JURNAL ELTEK
Vol. 24, No. 2, Oktober 2026, hal. 155~165
p-ISSN: 1693 – 4024 | e-ISSN: 2355-0740
DOI: 10.33795/eltek.v24i2.10869

Semi-fragile watermarking berbasis DWT-Haar pada *gateway* IoT ESP32 untuk verifikasi integritas data detak jantung

Syauqii Usaiyyah Kristanto[1], Rahmawati Hasanah[2], Teguh Ginanjar[3]
e-mail: syauqii.usaiyyah.tkom23@polban.ac.id, rahmawati@polban.ac.id, teguh.ginanjar@polban.ac.id
[1,2,3]Jurusan Teknik Elektro, Politeknik Negeri Bandung, Indonesia

Informasi Artikel

Riwayat Artikel
Diterima 3 Agustus 2026
Direvisi 8 Oktober 2026
Diterbitkan 30 Oktober 2026

Kata kunci:

ESP32
gateway IoT
integritas data
semi-fragile watermarking
transformasi wavelet diskrit

ABSTRAK

Perangkat *wearable* mengirimkan data detak jantung melalui kanal nirkabel yang tidak menyediakan jaminan bahwa nilai yang diterima sama dengan nilai yang dikirim. Perlindungan kriptografis konvensional sulit diterapkan pada *gateway* bersumber daya terbatas. Skema *fragile watermarking* juga tidak sesuai karena menolak setiap perubahan, termasuk kompresi yang sebenarnya tidak berbahaya. Penelitian ini mengimplementasikan mekanisme *semi-fragile watermarking* pada *gateway* tertanam untuk memverifikasi integritas data detak jantung. Setiap blok berisi 16 sampel data detak jantung yang didekomposisi menggunakan transformasi wavelet Haar tingkat satu. *Watermark* dibangkitkan dari koefisien aproksimasi melalui fungsi *hash* kriptografis, lalu disisipkan ke koefisien detail melalui modulasi indeks kuantisasi. Sistem divalidasi secara menyeluruh menggunakan *smartwatch* komersial berbasis sensor fotopletismografi (PPG) dengan antarmuka BLE yang diuji pada 8 subjek dalam 16 sesi. Sebanyak 247 blok yang terkumpul dievaluasi melalui 16 skenario ketahanan. Ekstraksi *watermark* berlangsung tanpa kesalahan pada kondisi transmisi normal. Kualitas sinyal rata-rata mencapai 41,59 desibel, akurasi deteksi manipulasi mencapai 96,1 persen, dan waktu komputasi rata-rata 87,16 milidetik per blok. Hasil tersebut menegaskan bahwa verifikasi integritas yang ringan layak dijalankan pada *gateway* tertanam berbiaya rendah tanpa perangkat keras kriptografis khusus.

Keywords:

ESP32
IoT gateway
data integrity
semi-fragile watermarking
discrete wavelet transform

ABSTRACT

Wearable devices transmit heart rate data across wireless channels that offer no inherent guarantee that the values received match those that were sent. Conventional cryptographic protection is hard to deploy on resource-constrained gateway hardware. Fragile protection is unsuitable as well, because it rejects every modification, including harmless compression. This study implements a semi-fragile watermarking mechanism on an embedded gateway to verify heart rate data integrity. Each block of 16 samples of heart rate data is decomposed by a first-level Haar wavelet transform. A watermark is then derived from the approximation coefficients through a cryptographic hash function and embedded into the detail coefficients by quantization index modulation. The system was validated end to end on a commercial smartwatch with a photoplethysmography (PPG) sensor over BLE test by 8 subjects across 16 sessions. The resulting 247 blocks were evaluated under 16 robustness scenarios. Watermark extraction was error free under normal transmission. Average signal quality reached 41.59 decibels, tamper detection accuracy reached 96.1 percent, and computation averaged 87.16 milliseconds per block. These results confirm that lightweight integrity verification is feasible on low-cost embedded gateways without dedicated cryptographic hardware.

Penulis Korespondensi:
Rahmawati Hasanah,
Program Studi Teknik Telekomunikasi, Jurusan Teknik Elektro,
Politeknik Negeri Bandung,
Jl. Gegerkalong Hilir, Ciwaruga, Bandung Barat, Jawa Barat, Indonesia.
Email: rahmawati@polban.ac.id

1. PENDAHULUAN

Pemantauan tanda vital secara berkelanjutan telah bergeser dari ruang klinik ke perangkat yang dikenakan pengguna sehari-hari. Sejumlah penelitian di Indonesia telah membangun sistem pemantauan detak jantung berbasis IoT yang mengalirkan pembacaan sensor ke *server* secara otomatis [1], [2], termasuk untuk deteksi dini kondisi fisiologis tertentu [3]. Arah ini menempatkan *gateway* sebagai simpul yang menjembatani perangkat *wearable* dengan sistem pemantauan jarak jauh, sekaligus titik paling strategis untuk menegakkan jaminan mutu data sebelum dipakai mengambil keputusan klinis. Perangkat *wearable* yang menjadi objek penelitian ini adalah *smartwatch* komersial yang mengukur detak jantung melalui sensor fotopletismografi (PPG) dan mengirim satu nilai denyut per notifikasi *Bluetooth Low Energy* (BLE). Data ringkas semacam ini rentan diubah tanpa terdeteksi karena tidak membawa informasi redundan untuk pemeriksaan silang. Semi-fragile *watermarking* menjawab kebutuhan itu dengan menyisipkan *watermark* tervalidasi langsung ke nilai sinyal: *watermark* tetap bertahan terhadap perubahan ringan yang wajar seperti kompresi, tetapi rusak ketika nilai dimanipulasi. Karena ringan, penyisipan dan verifikasi ini dapat berjalan di *gateway* ESP32, tepat pada titik data pertama kali memasuki jaringan.

Persoalannya, jalur nirkabel tidak menjamin nilai yang diterima identik dengan yang dikirim. Perubahan bisa terjadi tak sengaja akibat gangguan kanal, maupun sengaja melalui serangan *Man-in-the-Middle* [4], [5]. Pada data medis, pergeseran nilai yang tak terdeteksi dapat menggiring interpretasi keliru atas kondisi pasien. Perlindungan kriptografis konvensional menjawab kebutuhan ini, tetapi penerapannya pada *gateway* mikrokontroler terkendala keterbatasan daya komputasi dan energi [5]. Selain itu, pemantauan berkelanjutan menghasilkan data besar sehingga kompresi kerap diterapkan, dan kondisi ini menyulitkan *fragile watermarking* yang menandai setiap perubahan sekecil apa pun sebagai pelanggaran.

Pendekatan *semi-fragile watermarking* menengahi dua tuntutan berlawanan: toleran terhadap modifikasi ringan namun peka terhadap perubahan yang melampaui ambang. Sebagian besar penelitian pada arah ini masih berpusat pada citra dua dimensi: kombinasi wavelet dan dekomposisi nilai singular yang tahan serangan geometris [6], enkripsi berbasis kekacauan (*chaotic*) dengan *compressive sensing* untuk keamanan dan kapasitas penyisipan [7], transformasi contourlet yang tahan pemotongan pada IoT [8], penyisipan berbasis kuantisasi DCT untuk lokalisasi manipulasi [9], hingga wavelet bilangan bulat berkuantisasi yang mendeteksi sekaligus memulihkan bagian citra [10]. Untuk sinyal biomedis satu dimensi, *watermark* pada elektrokardiogram diteliti memakai model pembelajaran mendalam sebagai pembangkit [11]. Pada sinyal tercuplik umum, skema rapuh berbasis kode autentikasi pesan melindungi integritas per blok [12] dan diperluas ke audio [13], sedangkan pemodelan statistik berbasis distribusi eksponensial teritlak (*generalized linear exponential*) dikaji pada [14].

