

Reversible Watermarking Menggunakan Metode Difference Expansion Pada Audio Digital

Aulia Arham ^{✉ 1,2}, Rika Ampuh Hadiguna ²

Program Studi Sistem Informasi UIN Imam Bonjol Padang¹

Pendidikan Profesi Insinyur Universitas Andalas²

auliaarham@uinib.ac.id¹, hadiguna@ft.unand.ac.id²

Received 07 Mei 2024,

Accepted 21 September 2024,

Published 30 September 2024

Abstrak

Pesatnya perkembangan teknologi informasi dan komunikasi memberikan kemudahan dalam segala aspek kehidupan, tetapi juga menimbulkan tantangan tersendiri, terutama terkait keamanan data dan privasi. Kriptografi dan steganografi merupakan dua teknik yang digunakan untuk melindungi data. Kriptografi mengamankan informasi dengan mengenkripsi pesan, steganografi menyembunyikan keberadaan data pada media lain. Penyisipan data pada media digital seperti gambar, *audio*, dan *video* membutuhkan metode khusus agar tidak terjadi kerusakan pada media tersebut setelah ekstraksi data. Pada penelitian ini, diusulkan metode *Reversible Data Hiding* (RDH) pada *audio* digital. Metode ini dapat mengembalikan media penampung kedalam bentuk aslinya tanpa terjadi kerusakan menggunakan metode *Difference Expansion* dan Fungsi Modulus. Metode ini diimplementasikan pada *audio* digital dengan menyisipkan data pada selisih 2-bit LSB pasangan sampel *audio*. Berdasarkan eksperimen yang kami lakukan pada 15 *audio* digital pada metode yang diusulkan, kapasitas penyisipan cukup besar dengan kualitas *audio* yang baik. Kapasitas penyisipan dari metode yang diusulkan dapat mencapai 0,2515 bps (bit per sampel) dengan PSNR 103,5869 dB. Hasil eksperimen menunjukkan bahwa metode yang diusulkan memiliki kinerja yang unggul dibandingkan dengan metode sebelumnya.

Kata Kunci: Kriptografi; Steganografi; *Reversible Data Hiding*, *Difference Expansion*, Fungsi Modulus;

Abstract

The rapid development of information and communication technology brings convenience to all aspects of life but also presents challenges, particularly in terms of data security and privacy. Cryptography and steganography are two techniques used to protect data. Cryptography secures information by encrypting messages, while steganography conceals data within other media. Inserting data into digital media such as images, audio, and video requires specialized methods to avoid damaging the media during data extraction. This research proposes a *Reversible Data Hiding* (RDH) method for digital audio. This method restores the storage media to its original form without damage, utilizing the *Difference Expansion* and *Modulus Function* techniques. The method is implemented in digital audio by inserting data in the 2-bit LSB difference of audio sample pairs. Based on experiments conducted using the proposed method on 15 digital audio files, the embedding capacity is substantial while maintaining good audio quality. The embedding capacity of the proposed method reaches 0.2515 bps (bits per

sample) with a PSNR of 103.5869 dB. Experimental results demonstrate that the proposed method outperforms previous methods in terms of performance.

Keywords: *Cryptography; Steganography; Reversible Data Hiding; Difference Expansion; Modulus Function;*

✉ Corresponding author

PENDAHULUAN

Selama beberapa dekade terakhir, terjadi pertumbuhan yang signifikan dalam teknologi informasi dan komunikasi. Perkembangan ini mempermudah masyarakat dalam mengirimkan data antar perangkat di mana saja dan kapan saja [1]–[4]. Bahkan, perangkat terbatas seperti ponsel pintar sekarang mampu memproses data dengan kecepatan yang jauh lebih tinggi daripada sebelumnya. Namun, kemajuan ini juga menarik perhatian pengguna yang tidak sah yang secara aktif menyerang sistem komputer dengan cara seperti menyadap data yang dikirimkan, yang pada gilirannya menimbulkan masalah keamanan terhadap informasi rahasia dan pribadi seperti data keuangan dan medis.

Sejumlah metode telah diajukan untuk mengatasi masalah keamanan ini, yang dapat dibagi menjadi dua kelompok utama: keamanan jaringan dan keamanan informasi, yang saling mendukung. Keamanan jaringan dapat ditingkatkan dengan merancang *intrusion detection system* (IDS), *honeypot*, atau alat keamanan lainnya yang relevan; sementara itu, alat keamanan dapat dirancang untuk menyembunyikan informasi rahasia. Penyembunyian informasi ini bisa dilakukan melalui berbagai cara, termasuk enkripsi atau penyisipan informasi rahasia dalam suatu media [5]–[7], yang dikenal sebagai metode penyembunyian data. Dalam konteks ini, istilah "*hide*" dan "*embedding*" memiliki makna yang sama.

