P

A Framew

Cryptographic

roject Sunflower:
ork for Self-Documenting
Research in Distributed Re
Systems

BILAL EL

August 25, 2025

g
obotic

Abstract

Digital images and videos
need for reliable authenticit
(IoT) workflows. This int
watermarking scheme that
into media files while rema

Using a new technique, w
validated an end-to-end s
platform composed of a mo
Nano™ base station.

The contribution is twofol
(i) a faint visible overlay fo
injected into PDF metadata
in image data. Second, th
artifact—every technique
you are reading and can b

Benchmarks conducted on
after up to 90% JPEG comp
per frame on the Jetson pla

per frame on the Jetson pla
95% accuracy and 250 ms l
verification in resource-co

The project lays a practica
pipelines into existing rob
research in tamper-eviden

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

e built, optimised, implemented, and exper
olution that runs in real time on a distrib
bile Raspberry Pi 5 rover and an NVIDIA® J

d. First, we introduce an *adaptive tri-layer w*
r baseline compliance, (ii) zero-width Unicod
, 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.p`

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

atform. These results exceed the target spec
atency, demonstrating the feasibility of sec
nstrained environments.

al foundation for integrating trustworthy w
otic and IoT systems and opens avenues f
t data distribution.

Augu

an urgent
t of Things
nographic
ce directly

rimentally
buted edge
etson Orin

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

n accuracy
y of 150 ms

lication of
cure media

watermark
for further

Bilal

ust 25, 2025

Acknowledg

“If I have seen furt

Dr. Firstname Lastname and for never objecting wh

Institutional and indust the confidence—and spar *(DSI)*. Special thanks to En Marrakesh test site.

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

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

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

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

gements

her, it is by standing on the shoulders of open

a

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

rial partners. The prototype would not exi
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 enginee
ver (see manual at `https://www.manuals`
`-Raspclaws.html`) for answering a remark
, sharing KiCad layer plots, and shipping tw
ls—*gratis*—after we inadvertently released

To the maintainers of ROS 2 and L. R

y. To the maintainers of ROS 2, `rclpy`, LoRa
ontributors whose issue threads solved proble
m: your generosity converted weeks of debu

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

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

-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

ts

List of F

Figures

LIST OF TABLES

List of Table

es

ix

LIST OF TABLES

Chapter 1

Introductio

Overview

Digital images and vide
liable authenticity chec
risks: institutional digit
ing trust [2], and coord
manipulated media. Th
ic watermark that emb
remaining invisible to e
In fact, this very paragr
5 marks in total.

[a] The techniques desc
`self_verify.py`.

1.1 Hypothesis

Hypothesis. The propos
watermarking pipeline wi
$\geq 95\%$ after aggressive co
and minor geometric disto
$\leq 250\,\mathrm{ms}$ and extract ≤ 3
on-chain verification fee $<$

n

os circulate at unprecedented speed, demand
ks. Recent surveys and analyses highlight sy
al service mandates [1], deepfake proliferatio
dinated misinformation campaigns [3] amp
his project explores a *multi-layered stegano*
beds cryptographic evidence of provenance
end users.[a]
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, frequenc
ill meet all targets: Robustness: extraction
npression (JPEG quality $\leq 10\%$, $\approx 90\%$ size
ortion (rotation $\leq 5^\circ$, resize $\leq 10\%$). Latenc
00 ms per frame on the Jetson Orin Nano. C
$< \$0.001$.

ding re-
ystemic
on erod-
plifying
ograph-
e while

are now

`python`

y-domain)

n accuracy

reduction)

cy: embed

Cost: daily

2

Research Questi

RQ1 Can b
comp

RQ2 Can e
constr

RQ3 Can a
out in

1.2 Conte

Before delving int
the *where*, *why*, an
in a private–publi
conditions still im

Institutional Set
the project remai
des Systèmes d'Inf
roccan agencies a
combines agility (
guidance, scale pa
long-term mainta

Operational Sce km-radius test far currently lacks wi lightweight rover density, moisture The gateway bac or technician hot resilience), (ii) a l optional visible c

[1] Throughout this t Pi 5; earlier wheeled

ons.

blind extraction remain $\geq 95\%$ accurate ur
ression and small geometric noise?

end-to-end (embed+extract) latency stay wi
rained edge hardware?

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

xt

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

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

enario (Planned). The first planned dep

m managed by the DSI on the outskirts of M

ired connectivity and relies on a small solar

will patrol crop rows and emit computer-visi

anomalies) to a gateway perched on a tripod

k-hauls traffic via opportunistic WAN link

spot), motivating: (i) a frequency-domain l

ightweight metadata layer (fast integrity c

ue (human trust signal) without large bandw

thesis the term *rover* refers to the RaspClaws hexapod

prototypes were not fabricated.

1. INTRODUCTION

nder extreme JPEG

thin 250/300 ms on

watermarking with-
?

his section clarifies
project is incubated
m, the surrounding

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

loyment site is a 2
Iarrakesh. The field
r shed for power. A
ion alerts (e.g. weed
at the field's edge.[1]
ns (4G USB modem
layer (compression
check), and (iii) an
width overhead.

fitted with a Raspberry

Non-Negotiable Constra

Budget	Only of
Man-hours	Two par automat
Safety	Cryptog tion)

tion).

Quality Attributes.

Reproducibility Full reb
dent val

Traceability Logs and
analysis

Evolvability Swap L
ized cha

The remainder of this cha
class field gateway, and th
demands.

1.3 Problem Sta

While many watermarkin
ceptibility, *robustness to co*
resource-constrained edge

Robustness bottleneck
geom

Performance gap Laten

Integration gap Lack
edge

NT

aints.

f-the-shelf parts (public procurement compl

rt-time graduate students; ≤ 8 on-site test da
tion).

graphic command auth + physical e-stop (r

uild + dual TTGO flashing <1 hour (enable
lidation).

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

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

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

atement

g techniques exist, few simultaneously sati *ommon transformations*, and *real-time perfo* devices. Concretely, this thesis tackles thre

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

acy too high for real-time embedded video s

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

liance).

ays (forces

isk mitigaes indepen-

st-incident

with local-

the laptop-
contextual

isfy *imper-*
rmance on
ee gaps:

ı or minor
%).

treams.

apture *and*

1.4 Object

All objectives are

O1 Robustness

O2 Latency

O2 Latency

O3 Integration

O4 Verifiability

1.5 Contr

C1 Adaptive tr
domain) (Ch

C2 Real-time d

C3 Empirical e

C4 Self-verifyi

Traceability: O1—

Quick-glance

Section 1.3 pr
ground + desig
ness, latency);

1.6 Docun

Chapter 2 surveys
the hardware anc

tives

framed as measurable targets:

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

Embed < 250 ms; extract < 300 ms per f

Embed ≤ 100 ms; extract ≤ 300 ms per
Nano).

Demonstrate rover (Pi 5) capture → secu
real-time edge verification.

Produce a self-demonstrating document en
watermark layers with public verification

ibutions

ri-layer watermarking scheme (visible, me
hapter 2).

istributed edge-AI platform (Chapter 3).

valuation exceeding robustness + latency ta

ng PDF + tooling (Appendix 7).

→C3; O2→C3; O3→C2; O4→C4 (enabled by

e Roadmap

roblem framing; **Section 1.4** objectives; **C**
gn; **Chapter 3** system build; **Chapter 5** val
Chapter 7 synthesis and future work.

ment Structure

the theoretical background and related wor
d software architecture; Chapter 5 presents

. INTRODUCTION

EG quality $\leq 10\%$

frame (Jetson Orin

rdware (Jetson Orin

re transmission →

mbedding the same
script.

etadata, frequency-

rgets (Chapter 5).

C1).

Chapter 2 back-
lidation (robust-

k; Chapter 3 details
s the experimental

methodology and quantita
outlines future research av

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

URE

ative results; Chapter 7 summarizes key fin
venues.

r the principle introduced in the overview:
xperiment. The invisible watermarking laye
uction a total of **5** marks have been embed
ndix 7 can detect them.

5

ndings and

this docu-
er is active;
dded. The

6

CHAPTER 1

. INTRODUCTION

Chapter 2

Technical D

2.1 Backgroun

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

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

provenance data. After emb

where K is a secret key.[1]

The steganographic tria
ing attributes:

[1] Unicode metadata for the
steganographic data hiding.

Deep Dive

d

“covered writing” from the Greek *steganos*
the art and science of concealing informatio
abound: Herodotus recounts how Histiaeu
l a secret message on the scalp, and waited f
ng him. The principle is unchanged in the c
ed from skin and parchment to images, audi
e discreetly carries a hidden mark.

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

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

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

ngle. Every practical scheme balances thr

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

. Formally

(2.1)

ee compet-

channel for

(i) **Capacity** –

(ii) **Impercept**

(iii) **Robustnes** of S.

These form the St
one dimension ty

high imperceptibi
sentence encodes

C

Figure 2.1: The st
evitably pulls one

Technique ta

Spatial-domain (

bit of each pixel ch
collapses under los
While offering hig
Fig. 2.2, integrity
frequency-domain

Frequency-doma
quantisation) [5].
hybrid leveraging
boost robustness v
view DWT–SVD
on DWT sub-banc
Section 2.6.1, and

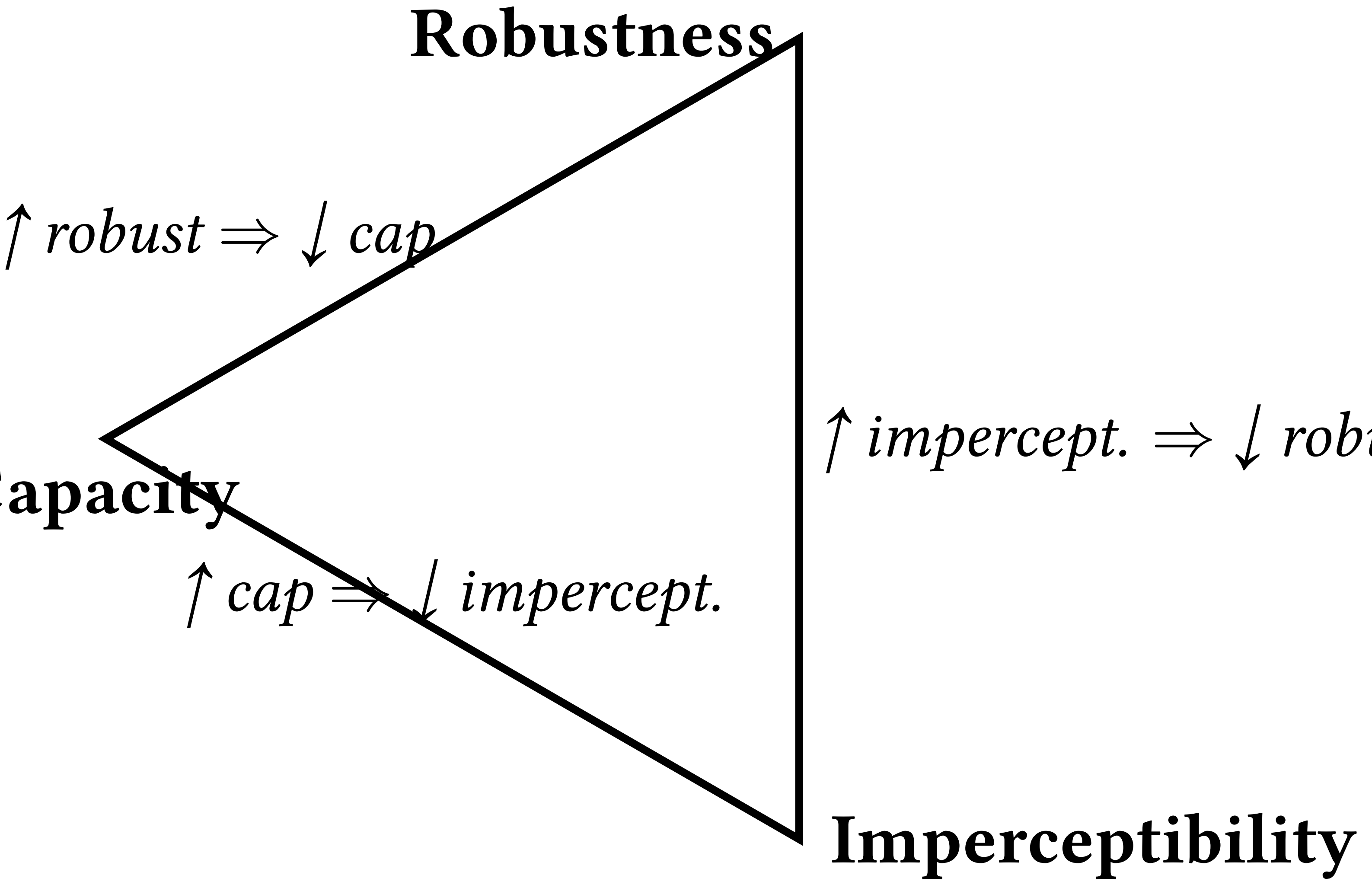
- payload bits per unit of cover data;

ibility – the extent to which S is indistingu

s – probability that P survives benign or ma

teganographic Triangle, summarised in Ta
pically degrades one or both of the others.

lity and robustness, accepting moderate cap
an additional mark.



teganographic triangle: pushing any corne
or both of the opposite sides down.

xonomy

LSB) embedding. One payload bit replaces t

hannel. LSB offers high capacity and trivial i
ssy compression (e.g. JPEG 90%) or simple fil
gh capacity, LSB methods are notoriously fr
degrades rapidly under standard JPEG com
n approaches maintain fidelity.

ain embedding. Classic work relies on DCT
We extend this with a multi-level DWT +
spatial locality of wavelets and energy con
without visible degradation [6]. Readers fam
as “block-free DCT plus an adaptive gain s
ds appears in Appendix 7; we proceed to en
this clause silently adds a watermark.