Dari rangkaian karya tersebut terbaca satu kesenjangan. Skema *semi-fragile* untuk sinyal biomedis satu dimensi umumnya dievaluasi lewat simulasi komputer, bukan dijalankan langsung di perangkat tertanam yang benar-benar terbatas sumber dayanya, padahal di *gateway* itulah verifikasi paling bermakna karena dilakukan sedekat mungkin dengan sumber data. Penelitian skema integritas ringan untuk IoT umumnya berhenti di lapisan *cloud* dan mengandalkan *server semi-trusted* sebagai pemverifikasi [15]. Di sisi perangkat keras, ESP32 terbukti sanggup menjadi *gateway* rumah cerdas [16], tetapi kemampuannya menanggung beban kriptografi dan transformasi sinyal sekaligus untuk verifikasi integritas belum banyak dikarakterisasi secara kuantitatif. Dibandingkan karya-karya itu, pendekatan yang diusulkan berbeda pada tiga hal yang saling menguatkan: domain sinyal biomedis satu dimensi waktu-nyata (bukan citra [6], [8]-[10]), seluruh rantai penyisipan dieksekusi langsung di ESP32 (bukan disimulasikan [9]-[12]), dan verifikasi di sisi tepi dekat sumber data (bukan server *cloud semi-trusted* [15]).

Penelitian ini mengisi kesenjangan tersebut melalui empat kontribusi. Pertama, seluruh rantai pemrosesan (transformasi wavelet Haar level satu, pembangkitan *watermark* dengan hash kriptografis SHA-256, dan penyisipan melalui *Quantization Index Modulation*, QIM) diimplementasikan dan dieksekusi langsung di ESP32. Kedua, sistem divalidasi menyeluruh dari akuisisi melalui *Bluetooth Low Energy* (BLE) hingga verifikasi di *dashboard* melalui MQTT, memakai data detak jantung dari 8 subjek yang mewakili 4 kategori usia dalam dua kondisi aktivitas. Ketiga, evaluasi ketahanan disusun ke dalam 16 skenario yang membedakan gangguan wajar dari manipulasi disengaja melalui 3 kelompok target, sehingga sifat *semi-fragile* diuji sebagai dua tuntutan terpisah. Keempat, komposisi latensi diurai per komponen untuk menetapkan beban komputasi *watermarking* secara kuantitatif.

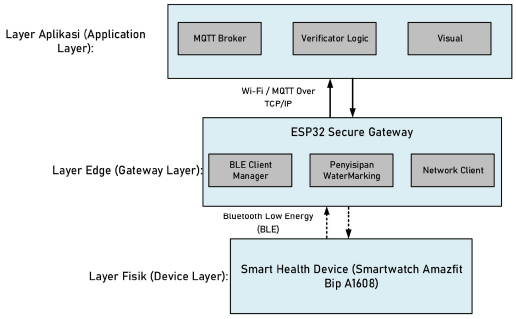
Tujuan yang hendak dicapai adalah merancang dan mengimplementasikan *gateway* IoT berbasis ESP32 yang memadukan akuisisi data dari perangkat *wearable* dengan mekanisme verifikasi integritas berbasis *semi-fragile watermarking*, mewujudkan algoritma penyisipan dan verifikasi tersebut pada mikrokontroler dengan sumber daya terbatas, serta mengevaluasi kinerjanya melalui parameter *Bit Error Rate*

(BER), *Peak Signal-to-Noise Ratio* (PSNR), dan *Mean Square Error* (MSE) pada kondisi transmisi normal, kompresi data, gangguan kanal, dan serangan manipulasi data.

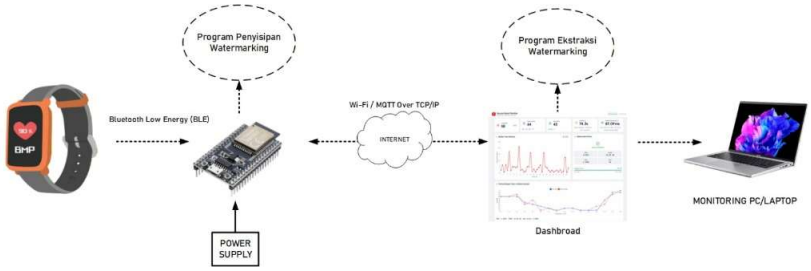
2. METODE PENELITIAN

2.1 Arsitektur sistem

Sistem dibangun sebagai tiga lapisan terintegrasi yang bekerja sekuensial dari sumber sinyal hingga titik verifikasi, sebagaimana ditunjukkan pada Gambar 1. *Device layer* diwakili *smartwatch* komersial Amazfit Bip A1608 yang membaca detak jantung melalui sensor fotopletismografi dan memaparkan data melalui *Heart Rate Service* dengan UUID 0x180D serta *Heart Rate Measurement Characteristic* dengan UUID 0x2A37, mengikuti profil standar *Bluetooth Low Energy (*BLE*)* [17]. Pada *edge layer,* dijalankan mikrokontroler ESP32 bermodul ESP-WROOM-32 dengan prosesor dua inti Xtensa LX6 berkecepatan 240 MHz, SRAM 520 kB, dan flash 4 MB, yang menerima data detak jantung dari *smartwatch* melalui BLE, serta mengeksekusi program penyisipan watermark lalu meneruskan hasilnya ke jaringan MQTT. *Application layer* berupa *dashboard* web yang terhubung ke broker EMQX melalui MQTT di atas WebSocket pada porta 8084 [18] dan menjalankan verifikasi integritas secara mandiri. Penempatan penyisipan pada *edge layer* menyempitkan rentang jalur yang belum terlindungi hanya sampai tautan BLE antara *smartwatch* dan *gateway*. Adapun ilustrasi sistem ditunjukkan pada Gambar 2.



Gambar 1. Arsitektur sistem *secure* IoT *gateway* tiga lapisan



Gambar 2. Ilustrasi sistem

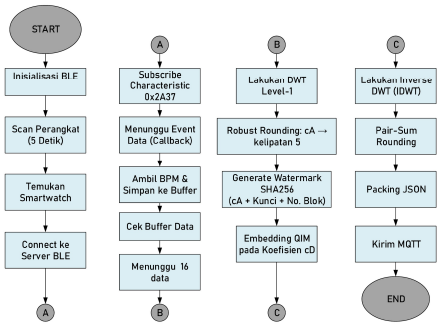
2.2 Skema penyisipan *watermark*

Setiap notifikasi *Bluetooth Low Energy* yang masuk memicu fungsi *callback* yang mengambil nilai detak jantung dari byte kedua muatan lalu menyimpannya ke penyangga berkapasitas 16 elemen. Ukuran blok 16 sampel dipilih karena Haar level satu menghasilkan tepat delapan koefisien detail, sehingga kapasitas penyisipan cocok untuk *watermark* delapan bit (satu bit per koefisien). Ukuran pangkat dua ini menjaga dekomposisi tetap simetris, sedangkan blok lebih besar hanya memperpanjang waktu pengisian penyangga. Ketika penyangga penuh, terbentuk satu blok sinyal x[n] sepanjang 16 sampel dan rantai pemrosesan empat tahap dieksekusi sebagaimana disajikan pada Gambar 3.

Tahap pertama mendekomposisi blok menggunakan transformasi wavelet Haar (Discrete Wavelet Transform Haar, DWT-Haar) level satu menjadi delapan koefisien aproksimasi dan delapan koefisien detail, mengikuti Persamaan (1).