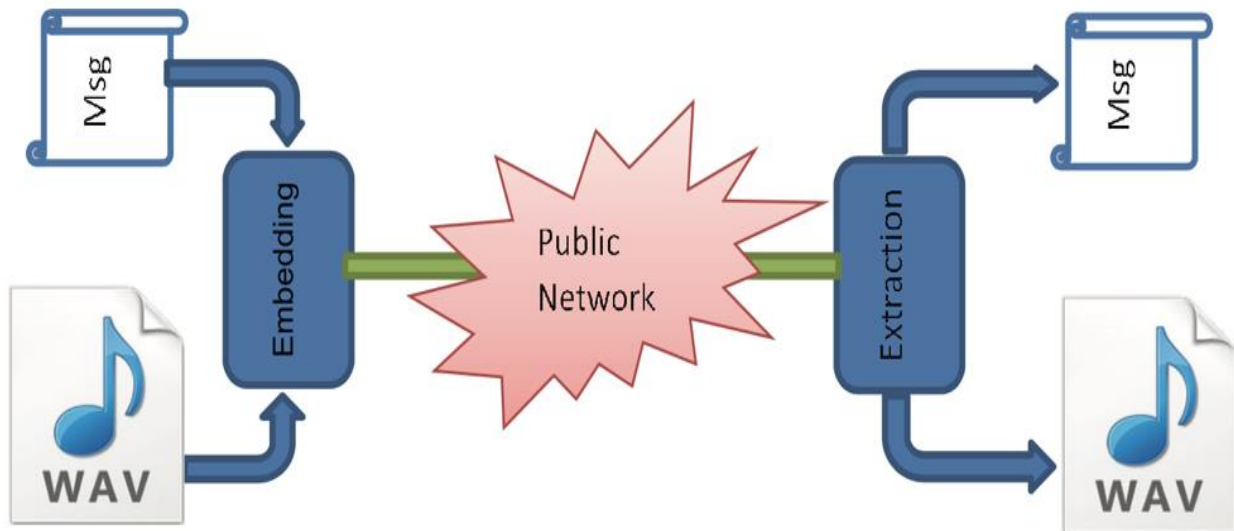
Dalam implementasinya, penyembunyian data dapat menggunakan berbagai media seperti gambar, *audio*, *video*, atau teks untuk membawa informasi rahasia [8]–[12]. Setiap media pembawa memiliki karakteristiknya sendiri. Misalnya, gambar berkaitan dengan kualitas visual, sedangkan *audio* berkaitan dengan kualitas suara. Dalam istilah penyembunyian data, kualitas didefinisikan sebagai tingkat kesamaan pembawa sebelum dan sesudah informasi rahasia disisipkan, tidak tergantung pada jenis media yang digunakan. Faktanya, penelitian di bidang penyembunyian data umumnya lebih terfokus pada penggunaan gambar, sedangkan eksplorasi *audio* relatif lebih sedikit, bahkan lebih sedikit dibandingkan dengan *video*. Proses penyisipan dapat dilakukan baik dalam domain spasial, di mana informasi rahasia langsung disematkan dalam media pembawa, maupun dalam domain frekuensi, di mana media pembawa harus diubah terlebih dahulu sebelum proses penyisipan dilakukan, misalnya dengan menggunakan *Fast Fourier Transform* (FFT) atau *Transformasi Wavelet* [13], [14].

Pada era digital saat ini, dengan semakin meluasnya distribusi konten *audio*

digital melalui *internet* dan teknologi penyiaran digital, seperti streaming musik dan *audio*, ada kebutuhan yang semakin meningkat untuk melindungi hak cipta dan keaslian konten tersebut [15]. Di sisi lain, pengguna juga menginginkan privasi dan kontrol atas informasi pribadi mereka yang dapat terkandung dalam data *audio* digital. Salah satu teknik yang umum digunakan untuk memperkuat keamanan dan melindungi hak cipta adalah *watermarking*. *Watermarking* pada dasarnya adalah proses menyisipkan informasi tambahan ke dalam konten digital yang tidak terlihat secara kasat mata tetapi dapat dideteksi oleh algoritma khusus. Ini memungkinkan identifikasi pemilik hak cipta atau informasi tambahan lainnya yang terkait dengan konten tersebut.

Reversible watermarking adalah varian dari teknik *watermarking* yang memungkinkan untuk menghilangkan *watermark* tanpa kehilangan data asli yang tidak diubah [16]. Ini berarti *audio* asli dapat dipulihkan sepenuhnya setelah *watermark* dihapus [17], yang sangat penting dalam aplikasi di mana kualitas *audio* sangat penting, seperti penyiaran *audio* berkualitas tinggi atau produksi musik. *Difference Expansion* (DE) adalah salah satu teknik dalam *reversible watermarking* yang memanfaatkan perbedaan antara dua piksel atau sampel dalam citra atau *audio* [18]. Ini memungkinkan informasi tambahan disisipkan dengan mengubah nilai perbedaan antara sampel *audio*. Metode *Difference Expansion* pertama kali diperkenalkan oleh Tian pada penelitian [19], [20], kemudian sejumlah peneliti selanjutnya telah membuat perbaikan yang signifikan terhadap metode ini seperti pada penelitian [16], [21], [30]–[33], [22]–[29] yang diimplementasikan pada media gambar dan pada penelitian [9], [34], [35] diimplementasikan pada media *audio*. Beberapa Penelitian seperti [30], [31], [36]–[38] menggunakan *Modulus function* untuk meningkatkan metode *Difference Expansion* dan memodifikasi nilai-nilai yang disisipkan dalam domain yang ditentukan.

Dengan kemajuan teknologi pemrosesan sinyal digital dan analisis statistik, metode DE dan *Modulus Function* telah menjadi pilihan yang populer dalam *reversible watermarking* karena efisiensinya dan kemampuannya untuk menyisipkan informasi tambahan tanpa mengorbankan kualitas *audio* asli. Dengan demikian, latar belakang tentang *reversible watermarking* pada *audio* digital menggunakan metode *Difference Expansion* (DE) dan *Modulus Function* melibatkan kebutuhan akan keamanan dan privasi dalam distribusi konten digital, serta evolusi teknologi dan teknik pemrosesan sinyal digital. Teknik-teknik ini memungkinkan penambahan informasi tambahan ke dalam *audio* digital tanpa mengorbankan kualitas asli *audio* dan mempertahankan kemampuan untuk menghapus *watermark* secara *reversibel*.