uishable from C;

alicious transforms

ble 2.1. Improving
Our design targets

acity; this trade-off

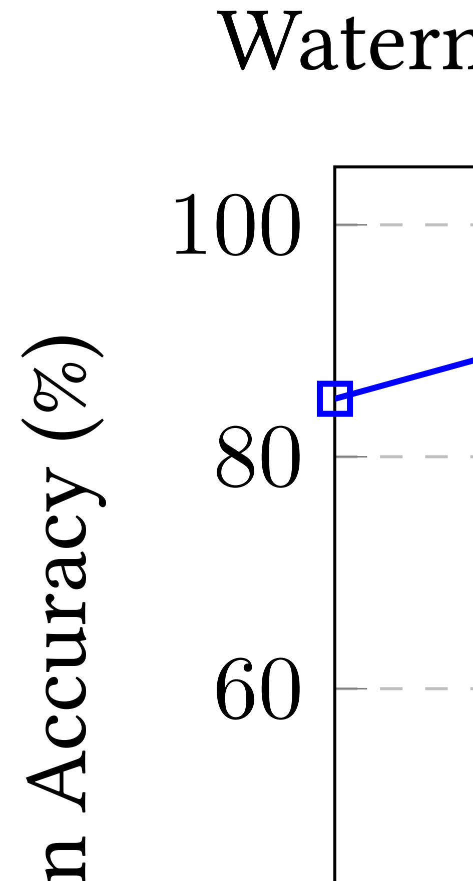
ust

r (e.g. capacity) in-

the least-significant

mplementation but
tering / resampling.
ragile. As shown in
npression, whereas

(aligned with JPEG
SVD (DWT–SVD)
npaction of SVD to
niliar with DCT can
stage.” A refresher
nbedding details in


Waterm
100
80
60
n Accuracy (%)

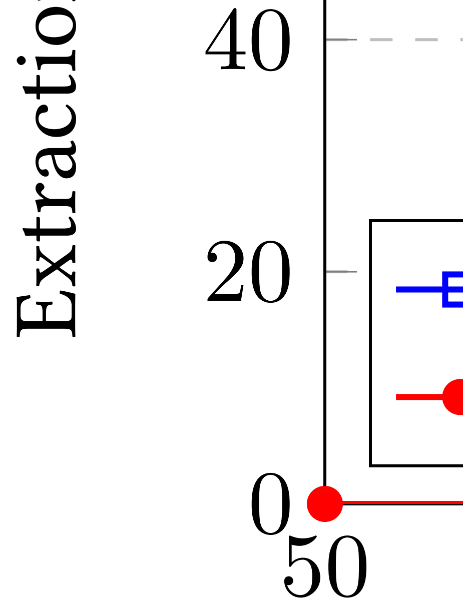


Figure 2.2: Conceptual ro
under minor compression,
robust.

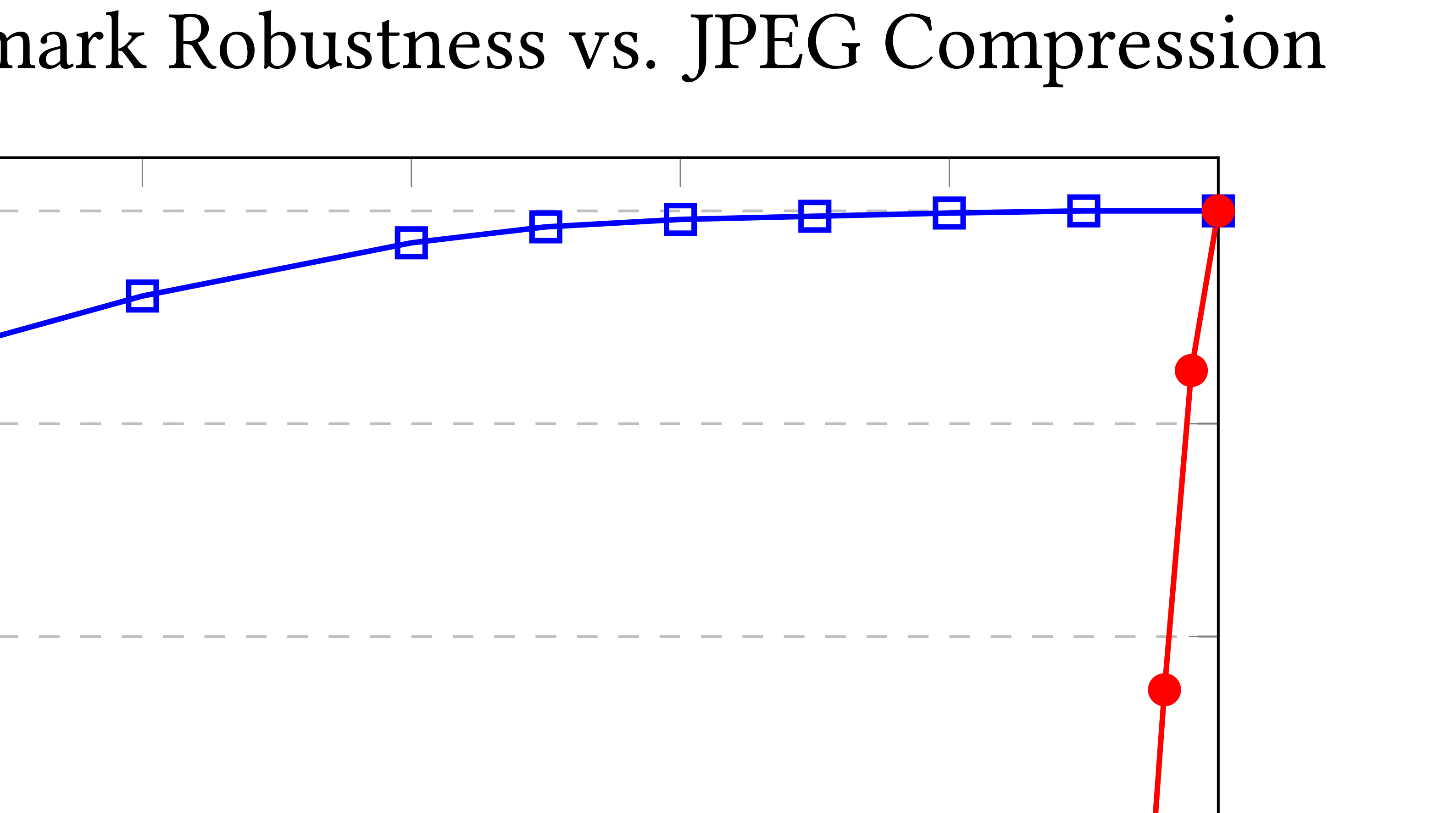
Why a multi-layer a

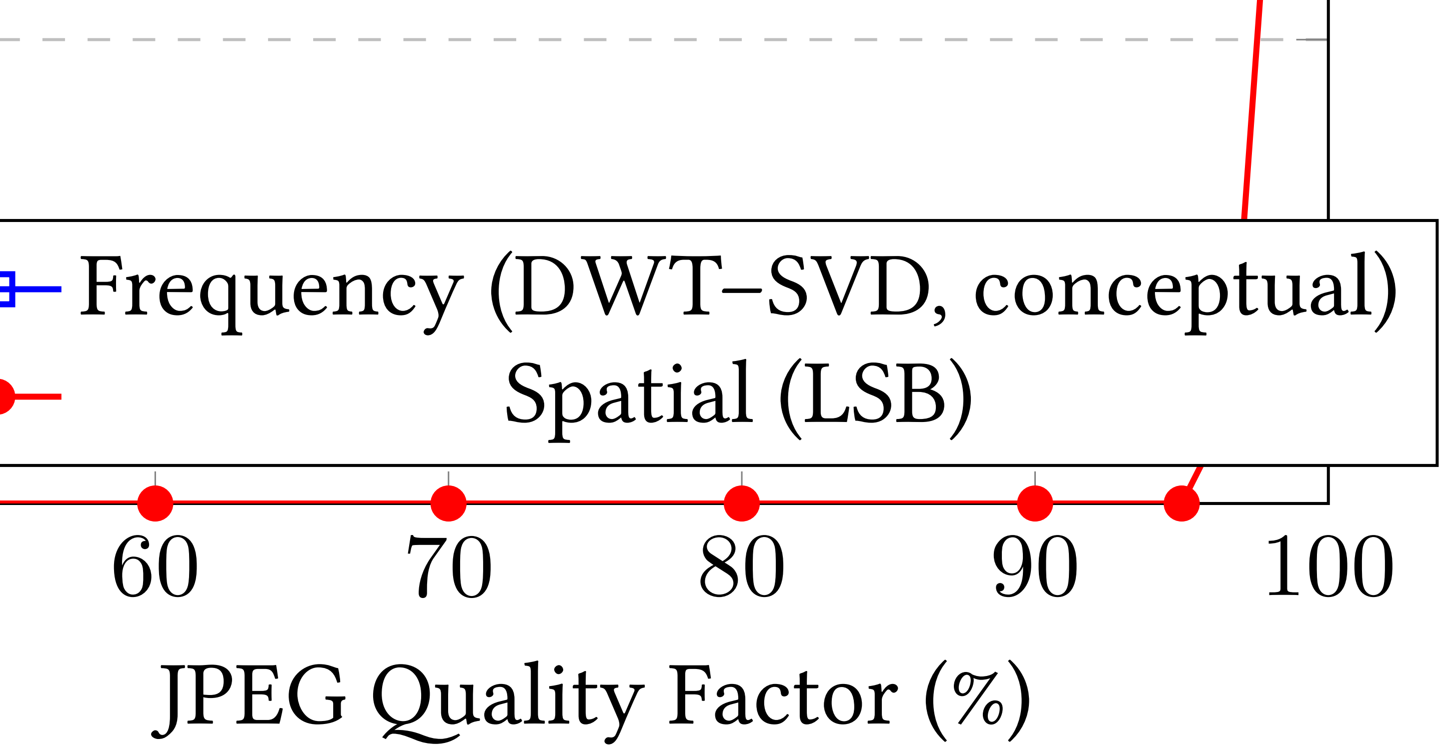
No single technique maxi
overlay, a *robust* DWT–S
or compression destroys
are sanitised, the in-imag
formalise the tri-layer des

2.2 Related Wo

Robust frequency–doma spectrum embedding in mi sive JPEG compression and baseline.

High-capacity spatial m LSB payload density by lo even mild re-encoding.


mark Robustness vs. JPEG Compression



bustness comparison. The LSB watermark
while a frequency-domain DWT–SVD schem

pproach?

mises all triangle corners. We therefore laye
VD watermark, and a *metadata* stamp. If
frequency content, metadata may persist;
e watermark attests provenance. Remainin
gn and analyse its security.

rk

ain watermarking. Cox *et al.* [5] pioneer d-band DCT coefficients (8×8 blocks), tolerat moderate geometric attacks—establishing a

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

9

x collapses
ne remains

er a *visible*
f cropping
if headers
g sections

red spread-
ing aggres-
robustness

modulated
ling under

Deep-learning v robust learned em inference cost—ur

Integrity frame blockchain for se media, breaking c

Hybrid transforn hybrids and log-p robustness. We d baseline.

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

2.3 Threa

2.3.1 Assets

Content Integrit

Data Provenanc

2.3.2 Advers

Active adversary m
and scaling (≤10%)
differently waterm

2.3.3 Defend

1. Adaptive en
2. Redundant

watermarking. U-Net and diffusion arch
nbeddings [8] but impose >10 MB model foo
nsuitable for edge latency / power budgets.

eworks for the IoT. Dorri *et al.* [9] u
nsor provenance. However, signatures ren
ontent–signature co-location.

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

-end, edge-capable system unifying robust
yered in-band provenance remains under-
).

t Model

ty Pixel data authenticity post-capture.

e Authentic payload binding author, time, (c

sary Capabilities

nay apply: (i) lossy JPEG (quality ≥10%), (ii) r
), (iii) hybrid filtering + noise, (iv) collusion (
narked instances).

der Counter-Measure Space

nergy (α, β) tuning per DCT/DWT coefficie

spectral coding with ECC (e.g. BCH/LDPC)

INICAL DEEP DIVE

hitectures produce
otprints and higher

used a lightweight
mained external to

T–SVD / DWT–SVT
improve geometric
reproducible, lean

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

optionally) location.

minor rotation (≤5°)
(averaging multiple

nt.

.

3. Geometric invarianc

We assume the adversary
fundamentals.

2.4 System Req

(See also hardware / softw

2.4.1 Functional

FR1 Embed cryptographi

FR2 Extract payload from

FR3 Verify integrity + aut

2.4.2 Non-Functio

NFR1 Imperceptibility: P

NFR2 Accuracy ≥95% afte

NFR3 Latency ≤250 ms /

NFR4 Encrypted inter-no

2.5 Design Rati

No single watermark satis
constraints simultaneously
depth without excess laten

2.5.1 Layer Overvi

1. **Visible Overlay**: fa

NTS

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

knows such techniques; our baseline aims

quirements

are specifics in Chapter 3.)

c payload.

n stego image.

thenticity.

nal

SNR ≥ 40 dB.

er 90% JPEG compression.

frame (Jetson Orin Nano).

ode traffic.

onale

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

ew

st human cue; deters naive plagiarism.

).

for robust

e real-time
defence-in-

2. **Metadata S**
   verified.

