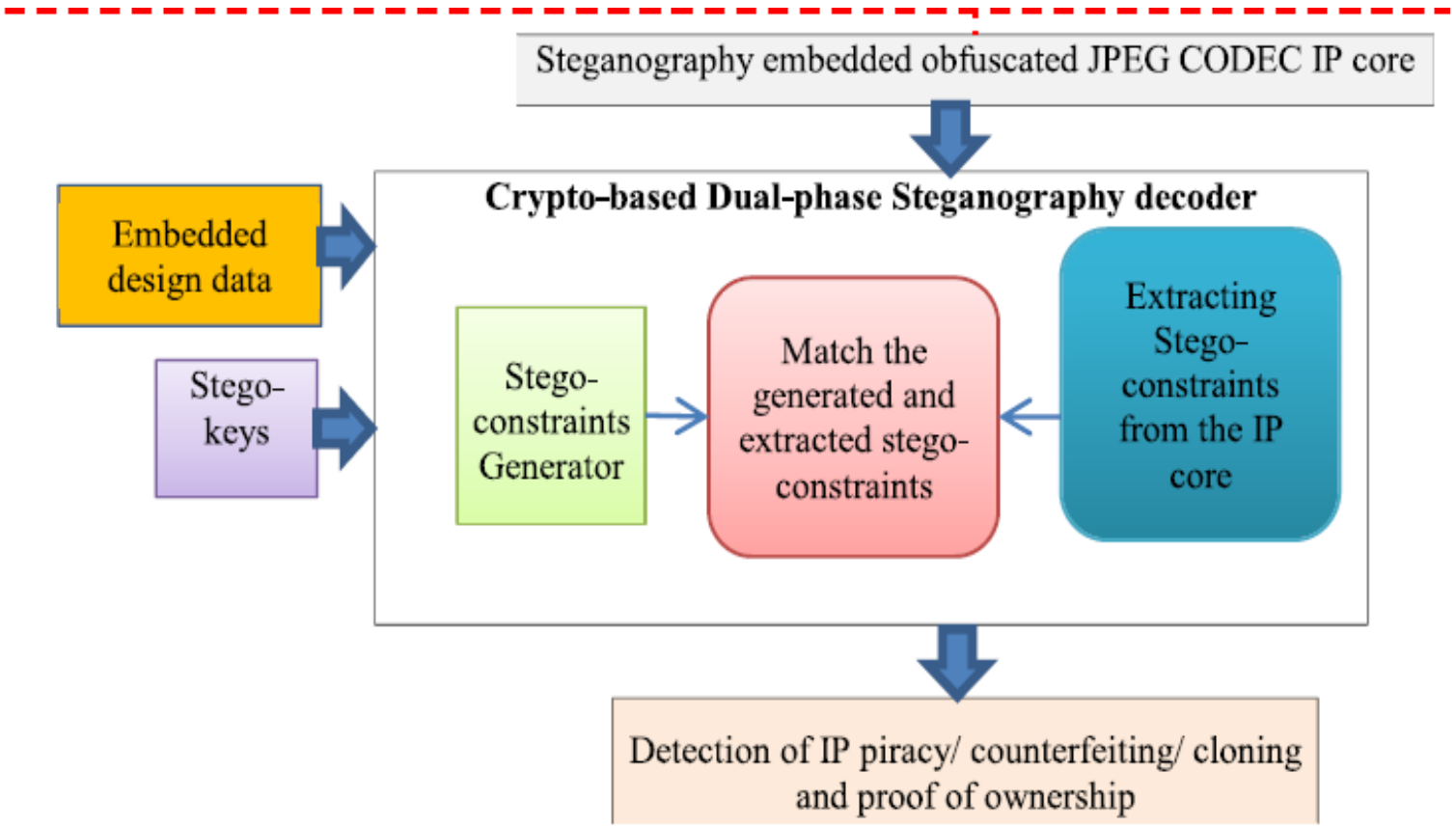
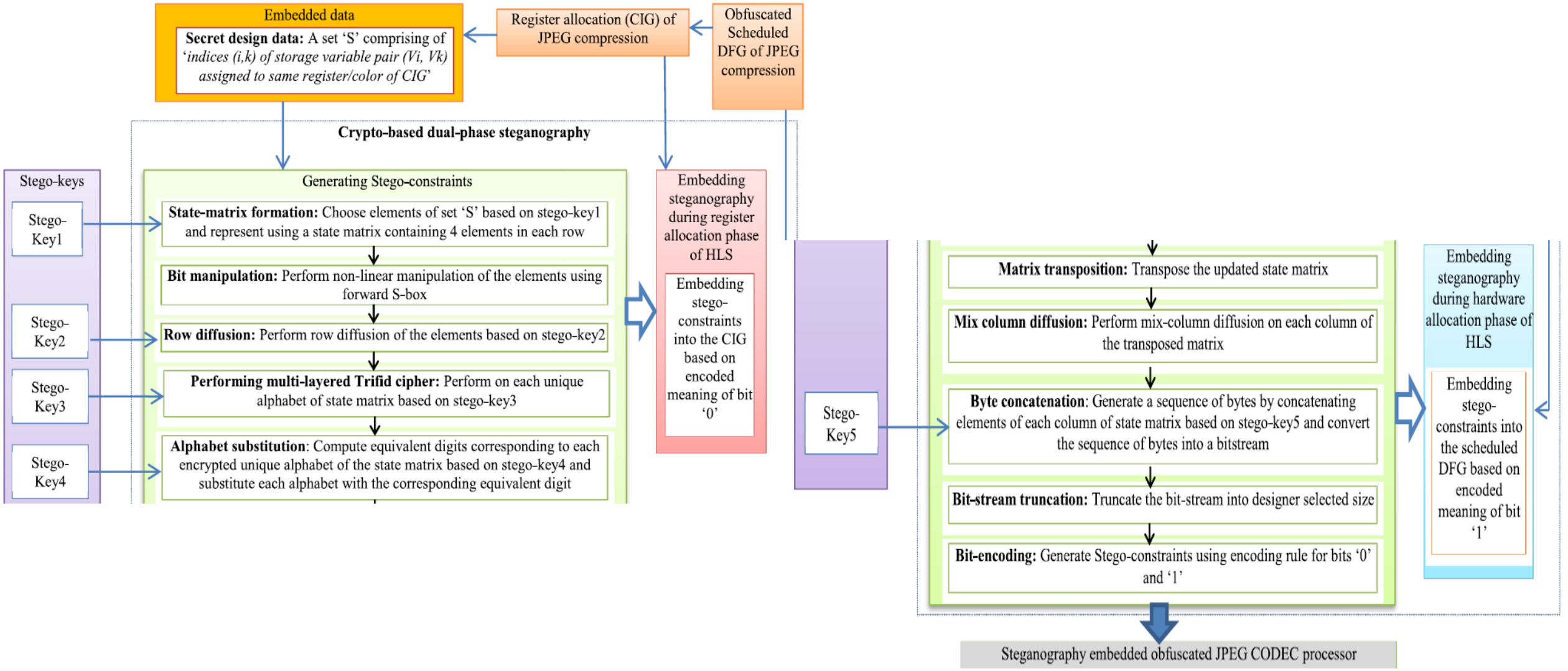


FIGURE 3(a). Proposed double line defense using structural obfuscation and crypto-based dual-phase steganography to secure JPEG CODEC processor used for compression of medical images.

