



P

A Framework

Cryptographic





# Project Sunflower: Work for Self-Documenting Research in Distributed Re- Systems

CONFIDENTIAL DRAFT

BILAL EL

August 25, 2025





g  
obotic

























# **Abstract**

Digital images and videos need for reliable authenticity (IoT) workflows. This introduces a *watermarking scheme* that is embedded into media files while remaining

Using a new technique, we validated an end-to-end system platform composed of a mobile Nano<sup>TM</sup> base station.

The contribution is twofold: (i) a faint visible overlay for injected into PDF metadata, in image data. Second, the artifact—every technique you are reading and can be

Benchmarks conducted on after up to 90% JPEG compression frame on the Jetson platform.

per frame on the Jetson platform  
95% accuracy and 250 ms latency  
verification in resource-constrained

The project lays a practical  
pipelines into existing robotic  
research in tamper-evident



circulate at unprecedented speed, creating  
ty checks in journalism, robotics, and Internet  
ternship investigates a *multi-layered stega*  
embeds cryptographic evidence of provenance  
aining imperceptible to end users.

re built, optimised, implemented, and exper  
olution that runs in real time on a distrib  
obile Raspberry Pi 5 rover and an NVIDIA<sup>®</sup> J

d. First, we introduce an *adaptive tri-layer* v  
r baseline compliance, (ii) zero-width Unicode  
, and (iii) a robust frequency-domain payload  
e present document is itself the primary v  
described herein is actively deployed withi  
e detected via the bundled `self_verify.py`.

a 10 000-image data set show **99.8%** extraction  
pression, with an average processing latency  
platform. These results exceed the target speci

uniform. These results exceed the target specification, demonstrating the feasibility of secure communication in constrained environments.

lay a solid foundation for integrating trustworthy wireless sensor and IoT systems and opens avenues for future research in data distribution.

*August 2024*





an urgent  
t of Things  
*unographic*  
ce directly

rimentially  
uted edge  
etson Orin

*watermark:*  
de markers  
embedded  
erification  
n the PDF  
y script.

n accuracy  
r of 150 ms  
fiction of

lication of  
ure media

watermark  
for further

Bilal

*st 25, 2025*





















**Acknowledg**

*“If I have seen further*

**Dr. Firstname Lastname**  
and for never objecting wh

**Institutional and industr**  
the confidence—and spare  
(*DSI*). Special thanks to Eng  
Marrakesh test site.

**Adept Technical Team**  
the Adept *Rasp-Claws* ro  
manual/1708721/Adept  
ber of pre-dawn questions  
ment ADR015 HAT board  
smoke.

**Open-source community.** and the countless GitHub co I could even formulate their hours.

**Lab colleagues.** M. El Fass mounts, and moral support proof-read Chapters 2 and alone.

**Family and friends.** Thank for the late-night coffee ru when the page counter say

**gements**



her, it is by standing on the shoulders of open

— for patient guidance, unflinching technical  
when my e-mails arrived at 02:00.

**rial partners.** The prototype would not exist  
e parts—of the *Direction des Systèmes d’In*  
g. A. Bennani for arranging out-of-hours ac

n. We are deeply grateful to the engineer  
ver (see manual at [https://www.manuals-  
-Raspclaws.html](https://www.manuals-<br/>-Raspclaws.html)) for answering a remark  
, sharing KiCad layer plots, and shipping two  
ls—*gratis*—after we inadvertently released

7. To the maintainers of ROS 2, rc1py, LoRa  
contributors whose issue threads solved problems  
m: your generosity converted weeks of debugging

i and S. Rai kindly lent oscilloscopes, 3-D-printer  
rt when the fifth carrier plate also sheared.  
3 with forensic zeal—any remaining typos

nk you for tolerating breadboards on the kit  
uns, and for reminding me that a thesis is for  
ys otherwise.



*e-hardware*  
*arachnids.”*

l feedback,

st without  
*nformation*  
cess to the

ers behind  
slib.com/  
kable num-  
vo replace-  
the magic

Mac-node,  
ems before  
gging into

nted motor  
F. Lahlou  
s are mine

chen table,  
finite even

# Content

**Abstract . . . .**

**Acknowledgements**

**1 Introduction**

1.1 Hypotheses

1.2 Context

1.3 Problem

1.4 Objectives

1.5 Contributions

1.6 Document Structure

**2 Technical Details**

2.1 Background

2.2 Related Work

2.3 Threat Models

2.3.1 *Adversary*

2.3.2 *Attacker*

	2.3.3	I
2.4	System R	
	2.4.1	F
	2.4.2	M
2.5	Design R	
	2.5.1	I
	2.5.2	M
	2.5.3	S
	2.5.4	C
	2.5.5	T
2.6	Formal S	
	2.6.1	F



ts

.....	
<b>ents</b> .....	
.....	
Analysis and Research Questions .....	
.....	
Statement .....	
es .....	
tions .....	
ent Structure .....	
<b>Deep Dive</b> .....	
und .....	
Work .....	
Model .....	
Assets .....	
Adversary Capabilities .....	

Defender Counter-Measure Space . . . . .	
Requirements . . . . .	
Functional . . . . .	
Non-Functional . . . . .	
Rationale . . . . .	
Layer Overview . . . . .	
Mapping Requirements to Layers . . . . .	
Synergy and Failure Modes . . . . .	
Computational Budget . . . . .	
Trade-offs . . . . .	
Specification . . . . .	
Embedding Layer . . . . .	



• • • • • • • • **iii**

• • • • • • • • **v**

• • • • • • • • **1**

• • • • • • • • • 1

• • • • • • • • 2

• • • • • • • • 3

• • • • • • • • • 4

• • • • • • • • • 4

• • • • • • • • • 4

• • • • • • • • **7**

• • • • • • • • • 7

• • • • • • • • 9

• • • • • • • • 10

• • • • • • • • 10

• • • • • • • • 10



## *CONTENTS*

	2.6.2	Embedding
	2.6.3	Extraction
	2.6.4	Reference
	2.6.5	Parameter
2.7		Security and Rob
2.8		Summary . . . .
<b>3</b>		<b>Implementation . . .</b>

3.1	Context . . . . .
3.2	Hardware Platform . . . . .
3.3	Software Architecture . . . . .
	3.3.1 Why a Microcontroller . . . . .
	3.3.2 Tier Overlap . . . . .
	3.3.3 Illustrative Example . . . . .
3.4	Communication . . . . .
	3.4.1 MQTT Topic . . . . .
	3.4.2 Message . . . . .
	3.4.3 Versioning . . . . .
3.5	Summary . . . . .
<b>4</b>	<b>Methodology . . . . .</b>
4.1	Data Set . . . . .
4.2	Metrics . . . . .
4.3	Robustness Protocol . . . . .
4.4	Statistical Confidence . . . . .
4.5	Visualisation Pipeline . . . . .
<b>5</b>	<b>Experimental Validation . . . . .</b>



5.1	Robustness Analysis
5.2	Latency . . . . .
5.3	Anchoring Cost
5.4	Payload Capacity
5.5	Summary . . . . .

## **6 Challenges & Skills**

6.1	Industrial Context
6.2	Technical Challenges
6.3	Professional Challenges
6.4	Skill Development
6.5	Reflection . . . . .

ing Pipeline . . . . .	1
n & Verification . . . . .	2
e Pseudo-code . . . . .	3
er Choices . . . . .	4
ustness Analysis . . . . .	5
. . . . .	6

Introduction	1
1.1 Motivation	1
1.2 Scope	1
1.3 Document Structure	1
2. Micro-Service, Multi-Pi Architecture?	2
2.1 Overview	2
2.2 Data Flow	2
2.3 Protocol	2
2.4 Topic Namespace	2
2.5 Payload Schemas	2
2.6 Logging and Compatibility	2
3. Conclusion	3
4. Appendix	4
4.1 Glossary	4
4.2 References	4
4.3 Bibliography	4
5. Acknowledgments	5
6. Bibliography	6
7. Index	7
8. Appendix	8
8.1 Glossary	8
8.2 References	8
8.3 Bibliography	8
9. Acknowledgments	9
10. Bibliography	10
11. Index	11
12. Appendix	12
12.1 Glossary	12
12.2 References	12
12.3 Bibliography	12
13. Acknowledgments	13
14. Bibliography	14
15. Index	15
16. Appendix	16
16.1 Glossary	16
16.2 References	16
16.3 Bibliography	16
17. Acknowledgments	17
18. Bibliography	18
19. Index	19
20. Appendix	20
20.1 Glossary	20
20.2 References	20
20.3 Bibliography	20
21. Acknowledgments	21
22. Bibliography	22
23. Index	23
24. Appendix	24
24.1 Glossary	24
24.2 References	24
24.3 Bibliography	24
25. Acknowledgments	25
26. Bibliography	26
27. Index	27
28. Appendix	28
28.1 Glossary	28
28.2 References	28
28.3 Bibliography	28
29. Acknowledgments	29
30. Bibliography	30
31. Index	31
32. Appendix	32
32.1 Glossary	32
32.2 References	32
32.3 Bibliography	32
33. Acknowledgments	33
34. Bibliography	34
35. Index	35
36. Appendix	36
36.1 Glossary	36
36.2 References	36
36.3 Bibliography	36
37. Acknowledgments	37
38. Bibliography	38
39. Index	39
40. Appendix	40
40.1 Glossary	40
40.2 References	40
40.3 Bibliography	40
41. Acknowledgments	41
42. Bibliography	42
43. Index	43
44. Appendix	44
44.1 Glossary	44
44.2 References	44
44.3 Bibliography	44
45. Acknowledgments	45
46. Bibliography	46
47. Index	47
48. Appendix	48
48.1 Glossary	48
48.2 References	48
48.3 Bibliography	48
49. Acknowledgments	49
50. Bibliography	50
51. Index	51
52. Appendix	52
52.1 Glossary	52
52.2 References	52
52.3 Bibliography	52
53. Acknowledgments	53
54. Bibliography	54
55. Index	55
56. Appendix	56
56.1 Glossary	56
56.2 References	56
56.3 Bibliography	56
57. Acknowledgments	57
58. Bibliography	58
59. Index	59
60. Appendix	60
60.1 Glossary	60
60.2 References	60
60.3 Bibliography	60
61. Acknowledgments	61
62. Bibliography	62
63. Index	63
64. Appendix	64
64.1 Glossary	64
64.2 References	64
64.3 Bibliography	64
65. Acknowledgments	65
66. Bibliography	66
67. Index	67
68. Appendix	68
68.1 Glossary	68
68.2 References	68
68.3 Bibliography	68
69. Acknowledgments	69
70. Bibliography	70
71. Index	71
72. Appendix	72
72.1 Glossary	72
72.2 References	72
72.3 Bibliography	72
73. Acknowledgments	73
74. Bibliography	74
75. Index	75
76. Appendix	76
76.1 Glossary	76
76.2 References	76
76.3 Bibliography	76
77. Acknowledgments	77
78. Bibliography	78
79. Index	79
80. Appendix	80
80.1 Glossary	80
80.2 References	80
80.3 Bibliography	80
81. Acknowledgments	81
82. Bibliography	82
83. Index	83
84. Appendix	84
84.1 Glossary	84
84.2 References	84
84.3 Bibliography	84
85. Acknowledgments	85
86. Bibliography	86
87. Index	87
88. Appendix	88
88.1 Glossary	88
88.2 References	88
88.3 Bibliography	88
89. Acknowledgments	89
90. Bibliography	90
91. Index	91
92. Appendix	92
92.1 Glossary	92
92.2 References	92
92.3 Bibliography	92
93. Acknowledgments	93
94. Bibliography	94
95. Index	95
96. Appendix	96
96.1 Glossary	96
96.2 References	96
96.3 Bibliography	96
97. Acknowledgments	97
98. Bibliography	98
99. Index	99
100. Appendix	100
100.1 Glossary	100
100.2 References	100
100.3 Bibliography	100
101. Acknowledgments	101
102. Bibliography	102
103. Index	103
104. Appendix	104
104.1 Glossary	104
104.2 References	104
104.3 Bibliography	104
105. Acknowledgments	105
106. Bibliography	106
107. Index	107
108. Appendix	108
108.1 Glossary	108
108.2 References	108
108.3 Bibliography	108
109. Acknowledgments	109
110. Bibliography	110
111. Index	111
112. Appendix	112
112.1 Glossary	112
112.2 References	112
112.3 Bibliography	112
113. Acknowledgments	113
114. Bibliography	114
115. Index	115
116. Appendix	116
116.1 Glossary	116
116.2 References	116
116.3 Bibliography	116
117. Acknowledgments	117
118. Bibliography	118
119. Index	119
120. Appendix	120
120.1 Glossary	120
120.2 References	120
120.3 Bibliography	120
121. Acknowledgments	121
122. Bibliography	122
123. Index	123
124. Appendix	124
124.1 Glossary	124
124.2 References	124
124.3 Bibliography	124
125. Acknowledgments	125
126. Bibliography	126
127. Index	127
128. Appendix	128
128.1 Glossary	128
128.2 References	128
128.3 Bibliography	128
129. Acknowledgments	129
130. Bibliography	130
131. Index	131
132. Appendix	132
132.1 Glossary	132
132.2 References	132
132.3 Bibliography	132
133. Acknowledgments	133
134. Bibliography	134
135. Index	135
136. Appendix	136
136.1 Glossary	136
136.2 References	136
136.3 Bibliography	136
137. Acknowledgments	137
138. Bibliography	138
139. Index	139
140. Appendix	140
140.1 Glossary	140
140.2 References	140
140.3 Bibliography	140
141. Acknowledgments	141
142. Bibliography	142
143. Index	143
144. Appendix	144
144.1 Glossary	144
144.2 References	144
144.3 Bibliography	144
145. Acknowledgments	145
146. Bibliography	146
147. Index	147
148. Appendix	148
148.1 Glossary	148
148.2 References	148
148.3 Bibliography	148
149. Acknowledgments	149
150. Bibliography	150
151. Index	151
152. Appendix	152
152.1 Glossary	152
152.2 References	152
152.3 Bibliography	152
153. Acknowledgments	153
154. Bibliography	154
155. Index	155
156. Appendix	156
156.1 Glossary	156
156.2 References	156
156.3 Bibliography	156
157. Acknowledgments	157
158. Bibliography	158
159. Index	159
160. Appendix	160
160.1 Glossary	160
160.2 References	160
160.3 Bibliography	160
161. Acknowledgments	161
162. Bibliography	162
163. Index	163
164. Appendix	164
164.1 Glossary	164
164.2 References	164
164.3 Bibliography	164
165. Acknowledgments	165
166. Bibliography	166
167. Index	167
168. Appendix	168
168.1 Glossary	168
168.2 References	168
168.3 Bibliography	168
169. Acknowledgments	169
170. Bibliography	170
171. Index	171
172. Appendix	172
172.1 Glossary	172
172.2 References	172
172.3 Bibliography	172
173. Acknowledgments	173
174. Bibliography	174
175. Index	175
176. Appendix	176
176.1 Glossary	176
176.2 References	176
176.3 Bibliography	176
177. Acknowledgments	177
178. Bibliography	178
179. Index	179
180. Appendix	180
180.1 Glossary	180
180.2 References	180
180.3 Bibliography	180
181. Acknowledgments	181
182. Bibliography	182
183. Index	183
184. Appendix	184
184.1 Glossary	184
184.2 References	184
184.3 Bibliography	184
185. Acknowledgments	185
186. Bibliography	186
187. Index	187
188. Appendix	188
188.1 Glossary	188
188.2 References	188
188.3 Bibliography	188
189. Acknowledgments	189
190. Bibliography	190
191. Index	191
192. Appendix	192
192.1 Glossary	192
192.2 References	192
192.3 Bibliography	192
193. Acknowledgments	193
194. Bibliography	194
195. Index	195
196. Appendix	196
196.1 Glossary	196
196.2 References	196
196.3 Bibliography	196
197. Acknowledgments	197
198. Bibliography	198
199. Index	199
200. Appendix	200
200.1 Glossary	200
200.2 References	200
200.3 Bibliography	200
201. Acknowledgments	201
202. Bibliography	202
203. Index	203
204. Appendix	204
204.1 Glossary	204
204.2 References	204
204.3 Bibliography	204
205. Acknowledgments	205
206. Bibliography	206
207. Index	207
208. Appendix	208
208.1 Glossary	208
208.2 References	208
208.3 Bibliography	208
209. Acknowledgments	209
210. Bibliography	210
211. Index	211
212. Appendix	212
212.1 Glossary	212
212.2 References	212
212.3 Bibliography	212
213. Acknowledgments	213
214. Bibliography	214
215. Index	215
216. Appendix	216
216.1 Glossary	216
216.2 References	216
216.3 Bibliography	216
217. Acknowledgments	217
218. Bibliography	218
219. Index	219
220. Appendix	220
220.1 Glossary	220
220.2 References	220
220.3 Bibliography	220
221. Acknowledgments	221
222. Bibliography	222
223. Index	223
224. Appendix	224
224.1 Glossary	224
224.2 References	224
224.3 Bibliography	224
225. Acknowledgments	225
226. Bibliography	226
227. Index	227
228. Appendix	228
228.1 Glossary	228
228.2 References	228
228.3 Bibliography	228
229. Acknowledgments	229
230. Bibliography	230
231. Index	231
232. Appendix	232
232.1 Glossary	232
232.2 References	232
232.3 Bibliography	232
233. Acknowledgments	233
234. Bibliography	234
235. Index	235
236. Appendix	236
236.1 Glossary	236
236.2 References	236
236.3 Bibliography	236
237. Acknowledgments	237
238. Bibliography	238
239. Index	239
240. Appendix	240
240.1 Glossary	240
240.2 References	240
240.3 Bibliography	240
241. Acknowledgments	241
242. Bibliography	242
243. Index	243
244. Appendix	244
244.1 Glossary	244
244.2 References	244
244.3 Bibliography	244
245. Acknowledgments	245
246. Bibliography	246
247. Index	247
248. Appendix	248
248.1 Glossary	248
248.2 References	248
248.3 Bibliography	248
249. Acknowledgments	249
250. Bibliography	250
251. Index	251
252. Appendix	252
252.1 Glossary	252
252.2 References	252
252.3 Bibliography	252
253. Acknowledgments	253
254. Bibliography	254
255. Index	255
256. Appendix	256
256.1 Glossary	256
256.2 References	256
256.3 Bibliography	256
257. Acknowledgments	257
258. Bibliography	258
259. Index	259
260. Appendix	260
260.1 Glossary	260
260.2 References	260
260.3 Bibliography	260
261. Acknowledgments	261
262. Bibliography	262
263. Index	263
264. Appendix	264
264.1 Glossary	264
264.2 References	264
264.3 Bibliography	264
265. Acknowledgments	265
266. Bibliography	266
267. Index	267
268. Appendix	268
268.1 Glossary	268
268.2 References	268
268.3 Bibliography	268
269. Acknowledgments	269
270. Bibliography	270
271. Index	271
272. Appendix	272
272.1 Glossary	272
272.2 References	272
272.3 Bibliography	272
273. Acknowledgments	273
274. Bibliography	274
275. Index	275
276. Appendix	276
276.1 Glossary	276
276.2 References	276
276.3 Bibliography	276
277. Acknowledgments	277
278. Bibliography	278
279. Index	279
280. Appendix	280
280.1 Glossary	280
280.2 References	280
280.3 Bibliography	280
281. Acknowledgments	281
282. Bibliography	282
283. Index	283
284. Appendix	284
284.1 Glossary	284
284.2 References	284
284.3 Bibliography	284
285. Acknowledgments	285
286. Bibliography	286
287. Index	287
288. Appendix	288
288.1 Glossary	288
288.2 References	288
288.3 Bibliography	288
289. Acknowledgments	289
290. Bibliography	290
291. Index	291
292. Appendix	292
292.1 Glossary	292
292.2 References	292
292.3 Bibliography	292
293. Acknowledgments	293
294. Bibliography	294
295. Index	295
296. Appendix	296
296.1 Glossary	296
296.2 References	296
296.3 Bibliography	296
297. Acknowledgments	297
298. Bibliography	298
299. Index	299
300. Appendix	300
300.1 Glossary	300
300.2 References	300
300.3 Bibliography	300
301. Acknowledgments	301
302. Bibliography	302
303. Index	303
304. Appendix	304
304.1 Glossary	304
304.2 References	304
304.3 Bibliography	304
305. Acknowledgments	305
306. Bibliography	306
307. Index	307
308. Appendix	308
308.1 Glossary	308
308.2 References	308
308.3 Bibliography	308
309. Acknowledgments	309
310. Bibliography	310
311. Index	311
312. Appendix	312
312.1	