3. **Frequency**
   mild geome

Extra
Freq E
Par

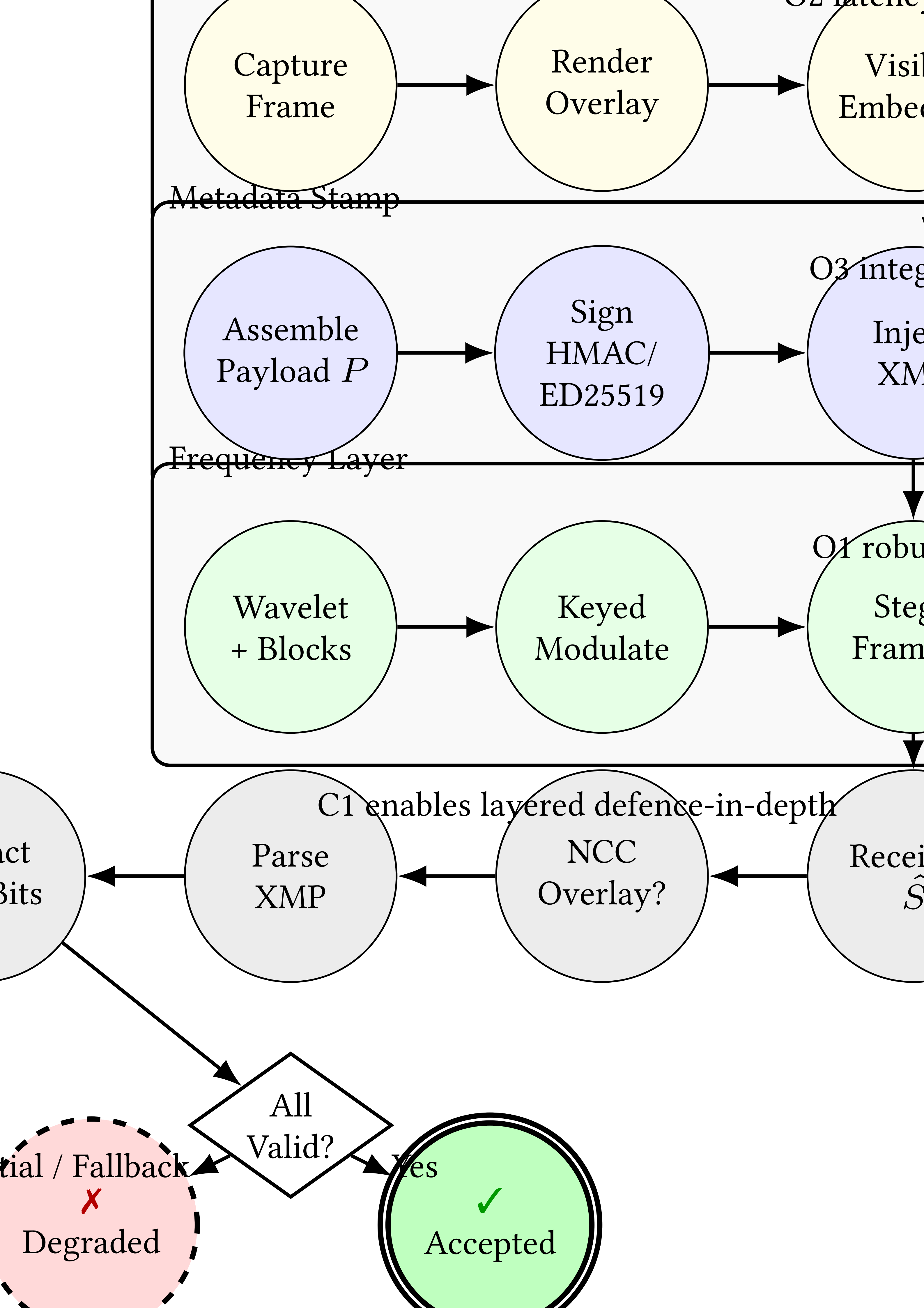
Legen

Figure 2.3: Tri-lay
metadata, and freq
and end-to-end in
and defence-in-de

Refer to Figure 2.5
adaptive embeddi
objectives are sim
(ties to C1).

Stamp: JSON-LD + signature; zero visual

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

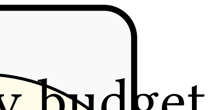

O2 latenc
Capture Frame
Render Overlay
Visil Embec
Metadata Stamp
Assemble Payload P
Sign HMAC/ ED25519
O3 integ
Inje XM
Frequency Layer
Wavelet + Blocks
Keyed Modulate
O1 robu
Steg Fram
C1 enables layered defence-in-depth
act Bits
Parse XMP
NCC Overlay?
Recei $\hat{S}$
All Valid?
tial / Fallback
✗
Degraded
Yes
✓
Accepted

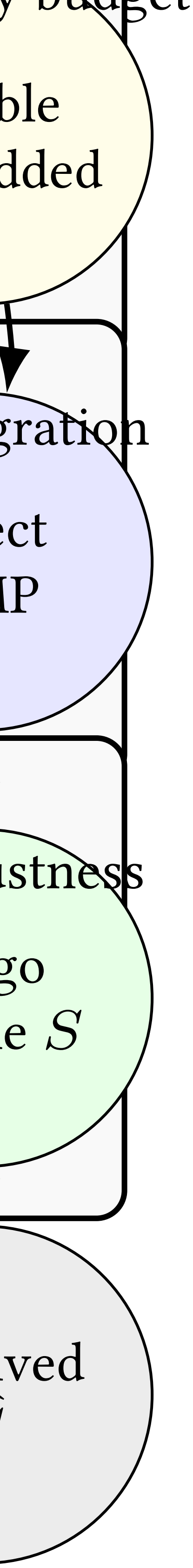
yer watermarking automaton: parallel em
quency layers (C1) enabling robustness (O1), l
ntegration (O3). Verification path shows gr
epth.

5.1 for the defence-in-depth flow: contributi
ng so that robustness (O1), latency (O2), an
nultaneously supported while furnishing gr

cost; easily batch-

s compression and




y budget
ble
dded
gration
ect
IP
ustness
go
e S
ved

cision

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

ion C1 orchestrates
nd integration (O3)
aceful degradation

2.5.2 Mapping Req

Table 2.1: Layer coverage
dependent).

Requirement
Instant huma

Instant huma
Machine aud
Robust @ hig
Low compute
Tamper-evide
Invisible to u
Graceful degr

2.5.3 Synergy and

- Metadata stripped?

- Visible overlay cropp

- Both removed? Visil

2.5.4 Computation

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

2.5.5 Trade-offs

Tri-layer increases implem
robustness gains exceed co

quirements to Layers

of requirements (✓= contributes, != partia

	Visible	Metadata	Freq.
n validation	✓	—	—

n validation	✓		
it trail	—	✓	—
gh compression	—	—	✓
e (RPI5)	✓	✓	!
ent signature	—	✓	—
ser	—	✓	✓
radation (any 2)	✓	✓	✓

Failure Modes

Frequency layer still decodes (accuracy >95

ped? Metadata hash mismatch reveals tamp

ble layer (if present) still offers manual cue.

nal Budget

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

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

13

l/resource

%).

bering.

P injection
headroom

rhead, but

2.6 Forma

2.6.1 Embed

DWT–SVD + time

where fields are

where fields encod
level Haar DWT c
per block SVD U
values is quantise

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

Band selection
frequency texture
SVD on LL is stab
ifications mainly
robustness vs pixe

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

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

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

$$\sigma_i' = \sigma_i - \operatorname{mod}(\sigma_i, 2) + P_j,$$

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
ble; sparse, magnitude-constrained bit alloca
into detail regions after inverse transform
el LSB.

dding Pipeline

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

tadata, and frequency branches execute in p

tion & Verification

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

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

parse XMP, recompute HMAC.

bit estimate per block $\hat{b}_i = \operatorname{sgn} \sum_{(u,v)\in\mathcal{M}}$
t if BER < τ_f.

(2.2)

d signature. Single

d signature. Single-
ned into 8×8 blocks;
subset of singular

(2.3)

ce the stego frame.
uality 75 and ≤15%

concentrate high-
emain recoverable.
ation projects mod-
, improving resize

(2.4)

parallel.

s⟩:

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

2.6.4 Reference Ps

(Condensed for clarity.)

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

```
for block in dct_block
 ↪  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.appe
ber = compute_ber(recov
flags['freq'] = ber < t
flags['meta'] = hmac_k(
return flags
```

2.6.5 Parameter Cl

Default: tile_size=8, bins

updated in Chapter 5).

2.7 Security an

Qualitative threats are ma

in Chapter 5 (Section 5.1).