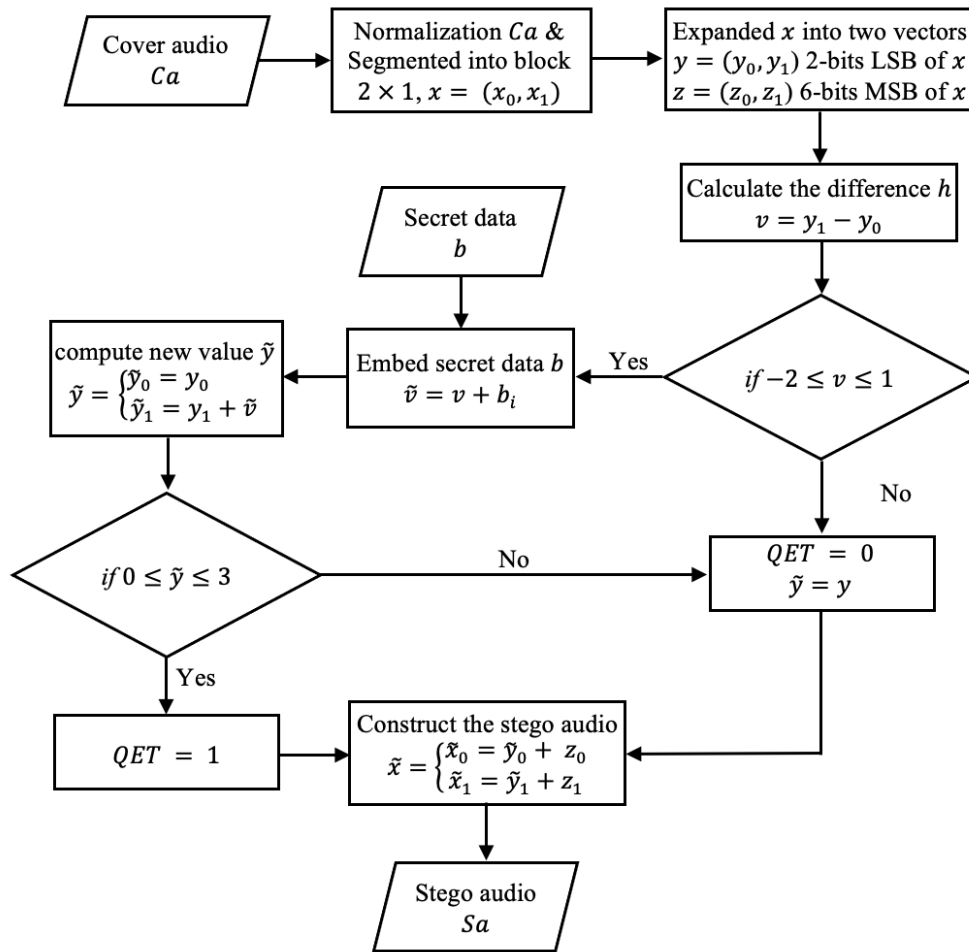
Gambar 1. Metode Reversible Watermarking Audio [39]

METODOLOGI

Metode *reversible watermarking* pada *audio* digital secara umum dibagi menjadi dua bagian yaitu sistem penyisipan data dan sistem ekstraksi data atau pendeteksian *watermark* seperti yang terlihat pada Gambar 1. dimana pada sistem penyisipan data terdapat 2 *input*-an yaitu *audio* digital sebagai *cover* media dan *message* sebagai data yang nanti disisipkan pada *audio* digital dan menghasilkan *output stego audio*. Pada sistem ekstraksi terdapat 1 *input*-an yaitu *stego audio* yang telah disisipkan data dan menghasilkan 2 *output*-an yaitu *cover audio* digital dan *message* sebagai data sebelumnya disisipkan data pada *audio* digital.

a) Penyisipan Data

Penyisipan data yang diusulkan ini dilakukan secara *reversibel* dengan menggunakan metode *Difference Expansion* dan fungsi modulus. Penyisipan data dilakukan dengan membandingkan dua sampel *audio* digital dan menyisipkan data pada selisih nilai antara -2 dan 1 ($-2 \geq s \geq 1$). Prosedur penyisipan data adalah komponen penting dari metode yang diusulkan, seperti yang ditunjukkan pada Gambar 2. Detail proses penyematan dijelaskan dalam langkah-langkah berikut:



Gambar 2. Prosedur Penyisipan Data

- 1) *Cover audio* dinormalisasi dengan mengubah nilai tipe data dari *file audio* sampel dari format *integer* (-32768 hingga 32767) menjadi *integer unsigned* (0 hingga 65535), sehingga semua sinyal *audio* bernilai positif.
- 2) *Cover audio* yang telah dinormalisasi kemudian disegmentasi menjadi blok-blok 2×1 , masing-masing berisi dua sampel data. Selanjutnya, setiap blok direpresentasikan sebagai vektor, dinotasikan sebagai $x = (x_0, x_1)$. Selanjutnya, setiap blok diperluas menjadi dua vektor. Vektor pertama terdiri dari 2-bit LSB masing-masing x , diekstraksi dan dinyatakan sebagai $y = (y_0, y_1)$. Vektor kedua terdiri dari 6-bit Most Significant Bit (MSB) dari setiap x , diekstraksi dan dinyatakan sebagai $z = (z_0, z_1)$.
- 3) Selisih nilai sampel dihitung pada setiap blok y , dan nilai tersebut disimpan dalam h menggunakan Persamaan (1).

$$v = x_0 - x_1 \quad (1)$$

- 4) Telusuri h untuk mengidentifikasi semua nilai yang memenuhi persyaratan penyematan dimana nilai h berada di antara -2 dan 1 ($-2 \leq s \leq 1$, jika h berada di luar kisaran ini, $QET = 0$).
- 5) Mendapatkan data rahasia dan menyimpannya dalam bit vektor b .

- 6) Sematkan data rahasia menggunakan Persamaan (2) untuk memperoleh nilai selisih baru, dilambangkan dengan h , di mana b mewakili bit rahasia tersembunyi dengan nilai nol atau satu.

$$\tilde{v} = v + b_1 \quad (2)$$

- 7) Gunakan nilai selisih baru $\tilde{v}$, yang berisi bit data rahasia, kemudian hitung nilai baru $\tilde{y}$ menggunakan Persamaan (3). Nilai $\tilde{y}$ yang baru harus memenuhi kondisi yang ditentukan dalam Persamaan (4) untuk mencegah *overflow* dan *underflow*. Maka *Qualified Embedding Table* $QET = 1$; sebaliknya, jika $\tilde{y}$ berada di luar rentang ini, $QET = 0$ dan $\tilde{y} = y$.