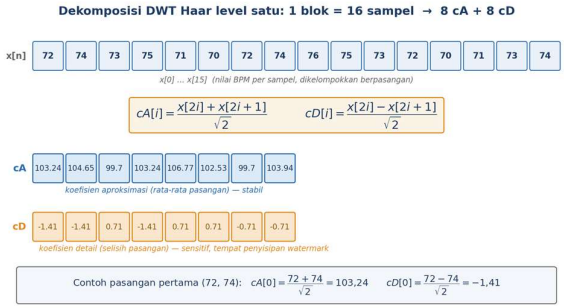
$$cA[i] = \frac{x[2i] + x[2i+1]}{\sqrt{2}} \quad , \quad cD[i] = \frac{x[2i] - x[2i+1]}{\sqrt{2}} \tag{1}$$

Pada persamaan tersebut, x[2i] dan x[2i+1] adalah pasangan sampel detak jantung yang berurutan, cA[i] merupakan koefisien aproksimasi yang merepresentasikan rata-rata terbobot pasangan itu, dan cD[i] merupakan koefisien detail yang merepresentasikan selisihnya, dengan indeks i bernilai 0 sampai 7.



Gambar 3. Diagram alir proses penyisipan *watermark* pada *gateway*

Pemisahan ini menghasilkan dua komponen dengan sifat berlawanan: koefisien aproksimasi bersifat stabil terhadap perubahan kecil yang saling meniadakan antar-pasangan, sedangkan koefisien detail sangat responsif terhadap perubahan selisih. Sifat inilah yang dimanfaatkan sebagai fondasi perilaku *semi-fragile*. Konstanta $1/\sqrt{2}$ dihitung sekali di awal program agar tidak diulang pada setiap blok, mengingat operasi pembagian merupakan beban nyata bagi mikrokontroler. Sebagai ilustrasi, Gambar 4 memperagakan dekomposisi satu blok berisi 16 sampel detak jantung menjadi delapan koefisien aproksimasi dan delapan koefisien detail. Sebagai contoh, pasangan pertama (72, 74) menghasilkan cA[0] = (72 + 74)/√2 ≈ 103,24 sebagai wakil tren rata-rata, dan cD[0] = (72 − 74)/√2 ≈ −1,41 sebagai wakil selisih. Bit *watermark* kemudian disisipkan pada koefisien detail cD yang lebih peka ini.



Gambar 4. Dekomposisi DWT Haar level satu untuk satu blok 16 sampel beserta contoh perhitungan

Tahap kedua membangkitkan *watermark*. Koefisien aproksimasi dibulatkan terlebih dahulu ke kelipatan lima melalui *robust rounding* supaya nilai acuan yang dipakai pengirim dan penerima tetap sama meskipun terjadi galat pembulatan ringan selama transmisi. Rangkaian koefisien hasil pembulatan digabungkan dengan kunci rahasia dan nomor blok, lalu dilewatkan ke fungsi hash SHA-256 [19]. Delapan bit pertama dari keluaran hash tersebut dipakai sebagai *watermark*. Penyertaan nomor blok memastikan blok yang isinya kebetulan sama tetap menghasilkan *watermark* berbeda, sehingga penyerang tidak dapat menukar posisi blok tanpa terdeteksi. Kunci rahasia yang sama ditanamkan pada *firmware* pengirim ESP32 dan pada program verifikasi penerima, sehingga hanya pihak yang memegang kunci dapat membangkitkan *watermark* yang sah. Pengelolaan dan implikasi keamanan kunci ini dibahas pada Sub-bab 3.8. Tahap ketiga menyisipkan kedelapan bit *watermark* ke koefisien detail menggunakan *Quantization Index Modulation* berbasis paritas dengan langkah kuantisasi Δ = 4,0, mengikuti Persamaan (2).

$$q[i] = \left\lfloor \frac{cD[i]}{\Delta} \right\rfloor, \quad cD'[i] = \begin{cases} q[i] \cdot \Delta, & \text{jika } q[i] \bmod 2 = b[i] \\ (q[i] + 1) \cdot \Delta, & \text{untuk keadaan lain} \end{cases} \tag{2}$$

Simbol q[i] menyatakan indeks kuantisasi hasil pembulatan ke bawah, cD'[i] adalah koefisien detail setelah penyisipan, b[i] adalah bit *watermark* ke-i yang bernilai 0 atau 1, dan Δ adalah langkah kuantisasi. Setiap bit dipetakan ke titik kuantisasi pada kelipatan Δ dengan paritas indeks yang berselang-seling, sehingga kisi bit

nol dan kisi bit satu yang bertetangga berjarak Δ. Penerima memulihkan bit dengan menentukan kelipatan Δ terdekat lalu membaca paritas indeksnya. Konsekuensinya, batas toleransi adalah setengah jarak antar-kisi, yaitu Δ/2 sebesar 2,0: selama distorsi yang dialami sebuah koefisien tidak melampaui nilai tersebut, bit yang tertanam tetap terbaca benar. Nilai Δ karenanya mengendalikan pertukaran antara toleransi terhadap gangguan dan besarnya distorsi yang ditimbulkan pada sinyal. Langkah kuantisasi Δ = 4,0 berasal dari pertukaran QIM: distorsi per koefisien dibatasi Δ/2 = 2,0 dan galat kuadrat rata-rata dibatasi $\Delta^2/4$ = 4,0, sehingga nilai ini menjaga PSNR tetap tinggi (41,59 dB) sekaligus memberi marjin toleransi 2,0 yang memisahkan gangguan wajar dari manipulasi. Memperbesar Δ akan menaikkan toleransi tetapi menurunkan PSNR sebanding Δ^2. Tahap keempat merekonstruksi sinyal melalui transformasi wavelet balik, diikuti *pair-sum rounding* agar sampel keluaran kembali berupa bilangan bulat tanpa mengubah jumlah tiap pasangan, lalu mengemas blok dalam format JSON untuk dikirim ke broker.

2.3 Skema verifikasi

Dashboard penerima menjalankan urutan yang mencerminkan proses pengirim. Blok yang diterima didekomposisi ulang dengan Haar level satu. *Watermark* tertanam diekstraksi dari koefisien detail berdasarkan kisi kuantisasi terdekat, sementara *watermark* acuan dibangkitkan ulang dari koefisien aproksimasi memakai kunci dan nomor blok yang sama. Kedua rangkaian bit dibandingkan: blok dinyatakan VALID bila BER tidak melampaui 12,5% dan INVALID bila melampauinya. Adapun batas ambang BER 12,5% ditetapkan tepat satu bit dari delapan bit *watermark*, sehingga batas keputusan berada pada kondisi paling banyak satu bit salah, membedakan gangguan ringan (maksimal satu bit kesalahan) dengan manipulasi (dua bit atau lebih kesalahan), dengan peluang lolos kebetulan hanya satu berbanding 256.

2.4 Rancangan pengujian

Pengumpulan data melibatkan 8 subjek (4 laki-laki, 4 perempuan) yang mewakili 4 kategori usia: anak-anak, remaja, dewasa, dan lansia. Rentang rata-rata detak jantung yang terekam 69-113 denyut per menit, konsisten dengan rentang fisiologis normal menurut acuan zona detak jantung target *American Heart Association*. Keseluruhan sesi menghasilkan 247 blok setara 3.952 sampel untuk menilai mutu penyisipan pada kondisi normal. Jumlah subjek ditetapkan agar sinyal uji mencakup rentang detak jantung lebar lintas usia dan aktivitas, bukan untuk simpulan epidemiologis maupun menguji akurasi klinis sensor.