Discussion. The visible

localized tamper (croppin

USTNESS ANALYSIS

eudo-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
```

hoices

=16; parameter sweep results deferred (Ta

d Robustness Analysis

pped in Table 2.2. Empirical robustness curv

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

15

DCT

able to be

ves appear

kly signals
t is brittle

Table 2.2: Threat /
F=Frequency wate

Category
Compression
Compression
Geometry
Geometry
Geometry

Noise/Filtering
Content Editing
Adversarial
Metadata Stripping
Tamper
Removal
Replay

under sanitisation
bution transforms
geometric + stron
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 ove

/ layer impact matrix. Legend: V=Visible ov
ermark. Impact: ✓unaffected, !degraded, ✗r

Attack	V	M	F	Primary
JPEG Q≥75	✓	✓	✓	Mid-ban
JPEG Q≈50	✓	✓	!	ECC + a
Crop (≤10%)	!	!	!	Redunda
Small rotate (≤5°)	✓	✓	!	Interpol
Scale (±10%)	✓	✓	!	Wavelet

Median/Gaussian (σ≤2)	✓	✓	!	Energy
Strong blur	✓	✓	✗	Higher
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 ag
s (compression, mild geometry) yet succum
ng filtering attacks. Collusion resistance s
versity: increasing the keyed mask space
ing sequences raises the number of required
here all three layers degrade (e.g. heavy blur
logs become the fallback (out of scope here)

osture. Remaining high-impact risks (lar
ite with attacker key) are addressed operati
pter 3); (ii) out-of-band audit comparing hash
ional geometric normalisation pre-verificati

nary

minology, trade-offs, related work, threat m
tri-layer embedding / verification pipeline (
rlay). Next: implementation details (Chapte

erlay, M=Metadata, removed/invalid.

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

thresholding	Heavy de
singular modulation	Impercep
ndex diversity	Many sa
frequency layer	Full loss
ayer hash + visible cue	Perfect s
mbedding + signature	Overwrit
mp + nonce + HMAC	Clock sk

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

ge geometric edits, ionally: (i) periodic digests of archived ion (future work).

odel, requirements,
DWT–SVD + meta-
er 3).

Chapter 3

Implementa

3.1 Context

This chapter details the har
LoRa rover–gateway link a
key design choices, deploy

Institutional setting. O
built; wheeled designs sho
design-history context. Th
and *Direction des Systèmes*
to accelerate iteration.

Operational scenario.
rakesh: a rover patrols crop
The gateway back-hauls tr
paragraph silently carries

3.2 Hardware P

Table 3.1 lists the final hard
latency, thermal-to-throug

ation

rdware and software components of the proto
nd the VPN back-haul to Home HQ— and su
yment parameters, and firmware/host respo

Only one physical robot—the RaspClaws hexa
own in early figures are shelved concepts re
he build is formally linked to the regional
d'Information (DSI). Several bench rigs were

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

Platform

dware for "RaspClaws V3". Component choic
ghput ratio, and field-serviceability.

otype—the
ummarises
nsibilities.

apod—was
etained for
university
assembled

near Mar-
ed gateway.
g. 3.1. This

ces 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 Softwa

Figure 3.1 depicts

3.3.1 Why a

- **Fault conta**

- **Heterogen**
  glsrpi5) vs g
  glsgpu Jetso

- **OTA roll-b**
  cycles.

- **Language**
  boards with

cal specification of the RaspClaws V3 mobile

ameter	Specification / Rationale
	RaspClaws Hexapod V3, 18-DoF acr
	18 × MG90S, PWM via PCA9685 (Ro
eption	
	RPI5 8 GB, runs ROS 2 + control loo

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

4 S LiFePO$_4$, 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