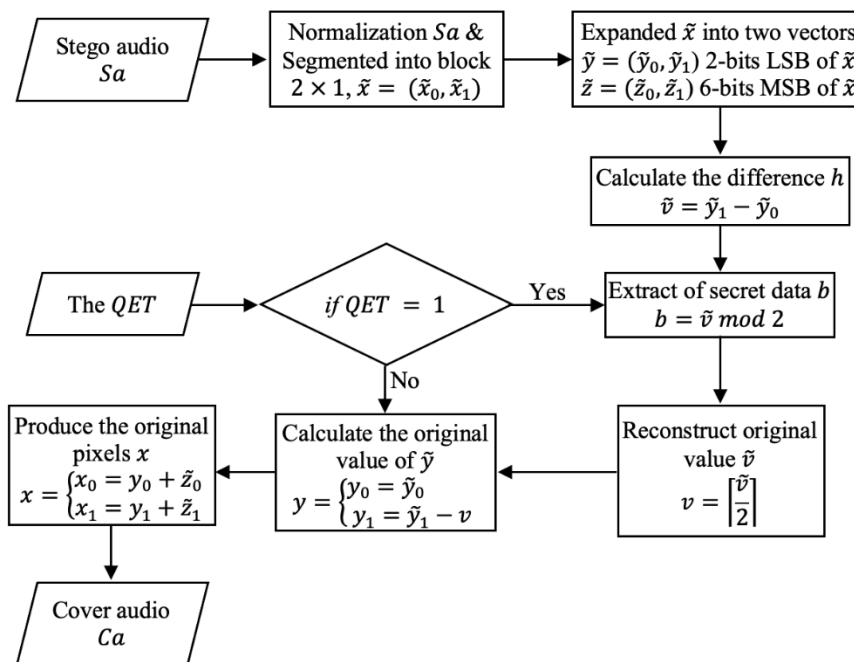
$$\tilde{y} = \begin{cases} \tilde{y}_0 = y_0 \\ \tilde{y}_1 = y_1 + \tilde{v} \end{cases} \quad (3)$$

$$\tilde{y} = \begin{cases} 0 \leq \tilde{y}_0 \leq 3 \\ 0 \leq y_1 + \tilde{v} \leq 3 \end{cases} \quad (4)$$

$$QET = \begin{cases} 0, \text{ if } 0 \leq \tilde{y} \leq 3 \\ 1, \text{ if } 0 \geq \tilde{y} + \tilde{v} \geq 3 \end{cases} \quad (5)$$

- 8) Gabungkan nilai $\tilde{y}$ dan z dengan menjumlahkannya menggunakan Persamaan (6) untuk menghasilkan piksel blok baru $\tilde{x}$ untuk *stego audio*.

$$\tilde{x} = \begin{cases} \tilde{x}_0 = \tilde{y}_0 + z_0 \\ \tilde{x}_1 = \tilde{y}_1 + z_1 \end{cases} \quad (6)$$



Gambar 3. Prosedur Ekstraksi Data

b) Ekstraksi Data

Proses ekstraksi data rahasia dari stego image mirip dengan proses penyisipan. Dalam proses ini menggunakan *Qualified Embedding Table*, yang ditentukan selama proses penyematan. Prosedur ini dapat dilihat pada Gambar 3. Detail proses ekstraksi dijelaskan pada langkah-langkah berikut:

- 1) *Stego audio* dinormalisasi dengan mengubah nilai tipe data dari *file audio* sampel dari format *integer* (-32.768 hingga 32.767) menjadi *integer unsigned* (0 hingga 65.535), sehingga semua sinyal *audio* bernilai positif.
- 2) *Stego audio* yang telah dinormalisasi kemudian disegmentasi menjadi blok-blok 2×1 , masing-masing berisi dua sampel data. Selanjutnya, setiap blok direpresentasikan sebagai vektor, dinotasikan sebagai $\tilde{x} = (\tilde{x}_0, \tilde{x}_1)$. Selanjutnya, setiap blok diperluas menjadi dua vektor. Vektor pertama terdiri dari 2-bit LSB masing-masing $\tilde{x}$, diekstraksi dan dinyatakan sebagai $\tilde{y} = (\tilde{y}_0, \tilde{y}_1)$. Vektor kedua terdiri dari 6-bit Most Significant Bit (MSB) dari setiap $\tilde{x}$, diekstraksi dan dinyatakan sebagai $\tilde{z} = (\tilde{z}_0, \tilde{z}_1)$.
- 3) Selisih nilai sampel dihitung pada setiap blok $\tilde{y}$, dan nilai tersebut disimpan dalam $\tilde{h}$ menggunakan Persamaan. (7).

$$\tilde{v} = \tilde{x}_0 - \tilde{x}_1 \quad (7)$$

- 4) Ekstraksi data rahasia dari nilai selisih $\tilde{v}$ melibatkan penggunaan fungsi modulus dan *Qualified Embedding Table QET*, sebagaimana diuraikan dalam Persamaan. (8). Ekstraksi hanya dilakukan jika $QET = 1$

$$b = \tilde{v} \bmod 2 \quad (8)$$

- 5) Rekonstruksi bentuk awal nilai selisih $\tilde{v}$ menggunakan Persamaan (9) dan hitung nilai awal $\tilde{y}$ menggunakan Persamaan (10). Selanjutnya, gabungkan nilai y dan $\tilde{z}$ dengan menjumlahkannya menggunakan Persamaan (11) untuk menghasilkan nilai asli sampel x dalam blok untuk 2×1 pada *audio* digital asli.

$$v = \begin{cases} v = \tilde{v}, & \text{if } QET = 0 \\ v = \left\lceil \frac{\tilde{v}}{2} \right\rceil, & \text{if } QET = 1 \end{cases} \quad (9)$$

$$y = \begin{cases} y_0 = \tilde{y}_0 \\ y_1 = \tilde{y}_1 + v \end{cases} \quad (10)$$

$$x = \begin{cases} x_0 = y_0 + \tilde{z}_0 \\ x_1 = y_1 + \tilde{z}_1 \end{cases} \quad (11)$$

HASIL DAN PEMBAHASAN

Pengujian metode yang diusulkan dilakukan secara menyeluruh untuk membandingkan performa, kapasitas muatan, dan kualitas audio dari teknik yang diusulkan dengan metode yang sudah ada sebagaimana dirujuk dalam referensi [30]. Untuk melakukan penilaian yang menyeluruh, simulasi dilakukan menggunakan 15 audio digital yang diambil dari kumpulan data yang disediakan oleh [40], seperti yang ditunjukkan pada Tabel 1. Eksperimen dijalankan dengan menggunakan perangkat lunak MATLAB versi 2022b pada prosesor Intel Core i5 dengan kecepatan 2,9 GHz dan memori 8 GB. Penggunaan berbagai jenis audio digital memberikan variasi dalam evaluasi, memungkinkan penilaian kinerja teknik di berbagai situasi dan kondisi yang berbeda.