Karakteristik subjek dirancang untuk merentangkan detak jantung lintas usia: kategori anak-anak (rentang usia 6–9 tahun), remaja (10–19 tahun), dewasa (20–59 tahun), dan lansia (60–100 tahun), masing-masing diwakili satu subjek laki-laki dan satu subjek perempuan. Setiap subjek menjalani dua sesi, yakni satu setelah aktivitas fisik ringan hingga sedang (cardio) dan satu dalam keadaan istirahat (*rest*), sehingga terkumpul 16 sesi. Tiap sesi menghasilkan sekitar 15 hingga 20 blok bergantung durasi perekaman, dan gabungan seluruh sesi memberikan 247 blok kondisi normal. Adapun data pengujian ketahanan sejumlah 807 blok berasal dari sinyal ber-*watermark* yang sama tetapi diproses melalui 16 skenario simulasi di sisi penerima, sehingga jumlahnya sengaja dibedakan dari 247 blok kondisi normal dan bukan merupakan kumpulan data yang sama. Karena penelitian menggunakan data detak jantung dari manusia, seluruh subjek dewasa memberikan persetujuan tertulis (*informed consent*) sebelum pengambilan data, sedangkan untuk subjek di bawah umur persetujuan diberikan oleh orang tua atau wali. Penelitian ini tidak melalui kaji etik komite formal. Prinsip etik dijaga melalui partisipasi sukarela, persetujuan tertulis (*informed consent*) seluruh subjek dewasa serta orang tua atau wali untuk subjek di bawah umur, penggunaan perangkat pengukuran non-invasif, dan anonimisasi seluruh data. Seluruh data diperoleh langsung dari *smartwatch* selama eksperimen melalui tautan BLE, lalu disimpan sebagai berkas terstruktur yang diberi kode subjek (kategori usia dan jenis kelamin) tanpa menyertakan identitas pribadi, sehingga data telah dianonimkan.

Ketahanan diuji melalui 16 skenario dalam 6 kategori. Kategori normal meneruskan data tanpa modifikasi sebagai acuan. Kompresi simetris pada tiga tingkat menambah nilai a pada sampel indeks genap dan menguranginya pada indeks ganjil dengan a = 0,5, 1,0, dan 2,0 (dinotasikan ×0,5, ×1,0, ×2,0), sehingga jumlah tiap pasangan dan koefisien aproksimasi tetap. Derau Gaussian aditif memakai pola simetris serupa via pembangkit Box-Muller pada tiga tingkat variansi σ^2 = 0,01, 1,0, dan 10,0. Kompresi kuantisasi membulatkan tiap sampel ke kelipatan langkah kuantisasi pada tiga tingkat yang dinotasikan Q50, Q30, dan Q10 (semakin kecil angka Q, semakin kasar kuantisasinya). Kategori serangan manipulasi mencakup penambahan tetap 30 denyut per menit ke seluruh sampel, penskalaan proporsional seluruh sampel dengan faktor tetap, dan penggunaan kunci verifikasi palsu di sisi penerima. Kategori terakhir mencakup kompresi delta *lossless* (dua orde, O1 dan O2) yang mengembalikan sinyal secara sempurna serta korupsi acak pada aliran data. Seluruh besaran ini diterapkan secara deterministik pada sinyal ber-*watermark* yang sama agar hasil antar-skenario dapat dibandingkan langsung.

Setiap skenario diberi target sesuai kelompoknya: TOLERAN mensyaratkan status tetap VALID, SENSITIF mensyaratkan INVALID, dan TENGAH ditempatkan pada wilayah peralihan tanpa target mengikat

untuk memetakan batas keputusan. Seluruh skenario dijalankan sebagai mode simulasi pada *dashboard* sehingga *firmware* ESP32 tidak diubah antar-skenario, dan tiap pengujian bekerja pada sinyal ber-*watermark* dari rantai yang sama. Tiap skenario dijalankan sebagai sesi tersendiri berisi sekitar 50 blok, sehingga seluruh pengujian ketahanan mencakup 807 blok setara 12.912 sampel, terpisah dari 247 blok (1.976 bit) kondisi normal pada Tabel 1.

2.5 Metrik evaluasi dan kriteria keberhasilan

Kinerja dinilai melalui tiga parameter kuantitatif yang dihitung per blok. *Bit Error Rate* (BER) mengukur proporsi bit *watermark* yang gagal diekstraksi dengan benar sebagaimana dinyatakan pada Persamaan (3), sedangkan kualitas sinyal setelah penyisipan diukur melalui *Peak Signal-to-Noise Ratio* (PSNR) yang dibangun di atas *Mean Square Error* (MSE) seperti pada Persamaan (4).

$$BER = \frac{\text{jumlah bit error}}{\text{total bit watermark}} \times 100\% \tag{3}$$

$$MSE = \frac{1}{N}\sum_{i=0}^{N-1}\left(x_{\text{asli}}[i] - x_{\text{proses}}[i]\right)^2 \;,\; PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \text{ dB} \tag{4}$$

Pada kedua persamaan tersebut, total bit *watermark* bernilai delapan untuk setiap blok, N adalah jumlah sampel dalam satu blok yang bernilai 16, x_asli[i] adalah sampel sebelum diproses, x_proses[i] adalah sampel setelah diproses, dan MAX adalah nilai rujukan maksimum sinyal yang ditetapkan sebesar 200 denyut per menit sebagai batas atas wajar detak jantung manusia. Enam target perancangan ditetapkan sebagai kriteria keberhasilan: BER = *0* pada kondisi normal, PSNR sekurang-kurangnya 35 dB setelah penyisipan, tingkat deteksi manipulasi sekurang-kurangnya 90% untuk kelompok SENSITIF, waktu komputasi di bawah 500 ms per blok, keandalan akuisisi dan pemrosesan tanpa kegagalan, dan latensi ujung ke ujung di bawah tiga detik per blok. Interval pengambilan sampel sebesar 1 Hz diperlakukan sebagai asumsi laju notifikasi ideal sesuai profil detak jantung BLE, bukan sebagai target rancangan, karena laju tersebut ditentukan *firmware* perangkat sumber dan berada di luar kendali *gateway*.

3. HASIL DAN PEMBAHASAN

3.1 Pencapaian terhadap target perancangan

Pengujian fungsional dilakukan untuk memastikan seluruh komponen bekerja sesuai rancangan. Ringkasan capaian disajikan pada Tabel 1, yang memuat 7 baris parameter, yaitu 6 target perancangan ditambah satu asumsi laju pengambilan sampel 1 Hz (bukan target rancangan, sebagaimana dijelaskan pada Sub-bab 2.5). Dari ketujuh parameter tersebut, lima tercapai penuh. Dua sisanya berkaitan dengan waktu dan bersumber dari penyebab yang sama, yaitu laju notifikasi perangkat sumber, yang diurai pada Sub-bab 3.5.