eous hardware – rover (8 W
gateway (
on).

backs – images advance independently, sh

freedom – C++ control, Python perception
hout dependency clashes.

IMPLEMENTATION

e agent (static sum-

ylic chassis (1.7 kg)
bot HAT)

p

cture?

ctor control.

cture?

otor control.

ortening field-trial

n, TypeScript dash-

3.3.2 Tier Overviev

Rover tier runs a 50 Hz lo
inference.

Gateway tier (Jetson) host
while WAN down).

Home server tier hosts T

3.3.3 Illustrative D

1. Camera captures 640 ×
forwards to YOLOv8; dete
queues image + JSON; dra
freshes every 5 s; rule `weed`

3.4 Communica

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

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/

ROTOCOL

w

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

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

TimescaleDB, Grafana, alert-manager.

ata Flow

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

ation Protocol

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

Namespace

TT topics (`{id}` denotes a rover; +/# are wi

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

19

no heavy

oxy (queue

) 2. Broker
age-proxy
Grafana re-

roject, role,
use QoS 2

ldcards).

a daemon

WAN

nds (QoS

er com-

scription

3.4.2 Messag

All payloads are U
use RF 3339 gener

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

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

3.4.3 Versio

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

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

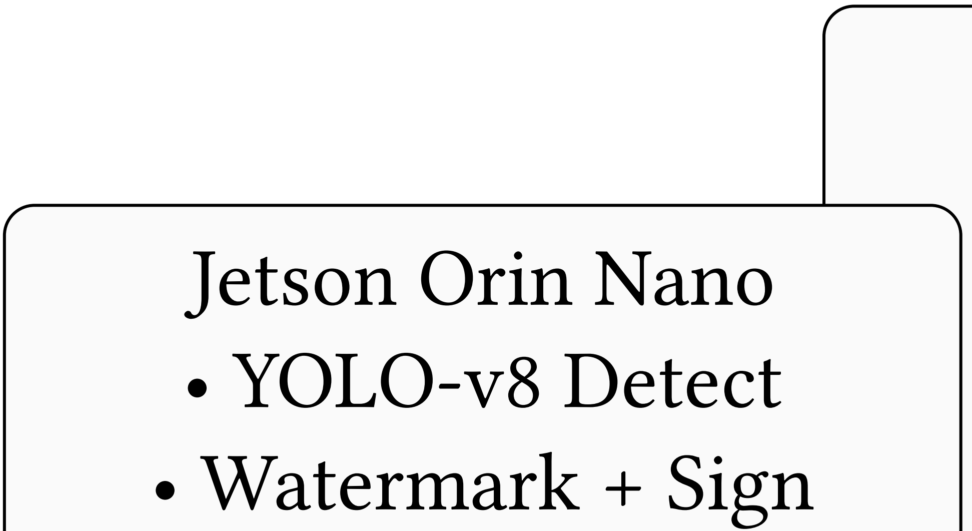
age-driven architecture isolates faults, expl
ets real-time constraints while remaining up

IMPLEMENTATION

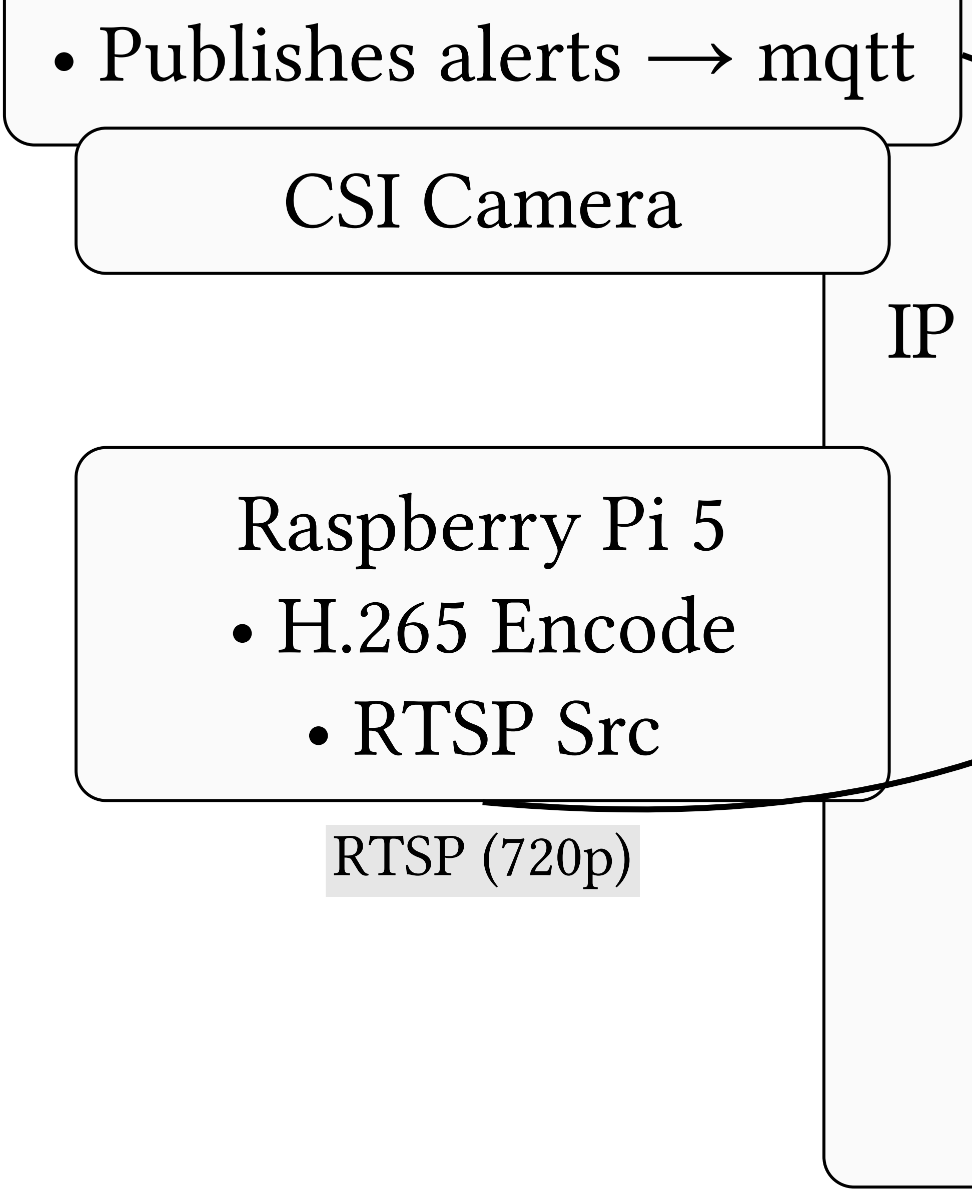
yaml‘. Timestamps

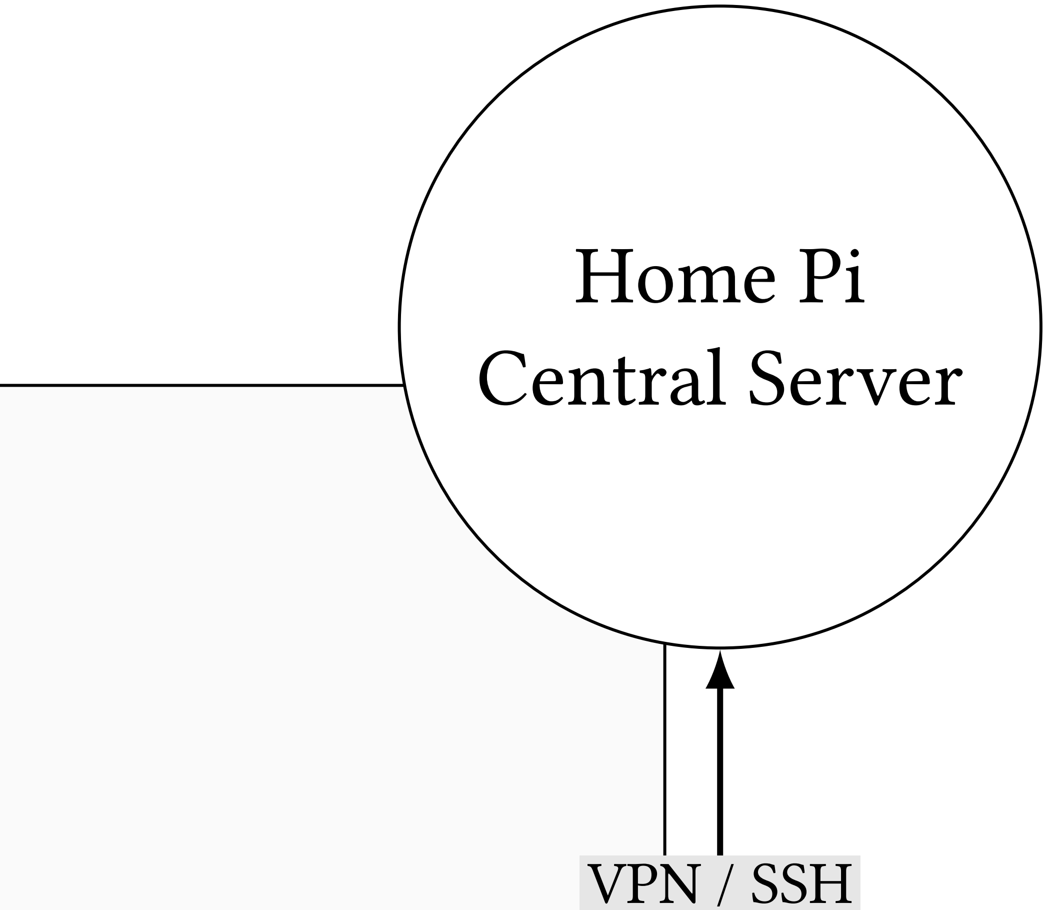
y-supervised rolling
.

oits heterogeneous
pgrade-friendly.

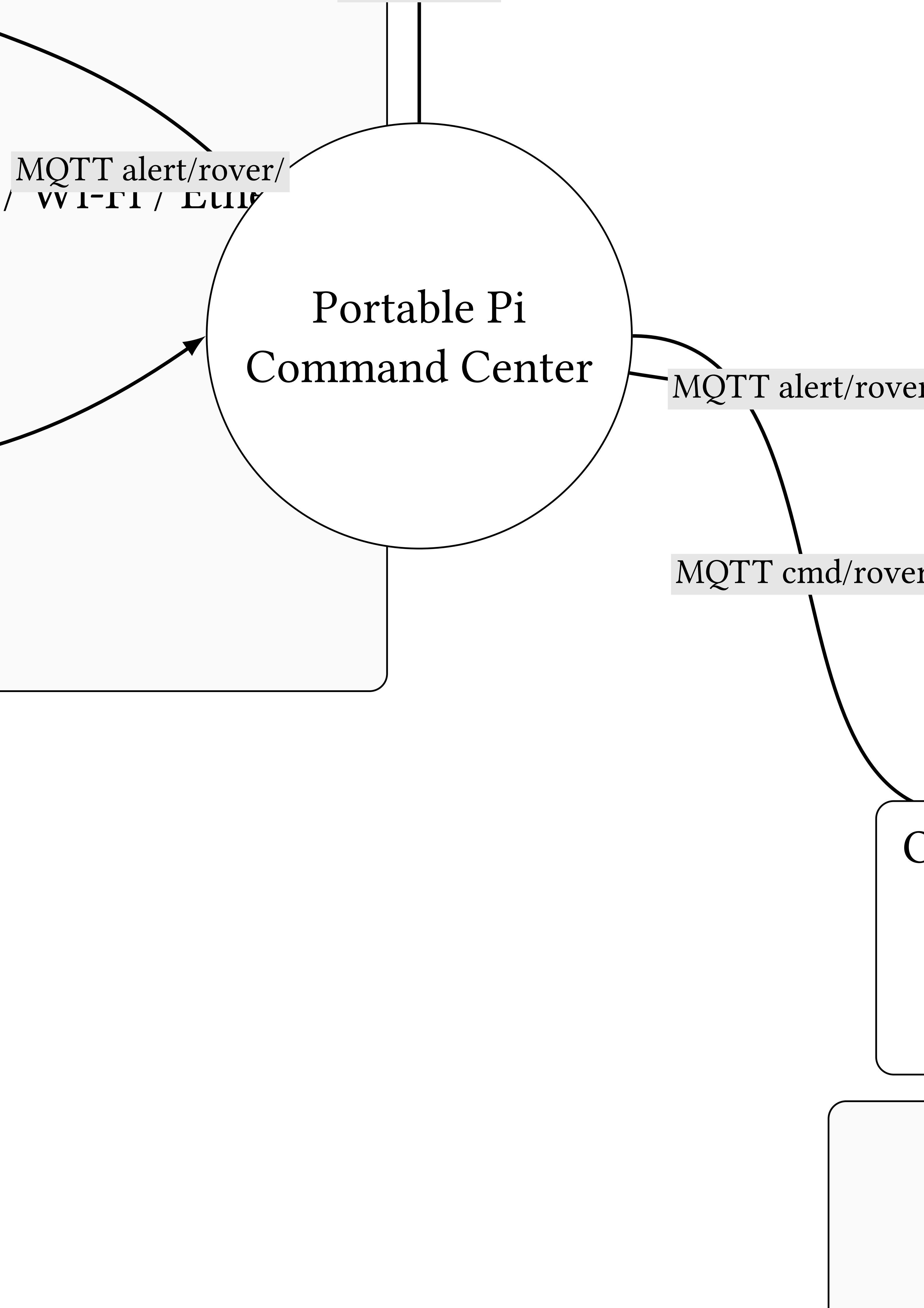


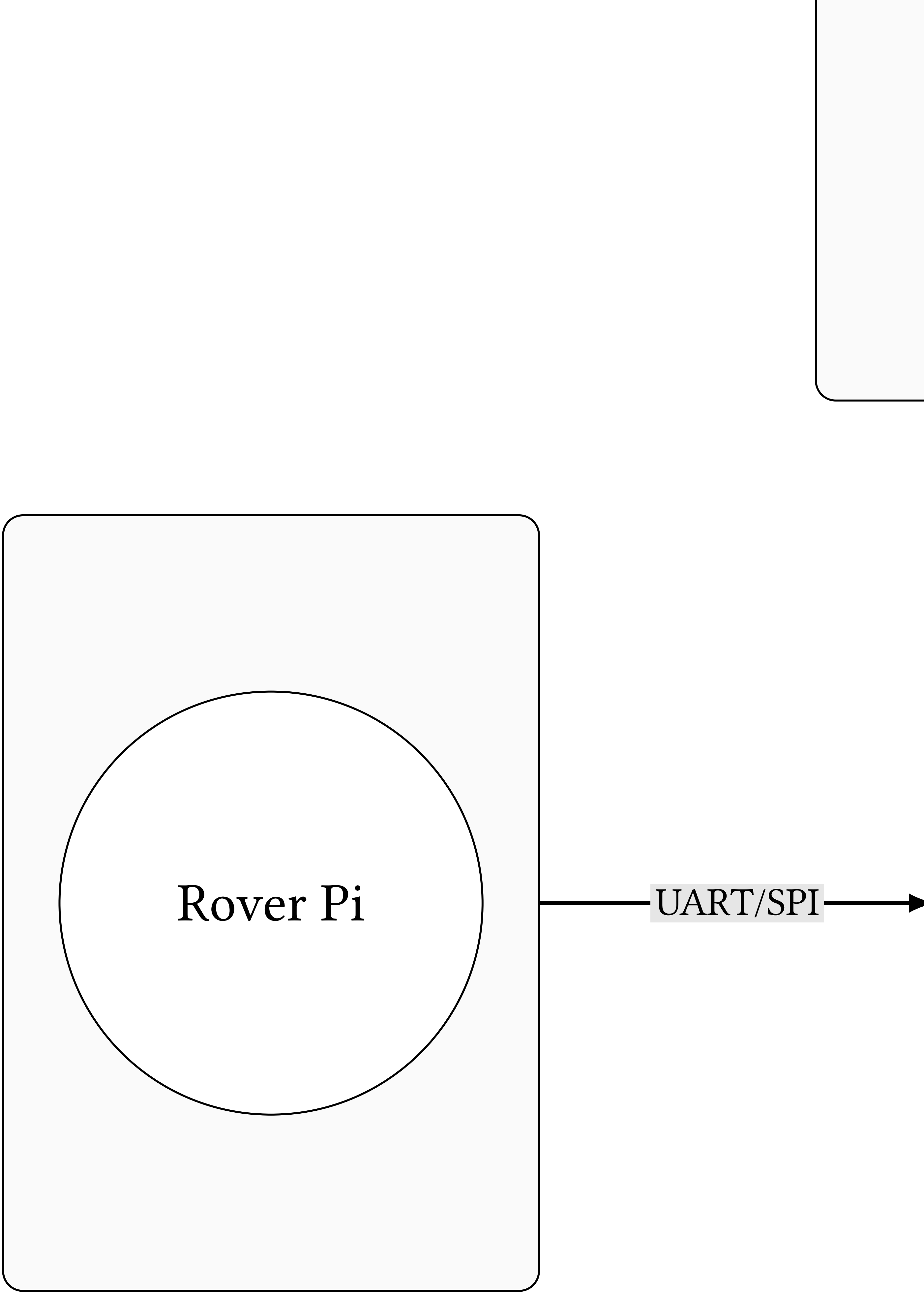
Jetson Orin Nano
• YOLO-v8 Detect
• Watermark + Sign


• Publishes alerts ⟶ mqtt
CSI Camera
IP
Raspberry Pi 5
• H.265 Encode
• RTSP Src
RTSP (720p)

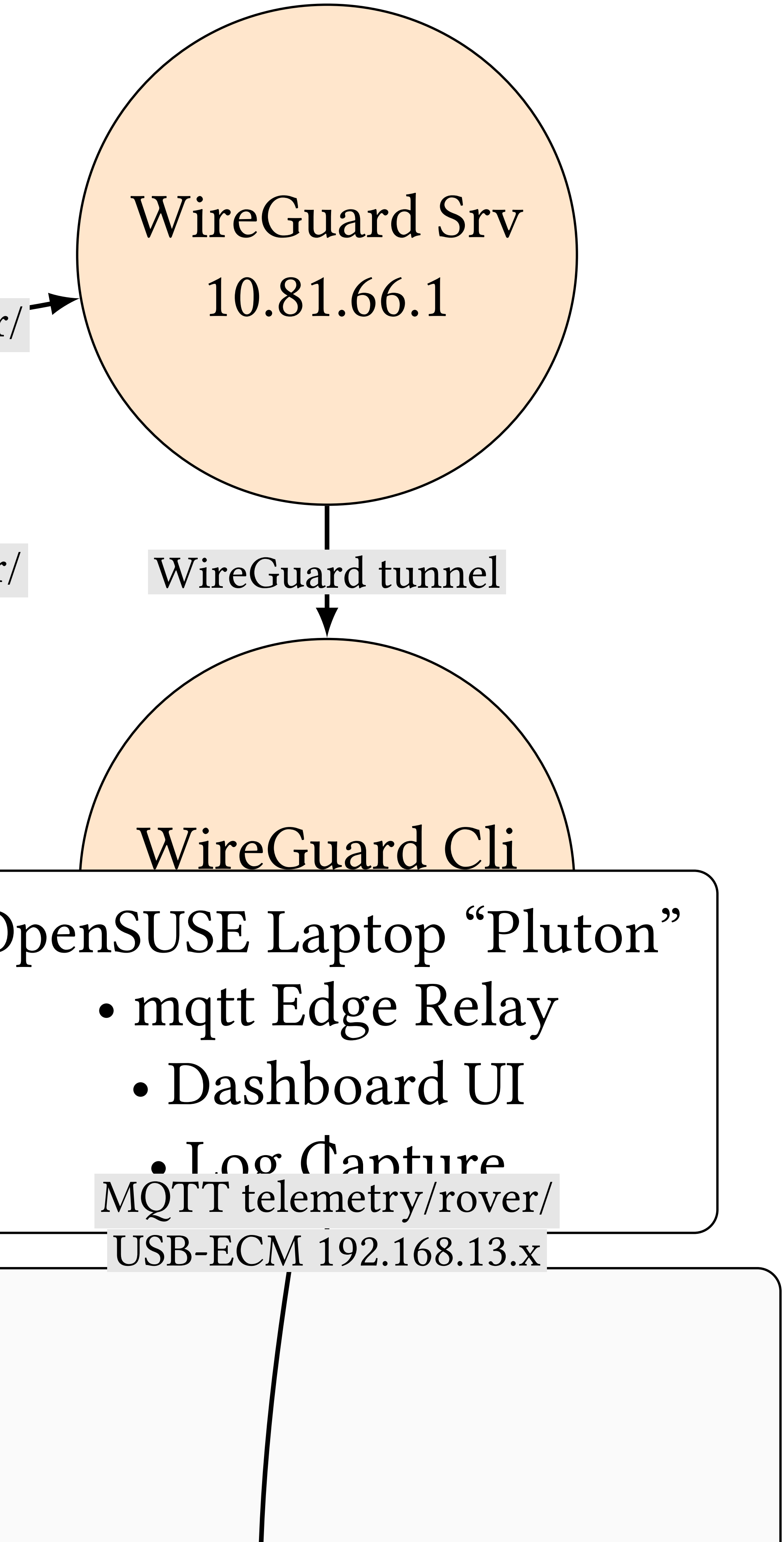


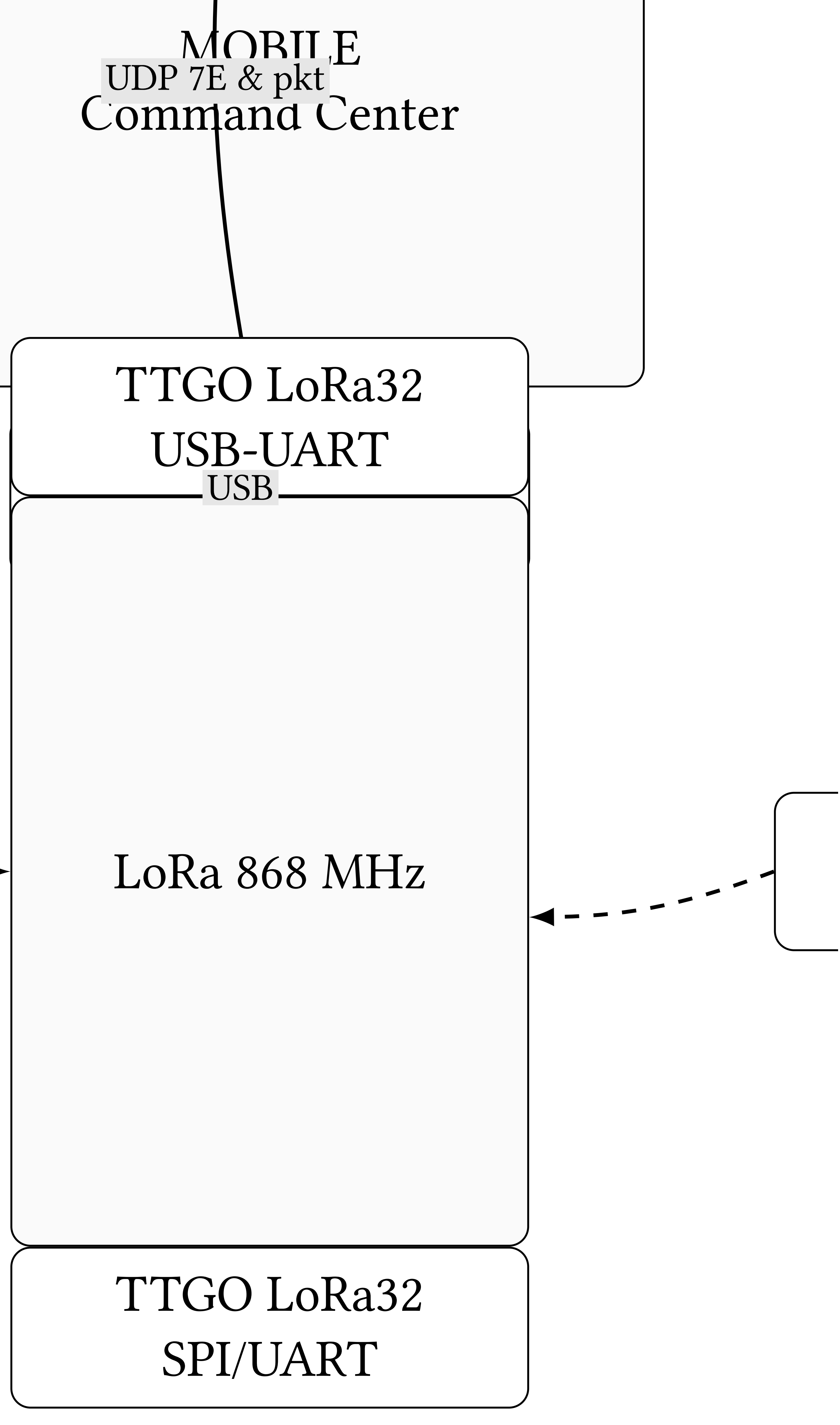
Home Pi
Central Server
VPN / SSH


MQTT alert/rover/
/ Wi-Fi / Ethe
Portable Pi
Command Center
MQTT alert/rover
MQTT cmd/rover
C


Rover Pi
UART/SPI

21


r/
WireGuard Srv
10.81.66.1
r/
WireGuard tunnel
WireGuard Cli
OpenSUSE Laptop “Pluton”
• mqtt Edge Relay
• Dashboard UI
• Log Capture
MQTT telemetry/rover/
USB-ECM 192.168.13.x


MOBILE
Command Center
UDP 7E & pkt
TTGO LoRa32
USB-UART
USB
LoRa 868 MHz
TTGO LoRa32
SPI/UART

22

IMPLEMENTATION

Chapter 4

Methodolog

This chapter outlines the
multi-layer watermark wit
performance.

4.1 Data Set

A corpus of 10 000 RGB im
2017 public data set, then c
Pi 5 rover camera resoluti
is 70/15/15 for train/valid
watermark dispersion stati

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

nages ($1920 \times 1080\,\text{px}$) was sampled from t
down-scaled to $1280 \times 720\,\text{px}$ to match the
ion. No further augmentation was applied
ation/test, each partition implicitly carryi
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
d; the split
ng unique

Peak Signal-to-N

PS

where $MAX = 25$

Structural Simi
nance–contrast–s

Latency. End-t
are logged with a

4.3 Robus

Each stego-image
every quality fact
is deemed satisfac
random carrier ma

Ta

4.4 Statist

For proportions su

$$CI_{95$$

with k successful

Noise Ratio (PSNR).

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

5 for 8-bit channels.

larity Index (SSIM). Computed with t
tructure triad.