• Proposed Methodology



• Proposed Methodology

Stego-key 1

Chooses elements of set ‘S’ according to six modes

Key-bits	Modes	Definition
000	1	Choose every 2 elements and skip next 2 elements
001	2	Choose every 4 elements and skip next 4 elements
010	3	Choose every 8 elements and skip next 8 elements
011	4	Choose every 16 elements and skip next 16 elements
100	5	Choose every 32 elements and skip next 32 elements
101	6	Choose every 64 elements and skip next 64 elements

Stego-key 2

Decides the number of elements (according to four modes) by which circular right shift for each row will be performed

Key-bits	Modes	Definition
00	1	Circular right shift by 1 element
01	2	Circular right shift by 2 element
01	3	Circular right shift by 3 element
11	4	Circular right shift by 4 element

Stego-key 3

Decides the key of encryption for each unique alphabet of the state matrix (a distinct key is chosen for each unique alphabet)

• Proposed Methodology

Stego-key 4

Decides the mode of computing equivalent to each encrypted alphabet

Key-bits	Modes	Definition
000	1	x*y*z
001	2	X+y+z
010	3	|x-y-z|
011	4	|x-y+z|
100	5	(z+y)/x
101	6	(z+x)*y

Stego-key 5

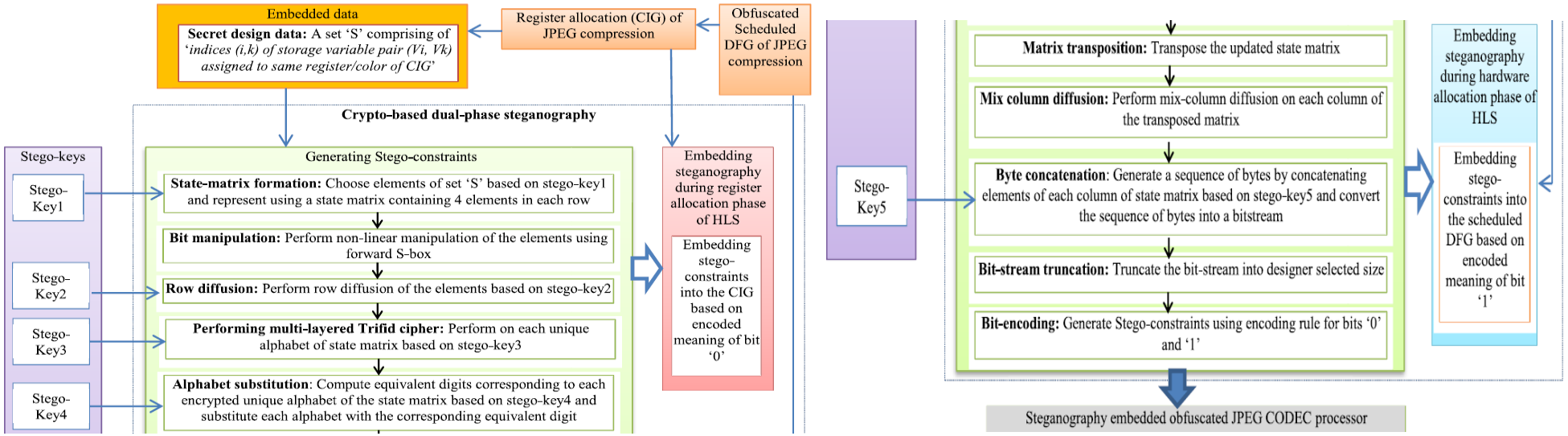
Decides the concatenation sequence of elements (based on six modes) for each coloum

Key-bits	Modes	Definition
000	1	E0E1E2E3
001	2	E0E1E3E2
010	3	E0E2E1E3
011	4	E0E2E3E1
100	5	E0E3E1E2
101	6	E0E3E2E1

• Proposed Methodology

TABLE 1. Encoding of bit `0' and `1' in JPEG compression design.

Bit	Encoded meaning
0	Embed an edge between node pairs (even, even) of CIG (during register allocation of HLS) of JPEG compression
1	In the JPEG compression scheduling/allocation, odd operations are assigned to FU of vendor type 1(U1) and even operations are assigned to FU of vendor type 2(U2) (during functional unit (FU) allocation phase of HLS)



• Proposed Methodology: Pseudo code of proposed double line of defense

First Line of Defense:

Inputs: DFG of JPEG compression processor, module library, resource constraints.

Output: Obfuscated scheduled DFG

Algorithm:

```
Read DFG;
perform_THT(){
travers all operations;
read data dependency of each operation;
if operations of same type are executing
sequentially, then execute them as parallel sub-
computations while altering data dependency
without changing functionality;
returned obfuscated DFG;}
Read module library
Read constraints file;
architectural_ synthesis()
end algorithms ;
```

Second Line of Defense:

Inputs: Obfuscated scheduled DFG, Stego-key1 to 5

Output: Steganography embedded obfuscated JPEG

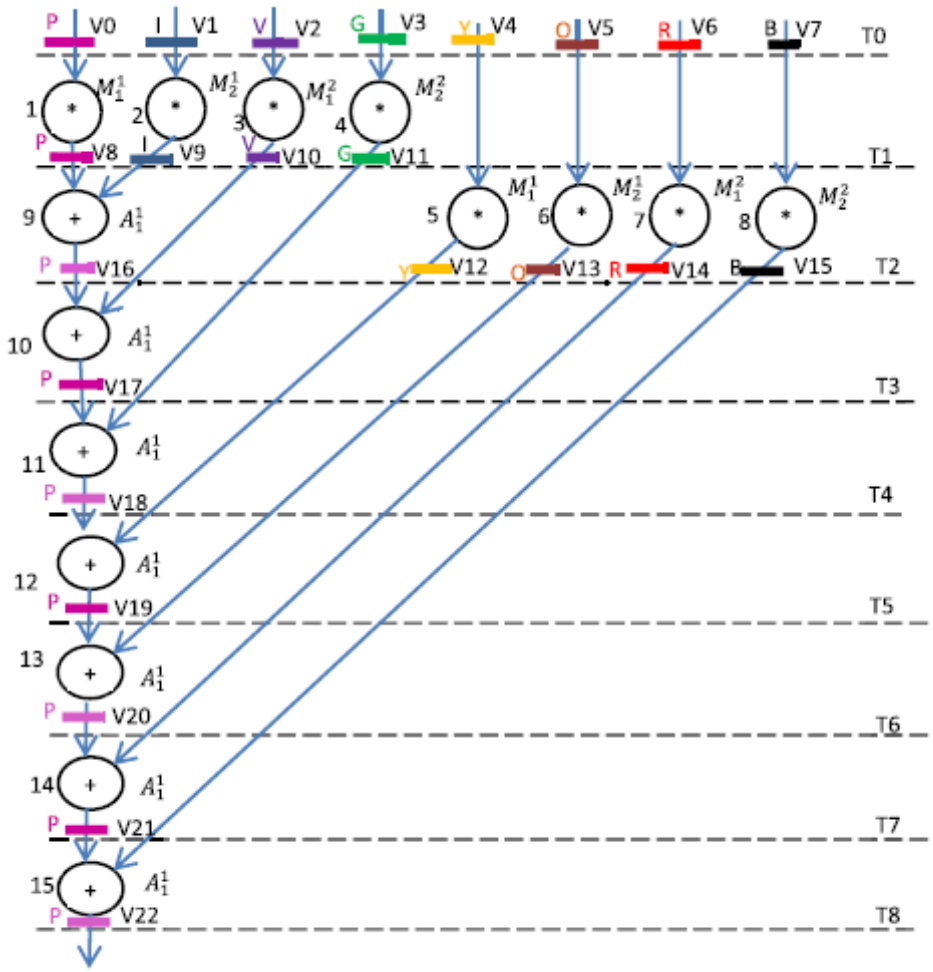
Algorithm:

```
Read obfuscated scheduled  DFG ;
create_CIG()
extract_secret_design_data()
state_matrix_formation()
bit_manipulation()
row_diffusion()
trifid_cipher()
alphabate_substitution()
matrix_transposition()
colum_diffusion()
byte_concatenation()
bitstream_truncation()
bit_encoding()
embedding_bit0()
embedding_bit1()
end algorithms ;
```

• Proposed Methodology

T	Pink	Indigo	Violet	Green	Yellow	Orange	Red	Black
0	V0	V1	V2	V3	V4	V5	V6	V7
1	V8	V9	V10	V11	V4	V5	V6	V7
2	V16	-	V10	V11	V12	V13	V14	V15
3	V17	-	-	V11	V12	V13	V14	V15
4	V18	-	-	-	V12	V13	V14	V15
5	V19	-	-	-	-	V13	V14	V15
6	V20	-	-	-	-	-	V14	V15
7	V21	-	-	-	-	-	-	V15
8	V22	-	-	-	-	-	-	-

• Proposed Methodology



T: control step
M_1^1 : first instance of multiplier of vendor type-1
M_2^1 : second instance of multiplier of vendor type-1
M_1^2 : first instance of multiplier of vendor type-2
A_1^1 : first instance of adder of vendor type-1
V0-V22: 23 storage variables
P, I, V, G, Y, O, R, B: eight different colors representing eight distinct registers

FIGURE 7. Scheduled and hardware allocated 8-point DCT using 1 (+) and 4 (•) before implanting steganography.

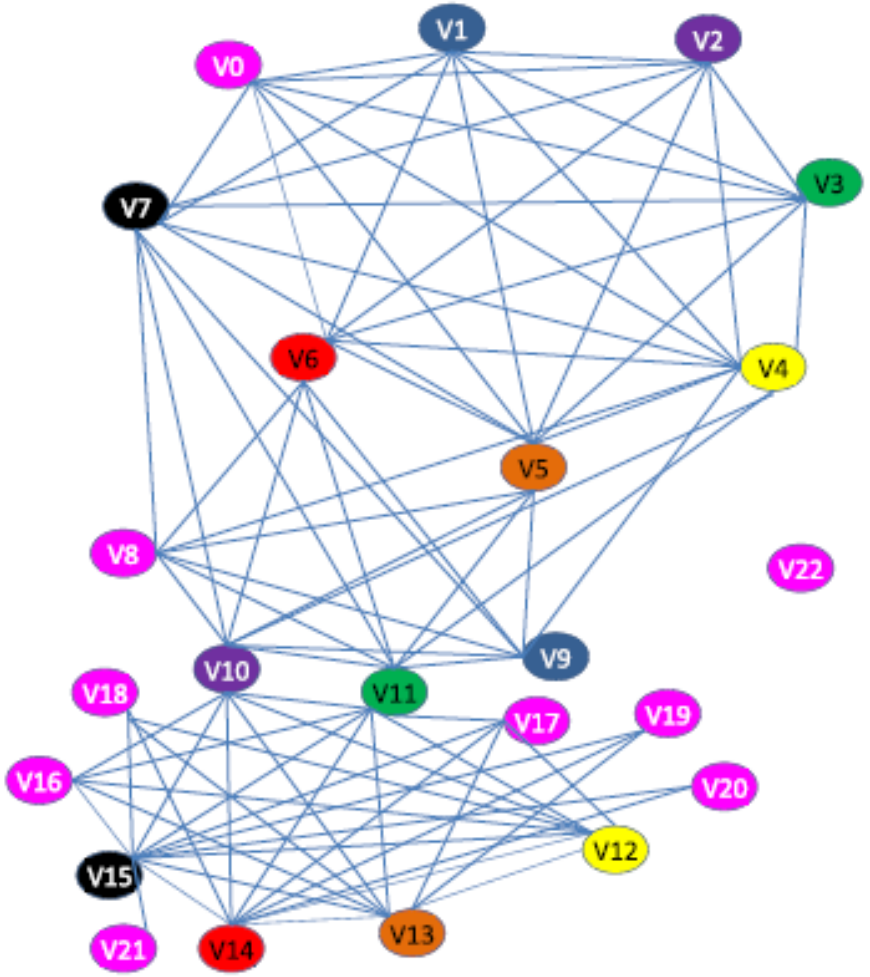


FIGURE 8. CIG of 8-point DCT before implanting hardware steganography.