a) Performa metode

Dari eksperimen yang telah dilakukan, metode yang diusulkan menunjukkan efektivitas dalam proses penyisipan dan ekstraksi. Kualitas audio tetap terjaga dengan baik setelah penyisipan, dan audio dapat dikembalikan ke bentuk aslinya tanpa kerusakan setelah ekstraksi data. Berdasarkan Tabel 2, waktu komputasi metode yang diusulkan tidak berbeda jauh dengan metode [30], meskipun metode yang diusulkan mampu menyisipkan data lebih besar dibandingkan metode [30]. Namun, jika membandingkan kapasitas penyisipan dengan waktu komputasi masing-masing metode, metode yang diusulkan jauh lebih cepat dalam semua percobaan. Pada Audio 1, metode yang diusulkan mampu menyisipkan 15.938 bit data per detik, sedangkan metode [30] hanya menyisipkan 3 bit data per detik. Pada Audio 15, metode yang diusulkan mampu menyisipkan 17.048 bit, sementara metode [30] tidak dapat menyisipkan data. Hal ini menunjukkan bahwa performa metode yang diusulkan jauh lebih unggul daripada metode [30].

Tabel 1. Kumpulan data *audio* untuk eksperimen

No	Instrumen	Name	Data	Genre
1	Cello (cel)	Audio 1	[cel][jaz_blu]0011__2	Country-Folk (cou_fol)
		Audio 2	[cel][cla]0007_1	Classical (cla)
		Audio 3	[cel][pop_roc]0060_2	Pop-Rock (pop-rock)
2	Acoustic guitar (gac)	Audio 4	[gac][jaz_blu]0549_2	Country-Folk (cou_fol)
		Audio 5	[gac][cla]0530_1	Classical (cla)
		Audio 6	[gac][pop_roc]0560_3	Pop-Rock (pop-rock)
3	Piano (pia)	Audio 7	[pia][jaz_blu]1348_1	Country-Folk (cou_fol)
		Audio 8	[pia][cla]1291_1	Classical (cla)
		Audio 9	[pia][pop_roc]1306_1	Pop-Rock (pop-rock)
4	Saxophone (sac)	Audio 10	[sax][jaz_blu]1605_2	Country-Folk (cou_fol)
		Audio 11	[sax][cla]1598_1	Classical (cla)
		Audio 12	[sax][pop_roc]1588_1	Pop-Rock (pop-rock)
5	Human Singing Voice (voi)	Audio 13	[voi][jaz_blu]2358_1	Country-Folk (cou_fol)
		Audio 14	[voi][nod][cou_fol]2442_1	Classical (cla)
		Audio 15	[pop_roc]2547_3	Pop-Rock (pop-rock)

b) Kapasitas penyisipan

Kapabilitas penyisipan data pada *audio* dihitung dalam satuan bit per sampel (bps) berdasarkan jumlah bit yang dapat disisipkan dalam *audio* dibagi dengan total sampel *audio*. Tabel 3 menunjukkan perbandingan kapasitas penyisipan data antara metode yang diusulkan dan metode [30]. Hasil pengujian menunjukkan bahwa metode yang diusulkan secara konsisten memiliki kapasitas penyisipan yang tinggi di semua *audio*, dan dibandingkan dengan metode [30], metode yang diusulkan menunjukkan kapasitas penyisipan yang jauh lebih tinggi, dengan rata-rata 0,25 bps dibandingkan dengan metode [19] yang hanya 0,0004 bps. Gambar 3 menampilkan perbandingan kapasitas penyisipan metode yang diusulkan pada semua data uji.

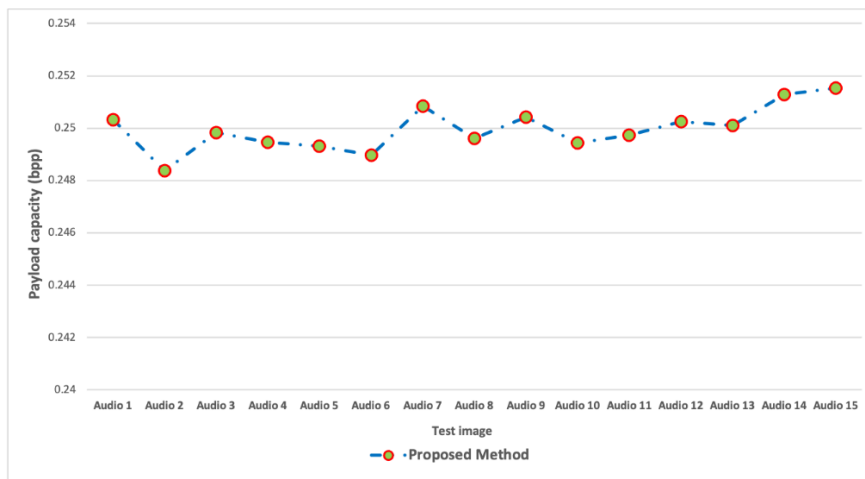
Tabel 2. Perbandingan waktu komputasi dengan metode terdahulu

No	Audio digital	Capacity (bits)		Computational Time (Second)		Embedding Data in 1s	
		Metode [30]	Proposed method	Metode [30]	Proposed method	Metode [30]	Proposed method
1	Audio 1	12	66.237	3,93	4,16	3	15.938
2	Audio 2	76	65.722	3,93	3,93	19	16.706
3	Audio 3	1	66.106	3,93	3,95	0	16.719
4	Audio 4	8	66.007	3,97	3,91	2	16.877
5	Audio 5	50	65.964	3,94	3,92	13	16.815
6	Audio 6	3	65.877	3,93	3,92	1	16.801
7	Audio 7	764	66.368	4,00	3,92	191	16.931
8	Audio 8	18	66.049	3,94	3,94	5	16.772
9	Audio 9	5	66.260	3,92	3,90	1	16.981
10	Audio 10	13	65.999	3,91	3,90	3	16.927
11	Audio 11	20	66.081	3,91	3,91	5	16.909
12	Audio 12	2	66.215	3,92	3,92	1	16.892
13	Audio 13	425	66.179	3,91	3,95	109	16.767
14	Audio 14	2	66.491	3,91	3,90	1	17.053
15	Audio 15	0	66.555	3,87	3,90	0	17.048