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

stness Protocol

e undergoes JPEG compression at the ratio
or c we extract the payload and compute A
ctory if 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 scor

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

extractions in n trials and $z = 1.96$.

. *METHODOLOGY*

dB,

the standard lumi-

t_{capture}; timestamps
verification harness.

s in Table 4.1. For
CC(c). Robustness
use distinct pseudo-

eep

e interval:

$$z^2 \Big) ,$$

4.5 Visualisatio

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

on Pipeline

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

a Go script
ecutes the
oducibility;

26

CHAPTER 4.

. *METHODOLOGY*

Chapter 5

Experiment

This chapter reports the e
against the objectives stat
comprises the 10 000-imag
per-batch dispersion statis

It bears repeating that the
PDF: every page you are re
While the plots below focu
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 watermarkin
ed in Section 1.4. Unless otherwise noted, t
ge corpus described in Chapter 4 and interna
tics.

e *primary* artefact for the metadata layer is
eading is watermarked with zero-width Unic
s on the frequency-domain layer, the stealth
v. 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° and uniform scaling

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

$= 1 - \mathrm{BER}$ is measured for each transform. the frequency-domain watermark maintai actor 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

$\leq 10\,\%$;

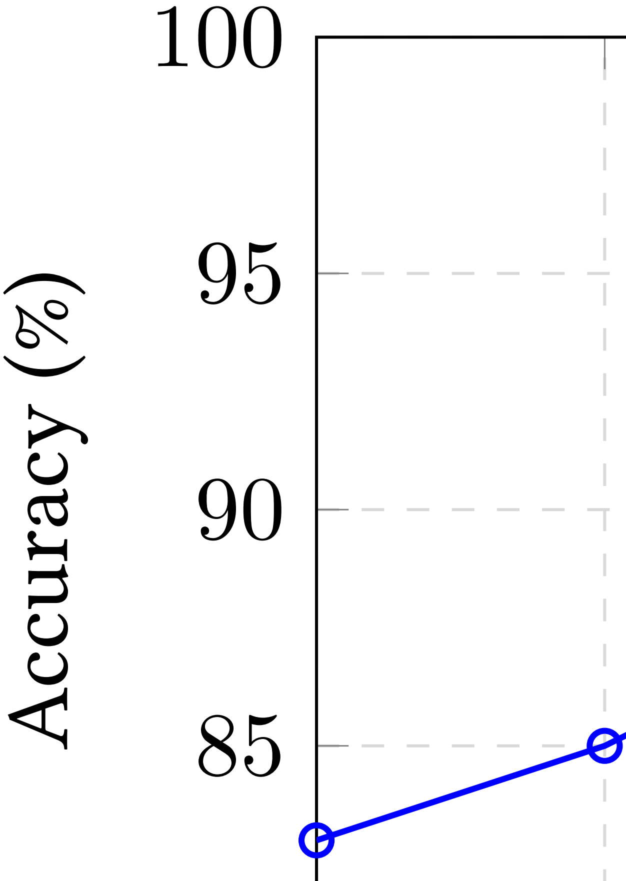
ortion pass

Figure 5.1

ns $\geq\ 95\%$

0%) ≥ 95 *%*”

or 20.


100
95
90
85
Accuracy (%)

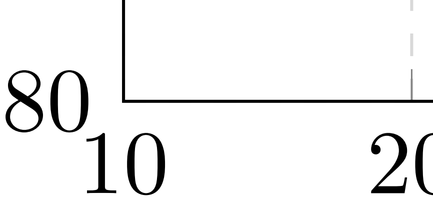


Figure 5.1:

5.2 Latenc

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

Key takeaway: Lat

5.3 Ancho

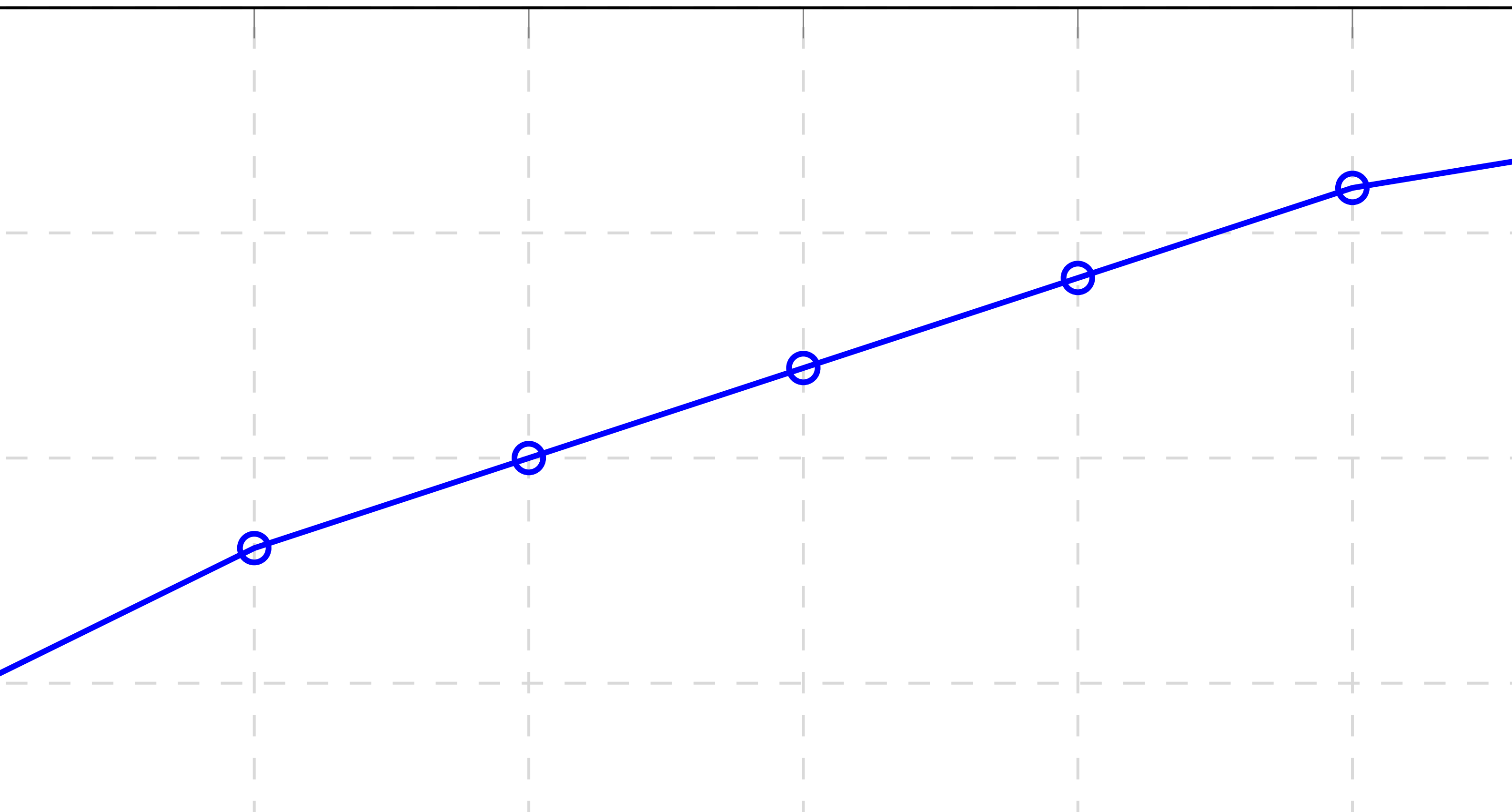
Per-batch on-cha

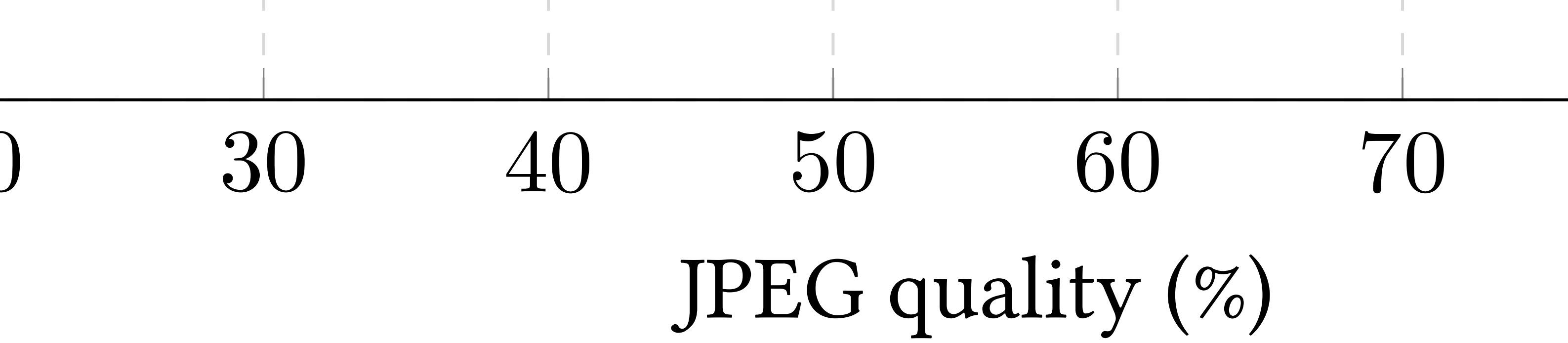
estimated sweet s
low.

Key takeaway: Ba

5.4 Payloa

Aggregate embed
marised below. *Ur*
after producing be





Extraction accuracy under varying JPEG co

cy

per frame is recorded as Latency $= t_{\text{extrac}}$ the median latency is $147 \pm 4\,\text{ms}$ (95 % CI), e timing harness injects a hidden tag into e

ency remains comfortably within real-time bu

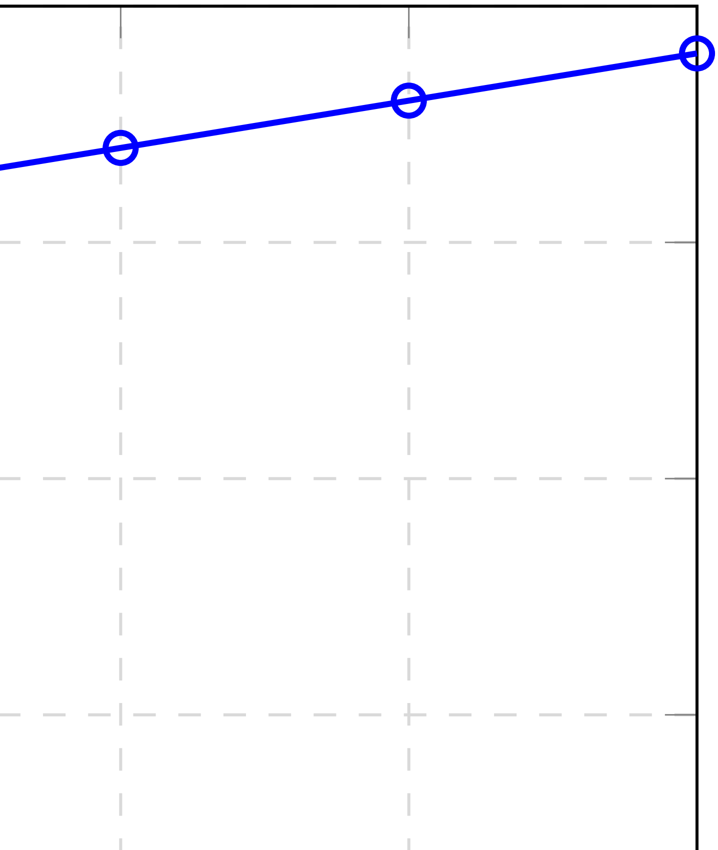
oring Cost

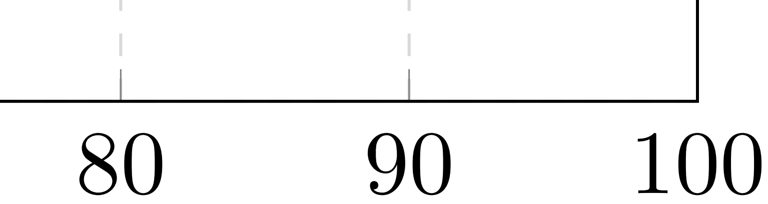
in anchoring fee is modelled as a function pot minimises marginal fee while keeping v

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

ad Capacity and Recovery

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





ompression.

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

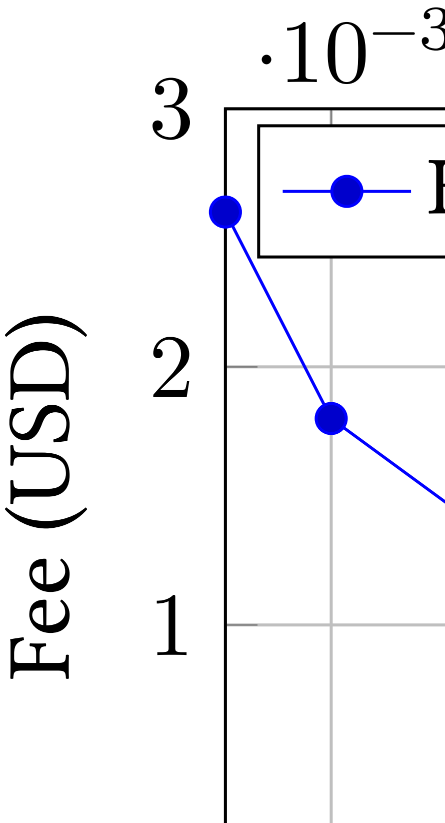
dget on both devices.

of batch size. The

verification latency

rmation delay.

mark run) is sum-
(run ‘make analyze‘


$\cdot 10^{-3}$
3
2
1
Fee (USD)
F

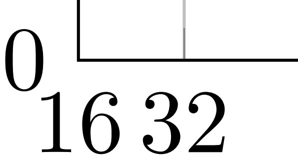


Figure 5.2: Digest anchori
0xABC123..789. Placehold

5.5 Summary

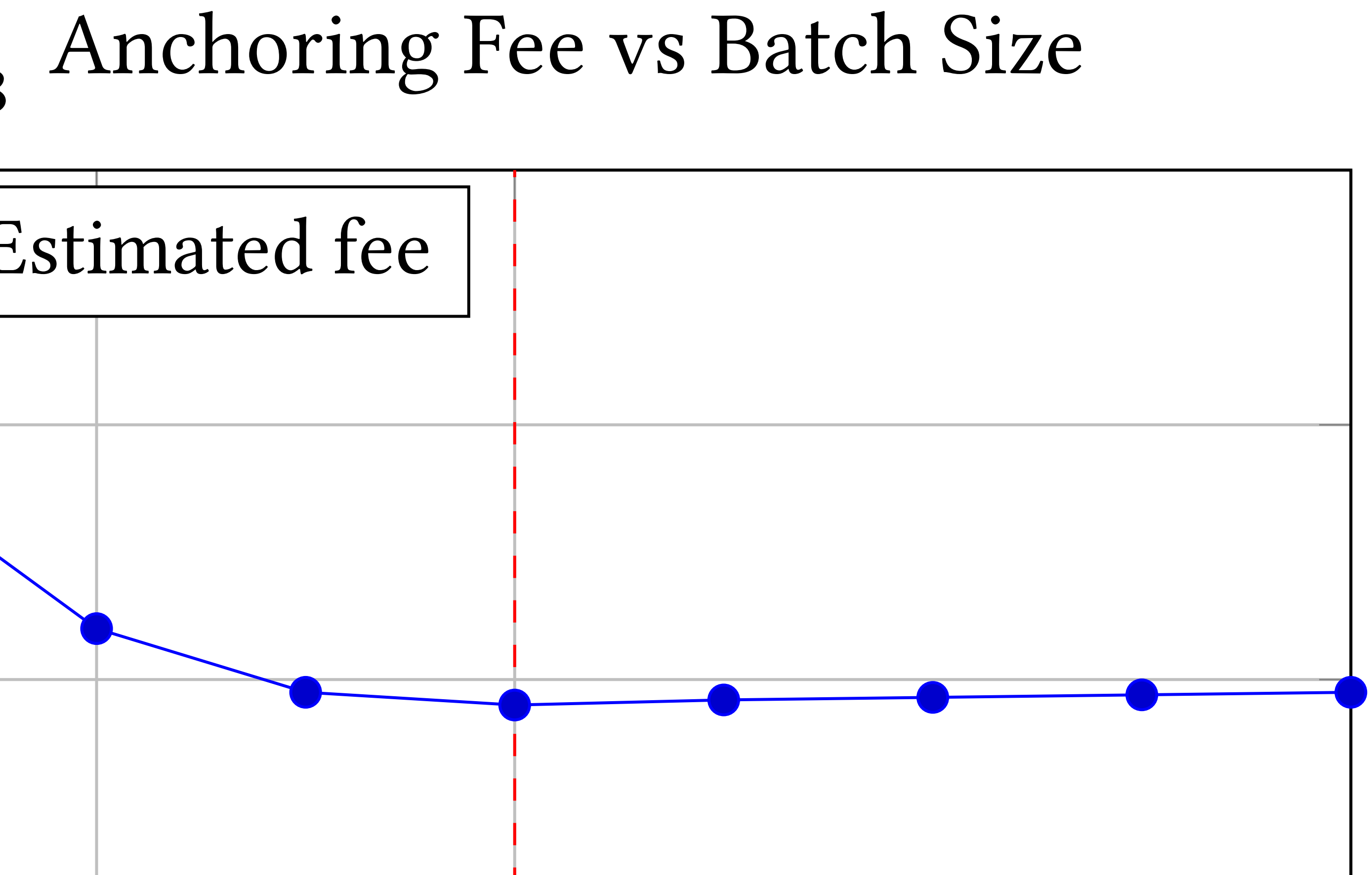
The proposed tri-layer wat

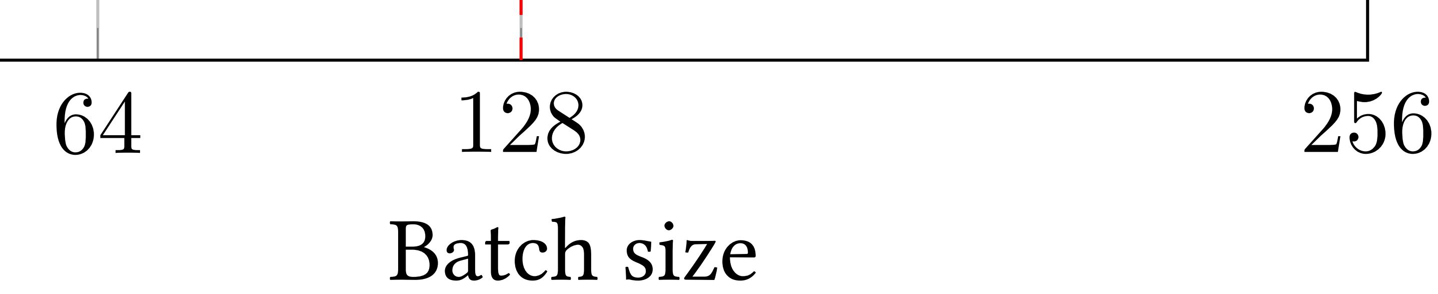
- Imperceptibility: me
- Robustness: ACC $\geq$
- Real-time: 147 ms m

Consequently the design s
maining variations (croppi
this paragraph deliberatel

Reproducibility. Run:

`hash>` to replicate benchm


Anchoring Fee vs Batch Size
Estimated fee



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

termark meets all quantitative objectives:

ean PSNR $= 42.6\,\text{dB}$ and SSIM $= 0.984$.

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

nedian 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
```