• Proposed Methodology

(a)

08	01	02	03
81	82	83	84
13	14	15	16
26	27	24	35
47	56	57	67

(b)

30	7C	77	7B
0C	13	EC	5F
7D	FA	59	47
F7	CC	18	96
A0	B1	5B	85

(c)

77	7B	30	7C
5F	0C	13	EC
FA	59	47	7D
96	F7	CC	18
A0	B1	5B	85

FIGURE 9. (a). Initial state matrix (b). After byte substitution (c). After row diffusion.

(a)

77	78	30	76
51	06	13	66
14	59	47	74
96	17	66	18
40	81	58	85

(b)

77	51	14	96	40
78	06	59	17	81
30	13	47	66	58
76	66	74	18	85

(c)

20	DD	F0	70	C5
A1	0E	1B	0A	34
F5	DB	5F	65	E5
3D	2A	CA	E0	08

FIGURE 10. (a). After TRIFID cipher. (b). After transposition. (c). After mix-column diffusion.

• Proposed Methodology

Alphabets	A	B	C	D	E	F
Corresponding state (output of TRIFID cipher)	211	323	321	233	313	322
Key bits (Stego-Key4)	001	001	000	010	101	010
Computed digit	4	8	6	4	6	1

$$\begin{pmatrix} E0 \\ E1 \\ E2 \\ E3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} * \begin{pmatrix} 77 \\ 78 \\ 30 \\ 76 \end{pmatrix} = \begin{pmatrix} 20 \\ A1 \\ F5 \\ 3D \end{pmatrix}$$

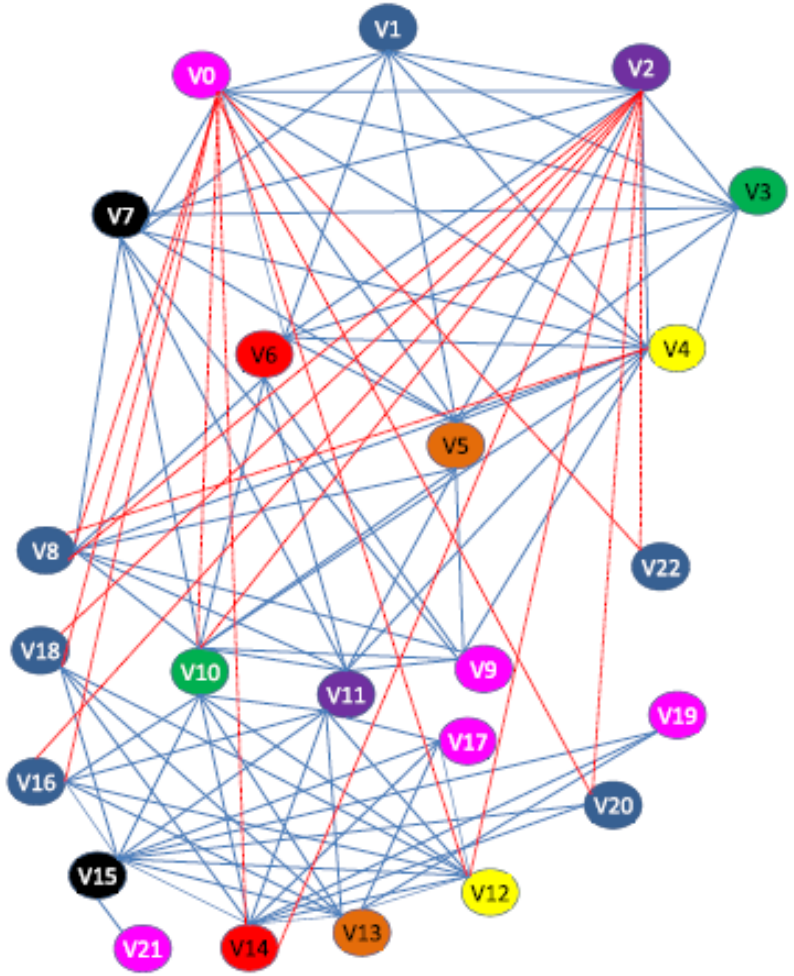


FIGURE 11. The CIG of 8-point DCT after implanting steganography during register allocation phase Note: Dotted red lines show the stego-constraints implanted (corresponding to 0s).

• Proposed Methodology

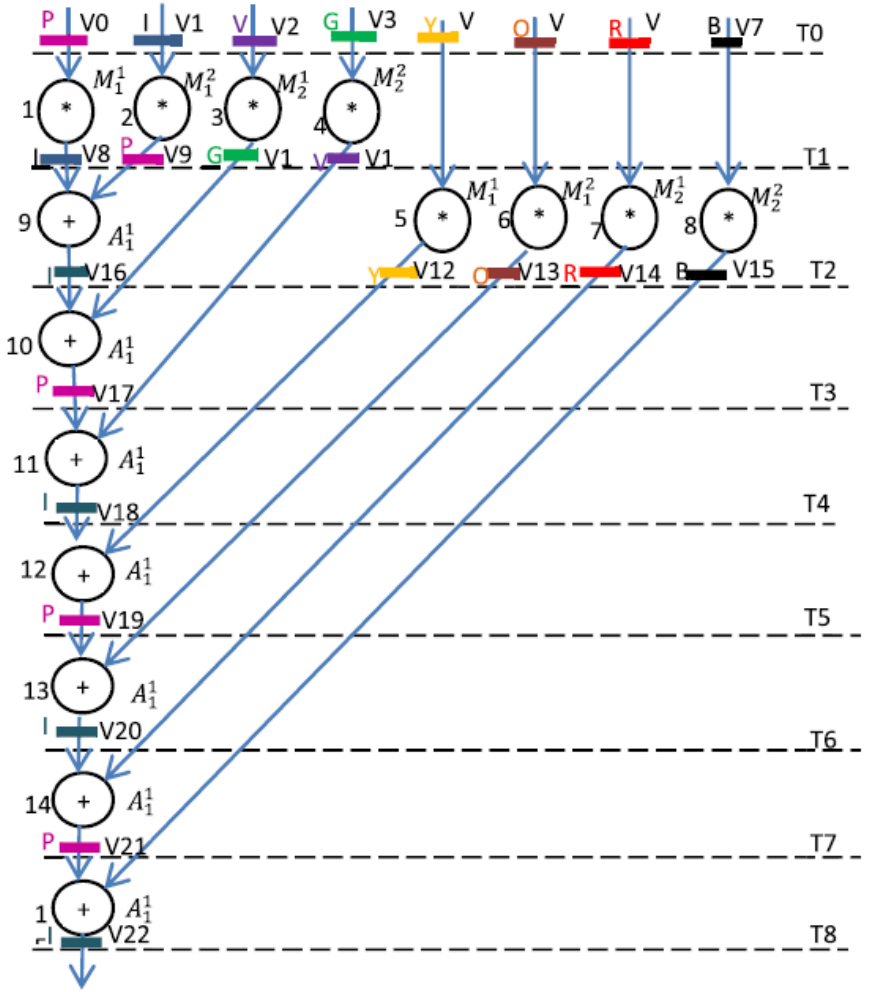


FIGURE 12. Scheduled and hardware allocated 8-point DCT using 1(+) and 4(*) after implanting steganography during both pase-1 and phase-2.