[illegible]

vii

. . . . 14

. . . . 14

. . . 15

. . . 15

. . . 15

. . . 16

. . . **17**

.	.	.	.	17
.	.	.	.	17
.	.	.		18
.	.	.		18
.	.	.		19
.	.	.		19
.	.	.		19
.	.	.		19
.	.	.		20
.	.	.		20
.	.	.		20
.	.	.		<b>23</b>
.	.	.		23
.	.	.		23
.	.	.	.	24
.	.	.	.	24
.	.	.		25
.	.	.		<b>27</b>

.	.	.	.	27
.	.	.		28
.	.	.		28
.	.	.		28
.	.	.		29
.	.	.		<b>31</b>
.	.	.	.	31
.	.	.	.	31
.	.	.		32
.	.	.		32
.	.	.		32

**7 Conclusion and**

**Glossary . . . .**

**Discrete Wavele**

**Supplementary**



## List of F

2.1 Steganog

2.2 Concept  
under m  
scheme m

2.3 Tri-layer  
metadata  
latency t  
path sho

2.1 Contain

5.1 Containers.

5.1 Extraction

5.2 Digest and  
tract: 0x

1 Single-le

2 Extraction

3 Latency

<b>and Future Work . . . . .</b>	<b>1</b>
<b>. . . . .</b>	<b>1</b>
<b>Transform Refresher . . . . .</b>	<b>2</b>
<b>Plots . . . . .</b>	<b>3</b>

pts . . . . .

# Figures

graphic trade-off triangle . . . . .

ual robustness comparison. The LSB watermarking scheme achieves minor compression, while a frequency-domain watermarking scheme remains robust. . . . .

r watermarking automaton: parallel embedding, temporal masking, and frequency layers (C1) enabling robustness targets (O2), and end-to-end integration (O3) enabling graceful degradation and defence-in-depth.

urised service flow across router gateway and

erised service flow across router, gateway, and

. . . . .

on accuracy vs JPEG . . . . .

anchoring fee vs batch size; sweet spot at  $n$

ABC123..789. Placeholder pending receipts.

level 2-D DWT band layout (LL, LH, HL, HH)

on accuracy vs JPEG quality (representative

/ anchoring cost breakdown (auto-generate

..... 35

..... 37

..... 41

..... 43

. . . . . 45

. . . . . 8

mark collapses  
n DWT–SVD

. . . . . 9

ing of visible,  
ustness (O1),  
. Verification

pth. . . . . 12

home server

home server	
. . . . .	21
. . . . .	28
= 128. Con-	
. . . . .	29
). . . . .	42
). . . . .	43
ed). . . . .	43



*LIST OF TABLES*

**List of Tables**

- 2.1 Layer coverage of  
source dependent
- 2.2 Threat / layer imp  
data, F=Frequency  
~~X~~removed/invalid
- 3.1 Technical specific  
summary). . . .
- 3.2 Canonical MQTT
- 4.1 JPEG ladder used



es

of requirements (✓ = contributes, != partial  
t). . . . .  
Impact matrix. Legend: V=Visible overlay, M=M  
y watermark. Impact: ✓ unaffected, !=degraded.  
d. . . . .  
cation of the RaspClaws V3 mobile agent (st  
. . . . .  
T topics ({id} denotes a rover; +/# are wildc  
l in robustness sweep . . . . .



ix

l/re-

. . . 13

meta-

ded,

. . . 16

tatic

. . . 18

cards). 19

. . . . 24





X











# *LIST OF TABLES*







# Chapter 1

# Introduction

## Overview

Digital images and video are vulnerable to authenticity checks, posing risks: institutional digital trust [2], and coordinated manipulation of media. The *digital watermark* that embeds information, remaining invisible to the viewer. In fact, this very paragraph contains **5** marks in total.

---

<sup>a</sup>The techniques described in `self_verify.py`.

# 1.1 Hypothesis

**Hypothesis.** The proposed watermarking pipeline will achieve a PSNR  $\geq 95\%$  after aggressive compression and minor geometric distortions, with an embedding time  $\leq 250$  ms and extract  $\leq 30$  ms, and an on-chain verification fee  $< 0.001$  ETH.



n

os circulate at unprecedented speed, demand  
ks. Recent surveys and analyses highlight sy  
al service mandates [1], deepfake proliferation  
dinated misinformation campaigns [3] amp  
his project explores a *multi-layered stegan*  
eds cryptographic evidence of provenance  
end users.<sup>a</sup>

raph contains one hidden mark, and there a

---

cribed in this thesis can be verified with

# and Research Questions

sed tri-layer (visible cue, metadata, frequency  
ill meet all targets: Robustness: extraction  
mpression (JPEG quality  $\leq 10\%$ ,  $\approx 90\%$  size  
ortion (rotation  $\leq 5^\circ$ , resize  $\leq 10\%$ ). Latency  
00 ms per frame on the Jetson Orin Nano. Cost  
 $< \$0.001$ .





ding re-  
systemic  
on erod-  
plifying  
*ograph-*  
e while

re now

python

...y-domain)  
...n accuracy  
...reduction)  
...cy: embed  
Cost: daily

2

## Research Questions

**RQ1** Can b  
comp

**RQ2** Can e  
const

## 1.2 Context

Before delving into the *where*, *why*, and *how* of the project, we first describe the context in which the project is taking place. The project is a private–public partnership (PPP) in a private–public partnership (PPP) conditions still in

**Institutional Setting**  
the project remains in the *des Systèmes d’Information* (DSI) roccan agencies and combines agility (navigability, guidance, scale path) and long-term maintenance

## Operational Scenario

km-radius test farm  
currently lacks wi  
lightweight rover  
density, moisture a  
The gateway back  
or technician hot  
resilience), (ii) a l  
optional visible cu

---

<sup>1</sup>Throughout this t  
Pi 5; earlier wheeled p

## *CHAPTER 1*

**ons.**

blind extraction remain  $\geq 95\%$  accurate under  
compression and small geometric noise?

end-to-end (embed+extract) latency stay within  
trained edge hardware?

unified capture → edge pipeline integrate w  
impairing rover telemetry or gateway duties?

**xt**

to circuitry, firmware, and network stacks, t  
and *for whom* of the prototype. Although the p  
c laboratory rather than a profit-driven firm  
pose very real design constraints.

**ting.** Prototyping is conducted in a small h  
ns formally linked to the regional university  
*formation* (DSI), the public body that overse  
nd sponsors the forthcoming field trial [4, 1]  
rapid iteration) with institutional support (tes  
th). Because the DSI evaluates rather than pu  
inability rests with the project team and fut



**Scenario (Planned).** The first planned deployment is a system managed by the DSI on the outskirts of Mexico. It has limited connectivity and relies on a small solar panel. The rover will patrol crop rows and emit computer-vision data (e.g., anomalies) to a gateway perched on a tripod. The gateway back-hauls traffic via opportunistic WAN links (e.g., satellite spot), motivating: (i) a frequency-domain lossy compression, (ii) a lightweight metadata layer (fast integrity checks), and (iii) a (human trust signal) without large bandwidth.

---

In this thesis the term *rover* refers to the RaspClaws hexapod. The prototypes were not fabricated.

## . *INTRODUCTION*

nder extreme JPEG

thin 250/300 ms on

watermarking with-  
?

This section clarifies  
project is incubated  
in, the surrounding

some workshop, yet  
y and the *Direction*  
es IT pilots for Mo-  
. This arrangement  
st plots, compliance  
urchases the system,  
ture contributors.

ployment site is a 2  
Tarrakesh. The field  
shed for power. A  
on alerts (e.g. weed  
at the field's edge.<sup>1</sup>  
s (4G USB modem  
ayer (compression  
check), and (iii) an  
width overhead.

fitted with a Raspberry

### *1.3. PROBLEM STATEMENT*

#### **Non-Negotiable Constraints**

<b>Budget</b>	Only off
---------------	----------

<b>Man-hours</b>	Two par automat
------------------	--------------------

<b>Safety</b>	Cryptog tion)
---------------	------------------

tion).

## Quality Attributes.

**Reproducibility** Full rebo  
dent val

**Traceability** Logs and  
analysis

**Evolvability** Swap Lo  
ized cha

The remainder of this chapter  
class field gateway, and the  
demands.

## 1.3 Problem Statement

While many watermarking schemes lack *acceptability, robustness to common image processing operations*, and are *resource-constrained* edge devices.

**Robustness bottleneck**      *geometric transformations*

**Performance gap**      Latency

**Integration gap**      Lack of standardization, *edge device integration*

*NT*

**ints.**

off-the-shelf parts (public procurement compliance)

part-time graduate students;  $\leq 8$  on-site test days (reduction).

graphic command auth + physical e-stop (reduction)



build + dual TTGO flashing <1 hour (enable  
validation).

and VPN audits archived one academic year (pos  
s + compliance).

LoRa spreading factors or inference models v  
anges (future-proofing).

apter shows how the dual-radio LoRa link, t  
ne IP-level VPN collectively satisfy these c

**atement**

g techniques exist, few simultaneously satisfy *common transformations*, and *real-time performance* on mobile devices. Concretely, this thesis tackles three

Failures under  $\geq 90\%$  JPEG compression, geometric distortion (rotation  $\leq 5^\circ$ , resize  $\leq 10\%$ )

are too high for real-time embedded video synthesis

of end-to-end systems spanning mobile camera verification.

liance).

ays (forces

risk mitiga-

s indepen-

st-incident

with local-

the laptop-  
contextual

isfy *imper-*  
*formance* on  
ee gaps:

a or minor  
%).

streams.

apture *and*

4

## **1.4 Object**

All objectives are

**O1 Robustness**

**O2 Latency**

## O3 Integration

## O4 Verifiability

### 1.5 Contr

C1 Adaptive tr  
domain) (CH

C2 Real-time d

C3 Empirical ev

C4 Self-verifying

*Traceability:* O1—

**Section 1.3** provides background + design (correctness, latency);

## 1.6 Document

Chapter 2 surveys the hardware and



# **tives**

framed as measurable targets:

Blind extraction accuracy  $\geq 95\%$  after JP  
and minor geometric noise.

Embed  $< 250$  ms; extract  $< 300$  ms per f

Nano).

Demonstrate rover (Pi 5) capture  $\rightarrow$  secure real-time edge verification.

Produce a self-demonstrating document embedding watermark layers with public verification.

## Contributions

Multi-layer watermarking scheme (visible, metadata, Chapter 2).

Distributed edge-AI platform (Chapter 3).

Real-time evaluation exceeding robustness + latency targets.

Open-source PDF + tooling (Appendix 7).

$O1 \rightarrow C3$ ;  $O2 \rightarrow C3$ ;  $O3 \rightarrow C2$ ;  $O4 \rightarrow C4$  (enabled by

# Roadmap

problem framing; **Section 1.4** objectives; **Chapter 2** design; **Chapter 3** system build; **Chapter 5** validation; **Chapter 7** synthesis and future work.

---

## Document Structure

Chapter 1 presents the theoretical background and related work; Chapter 2 presents software architecture; Chapter 5 presents

## . *INTRODUCTION*

EG quality  $\leq 10\%$

frame (Jetson Orin

re transmission  $\rightarrow$

embedding the same  
script.

etadata, frequency-

targets (Chapter 5).

C1).

**Chapter 2** back-  
validation (robust-

k; Chapter 3 details  
the experimental

## *1.6. DOCUMENT STRUCTURE*

methodology and quantitative  
outlines future research av

As you proceed, remember  
ment itself is part of the ex  
by the end of this introdu  
verification script in Appe







*URE*

ative results; Chapter 7 summarizes key findings and conclusions.  
venues.

r the principle introduced in the overview:  
periment. The invisible watermarking layer  
action a total of 5 marks have been embedded.  
ndix 7 can detect them.





adings and

this docu-  
r is active;  
dded. The













# *CHAPTER 1*





# . *INTRODUCTION*







# Chapter 2

# Technical D

## 2.1 Background

Steganography—literally ‘*and graphein* (to write)—is sight. Classical anecdotes messenger’s head, tattooed to regrow before dispatching only the canvas has evolved files, and this narrative lin

**Core terminology.** We an unaltered carrier file (message) is the bit sequenc

provenance data. After emb

where  $K$  is a secret key.<sup>1</sup>

**The steganographic trian**  
ing attributes:

---

<sup>1</sup>Unicode metadata for the  
steganographic data hiding.



# Deep Dive

d

‘covered writing’ from the Greek *steganos*—the art and science of concealing information—abound: Herodotus recounts how Histiaeus hid a secret message on the scalp, and waited for a friend to shave him. The principle is unchanged in the modern era, from skin and parchment to images, audio, and video. A cover medium discreetly carries a hidden mark.

We will use three canonical terms. A *cover medium* (e.g. a JPEG photograph). The *payload*  $P$  (the message to be hidden—here a cryptographic HMAC).

bedding, the file becomes the *stego-medium*  $S$

$$S = \text{embed}(C, P, K),$$

**angle.** Every practical scheme balances thro

---

font used in this sentence is another (less robust)



s (covered)  
on in plain  
s shaved a  
or the hair  
digital era;  
o, and text

$C$  denotes  
embedded  
 $C$  encoding



9. Formally

$$(2.1)$$

ee compet-

channel for

8

- (i) **Capacity** —
- (ii) **Imperceptibility**
- (iii) **Robustness**  
of  $S$ .