Tabel 1. Target spesifikasi dan realisasi sistem

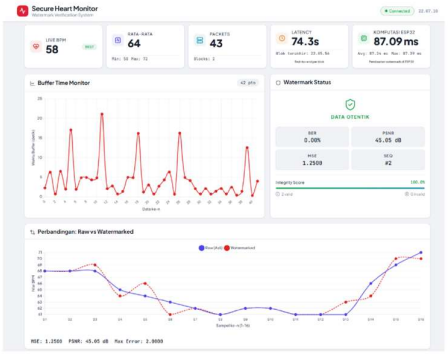
Parameter	Target	Realisasi	Status
BER kondisi normal	0%	0% (0 dari 1.976 bit)	Tercapai
PSNR rata-rata	≥ 35 dB	41,59 dB	Tercapai
Akurasi deteksi manipulasi	≥ 90%	96,1% (292 dari 304 blok)	Tercapai
Waktu komputasi per blok	< 500 ms	87,16 ms	Tercapai
Keandalan akuisisi dan pemrosesan	tanpa kegagalan	247 blok, 0 kegagalan	Tercapai
Latensi ujung ke ujung per blok	< 3 detik	didominasi tunggu notifikasi	Sebagian
Interval pengambilan sampel	1 Hz (asumsi profil)	4,78 detik per sampel	Di luar kendali

3.2 Kualitas penyisipan *watermark*

Pada kondisi transmisi normal, seluruh 1.976 bit *watermark* dari 247 blok terekstraksi tanpa satu pun kesalahan. Angka nol ini bukan sekadar capaian statistik melainkan syarat fungsional: setiap kesalahan bit pada kondisi tanpa gangguan berarti sistem tidak lagi mampu membedakan data yang utuh dari data yang bermasalah, sehingga seluruh mekanisme verifikasi kehilangan makna. Nilai nol memastikan bahwa setiap status INVALID yang muncul kemudian benar-benar berasal dari gangguan pada kanal, bukan dari ketidaksempurnaan rantai pemrosesan itu sendiri.

Distorsi penyisipan tetap kecil, dengan MSE rata-rata 3,01 (simpangan baku 1,15; selang kepercayaan 95% ±0,14) dan PSNR rata-rata 41,59 dB (simpangan baku 1,81; selang kepercayaan 95% ±0,23) yang dihitung atas seluruh 247 blok. Penyisipan memindahkan setiap koefisien detail ke kelipatan Δ terdekat berparitas sesuai, dan transformasi wavelet balik menyebar pergeseran itu ke dua sampel sehingga galat pada ranah sinyal jauh lebih kecil daripada pergeseran koefisiennya. Nilai 3,01 berada di bawah $\Delta^2/4 = 4{,}0$ yang lazim menjadi acuan kasar distorsi kuantisasi, sehingga penyisipan bekerja pada rentang yang dirancang. PSNR 41,59 dB

melampaui target 35 dB sejauh 6,59 dB. Dengan rujukan maksimum 200 denyut per menit, angka ini setara galat akar rata-rata kuadrat di bawah dua denyut per menit, besaran yang sangat kecil relatif terhadap rentang detak jantung. Perlu ditegaskan bahwa penelitian ini tidak melakukan validasi klinis, sehingga interpretasi PSNR dan MSE dibatasi pada mutu penyisipan sinyal dan bukan klaim terhadap kategori klinis detak jantung. Nilai-nilai tersebut ditampilkan pada dashboard web (Gambar 4).



Gambar 4. Tampilan *dashboard* web

3.3 Bukti sifat *semi-fragile*

Sifat *semi-fragile* dinilai dari dua tuntutan yang berlawanan sekaligus: bertahan pada gangguan wajar dan rusak pada manipulasi disengaja. Hasil pengujian enam belas skenario dirangkum pada Tabel 2, sedangkan perbandingan akurasi antar-skenario divisualisasikan pada Gambar 5.

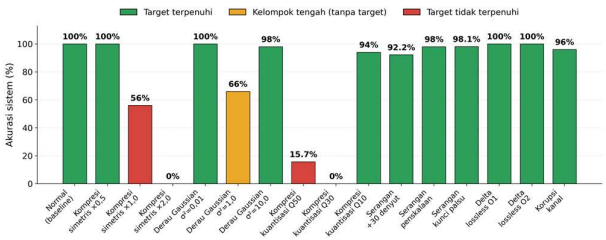
Tabel 2. Hasil pengujian ketahanan pada enam belas skenario

No	Skenario	Grup	Blok	Blok VALID (%)	BER (%)	Status target
1	Normal (baseline)	TOLERAN	51	100	0,00	Terpenuhi
2	Kompresi simetris ×0,5	TOLERAN	50	100	0,00	Terpenuhi
3	Kompresi simetris ×1,0	TOLERAN	50	56	18,50	Gagal
4	Kompresi simetris ×2,0	TENGAH	51	0	100,00	—
5	Derau Gaussian σ^2=0,01	TOLERAN	50	100	0,00	Terpenuhi
6	Derau Gaussian σ^2=1,0	TENGAH	50	66	14,25	—
7	Derau Gaussian σ^2=10,0	SENSITIF	50	2	48,75	Terpenuhi
8	Kompresi kuantisasi Q50	TOLERAN	51	15,7	42,89	Gagal
9	Kompresi kuantisasi Q30	TENGAH	50	0	51,25	—
10	Kompresi kuantisasi Q10	SENSITIF	50	6	49,00	Terpenuhi
11	Serangan penambahan 30 denyut	SENSITIF	51	7,8	52,21	Terpenuhi
12	Serangan penskalaan linear	SENSITIF	50	2	49,25	Terpenuhi
13	Serangan kunci palsu	SENSITIF	53	1,9	47,64	Terpenuhi
14	Delta lossless O1	TOLERAN	50	100	0,00	Terpenuhi
15	Delta lossless O2	TOLERAN	50	100	0,00	Terpenuhi
16	Korupsi kanal	SENSITIF	50	4	53,00	Terpenuhi

Catatan: nilai BER pada tabel ini mengukur akibat gangguan terhadap proses ekstraksi *watermark*, sehingga berbeda dari BER kondisi normal yang bernilai nol pada Tabel 1.

Secara ringkas, hasil per kelompok dapat dibaca sebagai berikut. Ketujuh skenario TOLERAN mempertahankan rata-rata 81,7% blok VALID (lima di antaranya 100%), menandakan ketahanan terhadap gangguan wajar; keenam skenario SENSITIF menolak 96,1% blok (292 dari 304), menegaskan kepekaan terhadap manipulasi; dan ketiga skenario TENGAH tersebar di kedua sisi ambang untuk memetakan batas keputusan. Gambar 5 memvisualkan perbandingan akurasi antar-skenario ini.

Pada sisi toleransi, sistem mempertahankan status VALID pada seluruh blok untuk kompresi simetris tingkat rendah, derau Gaussian lemah, dan kedua kompresi delta *lossless*. Ketahanan terhadap delta *lossless* dapat diprediksi karena operasi itu mengembalikan sinyal sempurna. Yang lebih menjelaskan mekanisme skema ini adalah ketahanan terhadap kompresi dan derau simetris, yang memodifikasi sampel berpasangan dengan tanda berlawanan sehingga jumlah tiap pasangan tidak berubah. Koefisien aproksimasi bertahan dan watermark acuan yang dibangkitkan darinya tetap sama. Toleransi sistem karenanya bukan hasil pelonggaran ambang, melainkan konsekuensi langsung dari pemilihan domain penyisipan. Pada sisi sensitivitas, keenam skenario kelompok SENSITIF terdeteksi seluruhnya dengan akurasi gabungan 96,1%, yaitu 292 dari 304 blok dinyatakan INVALID. Perilaku ketiga skenario serangan memperkuat penjelasan di atas dari arah sebaliknya.



Gambar 5. Akurasi sistem per skenario pengujian

Penambahan 30 denyut per menit dan penskalaan proporsional sama-sama menggeser seluruh sampel searah, sehingga jumlah pasangan berubah, koefisien aproksimasi bergeser, dan *watermark* acuan yang dibangkitkan ulang tidak lagi cocok dengan yang tertanam. Serangan kunci palsu terdeteksi melalui jalur berbeda: data tidak diubah sama sekali, tetapi kunci yang salah menghasilkan keluaran hash yang sepenuhnya berbeda. Ketiganya menghasilkan BER mendekati 50%, yaitu tingkat yang setara dengan tebakan acak dan menandakan hilangnya seluruh korelasi antara *watermark* acuan dan *watermark* tertanam.