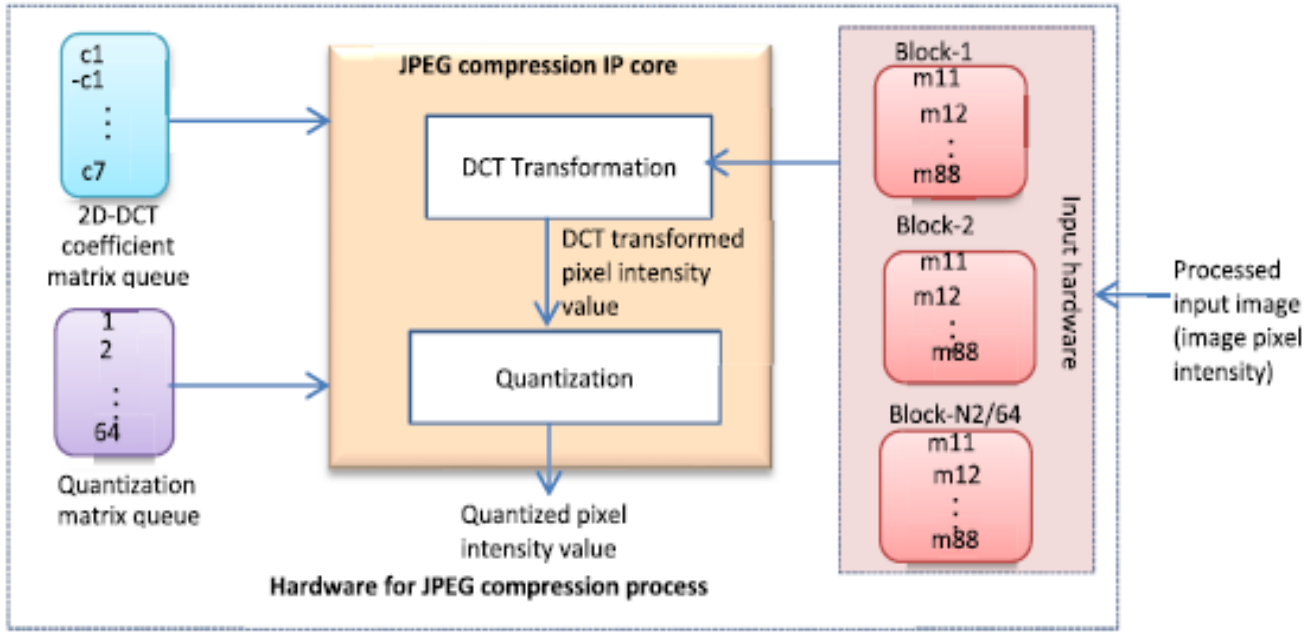


FIGURE 13. Hardware of JPEG compression process.

• Proposed Methodology

C4	C4	C4	C4	C4	C4	C4	C4
C1	C3	C5	C7	-C7	-C5	-C3	-C1
C2	C6	-C6	-C2	-C2	-C6	-C6	C2
C3	-C7	-C1	-C5	C5	C1	C7	-C3
C4	-C4	-C4	C4	C4	-C4	-C4	C4
C5	-C1	C7	C3	-C3	-C7	C1	-C5
C6	-C2	C2	-C6	-C6	C2	-C2	C6
C7	-C5	C3	-C1	C1	-C3	C5	-C7

FIGURE 14. 2D- DCT coefficient matrix.

• Proposed Methodology

TABLE 4. Register/color allocation of storage variables of 8-point DCT after implanting steganography.

T	Pink	Indigo	Violet	Green	Yellow	Orange	Red	Black
0	V0	V1	V2	V3	V4	V5	V6	V7
1	V9	V8	V11	V10	V4	V5	V6	V7
2	--	V16	V11	V10	V12	V13	V14	V15
3	V17	--	V11	--	V12	V13	V14	V15
4	--	V18	--	--	V12	V13	V14	V15
5	V19	--	--	--	--	V13	V14	V15
6	--	-V20	--	--	--	--	V14	V15
7	V21	--	--	--	--	--	--	V15
8	--	V22	--	--	--	--	--	--