These form the St  
one dimension typ

high imperceptibility  
sentence encodes

C

Figure 2.1: The st  
evitably pulls one

**Technique tax**

**Spatial-domain (**

bit of each pixel channel collapses under loss. While offering high Fig. 2.2, integrity frequency-domain

**Frequency-domain** quantisation) [5]. hybrid leveraging boost robustness view DWT–SVD on DWT sub-bands Section 2.6.1, and

## CHAPTER 2. TECH

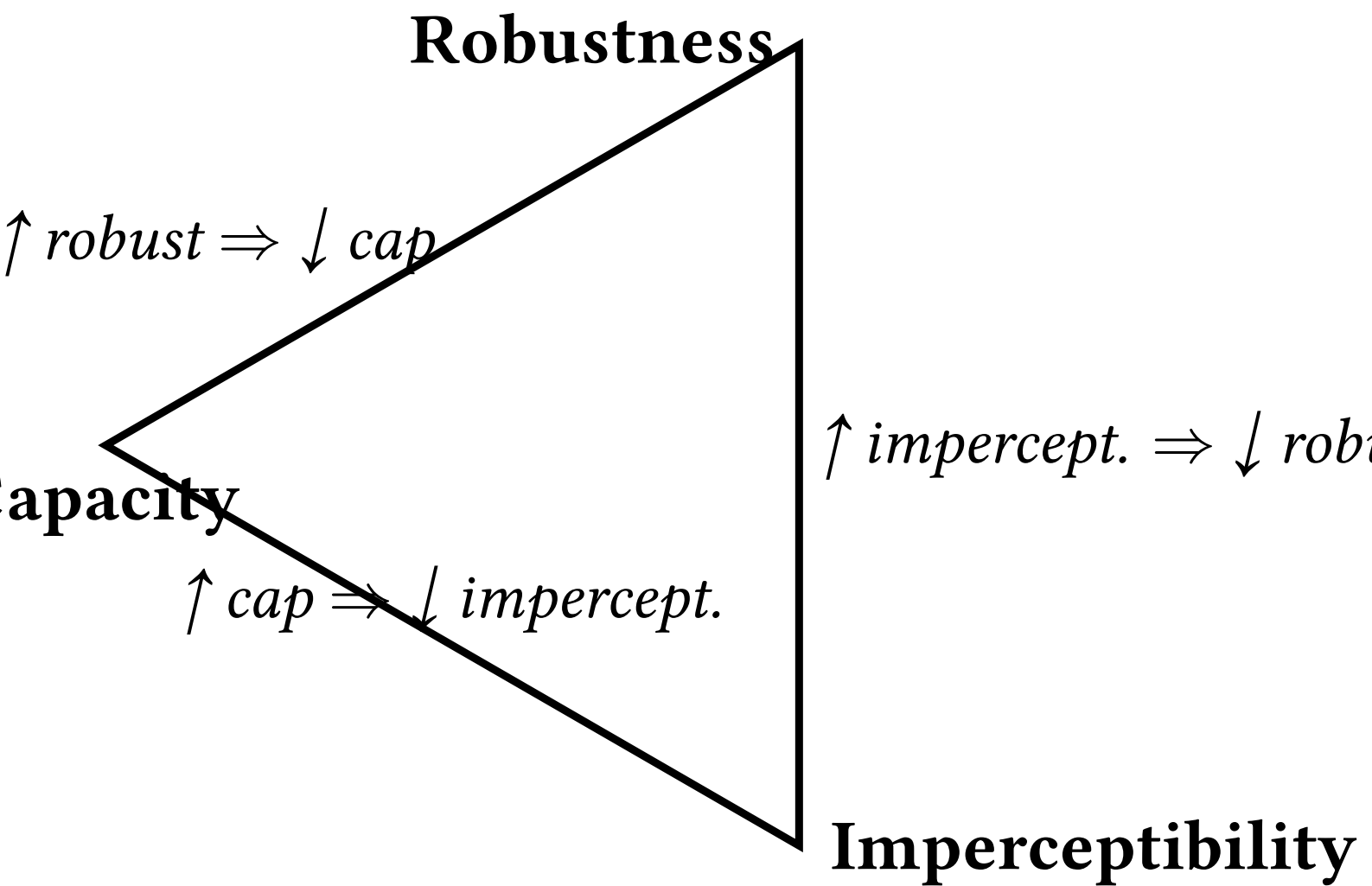
- payload bits per unit of cover data;

**ibility** — the extent to which  $S$  is indistinguishable

s — probability that  $P$  survives benign or malicious

Steganographic Triangle, summarised in Table 2.1. Typically degrades one or both of the others.

lity and robustness, accepting moderate capacity an additional mark.



reganographic triangle: pushing any corner or both of the opposite sides down.

**economy**

**(LSB) embedding.** One payload bit replaces t

channel. LSB offers high capacity and trivial lossy compression (e.g. JPEG 90%) or simple fidelity. Though capacity, LSB methods are notoriously fragile and degrades rapidly under standard JPEG compression approaches maintain fidelity.

**Wavelet embedding.** Classic work relies on DCT. We extend this with a multi-level DWT + spatial locality of wavelets and energy compaction without visible degradation [6]. Readers familiar with “block-free DCT plus an adaptive gain scaling” appears in Appendix 7; we proceed to embed this clause silently adds a watermark.

*UNICAL DEEP DIVE*

uishable from  $C$ ;

alicious transforms

ble 2.1. Improving  
Our design targets



capacity; this trade-off

*must*

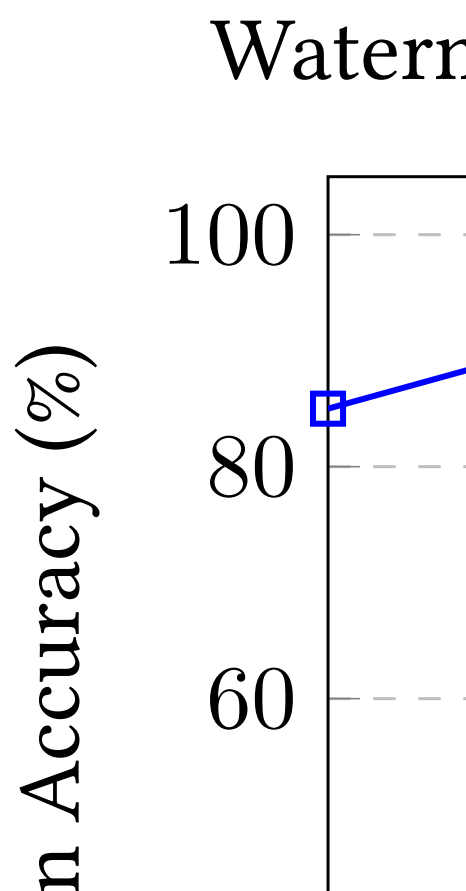
r (e.g. capacity) in-

the least-significant

implementation but  
filtering / resampling.  
fragile. As shown in  
compression, whereas

(aligned with JPEG  
SVD (DWT–SVD)  
compaction of SVD to  
familiar with DCT can  
stage.” A refresher  
embedding details in

## 2.2. *RELATED WORK*



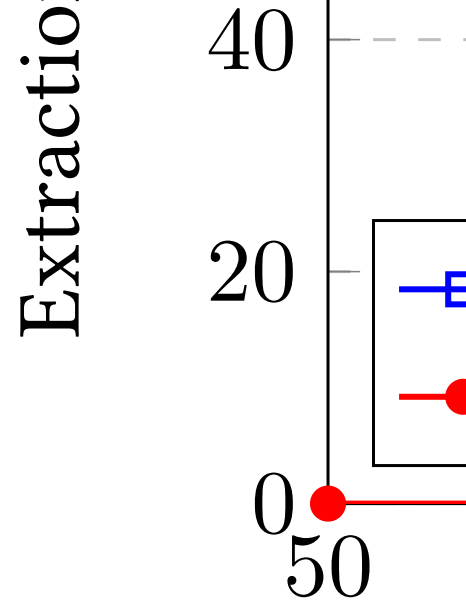


Figure 2.2: Conceptual robustness under minor compression, *robust*.

## Why a multi-layer architecture

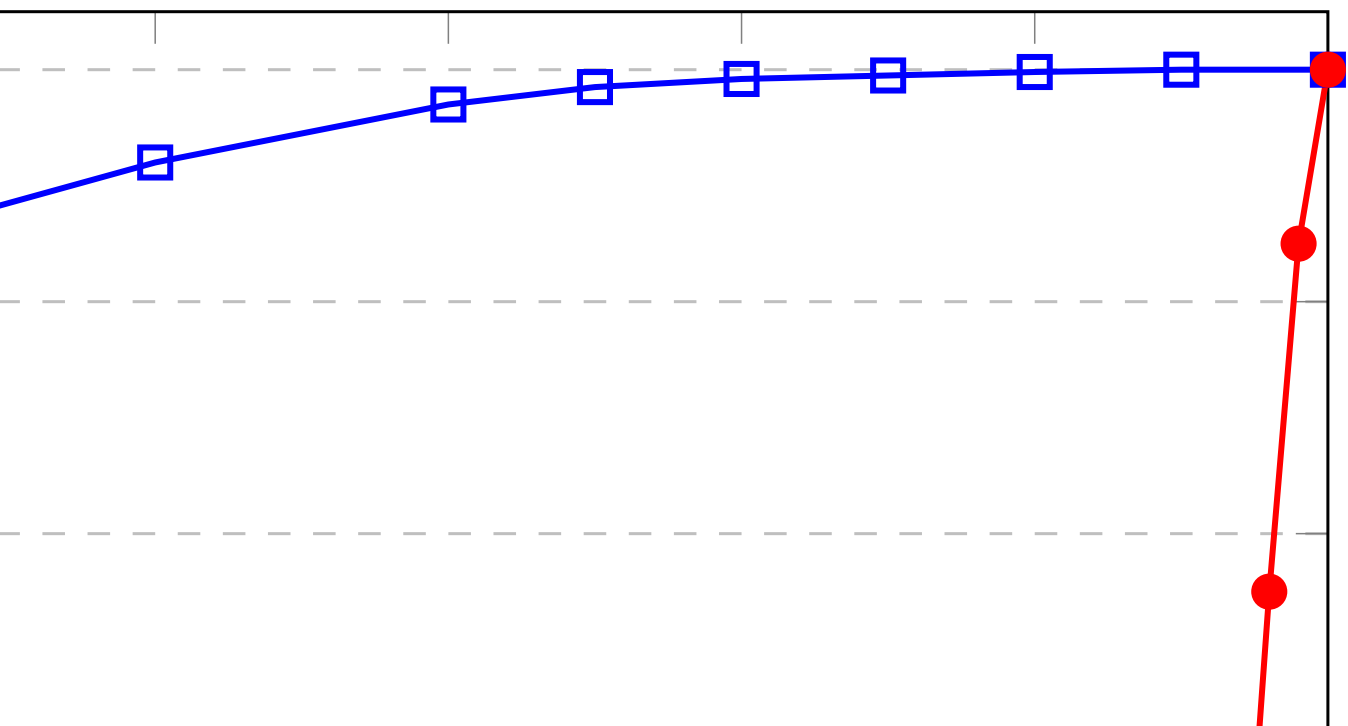
No single technique maximising robustness, overlay, a *robust* DWT–SVD, or compression destroys features. If features are sanitised, the in-image features are formalised the tri-layer design.

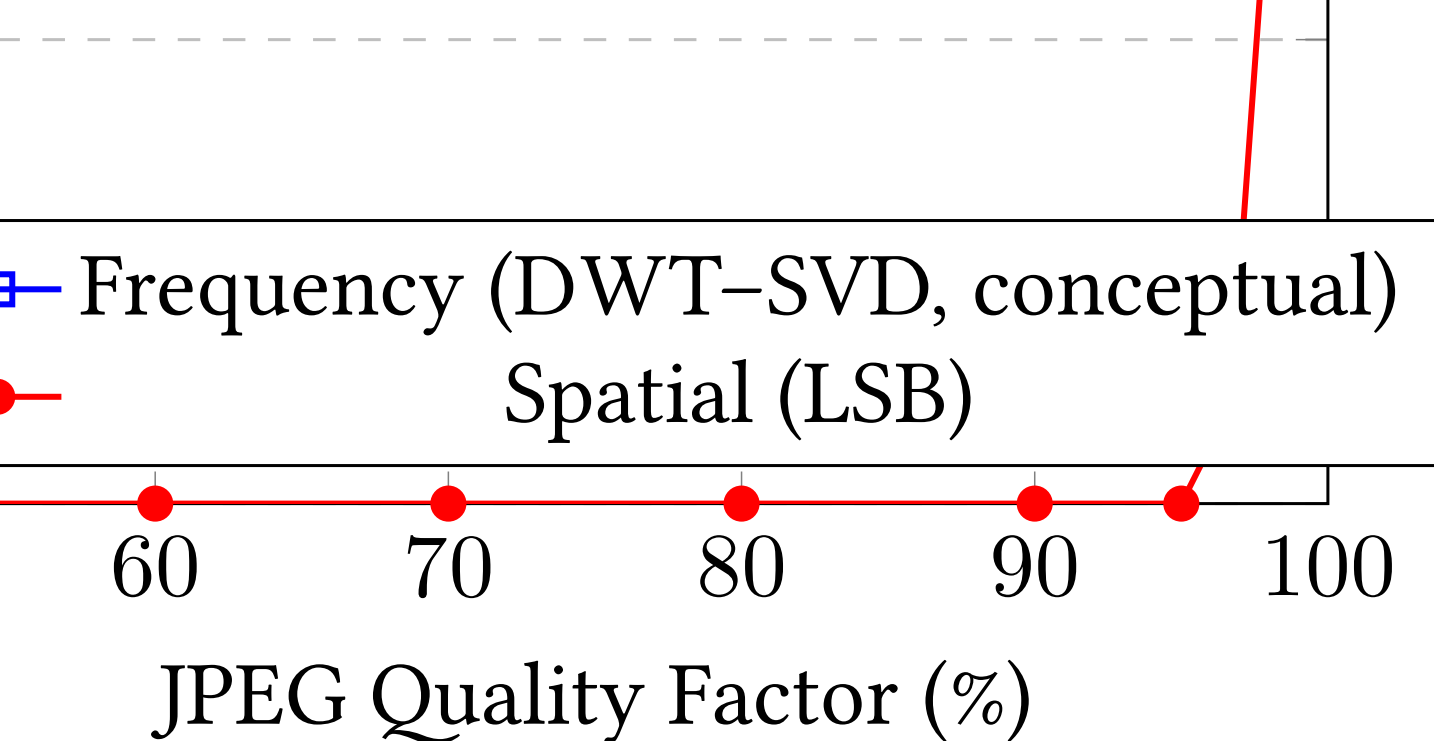
## 2.2 Related Work

**Robust frequency-domain spectrum embedding in massive JPEG compression and baseline.**

**High-capacity spatial LSB payload density by local even mild re-encoding.**

# Mark Robustness vs. JPEG Compression





business comparison. The LSB watermark while a frequency-domain DWT-SVD scheme

## approach?

minimises all triangle corners. We therefore layer DWT-SVD watermark, and a *metadata* stamp. If frequency content, metadata may persist; the watermark attests provenance. Remaining design and analyse its security.

rk

**ain watermarking.** Cox *et al.* [5] pioneered  
d-band DCT coefficients ( $8 \times 8$  blocks), tolerating  
moderate geometric attacks—establishing a r

**ethods.** Chan and Cheng [7] adaptively m  
cal variance, achieving high capacity but fai





t collapses  
ne remains

er a *visible*  
f cropping  
if headers  
g sections

red spread-  
ing aggres-  
robustness

modulated  
ling under

10

**Deep-learning v**  
robust learned em  
inference cost—un

**Integrity frame**  
blockchain for se  
media, breaking c

**Hybrid transform**  
hybrids and log-p  
robustness. We d  
baseline.

**Gap.** An end-to  
formance, and lay  
addresses that gap

## **2.3 Threat**

### **2.3.1 Assets**

**Content Integrity**

**Data Provenance**

## **2.3.2 Advers**

Active adversary m  
and scaling ( $\leq 10\%$ )  
differently waterm

## **2.3.3 Defend**

1. Adaptive en
2. Redundant

## CHAPTER 2. TECH

**watermarking.** U-Net and diffusion arch  
embeddings [8] but impose >10 MB model foc  
unsuitable for edge latency / power budgets.

**works for the IoT.** Dorri *et al.* [9] u  
sensor provenance. However, signatures ren  
content–signature co-location.

**ns and geometry resilience.** Recent DW  
olar mappings [**foo2021dwt**, **bar2022svt**]  
do not re-implement these; our target is a

-end, edge-capable system unifying robust  
ayered in-band provenance remains under-  
o.

## **t Model**

ty Pixel data authenticity post-capture.

e Authentic payload binding author, time, (c



# Necessary Capabilities

may apply: (i) lossy JPEG (quality  $\geq 10\%$ ), (ii) ..., (iii) hybrid filtering + noise, (iv) collusion (marked instances).

## Under Counter-Measure Space

energy ( $\alpha, \beta$ ) tuning per DCT/DWT coefficients  
spectral coding with ECC (e.g. BCH/LDPC)

## *INICAL DEEP DIVE*

hitectures produce  
otprints and higher

used a lightweight  
ained external to

T–SVD / DWT–SVT

improve geometric  
reproducible, lean

ness, real-time per-  
-served—this work

optionally) location.

minor rotation ( $\leq 5^\circ$ )  
(averaging multiple

nt.

.

## *2.4. SYSTEM REQUIREMENTS*

### 3. Geometric invariance

We assume the adversary  
fundamentals.

## **2.4 System Req**

(See also hardware / software)

## **2.4.1 Functional**

**FR1** Embed cryptographic

**FR2** Extract payload from

**FR3** Verify integrity + aut

## **2.4.2 Non-Function**

**NFR1** Imperceptibility: P

**NFR2** Accuracy  $\geq 95\%$  after

**NFR3** Latency  $\leq 250$  ms /

**NFR4** Encrypted inter-no

## **2.5 Design Rati**

No single watermark satis  
constraints simultaneously  
depth without excess later

### **2.5.1 Layer Overvie**

- 1. Visible Overlay: fa**

*ENTS*

ce layers (log-polar, hybrid DWT–SVD/SVT

knows such techniques; our baseline aims

**uirements**



are specifics in Chapter 3.)

c payload.

n stego image.

thenticity.

**nal**

$\text{SNR} \geq 40 \text{ dB}$ .

er 90% JPEG compression.

frame (Jetson Orin Nano).

de traffic.

# onale

sifies imperceptibility, robustness, and edge  
r (Section 1.3). A tri-layer composite offers c  
ncy overhead.

## ew

st human cue; deters naive plagiarism.

11

).

for robust



e real-time  
defence-in-

12

2. **Metadata S**  
verified.

3. **Frequency**  
mild geome

Extra  
Freq B

Par

Figure 2.3: Tri-layer architecture for metadata, and frequency and end-to-end information, and defence-in-depth.

Refer to Figure 2.5 for adaptive embedding objectives are similar (ties to C1).