Ketiga skenario TENGAH memberi informasi berbeda sifatnya. Ditempatkan pada wilayah peralihan tanpa target mengikat, hasilnya memetakan letak batas keputusan. Derau Gaussian menengah menghasilkan 66% blok VALID dengan BER rata-rata 14,25%, hanya sedikit di atas ambang 12,5% sehingga populasi blok terbelah hampir merata. Sebaliknya, kompresi simetris ×2,0 dan kuantisasi Q30 sepenuhnya di sisi sensitif tanpa satu pun blok bertahan. Pola ini menunjukkan batas keputusan bukan titik tajam melainkan pita peralihan sempit yang letaknya dapat diprediksi dari besar distorsi tiap koefisien.

Dari tujuh skenario kelompok TOLERAN, lima memenuhi target sepenuhnya. Dua sisanya, yaitu kompresi simetris ×1,0 dengan 56% blok VALID dan kompresi kuantisasi Q50 dengan 15,7% blok VALID, tidak mencapai target dan dibahas tersendiri pada subbab berikut. Dengan demikian, sistem bersifat *semi-fragile* secara dominan namun belum sepenuhnya toleran terhadap seluruh gangguan yang dikategorikan wajar: dua skenario kompresi *borderline* (kompresi simetris ×1,0 dan kuantisasi Q50) tetap terdeteksi sebagai INVALID. Hal ini dinyatakan sebagai keterbatasan yang jujur, bukan diklaim sebagai keberhasilan penuh terhadap seluruh gangguan wajar. Untuk merangkum kinerja deteksi secara menyeluruh, hasil kedua kelompok berlawanan disusun sebagai *confusion matrix* pada Tabel 3, dengan kelompok SENSITIF (manipulasi) diperlakukan sebagai kelas positif dan kelompok TOLERAN (gangguan wajar) sebagai kelas negatif. Kelompok TENGAH dikeluarkan karena tidak memiliki target status yang mengikat.

Tabel 3. *Confusion matrix* deteksi manipulasi (SENSITIF) versus gangguan wajar (TOLERAN)

	Diprediksi INVALID (positif)	**Diprediksi VALID (negatif)**
Aktual manipulasi (SENSITIF)	TP = 292	FN = 12
Aktual gangguan wajar (TOLERAN)	FP = 65	TN = 287

Dari matriks tersebut diperoleh *sensitivity* (kepekaan terhadap manipulasi) sebesar 96,1% (292/304), *specificity* (toleransi terhadap gangguan wajar) 81,5% (287/352), *precision* 81,8%, akurasi keseluruhan 88,3%, dan skor F1 88,4%. Seluruh 65 kesalahan positif (*false positive*) terkonsentrasi pada dua skenario TOLERAN yang gagal, yakni kompresi simetris faktor 1,0 (22 blok) dan kuantisasi Q50 (43 blok). Tanpa kedua skenario *borderline* tersebut *specificity* mendekati 100%. Ditinjau per jenis serangan, seluruh manipulasi terdeteksi tinggi: serangan kunci palsu, penskalaan proporsional, dan derau Gaussian kuat menjadi yang paling mudah dikenali (sekitar 98%), sedangkan penambahan tetap 30 denyut per menit menjadi yang paling sulit dengan tingkat deteksi 92,2% (empat blok lolos), diikuti kuantisasi Q10 pada 94,0%.

3.4 Batas toleransi kuantisasi sebagai penjelas kegagalan

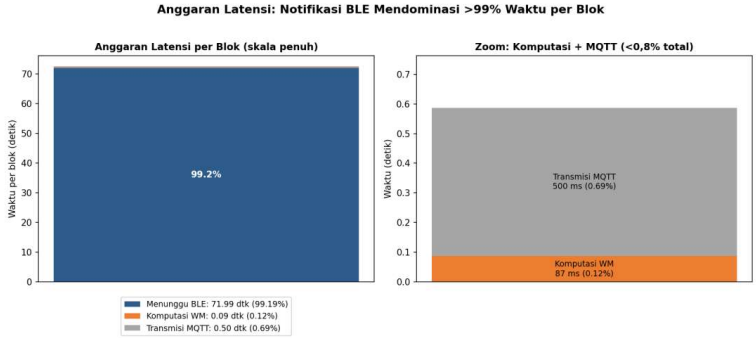
Kedua kegagalan dapat dijelaskan kuantitatif dari parameter kuantisasi. Ambang 12,5% setara satu bit salah dari delapan bit, sehingga blok tetap VALID selama tidak lebih dari satu koefisien detail terbaca pada kisi yang keliru. Sementara itu, penyisipan $\Delta = 4{,}0$ hanya sanggup menahan distorsi hingga setengah jarak antar-kisi, yaitu 2,0 satuan per koefisien. Pada kompresi simetris ×1,0, penambahan dan pengurangan satu satuan tiap pasangan diteruskan ke ranah wavelet sebagai pergeseran koefisien detail sebesar $\sqrt{2}$ kali nilai itu, sekitar 1,41 satuan, masih di bawah batas 2,0 tetapi hanya bersisa 0,59 satuan. Marjin sesempit itu mudah habis oleh galat pembulatan saat rekonstruksi, sehingga sebagian koefisien pada sebagian blok terlempar melewati kisi, menghasilkan BER rata-rata 18,50% dan blok VALID turun ke 56%. Pola ini konsisten dengan tetangganya: pada ×0,5 pergeseran hanya 0,71 satuan sehingga semua blok bertahan, sedangkan pada ×2,0 mencapai 2,83 satuan yang melampaui batas sehingga tidak satu pun bertahan.

Kompresi kuantisasi Q50 gagal melalui mekanisme lebih berat. Pembulatan sampel ke kelipatan empat menimbulkan galat hingga dua satuan, tepat di batas toleransi, tetapi persoalan utamanya adalah sifatnya yang tidak simetris antar-pasangan: pembulatan bekerja pada tiap sampel secara independen sehingga jumlah pasangan berubah dan koefisien aproksimasi bergeser. Akibatnya watermark acuan yang dibangkitkan ulang sudah berbeda sejak awal, terlepas dari apakah bit tertanam masih terbaca benar, sebab BER melonjak ke 42,89%, jauh melampaui kompresi simetris meski galatnya sebanding. Kedua kasus menunjukkan batas toleransi sistem ditentukan dua hal sekaligus, yaitu besar distorsi terhadap $\Delta/2$ dan simetri distorsi antar-pasangan sampel. Implikasi rancangannya, memperbesar Δ menaikkan toleransi terhadap gangguan bertipe pertama, tetapi menurunkan PSNR karena distorsi penyisipan tumbuh sebanding Δ^2, dan tidak memperbaiki gangguan bertipe kedua sama sekali.