• Proposed Methodology

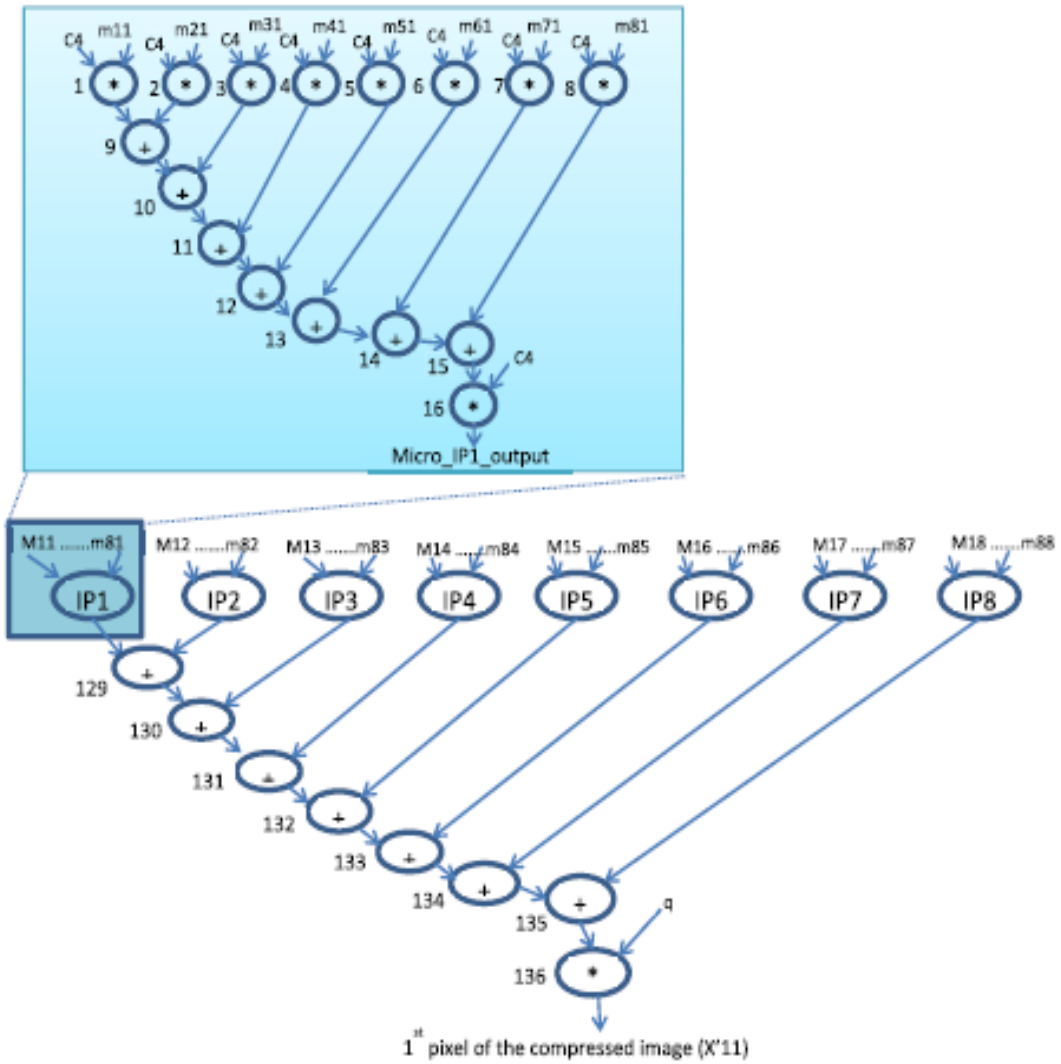


FIGURE 15. DFG of un-obfuscated JPEG compression IP core as macro IP comprising 8 micro-IPs underneath.

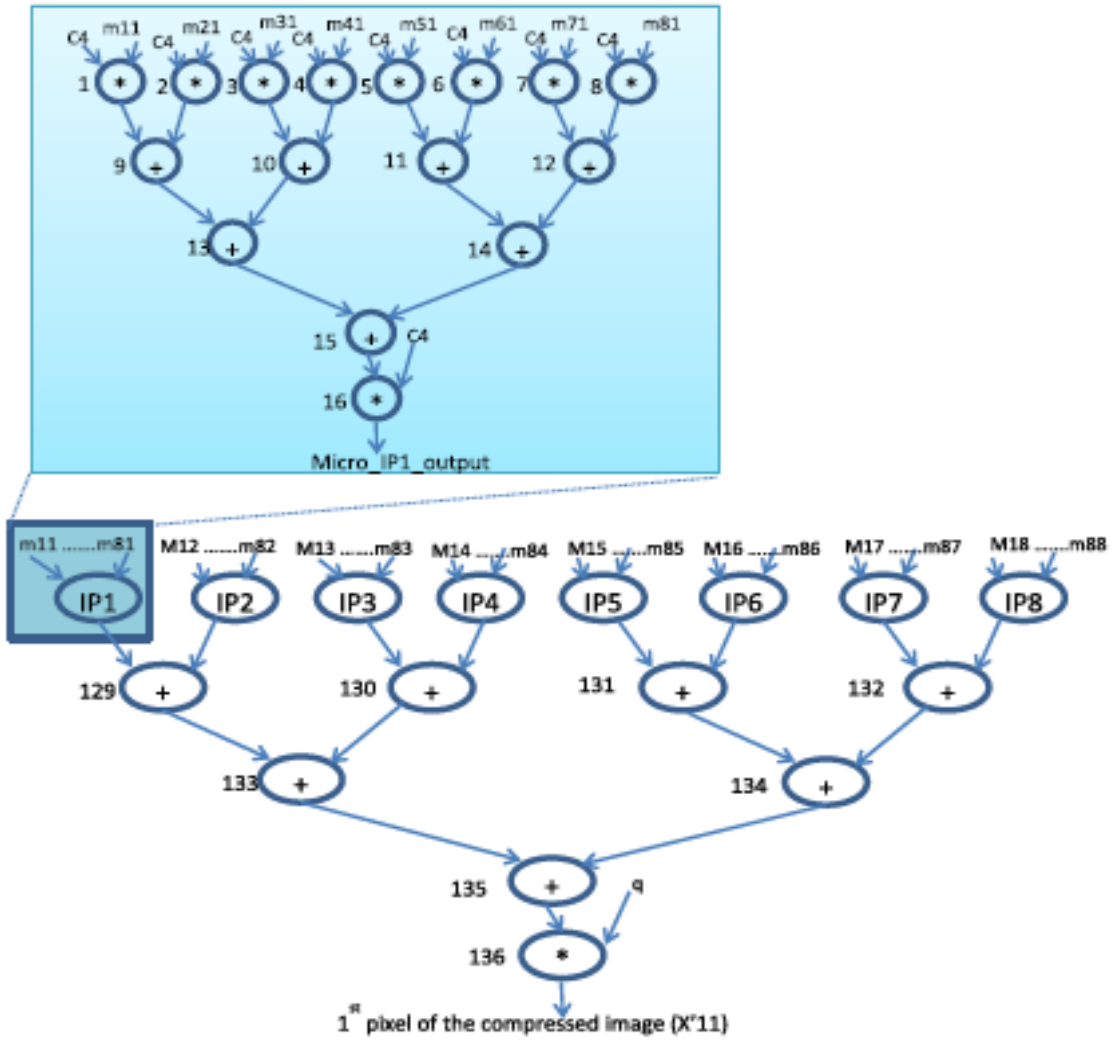


FIGURE 16. Structurally obfuscated DFG of JPEG CODEC IP core.

• Proposed Methodology

TABLE 6. Scheduling of JPEG compression hardware after implanting steganography.