Tabel 3. Perbandingan kapasitas penyisipan dengan metode terdahulu

No	Audio digital	Capacity (bits)		Payload capacity (bps)	
		Metode [30]	Proposed method	Metode [30]	Proposed method
1	Audio 1	12	66.237	0,0000	0,2503
2	Audio 2	76	65.722	0,0003	0,2484
3	Audio 3	1	66.106	0,0000	0,2498
4	Audio 4	8	66.007	0,0000	0,2495
5	Audio 5	50	65.964	0,0002	0,2493
6	Audio 6	3	65.877	0,0000	0,2490
7	Audio 7	764	66.368	0,0029	0,2508
8	Audio 8	18	66.049	0,0001	0,2496

9	Audio 9	5	66.260	0,0000	0,2504
10	Audio 10	13	65.999	0,0000	0,2494
11	Audio 11	20	66.081	0,0001	0,2497
12	Audio 12	2	66.215	0,0000	0,2503
13	Audio 13	425	66.179	0,0016	0,2501
14	Audio 14	2	66.491	0,0000	0,2513
15	Audio 15	0	66.555	0,0000	0,2515



Gambar 4. Perbandingan kapasitas penyisipan dari metode yang diusulkan pada semua data uji

c) Kualitas *audio*

Analisis kualitas *audio* dilakukan untuk memahami dampak penyisipan data terhadap *audio* dan menentukan hubungan antara kapasitas penyisipan dengan kualitas *audio* setelah penyisipan data. *Peak Signal-to-Noise Ratio* (PSNR) digunakan untuk menganalisis dan membandingkan kualitas *audio* sesuai persamaan (12). Evaluasi juga mencakup variasi ukuran data mulai dari 1 kb hingga 65 kb dengan interval 5 kb. Terakhir, pengujian dilakukan dengan memasukkan data secara maksimal ke dalam *audio*.

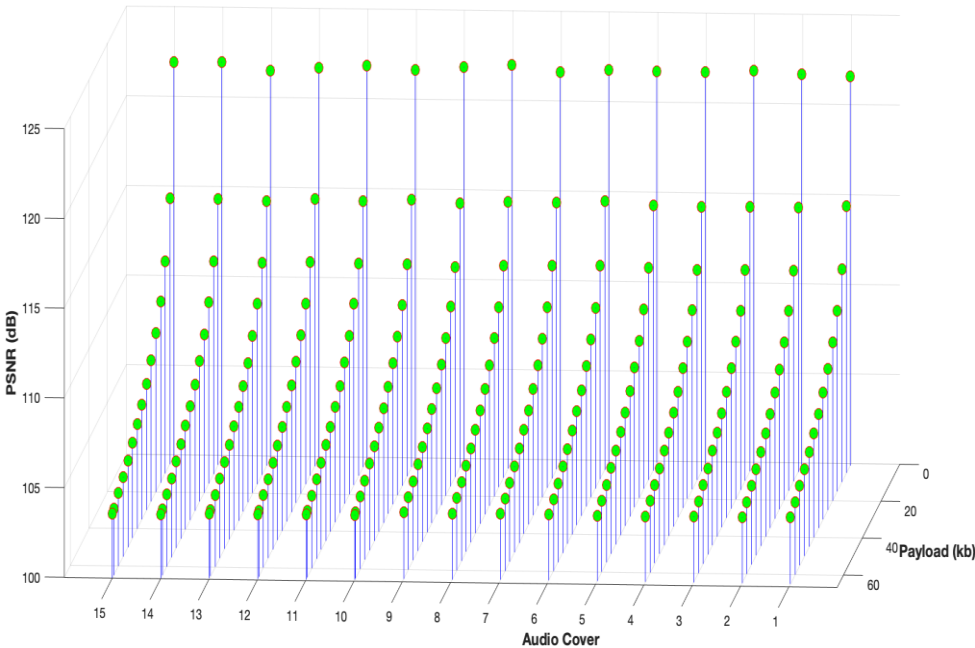
$$PSNR = 10 \log_{10} \frac{255^2}{\frac{1}{m \times n} \sum_i^{m-1} \sum_j^{n-1} |I(i,j) - I'(i,j)|^2} \quad (12)$$

Tabel 4. Perbandingan kualitas *audio stego* menggunakan PSNR

No	Audio Digital	Payload capacity (bps)		PSNR (dB)	
		Metode [30]	Proposed method	Metode [30]	Proposed method

1	Audio 1	0,0000	0,2503	135,6417	103,6028
2	Audio 2	0,0003	0,2484	127,8602	103,6065
3	Audio 3	0,0000	0,2498	na	103,5945
4	Audio 4	0,0000	0,2495	143,5656	103,5769
5	Audio 5	0,0002	0,2493	129,1252	103,5894
6	Audio 6	0,0000	0,2490	145,7841	103,6254
7	Audio 7	0,0029	0,2508	117,9930	103,5855
8	Audio 8	0,0001	0,2496	134,4275	103,5988
9	Audio 9	0,0000	0,2504	140,1414	103,6115
10	Audio 10	0,0000	0,2494	136,5759	103,6143
11	Audio 11	0,0001	0,2497	135,1147	103,6314
12	Audio 12	0,0000	0,2503	119,9408	103,6167
13	Audio 13	0,0016	0,2501	119,8809	103,6075
14	Audio 14	0,0000	0,2513	150,5553	103,5789
15	Audio 15	0,0000	0,2515	na	103,5869

Berdasarkan Tabel 4 dapat dilihat bahwa kualitas *audio* dari metode yang diusulkan tidak jauh berbeda dengan metode [19] walaupun penyisipan data dari metode yang diusulkan jauh lebih tinggi, seperti pada Audio 1, metode [19] memiliki PSNR 135,6417 dB sedangkan metode yang diusulkan memiliki PSNR 103,6028 dB. Begitu juga dengan Audio 7, metode [19] memiliki PSNR 117,9930 dB sedangkan metode yang diusulkan memiliki PSNR 103,5855 dB. Berdasarkan Gambar 4, terlihat bahwa semakin besar data yang disisipkan pada *audio* maka kualitas *audio* semakin menurun.