3.5 Anggaran latensi dan keterbatasan akuisisi

Interval pengambilan sampel yang tercatat rata-rata 4,78 detik dengan median 3,60 detik jauh dari target 1 Hz. Interval 4,78 detik tersebut adalah jarak antar-sampel. Karena satu blok berisi 16 sampel, waktu pengisian satu blok setara sekitar 15 interval atau kurang lebih 72 detik, sehingga angka ini konsisten dengan penantian notifikasi BLE 71,99 detik per blok. Untuk menetapkan sumber keterlambatan tersebut, komposisi waktu per blok diurai per komponen sebagaimana ditunjukkan pada Gambar 6. Penantian notifikasi BLE menyerap 71,99 detik atau 99,19% total waktu per blok, transmisi MQTT 0,50 detik (0,69%), dan komputasi *watermarking* hanya 0,09 detik (0,12%). Temuan ini memindahkan penyebab kegagalan target waktu dari algoritma ke perangkat sumber: interval notifikasi ditentukan *firmware smartwatch* dan di luar kendali *gateway*, sehingga target 1 Hz berada di luar jangkauan rancangan. Sebaliknya, komputasi 87,16 ms yang hanya 0,12% anggaran, diukur oleh pewaktu internal ESP32 pada setiap blok kondisi normal dengan simpangan baku hanya 0,13 ms (selang kepercayaan 95% ±0,02 ms), membuktikan beban transformasi wavelet, hash, dan kuantisasi sepenuhnya terserap ESP32 tanpa menjadi penghambat, bukti utama kelayakan verifikasi integritas *semi-fragile* pada perangkat tepi berbiaya rendah tanpa perangkat keras kriptografi khusus.

Sistem yang dibangun masih menyimpan keterbatasan yang perlu dinyatakan terbuka. Pengukuran waktu komputasi dibaca langsung dari dashboard karena sistem belum dilengkapi pencatatan dan ekspor metrik per blok ke basis data, sehingga penelusuran ulang terperinci belum dimungkinkan. Seluruh skenario gangguan juga dibangkitkan melalui simulasi terkendali di sisi penerima, bukan serangan nyata pada jaringan produksi. Selain itu, sistem baru menyatakan status keutuhan tanpa menunjukkan letak perubahan maupun memulihkan data yang termanipulasi.



Gambar 6. Komposisi anggaran latensi per blok

Perlu ditegaskan batas generalisasi hasil ini. Pengujian melibatkan 8 subjek dan sebagian besar skenario dibangkitkan melalui simulasi terkendali, sehingga temuan tidak dimaksudkan untuk simpulan klinis maupun epidemiologis. Delapan subjek dipilih untuk merentangkan detak jantung lintas 4 kategori usia dan dua kondisi aktivitas (69-113 denyut per menit), yakni menguji perilaku algoritma pada rentang masukan lebar, bukan mewakili sebaran populasi. Kecukupan bukti bertumpu pada jumlah blok, bukan jumlah subjek: kondisi normal menilai seluruh 1.976 bit dari 247 blok dengan BER nol, sedangkan tiap perilaku *semi-fragile* diuji pada ratusan blok per kelompok, sehingga batas keputusan terukur konsisten dan dapat direproduksi. Simulasi terkendali dipakai agar tiap gangguan dapat diisolasi dan diulang dengan besaran tepat, meski pengujian pada jaringan produksi tetap menjadi arah pelengkap.

3.6 Penggunaan sumber daya ESP32

Karena klaim utama penelitian ini adalah kelayakan *watermarking* pada perangkat berdaya rendah, penggunaan sumber daya ESP32 ditinjau dari tiga sisi. Dari sisi memori, *firmware* hasil kompilasi berukuran 1.640.947 byte (52% dari 3.145.728 byte ruang program) dengan memori dinamis global 60.840 byte (18%

dari 327.680 byte, menyisakan 266.840 byte untuk variabel lokal), dan seluruh proses memakai parameter berukuran tetap (16 sampel, 8 cA, 8 cD, 8 bit *watermark*) tanpa alokasi dinamis saat pemrosesan sehingga tidak terjadi fragmentasi. Dari sisi prosesor, satu inti Xtensa LX6 menuntaskan transformasi, *hash*, dan kuantisasi dalam waktu 87,16 ms per blok sementara inti kedua melayani komunikasi BLE. Dibanding siklus 72,58 detik per blok, komputasi hanya 0,12% sehingga prosesor menganggur lebih dari 99,8%. Karena penyisipan tanpa perangkat keras kriptografi khusus dan hanya aktif 0,12% siklus, tambahan energi akibat *watermarking* diperkirakan sangat kecil relatif terhadap konsumsi dasar yang didominasi mode tunggu BLE. Perlu ditegaskan bahwa perkiraan ini bersifat estimasi berbasis rendahnya *duty-cycle* prosesor dan belum didukung pengukuran arus atau daya nyata. Pengukuran konsumsi daya aktual menggunakan alat ukur arus menjadi keterbatasan penelitian ini sekaligus arah lanjutan yang disarankan.

3.7 Posisi terhadap penelitian terdahulu

Untuk memperjelas keunggulan dan keterbatasan pendekatan yang diusulkan, Tabel 4 membandingkannya dengan sejumlah penelitian *watermarking* terdahulu yang relevan.

Tabel 4. Perbandingan dengan penelitian *watermarking* terdahulu

Penelitian	Domain sinyal	Platform eksekusi	Lokasi verifikasi	Sifat & capaian
Tang & Zhou [6]	Citra 2-D	Simulasi komputer	—	*Robust* terhadap serangan geometris (fokus ketahanan, bukan integritas)
Amrullah & Ernawan [9]	Citra 2-D	Simulasi komputer	—	*Semi-fragile*, lokalisasi tamper; belum di perangkat tertanam
Sivasubramanian & Konganathan [10]	Citra 2-D	Simulasi komputer	—	Deteksi + pemulihan citra; belum di perangkat tertanam
Hsu dkk. [11]	Sinyal ECG 1-D	Komputer (*deep learning*)	—	*Watermark* ECG; pembangkit berat, tidak untuk MCU
Botta dkk. [12]	Sinyal tercuplik 1-D	Komputer	—	*Fragile* berbasis MAC; menolak semua perubahan
Abduljaleel dkk. [15]	Data IoT	*Cloud/server*	*Server semi-trusted*	Integritas ringan; verifikasi jauh dari sumber
Penelitian ini	Detak jantung 1-D (waktu-nyata)	Mikrokontroler ESP32 (tertanam)	Sisi tepi (*dashboard*)	*Semi-fragile end-to-end:* toleran gangguan wajar, deteksi manipulasi 96,1%, BER 0 pada kondisi normal

3.8 Analisis keamanan dan model ancaman

Model ancaman yang diasumsikan adalah penyerang yang mampu menyadap dan mengubah data pada kanal antara *gateway* dan *dashboard* (termasuk serangan *man-in-the-middle*), tetapi tidak memiliki akses ke kunci rahasia yang tertanam pada *firmware*. Tujuan penyerang mencakup pemalsuan nilai data, pengulangan (*replay*), penukaran urutan blok, serta pemalsuan *watermark* agar data manipulatif tetap dinilai VALID. Kerahasiaan isi data berada di luar lingkup dan dapat dilengkapi dengan enkripsi kanal seperti TLS secara terpisah.

Karena *watermark* yang ditanam hanya delapan bit, ruang kemungkinannya adalah $2^8 = 256$ kombinasi. Konsekuensinya, kekuatan kriptografis efektif per blok tidak setara dengan SHA-256 penuh: penyerang yang menebak *watermark* secara buta memiliki peluang lolos satu berbanding 256 per blok. Namun peluang tersebut menyusut cepat pada aliran data karena setiap blok diverifikasi secara independen. Agar sejumlah k blok manipulatif lolos serentak, peluangnya turun menjadi (1/256) pangkat k. Panjang delapan bit dipilih sebagai kompromi antara kapasitas penyisipan (satu bit per koefisien detail pada blok 16 sampel) dan distorsi sinyal. Menambah jumlah bit akan memperbesar distorsi atau menuntut blok yang lebih besar sehingga memperlama akuisisi. Untuk aplikasi berkeamanan lebih tinggi, panjang penanda dapat diperbesar dengan mengorbankan kapasitas atau memperbesar ukuran blok.