T	Operations assign to M_1^1	Operations assign to M_2^1	Operations assign to M_1^2	Operations assign to A_1^1	Operations assign to A_2^1	Operations assign to A_1^2
1	1	3	2	--	--	--
2	5	6	4	9	--	--
3	7	17	8	11	--	10
4	19	20	18	13	--	12
5	21	23	22	25	26	14
6	33	34	24	15	27	29
7	35	37	36	41	--	28
8	39	40	38	42	--	30
9	49	51	50	43	45	44
10	53	54	52	31	57	46
11	55	65	56	59	47	58
12	67	68	66	61	--	60
13	69	71	70	73	74	62
14	81	82	72	63	75	77
15	83	85	84	89	--	76
16	87	88	86	90	--	78
17	97	99	98	91	93	92
18	101	102	100	79	105	94
19	103	113	104	95	107	106
20	115	116	114	--	109	108
21	117	119	118	121	122	110
22	32	120	16	111	123	125
23	64	80	48	129	--	124
24	112	--	96	130	--	126
25	--	--	--	127	131	133
26	--	--	128	--	--	--
27	--	--	--	--	--	132
28	--	--	--	--	--	134
29	--	--	--	135	--	--
30	--	136	--	--	--	--

• Proposed Methodology

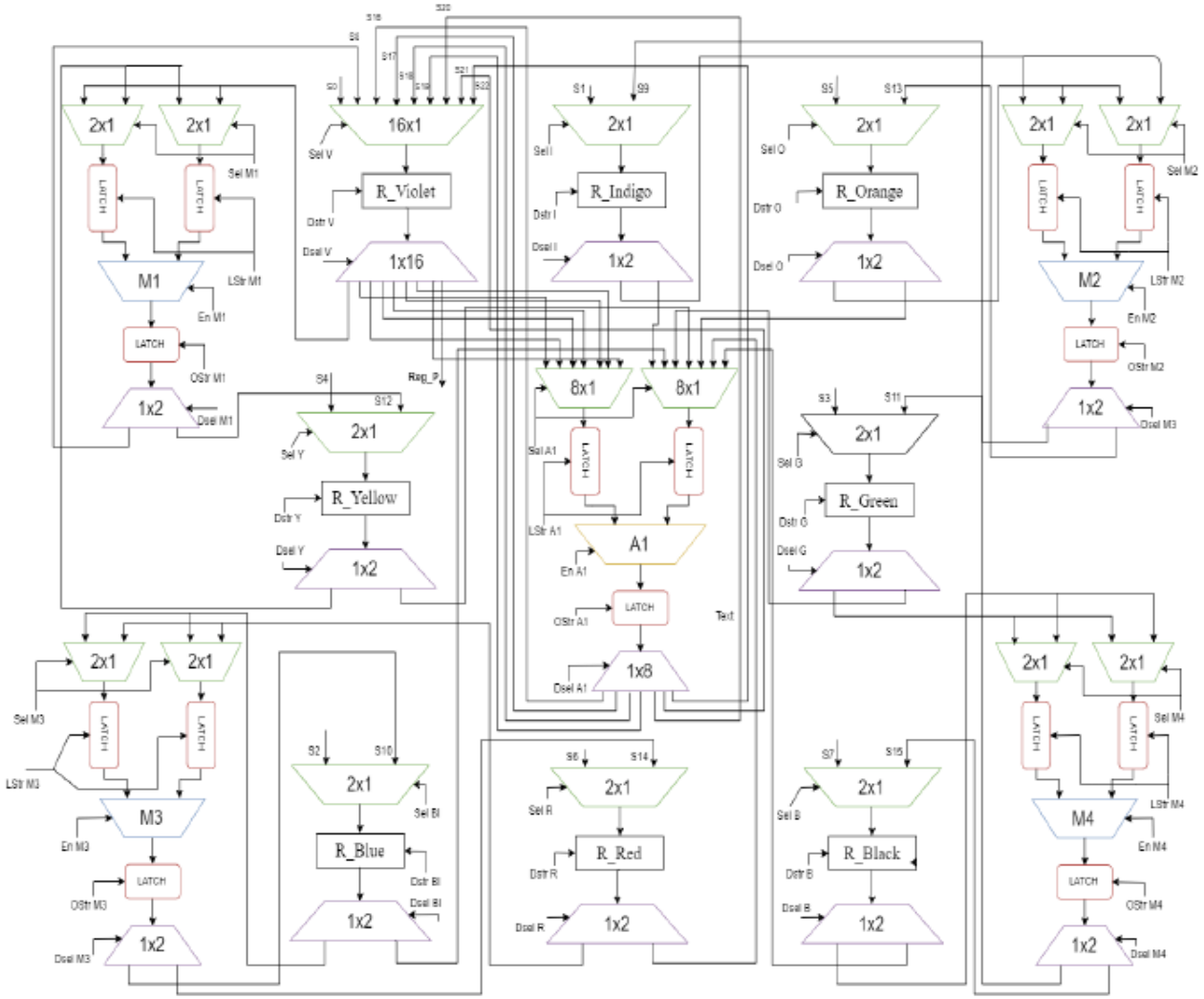


FIGURE 20. Un-obfuscated JPEG DCT core.

• Proposed Methodology

TABLE 8. Comparison of JPEG hardware pre and post structural obfuscation.

	Resource Configuration	Structural changes due to proposed obfuscation
Non-obfuscated JPEG hardware	4+, 8*, 12(8:1 mux), 12(16:1 mux), 6(1:8 demux), 6(1:16 demux)	10064 gates
Structurally obfuscated JPEG hardware	3+,3*,10(32:1mux), 2(16:1 mux), 5(1:32 demux), 1(1:16 demux)	

TABLE 9. Effective number of 0's and 1's for different size of stego-constraints.

Design solution (resource constraint)	Total # of constraint =100		Total # of constraint =200		Total # of constraint =300		Total # of constraint =400	
	Effective # of 0's embedded	Effective # of 1's embedded	Effective # of 0's embedded	Effective # of 1's embedded	Effective # of 0's embedded	Effective # of 1's embedded	Effective # of 0's embedded	Effective # of 1's embedded
3+, 3*	42	49	89	93	139	111	197	111
3+, 5*	48	48	97	94	148	122	203	122
5+, 5*	49	49	98	93	153	124	208	124
7+, 9*	40	59	87	108	135	131	186	131
9+, 9*	44	55	93	104	142	132	188	132
11+, 11*	53	46	109	89	160	131	217	131

• Proposed Methodology

TABLE 10. Security analysis (in terms of probability of coincidence) of proposed approach on varying size of stego-constraints for different design solutions.

Design solution	# of constraint =100		# of constraint =200		# of constraint =300		# of constraint =400	
	Pc^1	Pc^2	Pc^1	Pc^2	Pc^1	Pc^2	Pc^1	Pc^2
3+, 3*	5.21 e-1	1.6245e-3	2.5161e-1	4.4e-6	1.1589e-1	2.4e-7	4.715e-2	9.89e-8
3+, 5*	4.75e-1	1.732e-2	2.222e-1	3.39e-4	1.008e-1	2.228e-5	4.296e-1	9.497e-6
5+, 5*	4.68e-1	6.329e-2	2.188e-1	4.913e-3	9.328e-2	5.907e-4	3.976e-2	2.518e-4
7+, 9*	5.38e-1	2.092e-1	2.595e-1	4.61e-2	1.233e-1	1.515e-2	5.59e-2	6.87e-3
9+, 9*	5.06e-1	2.552e-1	2.364e-1	6.496e-2	1.106e-1	2.146e-2	5.42e-2	1.051e-2
11+, 11*	4.40e-1	3.001e-1	1.845e-1	8.816e-2	8.368e-2	2.821e-2	3.458e-2	1.166e-2

TABLE 11. Design cost analysis of proposed approach on varying size of stego-constraints for different design solutions.