Gambar 5. Perbandingan kualitas audio stego dari metode yang diusulkan dengan penyisipan data bervariasi

SIMPULAN

Perkembangan teknologi informasi dan komunikasi yang pesat memberikan kemudahan dalam berbagai aspek kehidupan, tetapi juga menghadirkan tantangan tersendiri, terutama terkait keamanan data dan privasi. Kriptografi dan steganografi adalah dua teknik yang digunakan untuk melindungi data. Kriptografi melindungi informasi dengan mengenkripsi pesan, sementara steganografi menyembunyikan keberadaan data dalam media lain. Penyisipan data dalam media seperti gambar, *audio*, dan *video* memerlukan metode khusus agar media tidak mengalami kerusakan setelah ekstraksi data. Dalam penelitian ini, kami mengusulkan metode penyisipan data yang dapat dikembalikan ke bentuk aslinya tanpa kerusakan, menggunakan metode *Difference Expansion* dan *Fungsi Modulus*. Metode ini diimplementasikan pada *audio* digital dengan menyisipkan data pada selisih 2-bit LSB pasangan sampel *audio*. Berdasarkan eksperimen yang dilakukan pada 15 *audio* digital, metode yang diusulkan menunjukkan kapasitas penyisipan data yang tinggi dengan kualitas *audio* yang baik. Metode ini dapat mencapai kapasitas penyisipan sebesar 0,2515 bps (bit per sampel) dengan PSNR 103,5869 dB. Hasil eksperimen membuktikan bahwa metode yang diusulkan unggul dibandingkan metode sebelumnya.

DAFTAR PUSTAKA

- [1] T. Ahmad, M. H. Amrizal, W. Wibisono, and R. M. Ijtihadie, "Hiding data in audio files: A smoothing-based approach to improve the quality of the stego audio," *Heliyon*, vol. 6, no. 3, p. e03464, 2020, doi: <https://doi.org/10.1016/j.heliyon.2020.e03464>.
- [2] R. Setiawan and T. Ahmad, "Improving the Performance of Data Hiding by Designing Three Samples-based Smoothing in Audio," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 2, pp. 196–204, Apr. 2020, doi: 10.22266/ijies2020.0430.19.
- [3] M. Al-Hooti and T. Ahmad, "Reversible Data Hiding in Audio Based on Discrete Cosine Transform and Location Maps," *Int. J. Intell. Eng. Syst.*, vol. 12, no. 3, pp. 41–49, Jun. 2019, doi: 10.22266/ijies2019.0630.05.
- [4] M. M. Amrulloh and T. Ahmad, "Minimizing Sample Space to Optimize Quality of Stego-Audio," *Int. J. Intell. Eng. Syst.*, vol. 15, no. 3, 2022, doi: 10.22266/ijies2022.0630.17.
- [5] A. Arham and N. Lestari, "Arnold's cat map secure multiple-layer reversible watermarking," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 33, no. 3, p. 1536, Mar. 2024, doi: 10.11591/ijeecs.v33.i3.pp1536-1545.
- [6] F. R. Shareef, "A novel crypto technique based ciphertext shifting," *Egypt. Informatics J.*, vol. 21, no. 2, pp. 83–90, Jul. 2020, doi: 10.1016/j.eij.2019.11.002.
- [7] A. Arham and H. Adi Nugroho, "Block-based optimization for enhancing reversible watermarking using reduce difference expansion," *Commun. Sci. Technol.*, vol. 9, no. 1, pp. 57–64, Jul. 2024, doi: 10.21924/cst.9.1.2024.1368.
- [8] Y.-T. Lin, C.-M. Wang, W.-S. Chen, F.-P. Lin, and W. Lin, "A Novel Data Hiding Algorithm for High Dynamic Range Images," *IEEE Trans. Multimed.*, vol. 19, no. 1, pp. 196–211, 2017, doi: 10.1109/TMM.2016.2605499.
- [9] M. B. Andra, T. Ahmad, and T. Usagawa, "Medical record protection with improved grde data hiding method on audio files," *Eng. Lett.*, vol. 25, no. 2, pp. 112 – 124, 2017, [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85019720247&partnerID=40&md5=a94371952e1074e7c4f3fa18581180c5>.

- [10] M. Ramalingam and N. A. M. Isa, "A data-hiding technique using scene-change detection for video steganography," *Comput. Electr. Eng.*, vol. 54, pp. 423–434, 2016, doi: <https://doi.org/10.1016/j.compeleceng.2015.10.005>.
- [11] A. A.-A. Gutub and K. A. Alaseri, "Refining Arabic text stego-techniques for shares memorization of counting-based secret sharing," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 9, pp. 1108–1120, 2021, doi: <https://doi.org/10.1016/j.jksuci.2019.06.014>.
- [12] S. Al-Nofaie, A. Gutub, and M. Al-Ghamdi, "Enhancing Arabic text steganography for personal usage utilizing pseudo-spaces," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 8, pp. 963–974, 2021, doi: <https://doi.org/10.1016/j.jksuci.2019.06.010>.
- [13] T. T. Manunggal and D. Arifianto, "Data protection using interaural quantified-phase steganography on stereo audio signals," in *2016 IEEE Region 10 Conference (TENCON)*, 2016, pp. 3817–3821, doi: 10.1109/TENCON.2016.7848778.
- [14] A. Miri and K. Faez, "Adaptive image steganography based on transform domain via genetic algorithm," *Optik (Stuttg.)*, vol. 145, pp. 158–168, 2017, doi: <https://doi.org/10.1016/j.ijleo.2017.07.043>.
- [15] S. Kumar, B. K. Singh, and M. Yadav, "A Recent Survey on Multimedia and Database Watermarking," *Multimed. Tools Appl.*, vol. 79, no. 27–28, pp. 20149–20197, Jul. 2020, doi: 10.1007/s11042-020-08881-y.
- [16] A. Arham, H. A. Nugroho, and T. B. Adji, "Multiple Layer Data Hiding Scheme Based on Difference Expansion of Quad," *Signal Processing*, vol. 137, pp. 52–62, 2017, doi: 10.1016/j.sigpro.2017.02.001.
- [17] A. Arham and N. Lestari, "Secure medical image watermarking based on reversible data hiding with Arnold's cat map," *Int. J. Adv. Intell. Informatics; Vol 9, No 3 Novemb. 2023*, 2023, doi: 10.26555/ijain.v9i3.1029.
- [18] A. Arham, H. A. Nugroho, and T. B. Adji, "Combination schemes Reversible Data Hiding for medical images," in *Proceedings - 2016 2nd International Conference on Science and Technology-Computer, ICST 2016*, 2017, pp. 44–49, doi: 10.1109/ICSTC.2016.7877345.
- [19] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, 2003, doi: 10.1109/TCSVT.2003.815962.
- [20] J. Tian, "Wavelet-based reversible watermarking for authentication," in *Security and Watermarking of Multimedia Contents IV*, 2002, vol. 4675, pp. 679–690, doi: 10.1117/12.465329.
- [21] A. M. Alattar, "Reversible watermark using difference expansion of triplets," in *IEEE International Conference on Image Processing, ICIP'2003*, 2003, vol. 1, pp. I-501–4 vol.1, doi: 10.1109/ICIP.2003.1247008.
- [22] A. M. Alattar, "Reversible watermark using difference expansion of quads," in *IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2004, vol. 3, pp. iii-377–80 vol.3, doi: 10.1109/ICASSP.2004.1326560.
- [23] J.-Y. Hsiao, K.-F. Chan, and J. M. Chang, "Block-based reversible data embedding," *Signal Processing*, vol. 89, no. 4, pp. 556–569, 2009, doi: 10.1016/j.sigpro.2008.10.018.
- [24] C.-L. Liu, D.-C. Lou, and C.-C. Lee, "Reversible Data Embedding Using Reduced Difference Expansion," in *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2007, vol. 1, pp. 433–436, doi: 10.1109/IIH-MSP.2007.267.
- [25] H. Yi, S. Wei, and H. Jianjun, "Improved reduced difference expansion based reversible data hiding scheme for digital images," in *International Conference on Electronic Measurement & Instruments*, 2009, pp. 4–318, doi: 10.1109/ICEMI.2009.5274054.
- [26] T. Ahmad, M. Holil, W. Wibisono, and I. Royyana Muslim, "An improved Quad and RDE-based medical data hiding method," in *Proceeding - IEEE CYBERNETICSCOM 2013: IEEE International Conference on Computational Intelligence and Cybernetics*, 2013, pp. 141–145, doi: 10.1109/CyberneticsCom.2013.6865798.
- [27] M. H. A. Al Huti, T. Ahmad, and S. Djanali, "Increasing the capacity of the secret data