Keamanan skema bertumpu pada kerahasiaan kunci: selama kunci tidak diketahui penyerang, *watermark* yang sah tidak dapat dibangkitkan meskipun algoritmanya diketahui publik (prinsip Kerckhoffs). Keterbatasannya, kunci saat ini berupa nilai statis yang ditanam sama pada pengirim dan penerima tanpa mekanisme rotasi maupun distribusi kunci asimetris. Hal ini menjadi arah pengembangan, misalnya penyimpanan pada elemen aman dan rotasi kunci berkala.

4. KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan *gateway* IoT berbasis ESP32 yang mengintegrasikan akuisisi data detak jantung dari perangkat *wearable* dengan mekanisme verifikasi integritas berbasis *semi-fragile watermarking*. Seluruh tahapan pemrosesan, meliputi transformasi DWT-Haar level satu,

pembangkitan *watermark* berbasis SHA-256, serta penyisipan menggunakan *Quantization Index Modulation* dengan langkah kuantisasi 4,0, dapat dijalankan secara penuh pada mikrokontroler tanpa kegagalan selama pengujian 247 blok. Pada kondisi transmisi normal, seluruh 1.976 bit *watermark* berhasil diekstraksi tanpa kesalahan, dengan PSNR rata-rata 41,59 dB dan MSE 3,01, yang menunjukkan tingkat distorsi penyisipan yang rendah.

Evaluasi terhadap 16 skenario menghasilkan sensitivitas sebesar 96,1% dalam mendeteksi manipulasi dan spesifisitas sebesar 81,5% terhadap gangguan yang dikategorikan wajar. Meskipun demikian, beberapa kondisi *borderline* masih menimbulkan kesalahan klasifikasi akibat perubahan pada koefisien aproksimasi. Analisis latensi menunjukkan bahwa proses *watermarking* hanya menyumbang 0,12% dari total waktu pemrosesan, sedangkan sebagian besar waktu dipengaruhi oleh proses akuisisi melalui BLE.

Hasil tersebut menunjukkan bahwa ESP32 memiliki potensi sebagai *gateway* berbiaya rendah untuk mendukung verifikasi integritas data biomedis secara langsung pada titik masuk jaringan. Penelitian selanjutnya perlu diarahkan pada pengembangan kuantisasi adaptif, dekomposisi wavelet bertingkat, penguatan mekanisme keamanan, pengukuran konsumsi energi secara langsung, serta pengujian pada lingkungan jaringan nyata, penguatan keamanan (rotasi dan penyimpanan kunci yang aman serta penanda *anti-replay*), dan pengujian pada jaringan produksi. Prinsip yang sama berpeluang diperluas ke sinyal biomedis lain seperti elektrokardiogram, saturasi oksigen, atau suhu tubuh.

5. DAFTAR PUSTAKA

[1] A. Z. Saputra, M. T. Habibie, and M. C. Irawan, "Rancang bangun alat monitoring detak jantung dan suhu tubuh berbasis Internet of Things (IoT)," *Jurnal Riset dan Aplikasi Mahasiswa Informatika (JRAMI)*, vol. 6, no. 1, pp. 86–92, 2025.

[2] M. U. Jannah, A. C. Nur'aidha, and D. Y. H. Kumarajati, "Sistem deteksi detak jantung berbasis sensor MAX30102, Arduino Uno, dan OLED display untuk pemantauan detak jantung secara real-time," *Jurnal Informatika dan Teknik Elektro Terapan (JITET)*, vol. 12, no. 3, pp. 1961–1965, Aug. 2024, doi: 10.23960/jitet.v12i3.4528.

[3] S. N. Marshella, R. Hasanah, and E. Habinuddin, "Prototype alat pendeteksi kantuk menggunakan sensor MAX30102 dan kamera dengan metode eye aspect ratio," *JITEL (Jurnal Ilmiah Telekomunikasi, Elektronika, dan Listrik Tenaga)*, vol. 4, no. 1, pp. 45–56, Mar. 2024, doi: 10.35313/jitel.v4.i1.2024.45-56.

[4] B. Bordel, R. Alcarria, T. Robles, and M. S. Iglesias, "Data authentication and anonymization in IoT scenarios and future 5G networks using chaotic digital watermarking," *IEEE Access*, vol. 9, pp. 22378–22398, 2021.

[5] R. Wazirali, R. Ahmad, A. Al-Amayreh, M. Al-Madi, and A. Khalifeh, "Secure watermarking schemes and their approaches in the IoT technology: An overview," *Electronics*, vol. 10, no. 14, art. 1744, Jul. 2021.

[6] M. Tang and F. Zhou, "A robust and secure watermarking algorithm based on DWT and SVD in the fractional order Fourier transform domain," *Array*, vol. 15, art. 100230, Sep. 2022.

[7] Z. Yang, Q. Sun, Y. Qi, S. Li, and F. Ren, "A hyper-chaotically encrypted robust digital image watermarking method with large capacity using compressive sensing on a hybrid domain," Entropy, vol. 24, no. 10, art. 1486, Oct. 2022, doi: 10.3390/e24101486.

[8] Y. Idham et al., "Development of a cropping resilient watermarking scheme based on contourlet transform for secure IoT communication," *Eastern-European Journal of Enterprise Technologies*, vol. 1, no. 2 (121), pp. 21–28, Feb. 2023.

[9] A. Amrullah and F. Ernawan, "Semi-fragile image watermarking using quantization-based DCT for tamper localization," *Computers, Materials & Continua*, vol. 86, no. 2, pp. 1–16, 2025, doi: 10.32604/cmc.2025.069229.

[10] N. Sivasubramanian and G. Konganathan, "A novel semi fragile watermarking technique for tamper detection and recovery using IWT and DCT," *Computing*, vol. 102, pp. 1365–1384, 2020.

[11] C.-Y. Hsu, C.-Y. Chang, Y.-C. Chen, J. Wu, and S.-T. Chen, "ECG sensor design assessment with variational autoencoder-based digital watermarking," *Sensors*, vol. 25, no. 7, art. 2321, Apr. 2025, doi: 10.3390/s25072321.

[12] M. Botta, D. Cavagnino, and A. Marra, "DIPS: Data integrity protection of signals," *Algorithms*, vol. 19, no. 3, art. 211, Mar. 2026, doi: 10.3390/a19030211.

[13] M. Botta, D. Cavagnino, and A. Marra, "Audio signal authentication and integrity protection," *Computers*, vol. 15, no. 4, art. 246, Apr. 2026, doi: 10.3390/computers15040246.

[14] P. Niu, J. Tang, W. Guo, and X. Wang, "Image watermarking framework in the UDTCWT-IPHFMs domain via vector BGLE modeling," Circuits, Systems, and Signal Processing, 2026, doi: 10.1007/s00034-026-03646-8.

[15] I. Q. Abduljaleel et al., "Lightweight integrity preserving scheme for secure data exchange in cloud-based IoT systems," *Applied Sciences*, vol. 13, no. 2, art. 691, Jan. 2023, doi: 10.3390/app13020691.

[16] F. Serepas, I. Papias, K. Christakis, N. Dimitropoulos, and V. Marinakis, "Lightweight embedded IoT gateway for smart homes based on an ESP32 microcontroller," *Computers*, vol. 14, no. 9, art. 391, Sep. 2025.

[17] Bluetooth SIG, *Bluetooth Core Specification*, Revision v5.3. Kirkland, WA, USA: Bluetooth Special Interest Group, Jul. 2021.

[18] OASIS, *MQTT Version 5.0*, OASIS Standard, Mar. 2019. [Daring]. Tersedia: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html

[19] National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, FIPS PUB 180-4, Aug. 2015, doi: 10.6028/NIST.FIPS.180-4.