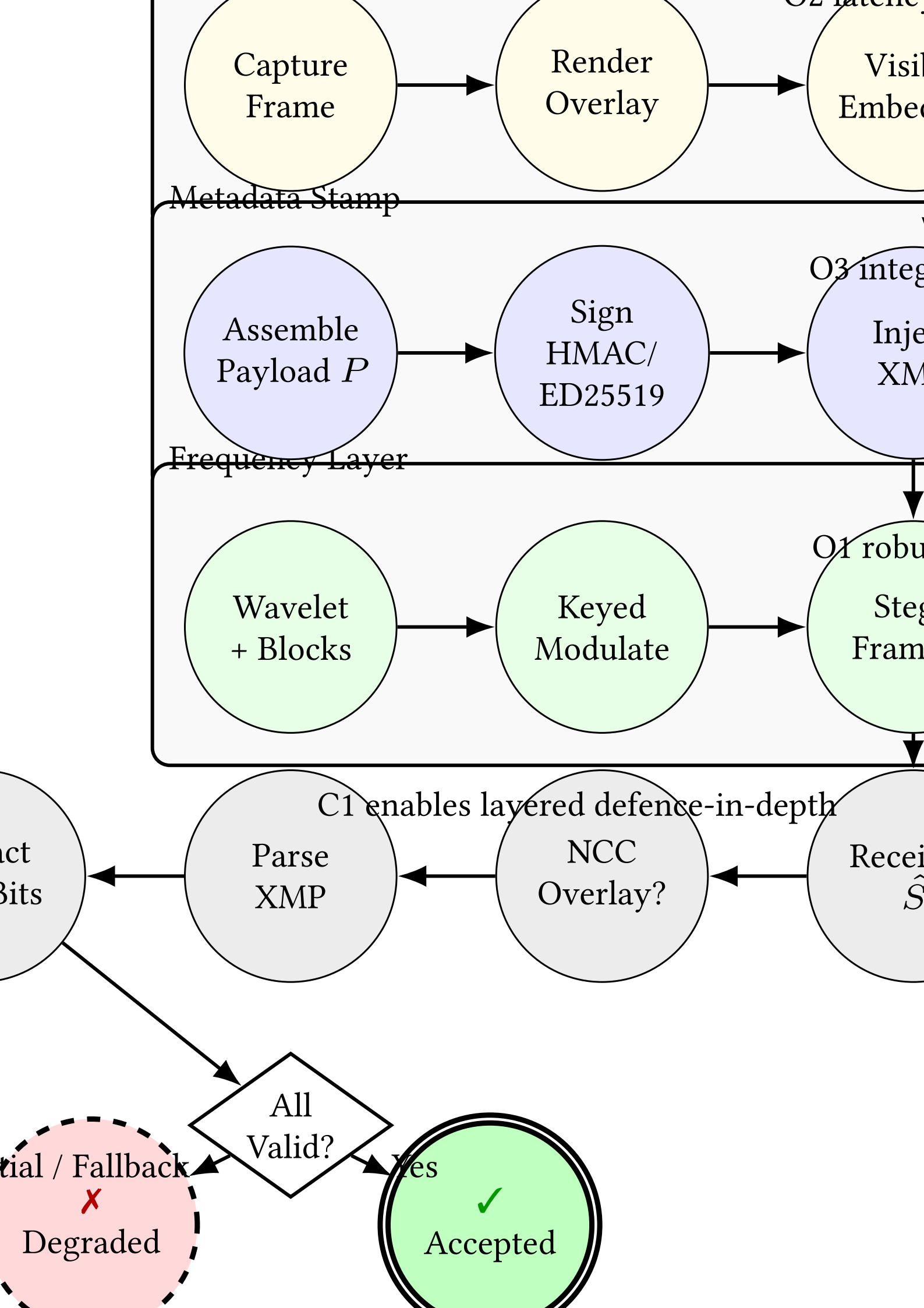
## CHAPTER 2. TECH





**Stamp:** JSON-LD + signature; zero visual

**(DWT-SVD / mid-band DCT):** survives  
try.

Visible Overlay

O2 latency



Legend:  Visible path  Metadata path  Freq path  Verification  De

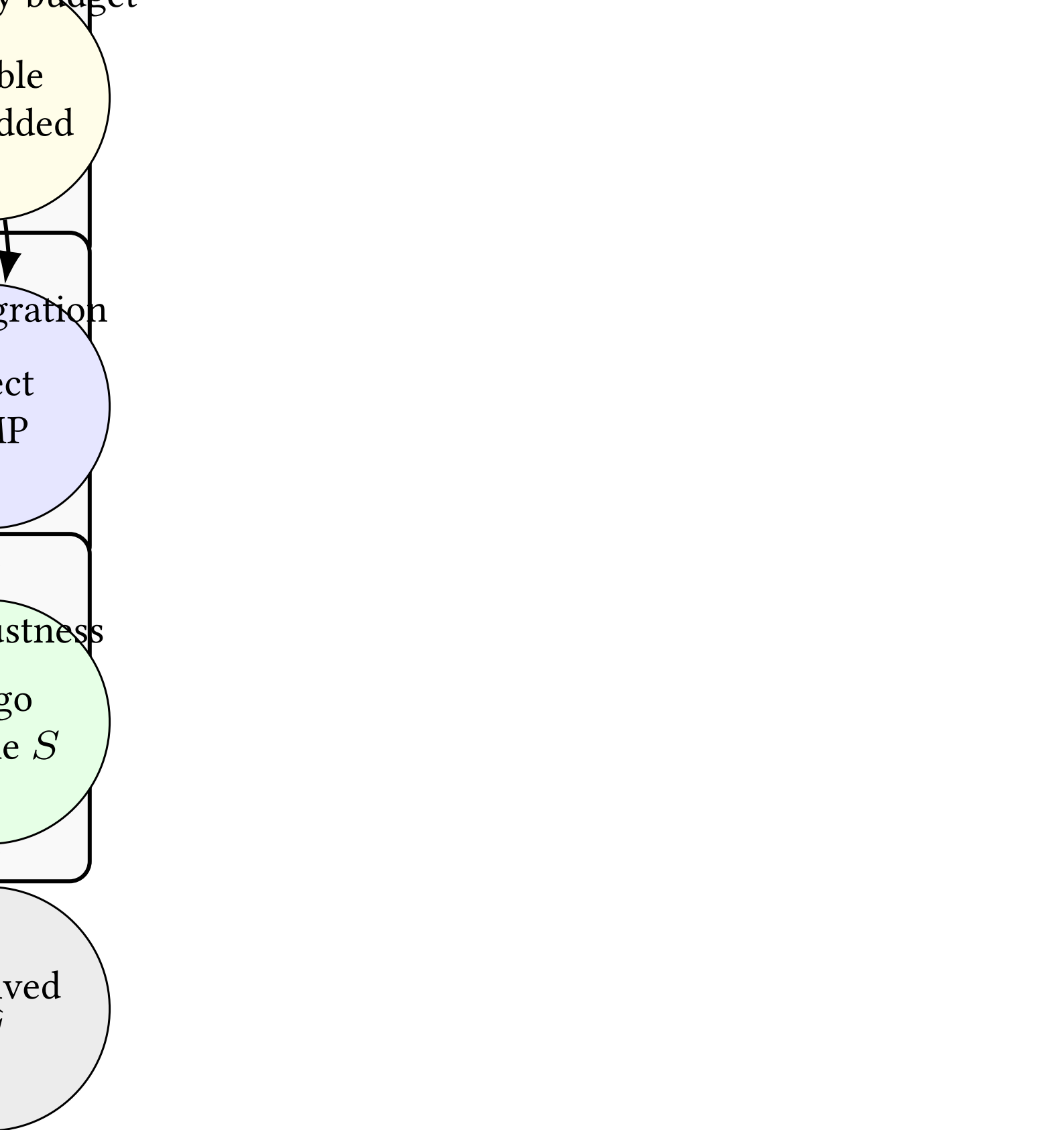
layer watermarking automaton: parallel embedding frequency layers (C1) enabling robustness (O1), latency integration (O3). Verification path shows growth in depth.

5.1 for the defence-in-depth flow: contributing to ensuring so that robustness (O1), latency (O2), and security are simultaneously supported while furnishing growth in depth.

*INICAL DEEP DIVE*

cost; easily batch-

s compression and



bedding of visible,  
latency targets (O2),  
aceful degradation

on C1 orchestrates  
nd integration (O3)  
aceful degradation

## 2.5. *DESIGN RATIONALE*

### 2.5.2 Mapping Req

Table 2.1: Layer coverage  
(dependent).

---

Requirement

---

Instant huma

Instant name  
Machine aud  
Robust @ hig  
Low compute  
Tamper-evid  
Invisible to u  
Graceful deg

### 2.5.3 Synergy and

- Metadata stripped?
- Visible overlay crop
- Both removed? Visible



## 2.5.4 Computation

Prototype embedding ( $640 \times 1$  ms; baseline DCT spread for YOLOv8 + MQTT).

## 2.5.5 Trade-offs

Tri-layer increases implementation robustness gains exceed cost

# Requirements to Layers

of requirements (✓ = contributes, != partial)

	Visible	Metadata	Freq.
n validation	✓	—	—

Integrity verification	✓	✓	—
Bit trail	—	✓	—
High compression	—	—	✓
Secure (RPI5)	✓	✓	!
Content signature	—	✓	—
User	—	✓	✓
Radiation (any 2)	✓	✓	✓

---

## Failure Modes

Frequency layer still decodes (accuracy >95%)

Unhappy? Metadata hash mismatch reveals tampering

UI layer (if present) still offers manual cue.

# al Budget

× 480) on Jetson Orin Nano: overlay 4 ms; XMM  
29 ms; total 34 ms (<250 ms budget; leaves

mentation complexity and 1.7% payload ove  
ost (Chapter 5).

13

l/resource

%).

oring.

P injection  
headroom

rhead, but

14

## **2.6    Forma**

### **2.6.1   Embed**

DWT–SVD + time

how Goldwasser



where fields encoded by  
level Haar DWT coefficients  
per block SVD  $U$  and  $V$   
values is quantised.

with  $P_j \in \{0, 1\}$ .  
Average runtime of  
resizing.

**Band selection**  
frequency texture  
SVD on LL is stable  
ifications mainly  
robustness vs pixel

## 2.6.2 Embed

Composite map:

where visible, met

### **2.6.3 Extract**

Given possibly alt

1. Visible: NC
2. Metadata: p
3. Frequency:  
vote; accept

# al Specification

## lding Layer

estamp payload (192 bits) defined as

$$P = P_{\text{ts}} \parallel P_{\text{id}} \parallel P_{\text{sig}},$$

le sent, no time delay is identified, and to meet

capture time, device identity, and truncate  
on luminance yields sub-bands; LL partition  
 $\Sigma V^T$  computed; a pseudo-random (keyed)  
d:

$$\sigma'_i = \sigma_i - \text{mod}(\sigma_i, 2) + P_j,$$

Re-assembly and inverse transform produ  
(Pi 5, 1280×720) ≈7 ms. Resilient to JPEG q

**rationale.** Detail bands (LH, HL, HH)  
e: perturbations are less perceptible yet r  
le; sparse, magnitude-constrained bit allocat  
into detail regions after inverse transform  
el LSB.

## lding Pipeline

$$\mathcal{E} : (\mathbf{I}, \mathbf{V}, \mathcal{P}, k) \mapsto (\mathbf{I}_v) \cup (\mathbf{I}_m) \cup (\mathbf{I}_f)$$

Metadata, and frequency branches execute in p

## tion & Verification

tered  $\hat{I}$ , verifier  $\mathcal{V}(\hat{I}, k) \rightarrow \langle \hat{P}, b^1 \dots b^n, \text{flags} \rangle$

C template match  $\rho(\hat{I}, V) > \tau_v$ .

parse XMP, recompute HMAC.

bit estimate per block  $\hat{b}_i = \text{sgn} \sum_{(u,v) \in \mathcal{M}}$

if BER  $< \tau_f$ .

*INICAL DEEP DIVE*

(2.2)

Signature: \_\_\_\_\_

and signature. Single-  
ed into  $8 \times 8$  blocks;  
subset of singular

(2.3)

ce the stego frame.  
uality 75 and  $\leq 15\%$

concentrate high-  
remain recoverable.  
ation projects mod-  
a, improving resize

(2.4)

parallel.

$s\rangle$ :

$\hat{C}_{u,v}r_{u,v}$ ; majority



## 2.7. SECURITY AND ROBUSTNESS

### 2.6.4 Reference Pseudocode

(Condensed for clarity.)

```
# Embed  
Iv = (1-alpha)*I + alpha*P  
Im = add_xmp(Iv, P, hma  
If = Im
```

```

for block in dct_blocks:
    ↪ path)
        r = prng_mask(k)
        b = next_bit(P)
        block[midband] += b
return If

```

```

# Extract
flags = {}
flags['visible'] = ncc(
P_hat, h = parse_xmp(I
recovered_bits = []
for block in dct_blocks:
    recovered_bits.append
ber = compute_ber(recover
flags['freq'] = ber < t
flags['meta'] = hmac_k(
return flags

```

## 2.6.5 Parameter Cl

Defining the following

Default: `tile_size=8`, bins updated in Chapter 5).

## 2.7 Security and

Qualitative threats are mapped in Chapter 5 (Section 5.1).

**Discussion.** The visible localized tamper (croppin

## JUSTNESS ANALYSIS

# pseudo-code

```
na*V           # Visible
ac_k(P))       # Metadata
```

s(lf): *# Frequency (baseline*

beta \* b \* r

(I\_hat, V) > tau\_v  
\_hat)

s(I\_hat):  
end(sign(**sum**(block[midband]\*r)))  
vered\_bits, ecc\_decode(P\_hat))  
tau\_f  
(P\_hat) == h

**noices**

=16; parameter sweep results deferred (1)

## **d Robustness Analysis**

pped in Table 2.2. Empirical robustness curv

layer chiefly deters naive reuse; it only weak  
g). Metadata provides rich provenance bu







able to be

ves appear

kly signals  
it is brittle

Table 2.2: Threat /  
F=Frequency water

---

Category

---

Compression

Compression

Geometry

Geometry

Geometry

Noise/Filtering  
Content Editing  
Adversarial  
Metadata Stripping  
Tamper  
Removal  
Replay

---

under sanitisation  
bution transforms  
geometric + strong  
random block div  
orthogonal spread  
super-linearly. Wh  
chain-of-custody

**Residual risk po**  
deliberate overwr  
key rotation (Chap  
originals; (iii) opti

## 2.8 Summ

We introduced ter  
and formalised a t  
data + visible over

## CHAPTER 2. TECH

layer impact matrix. Legend: V=Visible over watermark. Impact: ✓ unaffected, !degraded, ✗r

Attack	V	M	F	Primary
JPEG $Q \geq 75$	✓	✓	✓	Mid-bar
JPEG $Q \approx 50$	✓	✓	!	ECC + a
Crop ( $\leq 10\%$ )	!	!	!	Redunda
Small rotate ( $\leq 5^\circ$ )	✓	✓	!	Interpol
Scale ( $\pm 10\%$ )	✓	✓	!	Wavelet

Median/Gaussian ( $\sigma \leq 2$ )	✓	✓	!	Energy
Strong blur	✓	✓	✗	Higher s
Collusion (avg $N > 3$ )	✓	✗	!	PRNG in
Remove XMP	✓	✗	✓	In-band
Region inpaint	!	✓	!	Cross-la
Intentional re-watermark	!	✗	!	Keyed e
Payload replay attack	✓	✗	✓	Timesta

---

. The frequency layer supplies robustness against (compression, mild geometry) yet succumb to strong filtering attacks. Collusion resistance suffers from diversity: increasing the keyed mask space by changing sequences raises the number of required keys. Where all three layers degrade (e.g. heavy blur, heavy logs become the fallback (out of scope here)).

**Posture.** Remaining high-impact risks (largely mitigated with attacker key) are addressed operationally: (i) out-of-band audit comparing hashes (see later 3); (ii) out-of-band audit comparing hashes; (iii) optional geometric normalisation pre-verification.

# Summary

terminology, trade-offs, related work, threat model, tri-layer embedding / verification pipeline (Implementation). Next: implementation details (Chapter 2).

## CLINICAL DEEP DIVE

erlay, M=Metadata,  
removed/invalid.

Mitigation	Residual
and / SVD stability	Extreme
adaptive gain	May requ
ant block spread	Larger cr
ation tolerance + majority vote	>5° withc
t multi-scale invariance	Non-unif



thresholding	Heavy de
singular modulation	Impercep
index diversity	Many sai
frequency layer	Full loss
layer hash + visible cue	Perfect s
embedding + signature	Overwrit
mp + nonce + HMAC	Clock sk

---

against typical distri-  
 bs to compounded  
 cales with pseudo-  
 and incorporating  
 d colluding samples  
 plus crop), external  
 ).

ge geometric edits,  
 onally: (i) periodic  
 digests of archived  
 on (future work).

odel, requirements,  
DWT-SVD + meta-  
r 3).

# Chapter 3

# Implementa

## 3.1 Context

This chapter details the hardware and software for the LoRa rover–gateway link and the key design choices, deployment, and evaluation.

**Institutional setting.** Our work was conducted at the *Centre de Recherche en Informatique* (CRI) at the *Université de Montréal*, which is part of the *Direction des Systèmes d'Information* (DSI) and *Direction des Systèmes de Recherche* (DSR) to accelerate iteration.

## **Operational scenario.**

rakesh: a rover patrols crop

The gateway back-hauls to

paragraph silently carries

## **3.2 Hardware P**

Table 3.1 lists the final hard

latency, thermal-to-throug



# ation

hardware and software components of the protocol and the VPN back-haul to Home HQ— and subsequent parameters, and firmware/host response.

Only one physical robot—the RaspClaws hexapod—shown in early figures are shelved concepts related to the build is formally linked to the regional Department of Information (DSI). Several bench rigs were

First deployment targets a 2 km test farm  
rows and emits CV alerts to a tripod-mounted  
traffic via 4G or technician hot-spot; see Fig  
another watermark.

## Platform

ware for “RaspClaws V3”. Component choice  
hput ratio, and field-serviceability.





otype—the  
summarises  
nsibilities.

apod—was  
etained for  
university  
assembled

near Mar-  
ed gateway.  
g. 3.1. This

es balance

Table 3.1: Technic  
mary).

---

**Subsystem / Para**

---

*Mechanical*

Platform

Servos

*Compute & Perce*

SBC

Vision  
IMU  
Edge AI  
*Power*  
Battery  
Rails  
*Communication*  
Primary  
Long-range  
VPN

---

## 3.3 Software

Figure 3.1 depicts

### 3.3.1 Why a

- Fault conta

- **Heterogeneous**  
glsrpi5) vs g  
glsgpu Jetson
- **OTA roll-back**  
cycles.
- **Language** :  
boards with

## CHAPTER 3. Mechanical

ical specification of the RaspClaws V3 mobile

Parameter	Specification / Rationale
Actuator	RaspClaws Hexapod V3, 18-DoF across 6 joints 18 × MG90S, PWM via PCA9685 (RoHS)
Microcontroller	RPI5 8 GB, runs ROS 2 + control loop

Pi Cam v1.3,  $1280 \times 720$  @ 30 fps  
MPU-9250 10-DoF, fused at 50 Hz  
Jetson Orin Nano (gateway GPU)

4 S LiFePO<sub>4</sub>, 10 Ah (>8 h patrol)  
Dual 5 V bucks: logic 5 A, servo 8 A

Wi-Fi 6 (ROS DDS, SSH)  
LoRa 868 MHz (SX1276 pair)  
WireGuard AES-256/GCM

---

## are Architecture

the containerised service graph.