arks.

29

. Contract:

%.

pter 2. Re-
ture work;

t <short-

30

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
manda
cality,

Legacy code Existin
mentec
via gRI

& Skills

Context

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

vatermark pipeline

t

tion

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

Challenges

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

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

a 24-week

week sprint
ly encodes

Orin Nano
nemory lo-

rsely docu-
eroperated

Data throughpu

6.3 Profes

Regulatory

Stakeholder alig

Knowledge tran

6.4 Skill D

- Deepened e
brids) and li

- Gained prof

harnesses, r

- Practised ag
code review

6.5 Reflec

The dual academic
ing pragmatism. F
enforced relevance
exhaustive transf

t 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.

ssional Challenges

Test datasets filtered for GDPR complian vacy policy (face blurring, location scru bedding.

gnment Balancing academic experimentati driven Scrum required concise weekly de criteria, and traceable decisions.

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

Development

expertise in frequency-domain steganograpl ightweight CUDA acceleration patterns.

ficiency profiling mixed Python/C++ pipelin memory bandwidth counters).

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

tion

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

LLENGES & SKILLS

N-induced $\approx 80\,\mathrm{ms}$
xtraction pipelines
tigation paragraph

ce and internal pri-
ubbing) before em-

ion with milestone-
emos, clear rollback

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

hy (DWT–SVD hy-

es (`nvprof`, timing

uctured cross-team
n.

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

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

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

ture secure
additional

34

LLENGES & SKILLS

Chapter 7

Conclusion

Key takeaways

This thesis introduced **Pro** work that spans the full sta anchoring and field-level v tions:

1. **Tri-layer waterma** DWT–SVD frequen ceptibility (PSNR = and auditability.

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

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

These results collectively s
is robust, lightweight, and

and Future Work

ject Sunflower, a *self-documenting* waterm
ack from frequency-domain embedding to bl
verification. The work delivered three mai

ark design. A hybrid of zero-width Unico
cy embedding, and on-chain digests achiev
42.6 dB), robustness (ACC $\geq$ 95% at JPE

nce implementation. The end-to-end pip
power hardware (Raspberry Pi 5 and Jetson C
± 4 ms) and integrates with ROS and Wire

ooling. A `Makefile`-driven build guards d
es its own invisible metadata and ships with a
ot, enabling tamper-evident distribution.

atisfy the objectives laid out in Section 1.4: t
independently verifiable.

ark frame-
lock-chain
n contribu-

ode marks,
ves imper-
G QF = 70)

peline runs

Orin Nano;

eGuard for

lata prove-

an external

the system

Limitations

- **Adversaria**
attacks wer

- **Video strea**
frames; thro

- **Informal s**
formal proo

Future rese

Adversarial robu
mix anc

Video-rate pipel
VDEC s

Formal proofs *N*
channel
attacks.

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

systems.

s

al coverage. Only compression, geometric,
e tested; cropping and combined attacks re

am optimisation. The current implementa
oughput is bounded by per-frame I/O.

security model. While the scheme is *pra*
of of indistinguishability is still missing.

arch

ustness Extend the benchmark suite with c
d gradient-based attacks; evaluate defensive

ine Fuse watermark embedding with the J
stack and exploit Tensor-RT for sub-50 ms l

Model the frequency-domain embedder as
l and derive security bounds under adaptive
.

Sunflower demonstrates that rigorous watern
ints and open-science ideals. By releasing
the work invites others to replicate, critiq
king one small step toward trustworthy, sel

ND FUTURE WORK

and additive-noise
main unexplored.

ation processes still

ctically resilient, a

ropping, frequency-
e fine-tuning.

Jetson'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 Tra

DWT Discrete Wavelet T
images into frequen
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
cy 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
munication 31

age Authentication Code 7, 14, 16

10

Experts Group (image compression) iii, 1, 2

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

37

te platform

composing

bedding in

protection

for inter-

2, 7–11, 14,

g rover-to-

LSB Least Signifi

MQTT Message
messaging
components

Payload Secret c
typically cr

12, 16

PSNR Peak Signa

RaspClaws Phys
leg) providi

RF Radio Frequen

RPI5 Single-boar
processing

Scrum Agile fram

Steganographic
ume), imper
watermarki

SVD Singular Val

VPN Encrypted
field gatewa

cant Bit viii, 8, 9, 14

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

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

al-to-Noise Ratio 11

sical hexapod robot platform: six legs, 18 s
ng 3 DOF articulation per limb 17, 18

ncy 20

rd computer on RaspClaws for locomotion, s
13, 18

nework for iterative, incremental product d

Triangle Fundamental trade-off between
rceptibility (visual quality), and robustness (a
ng schemes 8

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

WireGuard tunnel providing secure comm
ay and Home HQ over public infrastructure

t publish-subscribe
ge between system

(denoted P); here
nance information

ervo motors (3 per

sensing, and vision

evelopment 32

capacity (data vol-
ttack resistance) in

unication between
3, 17, 18, 21, 32

Bibliograph

[1] Ministère de l'Équipem
2024-10-27. 2024. URL:
`Organisation/Page`

[2] J. Smith, A. Kumar, a
Survey of Detection
(2023), pp. 101–128.

[3] A. Doe, M. Fernández
paigns in the Wild: Ta
International Confere

[4] Direction des Systèm
Pilot Plan. Internal pi
2025.

[5] Ingemar J. Cox et al.
dia". In: *IEEE Transac*
DOI: `10.1109/83.65`

[6] A. Kumar, R. Singh, an
ing Scheme Using DV

matics Visualization 1

[7] Chi-Chun Chan and
LSB Substitution". In
1016/j.patcog.200

[8] J. Zhang, W. Chen, an
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/Gouv
es/Missions-de-la-DSI.aspx.

and L. Zhao. "Deepfakes and the Erosion o
and Mitigation". In: *Journal of Digital For*

z, and T. Nguyen. "Coordinated Misinforma
axonomy and Countermeasures". In: *Proceed*
nce on Web and Social Media. 2024.

nes d'Information. *Agricultural Field Data*
ilot planning document. Marrakesh regiona

"Secure Spread Spectrum Watermarking fo
ctions on Image Processing 6.12 (1997), pp. 1
0120.

nd P. Sharma. "A Robust and Secure Image W
WT–SVD and Chaos". In: *International Journ*

15.4 (2024), pp. 3596–3605.

Ling-Ming Cheng. “Hiding Data in Images
: *Pattern Recognition* 37.3 (2004), pp. 469–47
03.08.007.

nd N. Yu. “A Robust and Imperceptible Deep
Scheme”. In: *IEEE Transactions on Circuits a*
31.7 (2020), pp. 2845–2858. DOI: 10.1109/TC

chain for IoT Security and Privacy: The Cas
Proc. IEEE PerCom Workshops. 2017, pp. 618
2017.7917634.

. Accessed:
vernance/

of Trust: A
ensics 12.3

ation Cam-
dings of the

Collection
al test site.

r Multime-
1673–1687.

Watermark-
al on Infor-

by Simple
74. DOI: 10.

Learning-
nd Systems
SVT.2020.

se Study of
3–623. DOI:

40

BIBLIOGRAPHY

Discrete Wa
Refresher

Refresher

This appendix gives a com
Discrete Wavelet Transfor

1-D filter bank view. A
analysis via low–pass $h[n]$
by 2. For a 1-D signal $x[n]$

$$a_k = \sum_{n} x[n$$

Synthesis inverts this with

2-D extension. Applyi
columns yields four equal
detail), HL (horizontal deta
for our embedding; deeper

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

pact 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

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

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 i
levels increase latency and reduce spatial lo

levels increase latency and reduce spatial lo

onale. Natural images concentrate most w
selected singular values of wavelet-block c
ing on robustness/imperceptibility trade) all
moderate compression while staying belo

eger coefficients (fast on edge devices) and no
re elaborate biorthogonal wavelets (e.g. D
nperceptibility but raise compute cost.

-level) 2-D
x layer.

mplements
–sampling
are

esis filters.

rows then
H (vertical
is required
ocalisation

ocalisation.

variance in
oefficients
lows small
ow human

o boundary
aubechies

Reference Figur
mark selects bloc

1-Lev

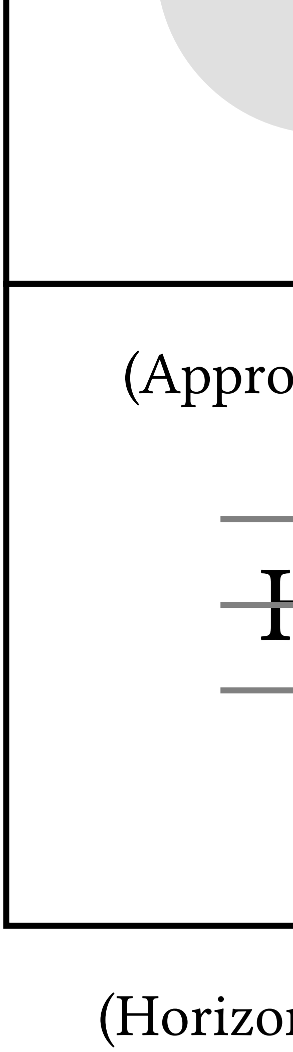
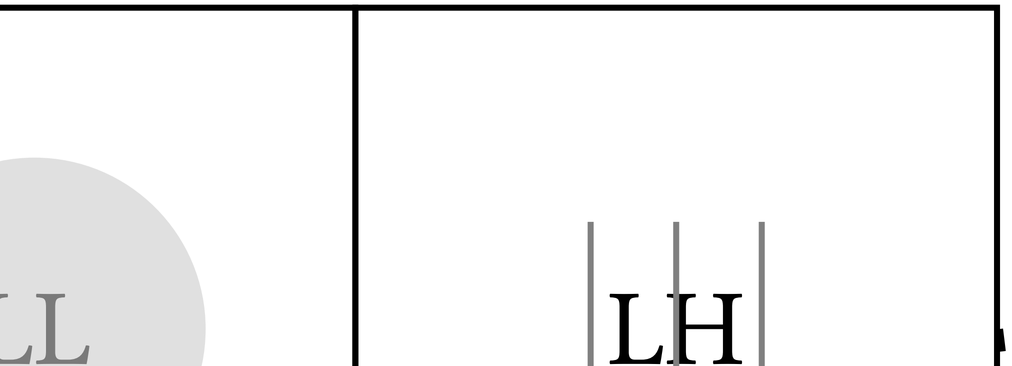