- using DEpixels blocks and adjusted RDE-based on grayscale images," in *International Conference on Information & Communication Technology and Systems*, 2015, pp. 225–230, doi: 10.1109/ICTS.2015.7379903.
- [28] Z. Syahlan and T. Ahmad, "Reversible data hiding method by extending reduced difference expansion," *Int. J. Adv. Intell. Informatics*, vol. 5, no. 2, pp. 101–112, 2019, doi: 10.26555/ijain.v5i2.351.
- [29] S. M. Abdullah and A. A. Manaf, "Multiple Layer Reversible Images Watermarking Using Enhancement of Difference Expansion Techniques," in *Networked Digital Technologies: Second International Conference, NDT 2010, Prague, Czech Republic, July 7-9, 2010. Proceedings, Part I 2*, 2010, pp. 333–342, doi: 10.1007/978-3-642-14292-5_35.
- [30] P. Maniriho and T. Ahmad, "Information hiding scheme for digital images using difference expansion and modulus function," *J. King Saud Univ. Inf. Sci.*, vol. 31, no. 3, pp. 335–347, 2019, doi: 10.1016/j.jksuci.2018.01.011.
- [31] M. S. Hossen, T. Ahmad, and N. J. D. L. Croix, "Data Hiding Scheme using Difference Expansion and Modulus Function," in *2023 2nd International Conference for Innovation in Technology (INOCON)*, 2023, pp. 1–6, doi: 10.1109/INOCON57975.2023.10100991.
- [32] A. Arham and O. S. Riza, "Reversible Data Hiding Using Hybrid Method of Difference Expansion on Medical Image," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 6, no. 2, pp. 11–19, 2020, doi: 10.26555/jiteki.v6i2.16965.
- [33] A. Arham, "Penyisipan Data Secara Reversible Pada Gambar Medis Menggunakan Metode Difference Expansion of Quad dan Fungsi Modulus," *JOSTECH J. Sci. Technol.*, vol. 4, no. 1, pp. 29–38, 2024, doi: 10.15548/jostech.v4i1.8257.
- [34] A. Arham, R. Rahmawati, and O. S. Riza, "Reversible Data Hiding pada Audio Digital Berbasis Difference Expansion," *Insearch Inf. Syst. Res. J.*, vol. 2, no. 01, pp. 28–35, 2022, doi: 10.15548/isrj.v2i01.4101.
- [35] K. Satish, T. Jayakar, C. Tobin, K. Madhavi, and K. Murali, "Chaos based spread spectrum image steganography," *IEEE Trans. Consum. Electron.*, vol. 50, no. 2, pp. 587–590, 2004, doi: 10.1109/TCE.2004.1309431.
- [36] S. Shen, L. Huang, and Q. Tian, "A novel data hiding for color images based on pixel value difference and modulus function," *Multimed. Tools Appl.*, vol. 74, no. 3, pp. 707–728, 2015, doi: 10.1007/s11042-014-2016-0.
- [37] Y. Kurniawan, L. A. Rahmania, T. Ahmad, W. Wibisono, and R. M. Ijtihadie, "Hiding secret data by using modulo function in quad difference expansion," in *2016 International Conference on Advanced Computer Science and Information Systems (ICACISIS)*, 2016, pp. 433–438, doi: 10.1109/ICACISIS.2016.7872741.
- [38] I. B. Prayogi and T. Ahmad, "Audio-based Data Hiding using All-in Modulo of Difference," in *2021 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, Jul. 2021, pp. 129–134, doi: 10.1109/ISITIA52817.2021.9502235.
- [39] M. H. A. Al-Hooti, S. Djanali, and T. Ahmad, "Audio Data Hiding Based on Sample Value Modification Using Modulus Function," *J. Inf. Process. Syst.*, vol. 12, no. 3, pp. 525–537, 2016, doi: 10.3745/JIPS.03.0054.
- [40] "IRMAS: a dataset for instrument recognition in musical audio signals." <https://www.upf.edu/web/mtg/irmas> (accessed Apr. 01, 2024).