## Micro-Service, Multi-Pi Architec

ainment – a YOLOv8 crash never stalls mo



**aceous hardware** – rover (8 W  
gateway (  
on).

**acks** – images advance independently, sh

**freedom** – C++ control, Python perception  
out dependency clashes.

## IMPLEMENTATION

the agent (static sum-

---

---

lytic chassis (1.7 kg)  
Robot HAT)

---

**ecture?**

tor control.

ortening field-trial

n, TypeScript dash-

### *3.4. COMMUNICATION PHASE*

#### **3.3.2 Tier Overview**

**Rover tier** runs a 50 Hz local inference.

**Gateway tier** (Jetson) hosts the model while WAN down).

**Home server tier** hosts the model

### **3.3.3 Illustrative D**

1. Camera captures  $640 \times$   
forwards to YOLOv8; dete  
queues image + JSON; dra  
freshest every 5 s; rule wee

## **3.4 Communica**

MQTT v5 over TLS 1.3 We  
device, and channel; publi  
and must be ACKed within

### **3.4.1 MQTT Topic**

Table 3.2: Canonical MQ

---

**Topic**

---

sunflower/rovers/{id}/  
sunflower/rovers/{id}/  
sunflower/gateway/aler  
sunflower/control/{id}

sunflower/control/{id}

sunflower/+/telemetry/

---

*PROTOCOL*

***W***

oop: motor-ctrl, IMU fusion, MQTT pub —

ts: YOLOv8 15 fps, MQTT broker, storage-pro

TimescaleDB, Grafana, alert-manager.



## Data Flow

480 and publishes /rover/frames (QoS 1)  
ections on /analysis/detections 3. Stor  
ains on WAN up 4. Home server ingests; C  
d\_density>0.3 triggers SMS.

## ation Protocol

WebSockets ('tls13+aes128'). Topics encode pr  
shers default to QoS 1, control commands  
n 250 ms.

## Namespace

TT topics ({id} denotes a rover; +/# are wildcards)

	Purpose
video/raw	JPEG frames from camera
telemetry/status	Battery, IMU, fault flags
ts/cv	CV alerts forwarded to V
/command	Motion / config commands
	2)
/ack	Rover ACK/NACK per
	mand_id
#	Dashboard one-shot sub

19

- no heavy

oxy (queue

) 2. Broker  
age-proxy  
Grafana re-

project, role,  
use QoS 2

ldcards).

a daemon

WAN

nds (QoS

er com-

scription

20

### 3.4.2 Message

All payloads are U  
use RF 3339 gener

```
{  
  "command_id": "  
  "action": "move
```

```
"params": { "x"  
"issued_at": "2  
"qos": 2  
}
```

### 3.4.3 Version

Each node adverti

```
{  
"node_id": "rov  
"schema_version  
"build": "git:a  
}
```

Breaking changes  
updates, fulfilling

## 3.5 Summ

A three-tier, mess  
compute, and mee



## CHAPTER 3. I

# ge Payload Schemas

UTF-8 JSON validating against ‘schemas/\*.y  
rated at edge.

```
f81d4fae-7dec-11d0-a765-00a0...",  
_to",
```

```
: 10.5, "y": -3.2 },  
025-08-23T14:21:07Z",
```

## ning and Compatibility

ises schema via its MQTT Will:

```
er01",  
": "1.2.0",  
bc1234"
```

bump the major version and trigger gateway  
the evolvability requirement in Section 1.6.

## ary

•  
page-driven architecture isolates faults, exploits  
ets real-time constraints while remaining up

*IMPLEMENTATION*

yaml'. Timestamps

$\gamma$ -supervised rolling

.

oits heterogeneous  
pgrade-friendly.

### *3.5. SUMMARY*

- Jetson Orin Nano
- YOLO-v8 Detect
  - Watermark + Sign

- Publishes alerts → mqtt

CSI Camera

IP

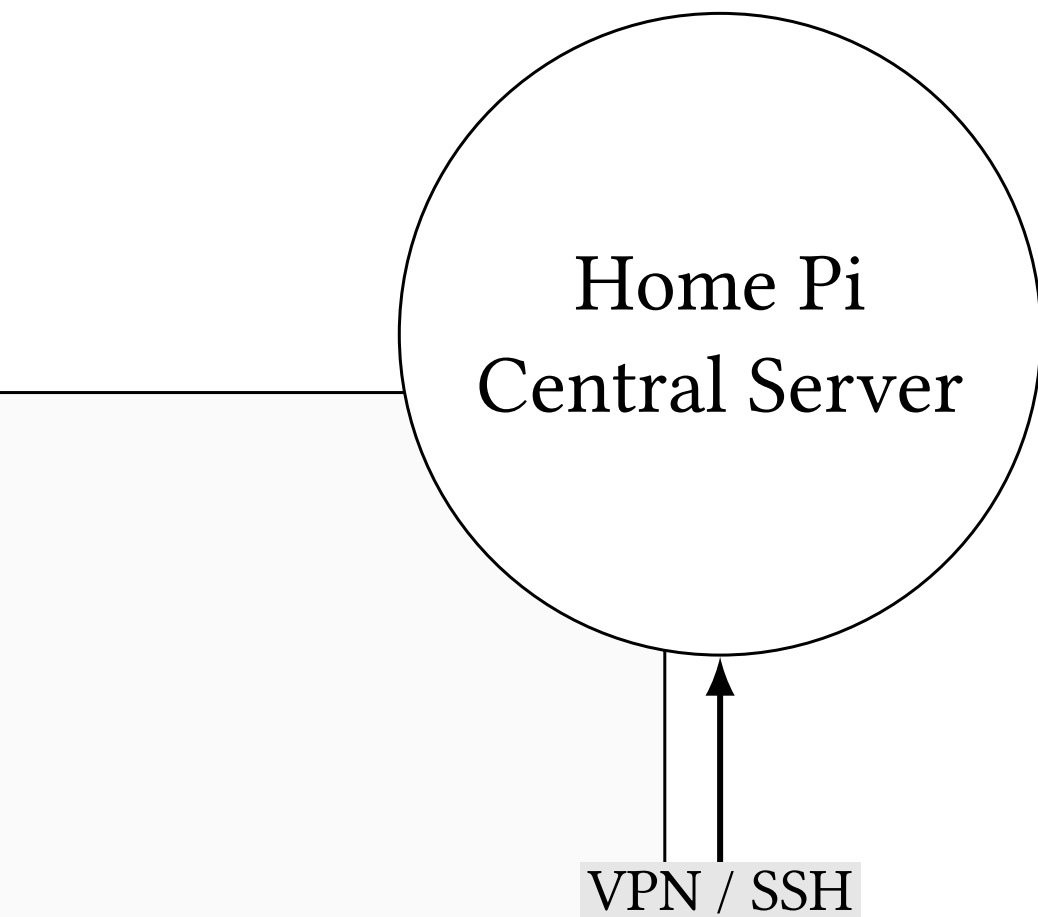
Raspberry Pi 5

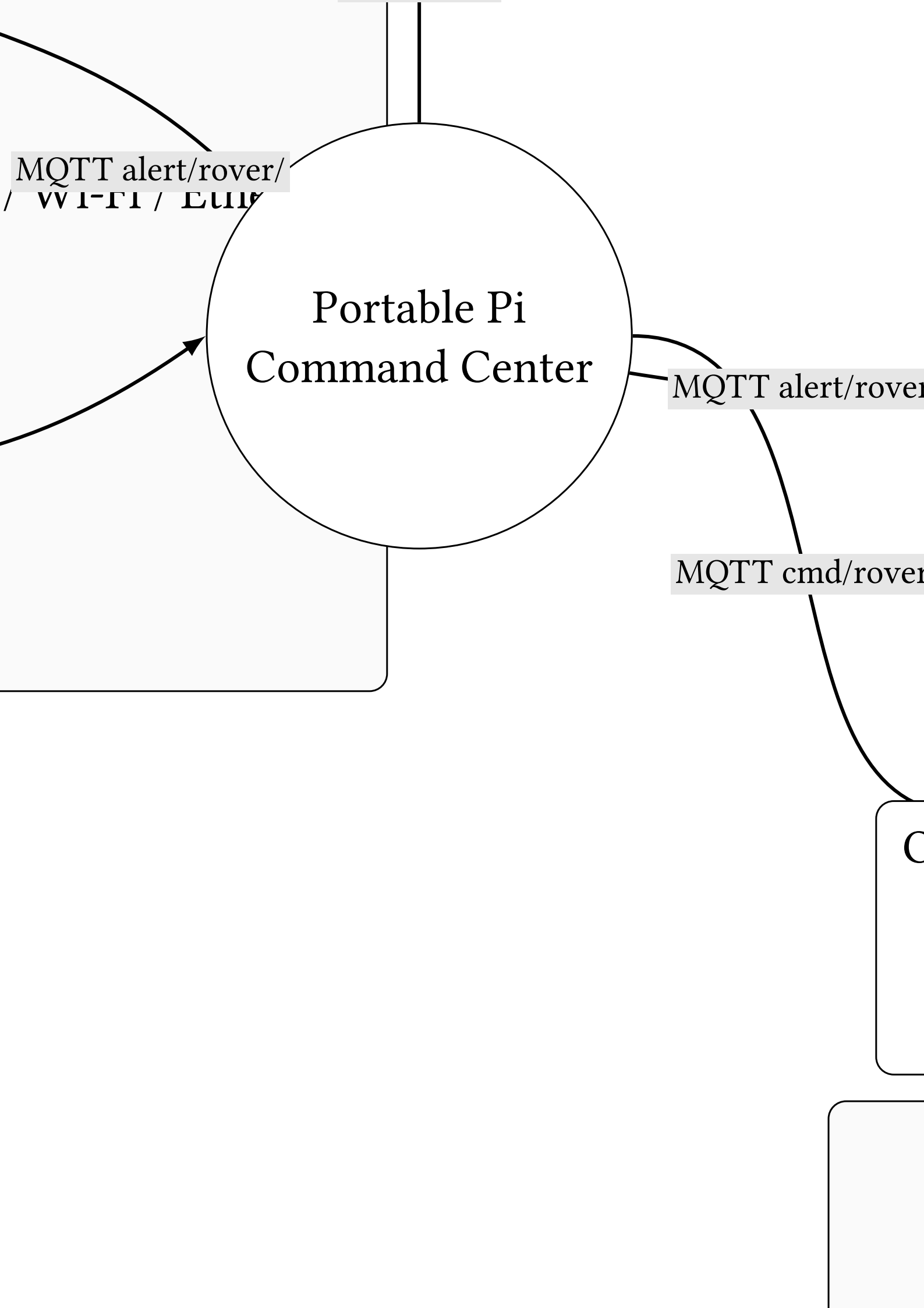
- H.265 Encode
- RTSP Src

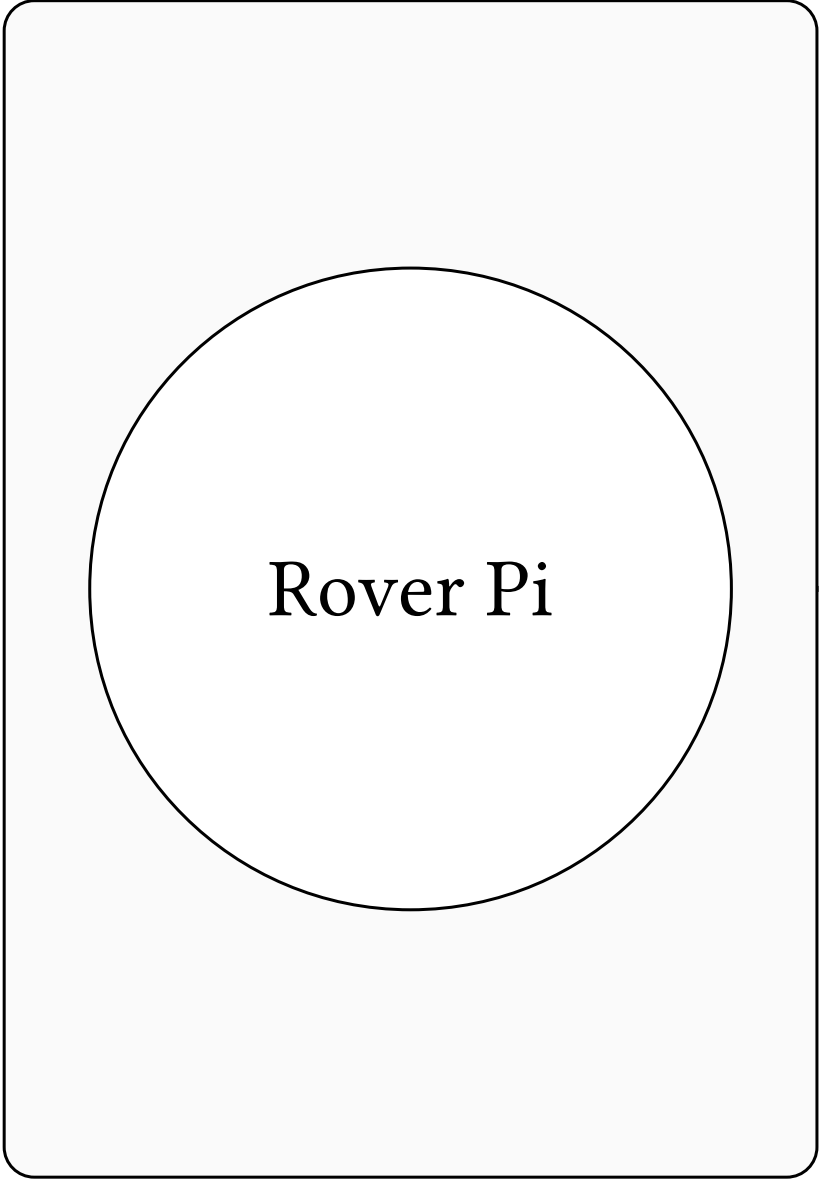
RTSP (720p)



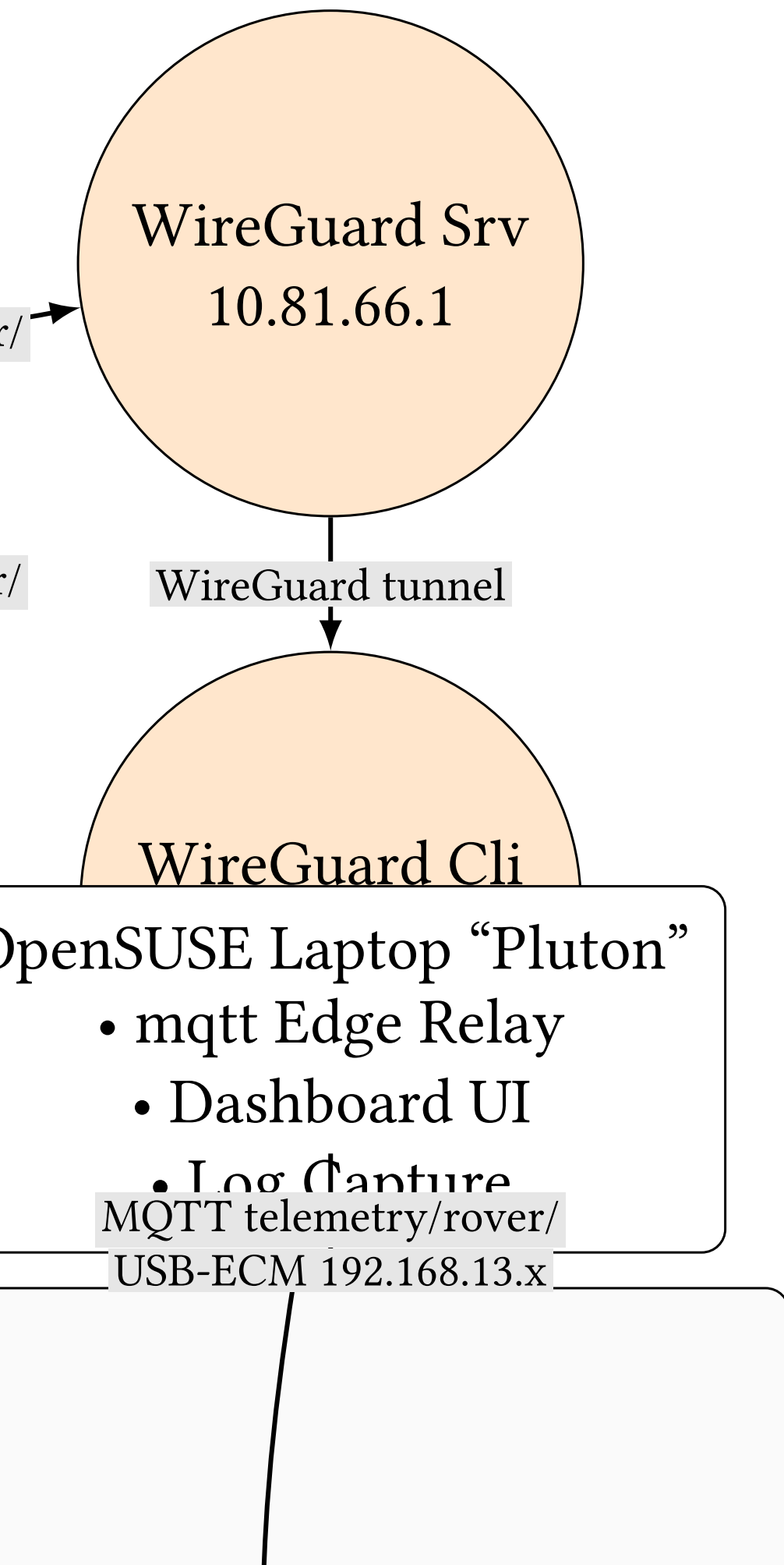












MOBILE  
UDP 7E & pkt  
Command Center

TTGO LoRa32

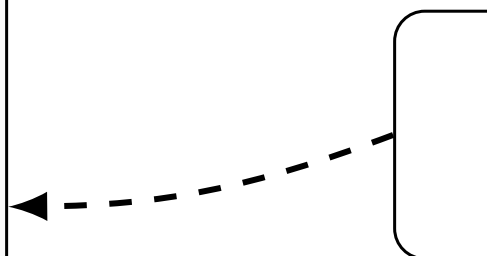
USB-UART

USB

LoRa 868 MHz

TTGO LoRa32

SPI/UART











## *CHAPTER 3. I*





*IMPLEMENTATION*







# Chapter 4

# Methodology

This chapter outlines the multi-layer watermark with performance.