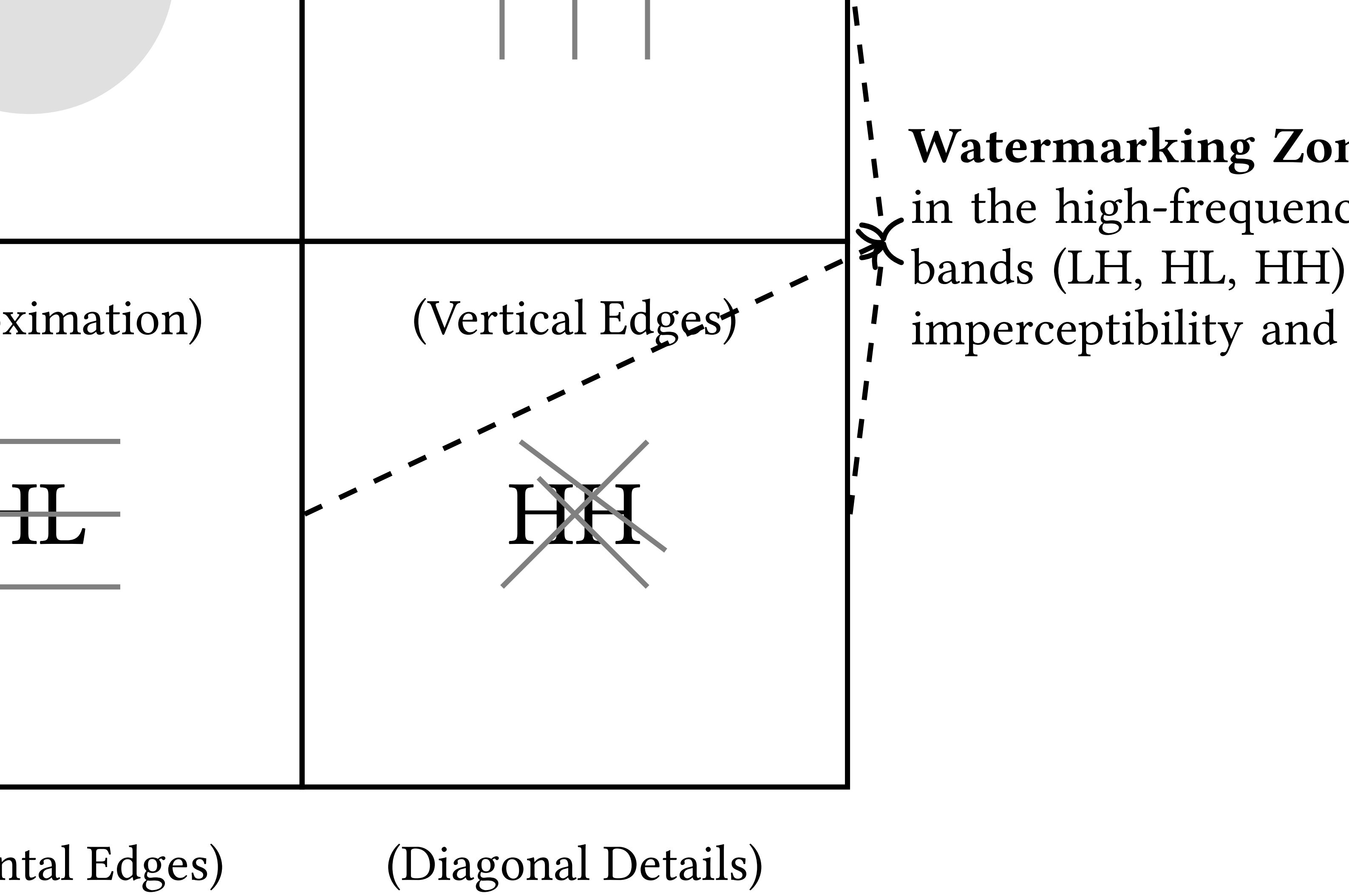
Figure 1:

Relation to Sect
SVD is applied af
transform underly

e. Figure 1 sketches the band layout (singl 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) assur
ter the DWT on a chosen band; this apper
ving that step.

e level). The water-

ne: Embed
cy detail
to balance
robustness.

, HL, HH).

nes the block-wise
ndix formalises the

Supplement

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

Robustness Curv

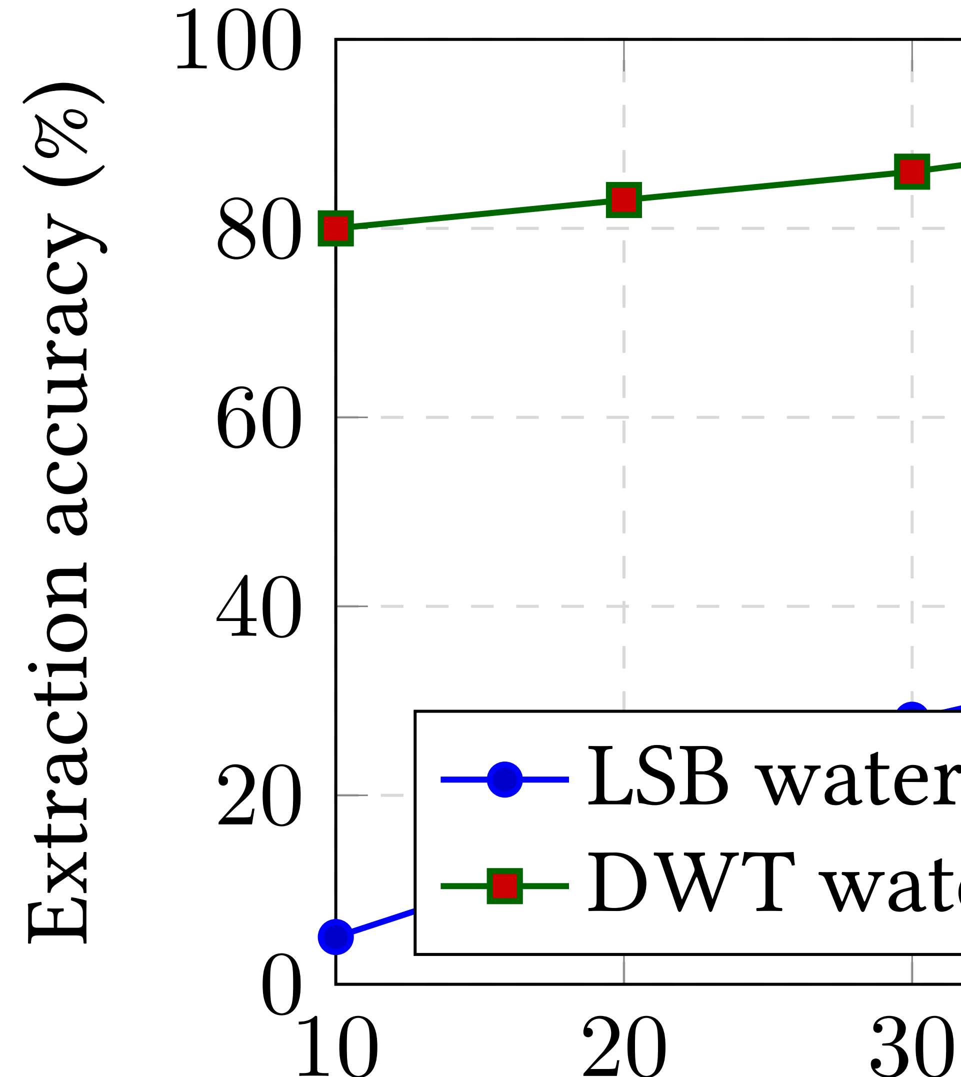


Figure 2: Extracti

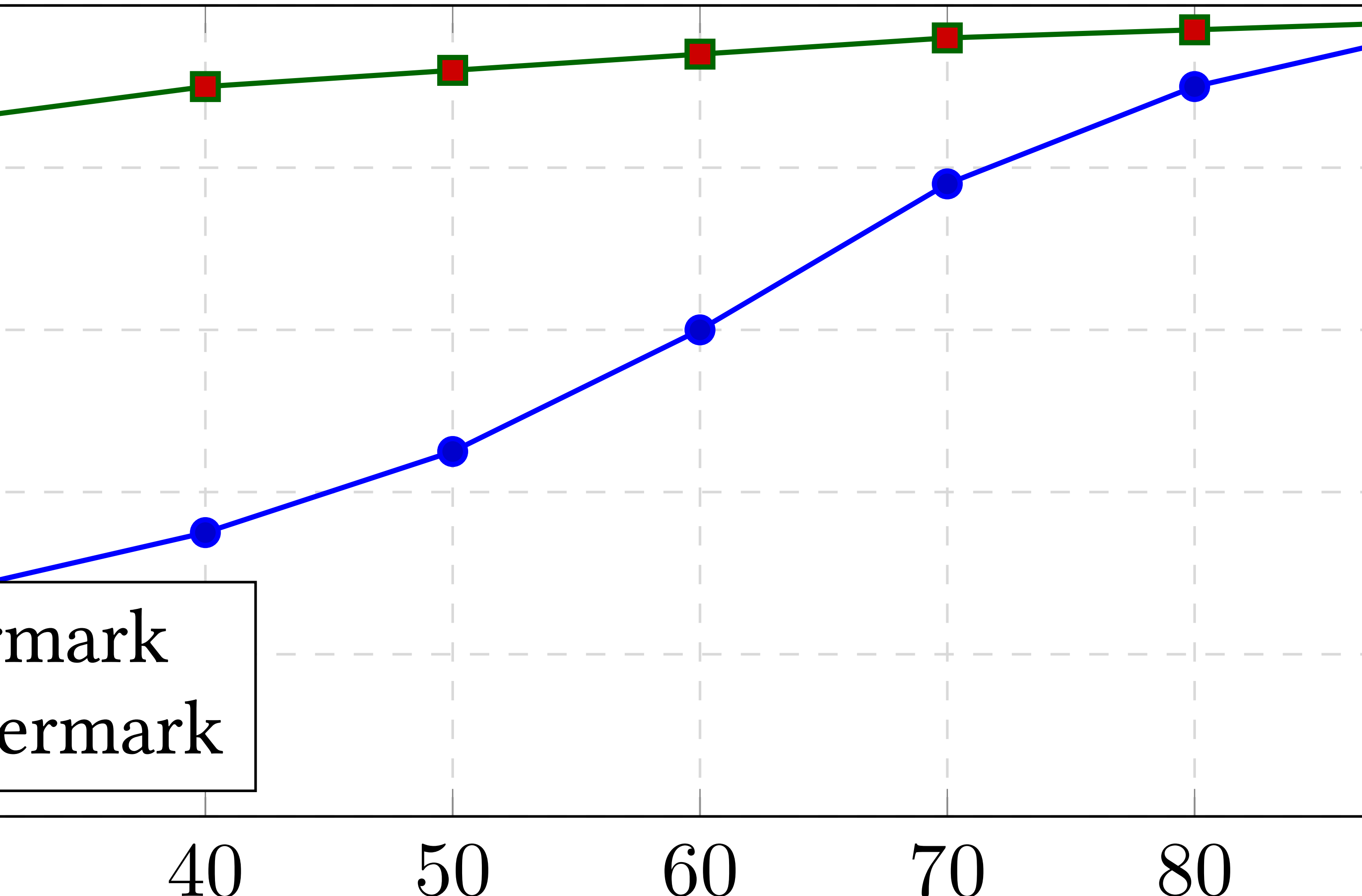
Latency Distribu

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 po

ves



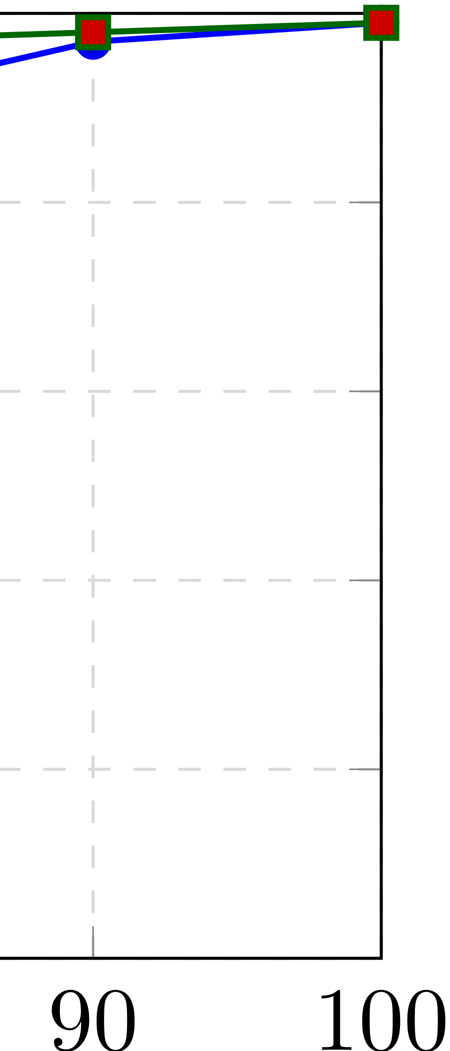
JPEG quality (%)

on accuracy vs JPEG quality (representative

ation

/ anchoring cost breakdown (auto-generated

cost figures
producible
ssible.



e).

d).

44

Summary T

Reproduction.

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

All plot inputs res

provenance hashe

Table

Invoke:

```
enerates metrics + figures
eds refreshed assets
```

ide under `toolset/` and `results/` subtree es for audit.

EMENTARY PLOTS

s; git history tracks

Verification

n Scripts

45

I

Total n

Victory Lap

Invisible-Watermark Disclosur

marks embedded: 26

Thank you for reading. Happy verifying!

re