Design solution	Pre-steganography cost	# of constraint= 100		# of constraint= 200		# of constraint= 300		# of constraint= 400	
		Cost (Phase-1)	Cost (Phase-1 & Phase-2)	Cost (Phase-1)	Cost (Phase-1 & Phase-2)	Cost (Phase-1)	Cost (Phase-1 & Phase-2)	Cost (Phase-1)	Cost (Phase-1 & Phase-2)
3+, 3*	0.2167	0.2167	0.2167	0.2167	0.2169	0.2167	0.2173	0.2167	0.2173
3+, 5*	0.1917	0.1917	0.1920	0.1917	0.1924	0.1917	0.1929	0.1917	0.1929
5+, 5*	0.1713	0.1713	0.1713	0.1713	0.1713	0.1713	0.1719	0.1713	0.1719
7+, 9*	0.1718	0.1718	0.1720	0.1718	0.1725	0.1718	0.1729	0.1718	0.1729
9+, 9*	0.1752	0.1752	0.1754	0.1752	0.1757	0.1752	0.1763	0.1752	0.1763
11+, 11*	0.1785	0.1785	0.1785	0.1785	0.1789	0.1785	0.1794	0.1785	0.1794

References

[1] D. A. Koff and H. Shulman, ``An overview of digital compression of medical images: Can we use lossy image compression in radiology?" Can. Assoc. Radiol. J., vol. 57, no. 4, pp. 211217, 2006.
[2] S. Gokturk, C. Tomasi, B. Girod, and C. Beaulieu, ``Medical image compression based on region of interest, with application to colon CT images,'' in Proc. Conf. 23rd Annu. Int. Conf. IEEE Eng. Med. Biol. Soc., vol. 3, Aug. 2005, pp. 24532456.
[3] S. B. Gokturk. Region of Interest Based Medical Image Compres- sion. Accessed: Aug. 2019. [Online]. Available: http://ai.stanford.edu/~gokturkb/Compression/FinalReport.htm
[4] Y.-Y. Chen and S.-C. Ti, ``Embedded medical image compression using DCT based subband decomposition and modied SPIHT data organization,'' in Proc. 4th IEEE Symp. Bioinf. Bioeng., Oct. 2004, pp. 167174.
[5] Y.-Y. Chen, ``Medical image compression using DCT-based subband decomposition and modied SPIHT data organization," Int. J. Med. Inform., vol. 76, no. 10, pp. 717725, Oct. 2007.
[6] R. Agarwal, C. S. Salimath, and K. Alam, ``Multiple image compression in medical imaging techniques using wavelets for speedy transmission and optimal storage," Biomed. Pharmacol. J., vol. 12, no. 1, pp. 183198, Mar. 2019.
[7] X. Zhang and M. Tehranipoor, ``Case study: Detecting hardware trojans in third-party digital IP cores," in Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust, San Diego CA, USA, Jun. 2011, pp. 6770.
[8] Maxim. Accessed: May. [Online]. Available: https://www.maxim integrated.com/en/app-notes/index.mvp/id/545
[9] SMT Corp. Counterfeit Detection. Accessed: May 2019. [Online]. Available: https://www.smtcorp.com/counterfeit-detection
[10] A. Sengupta, D. Roy, and S. P. Mohanty, ``Triple phase watermarking for reusable ip core protection during architecture synthesis," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 37, no. 4, pp. 742755, Apr. 2018.
[11] A. Sengupta, D. Roy, S. P. Mohanty, and P. Corcoran, ``DSP design protection in CE through algorithmic transformation based structural obfuscation,'' IEEE Trans. Consum. Electron., vol. 63, no. 4, pp. 467476, Nov. 2017.
[12] Y. Lao and K. K. Parhi, ``Obfuscating DSP circuits via highlevel transformations,'' IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 23, no. 5, pp. 819830, May 2015.

References

[13] A. Sengupta, D. Roy, S. P. Mohanty, and P. Corcoran, ``Low-cost obfuscated JPEG CODEC IP core for secure CE hardware," IEEE Trans. Con-sum. Electron., vol. 64, no. 3, pp. 365374, Aug. 2018.

[14] A. Sengupta, R. Sedaghat, and Z. Zeng, ``A high level synthesis design ow with a novel approach for efcient design space exploration in case of multi-parametric optimization objective," Microelectron. Rel., vol. 50,
no. 3, pp. 424437, Mar. 2010.

[15] M. C. McFarland, A. C. Parker, and R. Camposano, ``Tutorial on high level synthesis," in Proc. 25th ACM/IEEE Design Autom. Conf. (DAC), Hoboken, NJ, USA, Jun. 1988, pp. 330336.

[16] A. Sengupta and S. Bhadauria, ``Exploring low-cost optimal watermark for reusable IP cores during high level synthesis," IEEE Access, vol. 4, pp. 21982215, 2016.

[17] F. Koushanfar, I. Hong, and M. Potkonjak, ``Behavioral synthesis techniques for intellectual property protection," ACM Trans. Des. Autom. Electron. Syst., vol. 10, no. 3, pp. 523545, Jul. 2005.

[18] NanGate 15 nm Open Cell Library. Accessed: Jun. 2019. [Online]. Available: http://www.nangate.com/?pageid=2328

[19] Kegal. CT Medical Images. Accessed: Jul. 2019. [Online]. Available: https://www.kaggle.com/kmader/siim-medical-images/home

[20] A. Sengupta and M. Rathor, ``Protecting DSP kernels using robust hologrambased obfuscation," IEEE Trans. Consum. Electron., vol. 65, no. 1, pp. 99108, Feb. 2019.

[21] A. Sengupta and M. Rathor, ``IP core steganography for protecting DSP kernels used in CE systems," IEEE Trans. Consum. Electron., vol. 65, no. 4, pp. 506515, Nov. 2019.

[22] B. Le Gal and L. Bossuet, ``Automatic low-cost IP watermarking technique based on output mark insertions," Des. Autom. Embedded Syst., vol. 16, no. 2, pp. 7192, Jun. 2012.

[23] A. Sengupta and D. Roy, ``Anti-piracy aware IP chipset design for CE devices: Robust watermarking approach," IEEE Consum. Electron. Mag.,vol. 6, no. 2, pp. 24118, 2017.

THANK YOU