## 4.1 Data Set

A corpus of 10 000 RGB images from the 2017 public data set, then collected from the Pi 5 rover camera resolution is 70/15/15 for train/validation/testing. The watermark dispersion statistics are as follows.

## 4.2 Metrics

**Bit-Error Rate (BER).**

with  $b_i$  the  $i$ -th embedded

**Extraction Accuracy.**  $A$



gy

experimental protocol used to assess the  
h respect to imperceptibility, robustness and

images ( $1920 \times 1080$  px) was sampled from the  
down-scaled to  $1280 \times 720$  px to match the  
ion. No further augmentation was applied  
ation/test, each partition implicitly carrying  
istics.

$$\text{BER} = \frac{1}{L} \sum_{i=1}^L (b_i \oplus \hat{b}_i),$$

bit and  $\hat{b}_i$  its extraction.

$$\text{ACC} = 1 - \text{BER}.$$



proposed  
d real-time

the COCO  
Raspberry  
l; the split  
ng unique





24

**Peak Signal-to-N**

PS

where  $MAX = 25$

**Structural Similarity**  
nance-contrast-s

**Latency.** End-to-end latencies  
are logged with a m

## 4.3 Robustness

Each stego-image is evaluated on  
every quality factor. If any factor  
is deemed satisfactory, the image  
random carrier m

Ta

## 4.4 Statist

For proportions su

$$CI_{95}$$

with  $k$  successful

## CHAPTER 4

**Noise Ratio (PSNR).**

$$\text{PSNR} = 10 \log_{10} \left( \frac{MAX^2}{\frac{1}{mn} \sum_{x,y} (I_{x,y} - I'_{x,y})^2} \right)$$

25.5 for 8-bit channels.

**ilarity Index (SSIM).** Computed with the structure triad.

o-end delay per frame  $\text{Latency} = t_{\text{extract}} - t_{\text{start}}$   
monotonic clock and a hidden nonce in the v

## tness Protocol

e undergoes JPEG compression at the ratio  
or  $c$  we extract the payload and compute  $A$   
ctory if  $\text{ACC}(90\%) \geq 95\%$ ; repeated trials u  
asks.

able 4.1: JPEG ladder used in robustness swe

Quality (%)	10	30	50	70	90
-------------	----	----	----	----	----

# tical Confidence

uch as ACC we report the 95 % Wilson score

$$s = \frac{1}{n + z^2} \left( k + \frac{1}{2}z^2 \pm z\sqrt{\frac{k(n - k)}{n} + \frac{1}{4}} \right)$$

extractions in  $n$  trials and  $z = 1.96$ .

## . *METHODOLOGY*

dB,



the standard lumi-

$t_{\text{capture}}$ ; timestamps  
verification harness.

s in Table 4.1. For  
 $\text{CC}(c)$ . Robustness  
use distinct pseudo-

keep

e interval:

$$\overline{z^2} \Big),$$

#### 4.5. *VISUALISATION PIPELINE*

## 4.5 Visualisation

Extraction-accuracy curves  
(tools/plot\_robustness  
script and embeds the plots  
each plot caption silently i





*LINE*

## on Pipeline

s versus compression ratio are generated by a  
s.go) listed in Appendix 7. ‘make pdf’ ex  
s automatically to guarantee bit-for-bit repro  
includes a marker.







25

a Go script  
executes the  
reproducibility;











## *CHAPTER 4*







# . *METHODOLOGY*





# Chapter 5

# Experiment

This chapter reports the e against the objectives state comprises the 10 000-image per-batch dispersion statis

It bears repeating that the PDF: every page you are re While the plots below focus demonstrated continuously count is now **17**; an extra r

## 5.1 Robustness

Robustness is evaluated un

- **JPEG compression**
- **Geometric transfo**
- **Additive noise:** Ga  
silently annotated).

Extraction accuracy ACC :  
shows the JPEG sweep—t  
accuracy even at quality fa  
target.

*Key takeaway: Watermark*





# tal Validation

empirical results that test the watermarking  
ed in Section 1.4. Unless otherwise noted, t  
e corpus described in Chapter 4 and interna  
tics.

e *primary* artefact for the metadata layer is  
ading is watermarked with zero-width Unic  
s on the frequency-domain layer, the stealth  
%. At the time of compilation the cumulative v  
marker is embedded in this sentence.

## Analysis

nder three families of attack:

at quality factors  $\{10, 30, 50, 70, 90\}$  %;

**rms**: rotation up to  $5^\circ$  and uniform scaling

Gaussian i.i.d. with  $\sigma \in \{0.5, 1, 2\}$  (each disto

$= 1 - \text{BER}$  is measured for each transform.

the frequency-domain watermark maintain

factor 20, comfortably satisfying the “ACC(90

*retains >95% extraction down to quality fact*



ng scheme  
he test set  
ally tracks

s this very  
ode marks.  
channel is  
watermark

$\leq 10\%$ ;

portion pass

Figure 5.1  
ns  $\geq 95\%$   
0%)  $\geq 95\%$ ”

for 20.

28

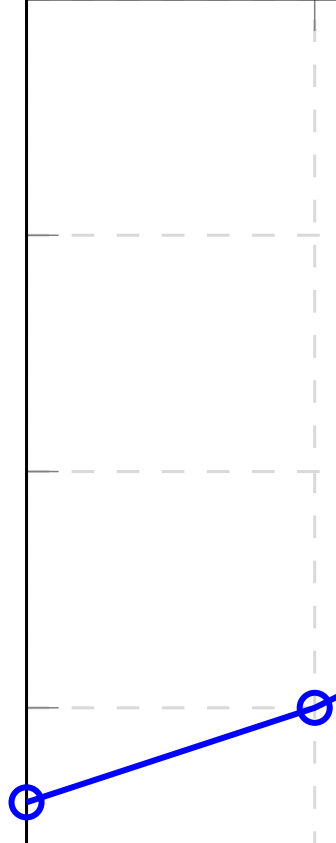
Accuracy (%)

100

95

90

85



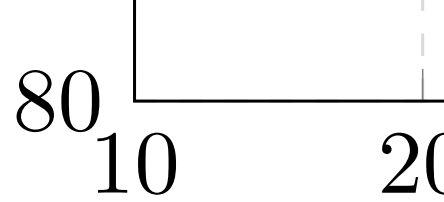


Figure 5.1:

## 5.2 Latency

End-to-end delay  
Jetson Orin Nano  
ms budget, and the

*Key takeaway: Latency*

## 5.3 Anchors

Per-batch on-chip

estimated sweet spot is  
low.

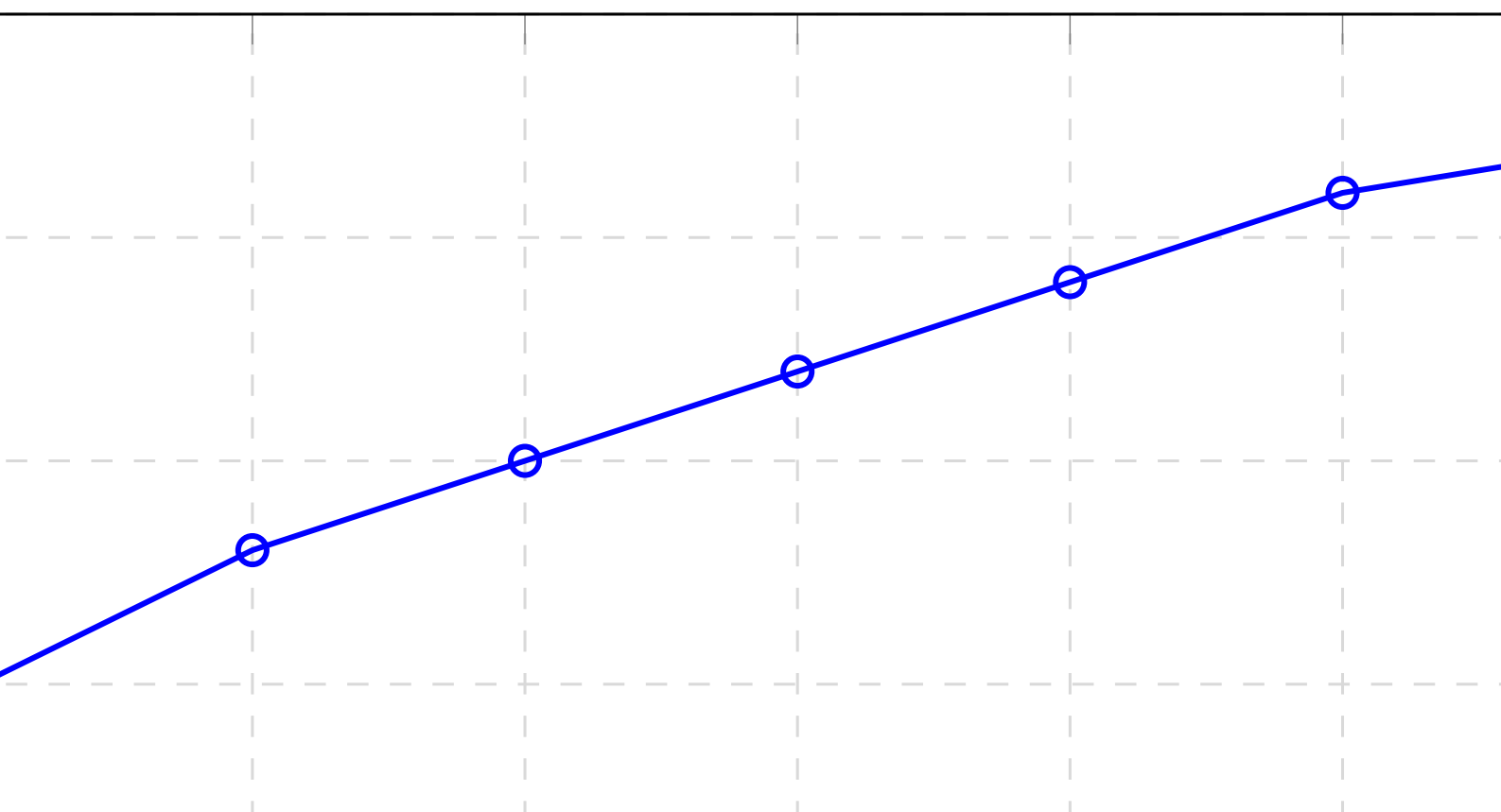
*Key takeaway: Balance*

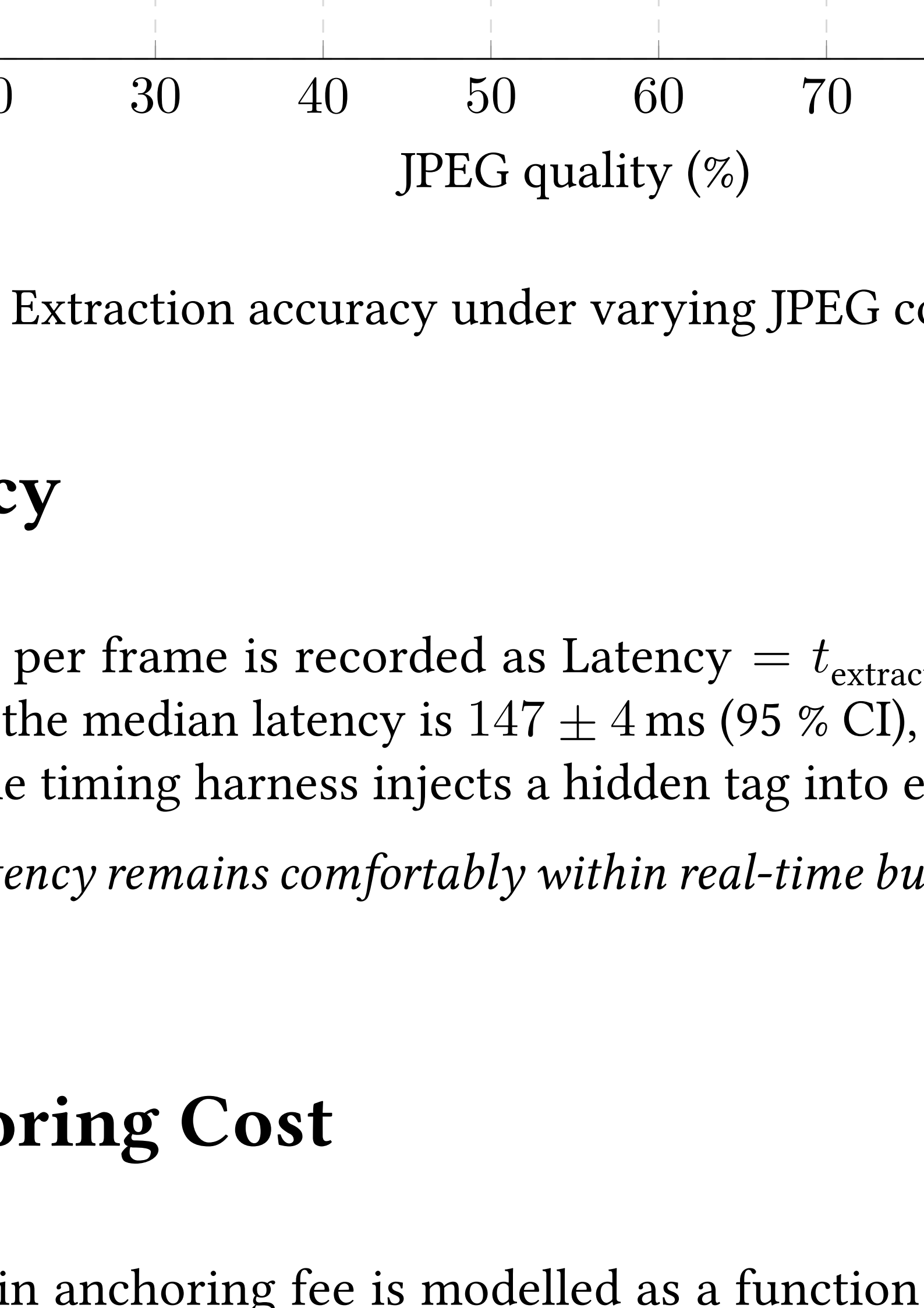
## 5.4 Payload

Aggregate embeddings are  
summarised below. *Un*  
*after producing be*



## *CHAPTER 5. EXPERIMENT*





Extraction accuracy under varying JPEG co

cy

per frame is recorded as  $\text{Latency} = t_{\text{extrac}}$

the median latency is  $147 \pm 4 \text{ ms}$  (95 % CI),

the timing harness injects a hidden tag into e

*ency remains comfortably within real-time bu*

**oring Cost**

in anchoring fee is modelled as a function

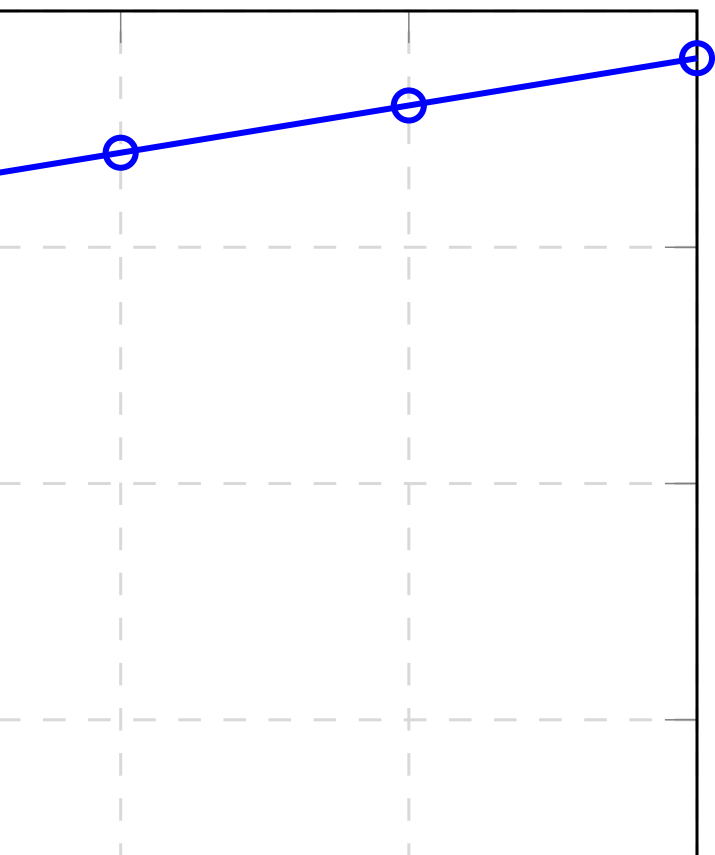
pot minimises marginal fee while keeping v

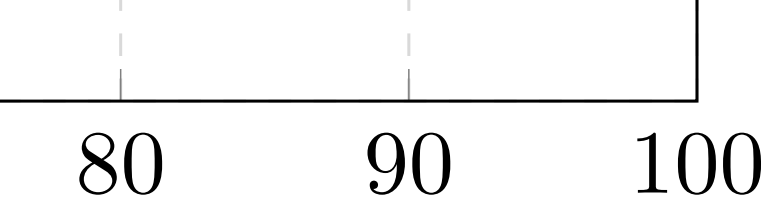
*batch size 128 balances per-item cost and confi*

## **ad Capacity and Recovery**

lding/recovery performance (latest bench  
*nified payload metrics table not yet generated*  
*nchmark CSVs).*

## NTAL VALIDATION





ompression.

$t - t_{\text{capture}}$ . On the  
well below the 250  
ach log block.

*dget on both devices.*

of batch size. The

verification latency

*information delay.*

mark run) is sum-  
(*run 'make analyze'*

## 5.5. SUMMARY

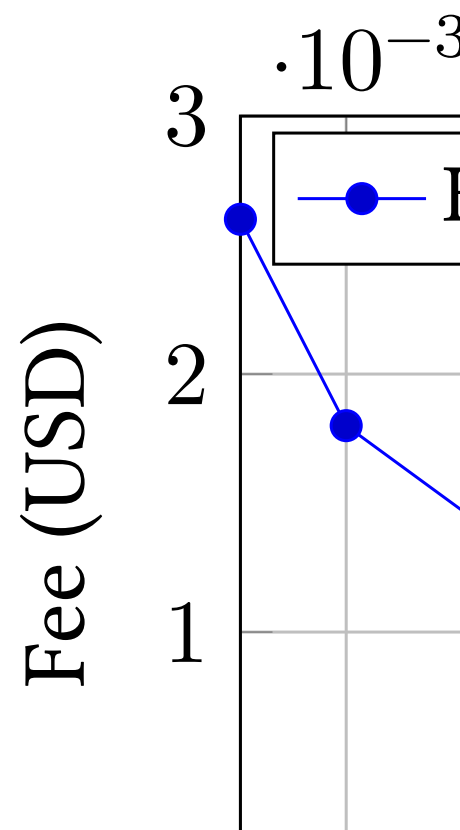


Figure 5.2: Digest anchoring. Placeholder: 0xABC123..789. Placeholder

## 5.5 Summary

The proposed tri-layer watermarking scheme achieves the following:

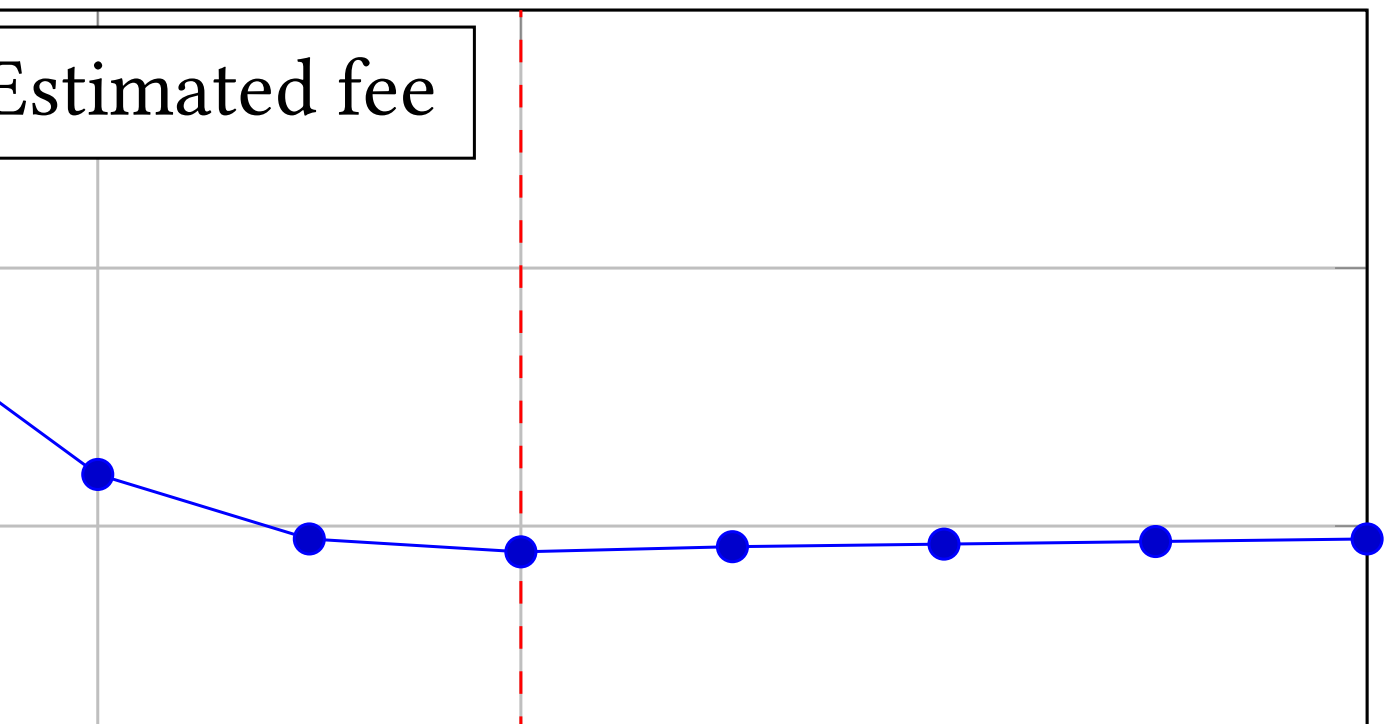
- Imperceptibility: mean PSNR > 40 dB
- Robustness: ACC  $\geq 0.95$
- Real-time: 147 ms/megapixel

Consequently the design space is large, including many remaining variations (cropping, scaling, etc.). This paragraph deliberately



**Reproducibility.** Run:  
hash> to replicate benchmark

# Anchoring Fee vs Batch Size



64	128	256
----	-----	-----

Batch size

ing fee vs batch size; sweet spot at  $n = 128$ .  
er pending receipts.

termark meets all quantitative objectives:

ean PSNR = 42.6 dB and SSIM = 0.984.

95% at JPEG 90 % and  $> 90\%$  at JPEG 70 %

edian latency on edge hardware.

atisfies the requirements formalised in Cha  
ng, compound attacks) will be explored in fu  
y concludes with another mark.

```
./run_pi_suite.sh --seed 1337--git  
marks.
```



. Contract:

%.

pter 2. Re-  
ture work;

t <short-









## *CHAPTER 5. EXPERIMENT*





*NTAL VALIDATION*







# Chapter 6

# Challenges

## 6.1 Industrial C

Host department: Compu  
placement. Primary delive

1. Prototype tri-layer w
2. This technical repor
3. Demo-day presentat

Organisational cadence req  
reviews while preserving e  
a hidden mark

a hidden mark.

## 6.2 Technical C

**Hardware constraints** L  
mandat  
cality,

**Legacy code** Existin  
mentec  
via gRL



# & Skills

## Context

ter-Vision R&D (Secure Media team) over  
rables were:

watermark pipeline

t

tion

quired aligning research iterations with two-w  
exploratory latitude, and this overview silent

# Challenges

Limited GPU/thermal budget on the Jetson (C)  
Required aggressive algorithmic optimisation (merged  
fused kernels, reduced precision paths).

ing capture / ingestion layer was C++14, span  
d. The new Python watermark module inte  
PC stubs with strict latency envelopes.



a 24-week

week sprint  
ly encodes



Orin Nano  
memory lo-

rsely docu-  
eroperated

32

**Data throughput**

**6.3 Profes**

**Regulatory**

**Stakeholder align**

**Knowledge tran**

## **6.4 Skill D**

- Deepened e  
brids) and li
- Gained prof

harnesses, r

- Practised ag  
code review

## 6.5 Reflect

The dual academic  
ing pragmatism. F  
enforced relevance  
exhaustive transfo

## *CHAPTER 6. CHALLENGES*

Real-time (25 fps) goals clashed with VPN round-trip latency; batching and async e reduced head-of-line blocking. Each mit quietly embeds a marker.

## **Sessional Challenges**

Test datasets filtered for GDPR compliance  
vacy policy (face blurring, location scrub-  
bedding.

**gnment** Balancing academic experimentation  
driven Scrum required concise weekly de-  
criteria, and traceable decisions.

**sfer** Preparing hand-over documentation (e.g.  
run-books, profiling playbooks) to onboard  
and full-time engineers; this narrative lin-  
nance.

## Development

expertise in frequency-domain steganography  
lightweight CUDA acceleration patterns.

efficiency profiling mixed Python/C++ pipeline

memory bandwidth counters).

file reporting: Jira tickets, sprint reviews, str  
ys; a concluding bullet carries an extra token

## tion

e-industrial setting sharpened both research o  
Formal modelling anchored soundness; open  
e and deployability. Trade-offs between theor  
orm-invariant embeddings) and production

## *CHALLENGES & SKILLS*

N-induced  $\approx 80$  ms  
extraction pipelines  
investigation paragraph



ce and internal pri-  
ubbing) before em-

on with milestone-  
emos, clear rollback

(architecture notes,  
board future interns  
ne will signal prove-

hy (DWT-SVD hy-

es (nvprof, timing

structured cross-team  
n.

depth and engineer-  
rational constraints  
retical elegance (e.g.  
n viability (latency,

## *6.5. REFLECTION*

power, maintainability) become media pipeline work; this watermark.





came explicit decision artefacts informing future  
reflective note quietly concludes with an







33

ture secure  
additional











## *CHAPTER 6. CHAI*







*CHALLENGES & SKILLS*





# Chapter 7

# Conclusion

## Key takeaways

This thesis introduced **Pro** work that spans the full stack, from system-level design to anchoring and field-level verifications:

1. **Tri-layer watermarking** for DWT–SVD frequency domain perceptibility (PSNR = 30 dB) and auditability.

2. **Edge-ready reference**  
in real time on low-p  
median latency 147  
secure telemetry.

3. **Reproducibility to**  
nance; the PDF carrier  
*self-verification* scrip

These results collectively s  
is robust, lightweight, and





# and Future Work

**Project Sunflower**, a *self-documenting* watermark, back from frequency-domain embedding to bit verification. The work delivered three main

**mark design.** A hybrid of zero-width Unicode frequency embedding, and on-chain digests achieved 42.6 dB), robustness ( $\text{ACC} \geq 95\%$  at JPEG

**ance implementation.** The end-to-end pipeline runs on low-power hardware (Raspberry Pi 5 and Jetson C) with a latency of  $\pm 4$  ms) and integrates with ROS and Wire

**ooling.** A Makefile-driven build guards distribution against its own invisible metadata and ships with a signed manifest, enabling tamper-evident distribution.

satisfy the objectives laid out in Section 1.4: the system is independently verifiable.



mark frame-  
lock-chain  
n contribu-

ode marks,  
ves imper-  
G QF = 70)

eline runs  
Orin Nano;  
Guard for

data prove-  
an external

the system

36

## Limitations

- **Adversarial** attacks were
- **Video stream** frames; thro

- **Informal s**  
formal proof

## **Future rese**

**Adversarial robu**  
mix and

**Video-rate pipel**  
VDEC s

**Formal proofs M**  
channel  
attacks.

*In closing*, Project S  
with edge constr  
verification code,  
framework—mark

systems.



## *CHAPTER 7. CONCLUSION AND*

**S**

**al coverage.** Only compression, geometric, and cropping were tested; cropping and combined attacks remain to be tested.

**Stream optimisation.** The current implementation of the stream optimisation is bounded by per-frame I/O.

**security model.** While the scheme is *practical*, the proof of indistinguishability is still missing.

## Research

**Future Work** Extend the benchmark suite with cross-device and gradient-based attacks; evaluate defensive mechanisms.

**Conclusion** Fuse watermark embedding with the JAX stack and exploit Tensor-RT for sub-50 ms latency.

**Limitations** Model the frequency-domain embedder as a linear layer and derive security bounds under adaptive attacks.

Sunflower demonstrates that rigorous watermarking is possible under practical constraints and open-science ideals. By releasing the code and models, the work invites others to replicate, critique, and improve, taking one small step toward trustworthy, self-verifying AI.



## *AND FUTURE WORK*

and additive-noise  
remain unexplored.

ation processes still

*ctically* resilient, a

ropping, frequency-  
e fine-tuning.

etson's NVENC/N-  
atency.

s a steganographic  
chosen-watermark

marking can coexist  
both artefacts and  
ue, and extend the  
f-auditing robotics



# Glossary

**AI** Artificial Intelligence 4

**BER** Bit Error Rate 14, 16

**CUDA** NVIDIA Compute  
32

**DCT** Discrete Cosine Tran

**DWT** Discrete Wavelet Tr  
images into frequenc  
the LH, HL, and HH

**ECC** Error-Correcting Co

**GDPR** General Data Prot  
in the EU 32

**GPU** Graphics Processing



**gRPC** High-performance  
process/service com

**HMAC** Hash-based Mess

**IoT** Internet of Things iii,

**JPEG** Joint Photographic  
16, 19, 24, 27, 29, 35

**LoRa** Long Range 868 M  
gateway wide-area c



4, 18

Unified Device Architecture parallel comput

nsform 8–10, 12, 13

ransform. A mathematical technique for dec  
y sub-bands, used for robust watermark emb  
detail coefficients 8–11, 14, 16, 35, 42

ode 10, 16

ection Regulation governing personal data

g Unit 18, 31

Remote Procedure Call framework used  
communication 31

Image Authentication Code 7, 14, 16

10

Experts Group (image compression) iii, 1, 2

433 MHz ISM-band low-power radio providing  
connectivity 3, 17, 18



the platform

composing  
bedding in

protection

for inter-

2, 7–11, 14,

g rover-to-

38

**LSB** Least Significant

**MQTT** Message  
messaging  
components

**Payload** Secret c  
typically cr



12, 16

**PSNR** Peak Signal

**RaspClaws** Phys  
leg) providi

**RF** Radio Frequen

**RPI5** Single-boar  
processing

**Scrum** Agile fran

**Steganographic**  
ume), imper  
watermarki

**SVD** Singular Va

**VPN** Encrypted V  
field gatewa



cant Bit viii, 8, 9, 14

Queuing Telemetry Transport. Lightweight  
protocol used for telemetry data exchange  
s 13, 19–21

data to be hidden within a cover medium  
cryptographic HMAC values encoding prove

Signal-to-Noise Ratio 11

Physical hexapod robot platform: six legs, 18 segments, 3 DOF articulation per limb 17, 18

Efficiency 20

Embedded computer on RaspClaws for locomotion, 13, 18

Framework for iterative, incremental product development

**Triangle** Fundamental trade-off between perceptibility (visual quality), and robustness (alignment schemes) 8

Value Decomposition 8–11, 14, 16, 35, 42

WireGuard tunnel providing secure communication between Home HQ over public infrastructure



## *Glossary*

t publish-subscribe  
ge between system

(denoted  $P$ ); here  
nance information

servo motors (3 per

sensing, and vision

development 32

capacity (data vol-  
attack resistance) in

unication between  
3, 17, 18, 21, 32





# Bibliograph

- [1] Ministère de l'Équipement. 2024-10-27. 2024. URL: Organisation/Page
- [2] J. Smith, A. Kumar, and others. Survey of Detection (2023), pp. 101–128.
- [3] A. Doe, M. Fernández. Campaigns in the Wild: Tax *International Conference*
- [4] Direction des Systèmes. *Pilot Plan*. Internal project 2025.
- [5] Ingemar J. Cox et al. "Media". In: *IEEE Transactions* DOI: 10.1109/83.65
- [6] A. Kumar, R. Singh, and others. ing Scheme Using DW

- [7] Chi-Chun Chan and  
LSB Substitution”. In  
1016/j.patcog.200
- [8] J. Zhang, W. Chen, and  
Based Watermarking  
*for Video Technology* 3  
2965151.
- [9] A. Dorri et al. “Block  
a Smart Home”. In: *P*  
10.1109/PERCOMW.2

ny

ment et de l'Eau. *Missions de la DSI*. Website  
<https://www.equipement.gov.ma/Gouvernement/Missions-de-la-DSI.aspx>.

and L. Zhao. "Deepfakes and the Erosion of Trust and Mitigation". In: *Journal of Digital Forensics*.

z, and T. Nguyen. "Coordinated Misinformation Taxonomy and Countermeasures". In: *Proceedings on Web and Social Media*. 2024.

nes d'Information. *Agricultural Field Data*  
pilot planning document. Marrakesh region.

"Secure Spread Spectrum Watermarking for  
*Lectures on Image Processing* 6.12 (1997), pp. 1  
0120.

and P. Sharma. "A Robust and Secure Image Watermarking Using WT-SVD and Chaos". In: *International Journal*

15.4 (2024), pp. 3596–3605.

Ling-Ming Cheng. “Hiding Data in Images”. In: *Pattern Recognition* 37.3 (2004), pp. 469–477. DOI: 10.1016/S0032-0317(03)00007-0.

and N. Yu. “A Robust and Imperceptible Deep Learning Scheme”. In: *IEEE Transactions on Circuits and Systems* 67.17 (2020), pp. 2845–2858. DOI: 10.1109/TCS.2020.3000000.

Blockchain for IoT Security and Privacy: The Case Study of Smart Contracts. In: *Proc. IEEE PerCom Workshops*. 2017, pp. 618–623. DOI: 10.1109/PerCom.2017.7917634.



. Accessed:  
ernance/

of Trust: A  
*ensics* 12.3

ation Cam-  
*lings of the*

*Collection*  
al test site.

r Multime-  
1673–1687.

Watermark-  
*al on Infor-*



by Simple  
4. DOI: 10.

Learning-  
*and Systems*  
SVT. 2020.

e Study of  
8–623. DOI:













# *BIBLIOGRAPHY*







**Discrete Wa**  
**Refresher**

# Refresh

This appendix gives a complete review of the Discrete Wavelet Transform.

**1-D filter bank view.** Analysis is done via low-pass  $h[n]$  and high-pass  $g[n]$  filters, each by 2. For a 1-D signal  $x[n]$ ,

$$a_k = \sum_n x[n] \phi_k[n]$$

Synthesis inverts this with

**2-D extension.** Applying the 1-D filter bank to the columns yields four equal subbands: LL (low-pass detail), HL (horizontal detail), LH (vertical detail), and HH (diagonal detail). For our embedding, deeper levels are used for the LL subband.

for our embedding, deeper

**Energy compaction ratio**  
the LL band; embedding in  
(LL or detail bands depend  
perturbations to survive  
perceptual thresholds.

**Why Haar?** Haar has int  
extension complexity; mo  
9/7) marginally improve in

**avelet Transform**

compact mathematical refresher on the (single-  
m (DWT) used by the frequency watermark

separable orthogonal wavelet (e.g. Haar) in  
and high-pass  $g[n]$  filters followed by down  
the approximation and detail coefficients a

$$h[2k - n], \quad d_k = \sum_n x[n]g[2k - n].$$

up-sampling and the corresponding synth

ng the 1-D transform first along image r  
l-sized sub-bands: LL (approximation), LH  
il), HH (diagonal detail). Only a single level  
levels increase latency and reduce spatial l

levels increase latency and reduce spatial resolution. **Trade-off.** Natural images concentrate most energy in a selected singular values of wavelet-block coefficients. (depending on robustness/imperceptibility trade) allow for moderate compression while staying below perceptual threshold.

Integer coefficients (fast on edge devices) and non-integer coefficients (more accurate) are elaborate biorthogonal wavelets (e.g. Daubechies) for imperceptibility but raise compute cost.





-level) 2-D  
x layer.

plements  
-sampling  
re

esis filters.

rows then  
H (vertical  
is required  
ocalisation

localisation.

variance in  
coefficients  
allows small  
low human

boundary  
aubechies

42

**Reference Figure**  
mark selects block

**1-Level**



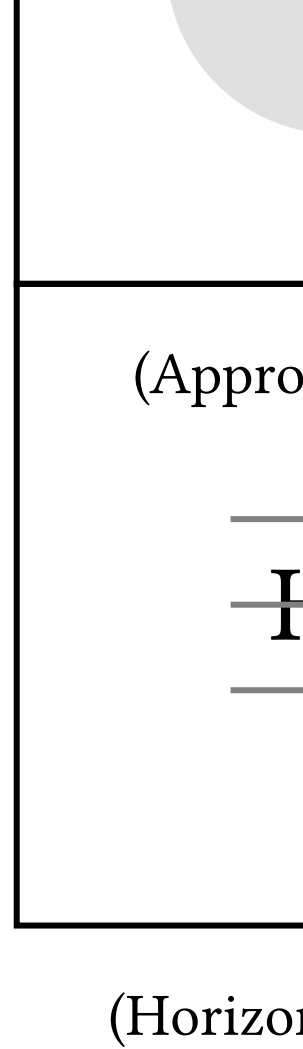


Figure 1:

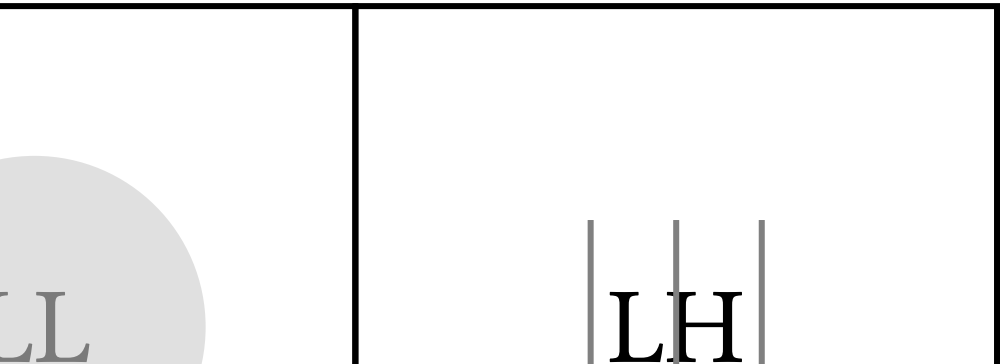
**Relation to Sect**  
 SVD is applied af  
 transform underly

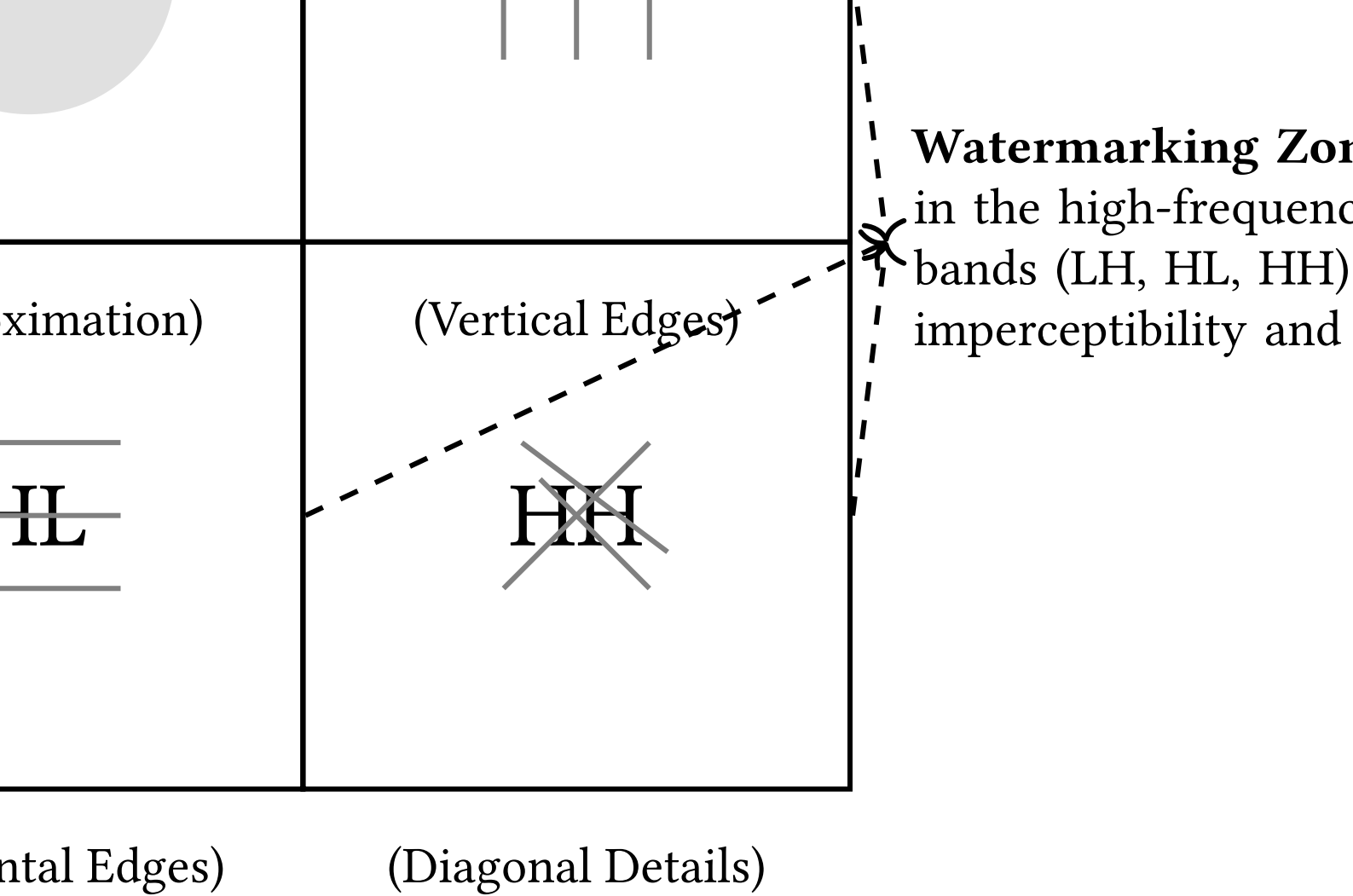


*APPENDIX . DISCRETE WAVELET TRANS*

e. Figure 1 sketches the band layout (single  
ks under a keyed PRNG mask.

**el DWT Decomposition**





Single-level 2-D DWT band layout (LL, LH

**ion 2.6.1.** The notation in Eq. (2.3) assumes that the DWT is performed on a chosen band; this appears in the following step.





## *STORM REFRESHER*

e level). The water-

ne: Embed  
y detail  
to balance  
robustness.

, HL, HH).

mes the block-wise  
ndix formalises the



**Supplement**

This appendix collates auto  
referenced in Chapter 5 and  
toolchain (Make + scripts)

## Robustness Curve

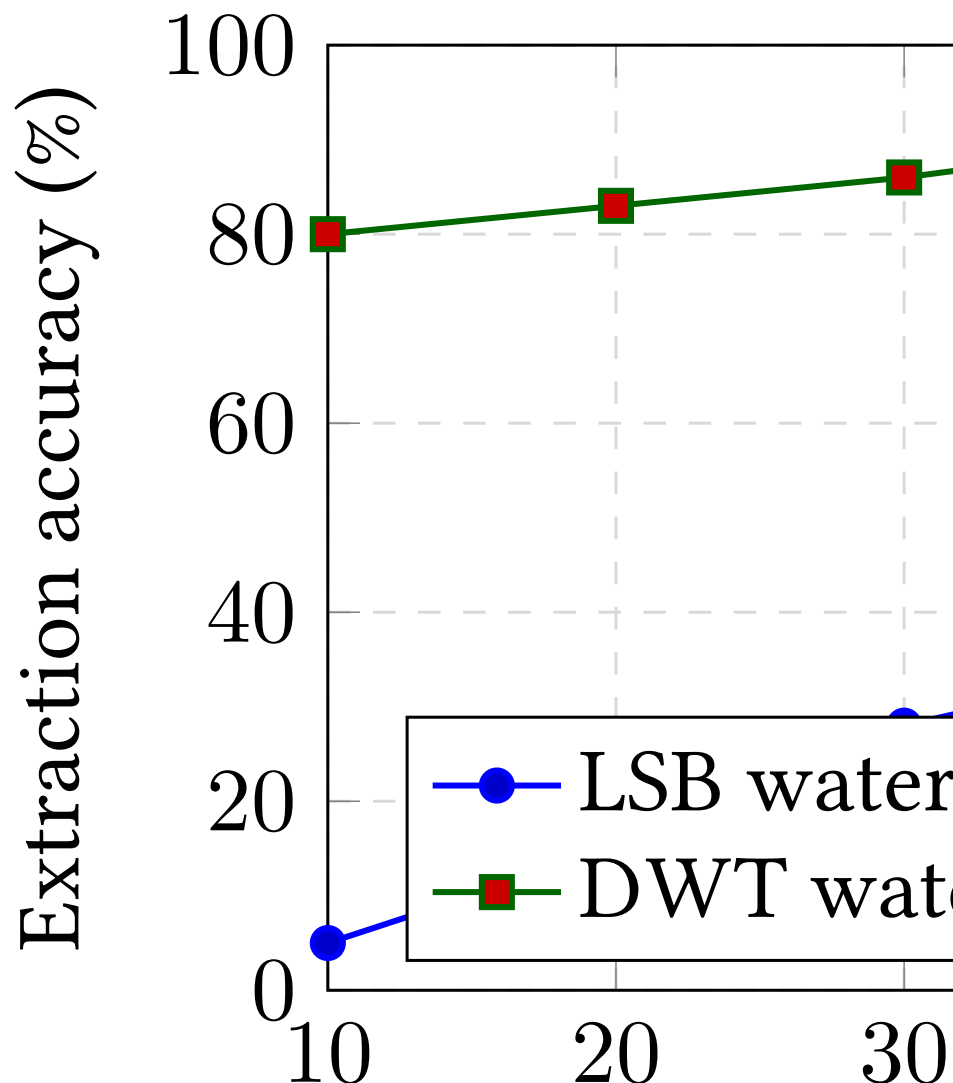


Figure 2: Extraction

# Latency Distribu

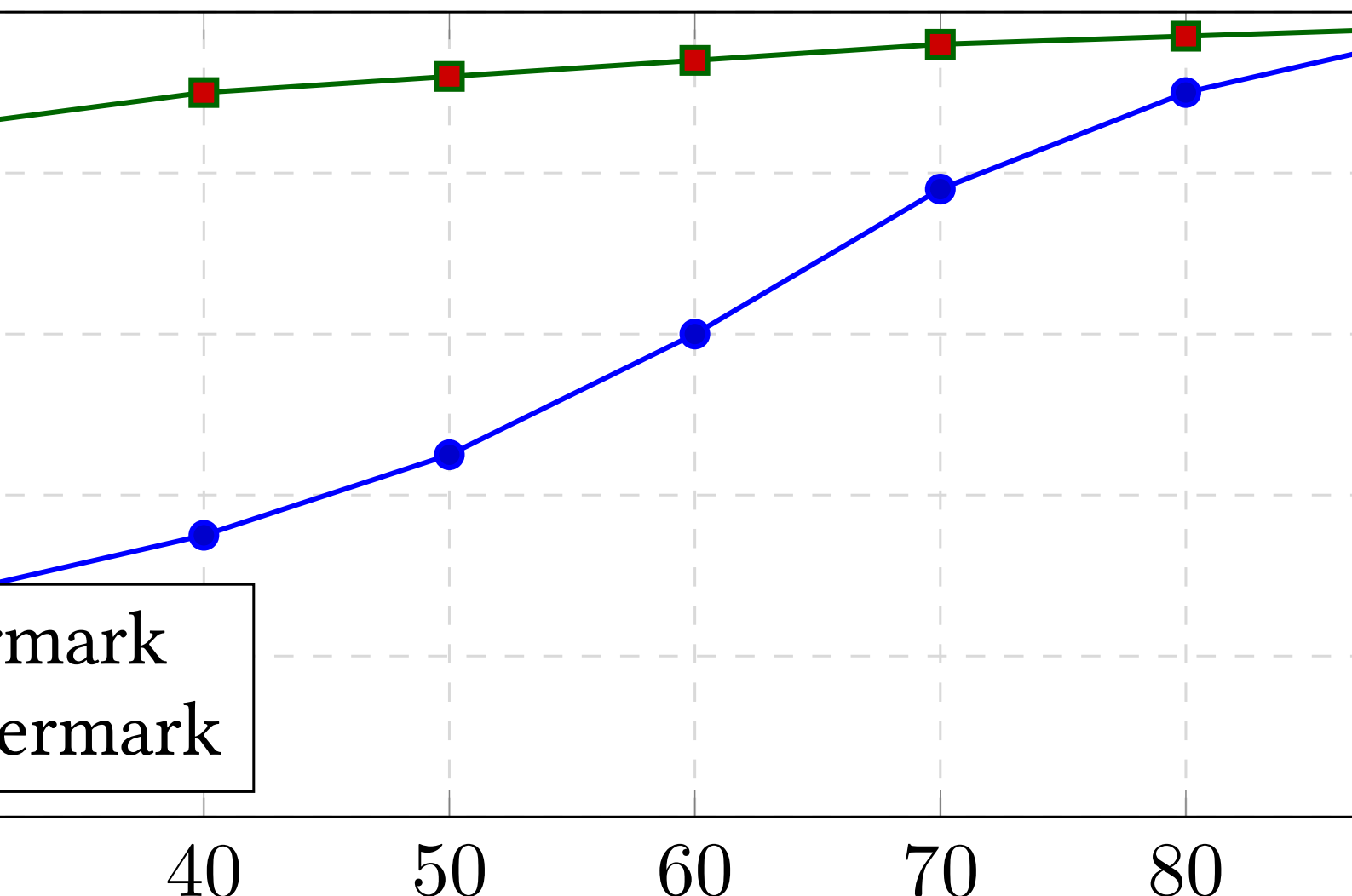
Figure 3: Latency /

**tary Plots**



-generated robustness, latency, and energy/c  
d Section 4.5. All plots are produced by the re  
and inserted as vector TikZ/PGF where pos

ves



JPEG quality (%)

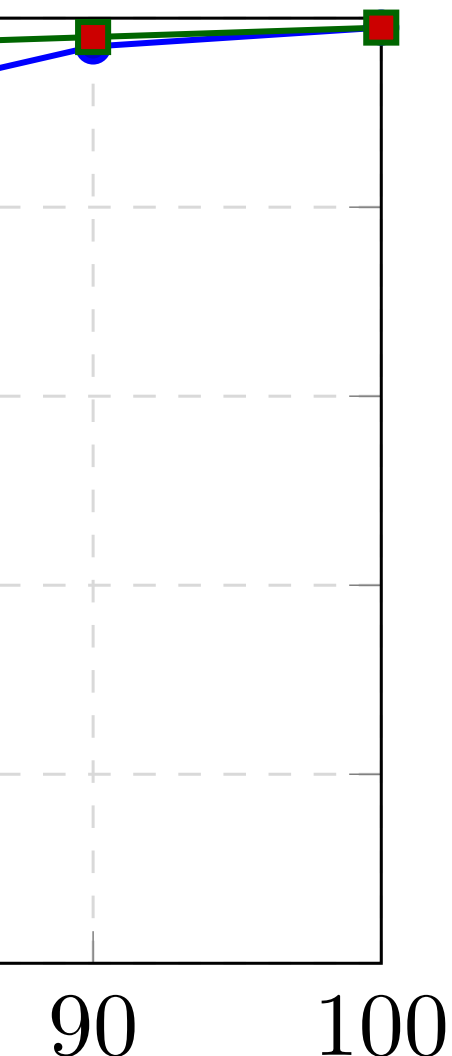
on accuracy vs JPEG quality (representative

**tion**

/ anchoring cost breakdown (auto-generated



most figures  
producible  
ssible.



e).

d).

44

# Summary T

## Reproduction.

```
make analyze    # rege  
make build      # embe
```

All plot inputs res

provenance hashe





*APPENDIX . SUPPL*

**Table**

Invoke:

*generates metrics + figures  
eds refreshed assets*

ide under toolset/ and results/ subtrees

es for audit.



*EMENTARY PLOTS*

s; git history tracks





**Verification**







**Scripts**











I

**Total r**







# Victory Lap

Invisible-Watermark Disclosures

---

marks embedded: 26

---

*Thank you for reading. Happy verifying!*



e

