Focus **ACT**ion **O**f **R**esearch **M**athematic
Volume 6, No. 02, July – December, 2023
Page 112-124

ISSN: 2655-3511 (print)
ISSN: 2656-307X (online)
DOI:10.30762/f_m.v6i2. 1678

Implementasi Teori Koding dengan Kode Hamming yang Diperluas pada Steganografi

Nur Hamid[1], Nurul Jannah[2*]
[1,2] Pendidikan Matematika, Universitas Nurul Jadid Paiton Probolinggo, Indonesia
**Penulis Korespondensi. Kotaanyar, 67293, Kab. Probolinggo, Indonesia*
E-mail: *nurhamid@unuja.ac.id* [1)]
nuruljannah05102001@gmail.com [2*)]

Kata Kunci

Kode Linier, Kode Hamming yang diperluas, steganografi

Linear code, extended Hamming code, steganography

ABSTRAK

Keamanan data perlu diperhatikan agar terhindar dari kebisingan saat pengiriman data atau pembobolan data oleh peretas. Dalam artikel ini, diimplementasikan pengamanan data dengan menggunakan gabungan teori koding dan steganografi. Kode yang digunakan adalah kode Hamming yang diperluas [8,4]. Media yang digunakan adalah gambar *grayscale* berukuran 360×640 dengan panjang karakter yang disisipkan sebanyak 50,100,150,200,250 dan 300 karakter dengan 6 kali percobaan. Sebagai tambahan, ditampilkan nilai PSNR yang diperoleh dan juga waktu komputasi.

Data security needs to be considered to avoid noise when sending data or data breaches by hackers. In this article, we implement data security using a combination of coding theory and steganography. The code used is an extended Hamming code [8.4]. The media used is a grayscale image of size 360×640 *of lengths 50,100,150,200,250 and 300 characters with 6 attempts. In addition, we show the PSNR result obtained and also the computation time.*

PENDAHULUAN

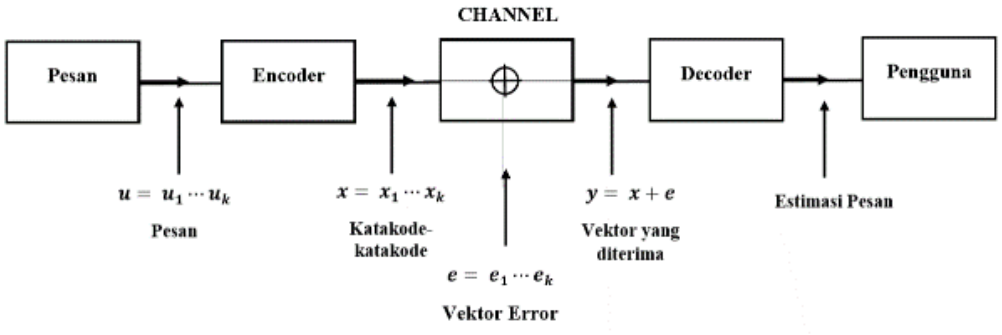
Perkembangan teknologi mempermudah masyarakat saat ini untuk melakukan berbagai aktivitas dalam satu waktu. Masyarakat dapat bertukar pesan dan data tanpa batas tempat. Tentunya, pertukaran pesan dan pemindahan data dapat dilakukan dengan mudah.

Meski demikian, tidak dipungkiri bahwa ada kemungkinan terjadi kesalahan saat pengiriman pesan. Hal ini disebabkan oleh adanya kebisingan atau juga terjadi

pembobolan data oleh pihak yang tidak bertanggung jawab.

Berdasarkan catatan Tempo dari Januari hingga September 2022, telah terjadi tujuh kasus besar dugaan kebocoran data pribadi di wilayah Indonesia. Kasus tersebut contohnya adalah kasus kebocoran data Bank Indonesia yang terjadi pada Januari 2022. Terdapat kurang lebih 16 komputer di Kantor Cabang Bank Indonesia di Bengkulu mengalami kebocoran dan terselesaikan oleh Badan Siber dan Sandi Negara (BSSN). Faktanya, hal ini tidak hanya terjadi di Kantor Cabang Bengkulu, namun juga di 20 kota lainnya dengan jumlah dokumen lebih dari 52 ribu dengan ukuran sebesar 74,82 GB dan berasal dari 200 komputer (Nurhadi, 2022).

Salah satu cara memperbaiki kesalahan saat pengiriman pesan adalah dengan teori koding. Skema pesan dengan teori koding dapat dilihat pada Gambar 1.



Gambar 1. Skema Komunikasi

Teori koding bermula dari penelitian Shannon pada tahun 1948. Shannon menjelaskan konsep awal tentang teori koding untuk mendeteksi adanya kesalahan dan memungkinkan untuk melakukan pengoreksian, sehingga masalah mendasar dalam teori koding adalah menentukan pesan apa yang dikirim berdasarkan apa yang diterima. Hingga saat ini teori koding telah berkembang pesat, sehingga memunculkan berbagai jenis kode, salah satunya adalah kode linier (Riyanto, 2020).

Kode linier adalah tipe kode yang sangat sering dipelajari karena mudah untuk dipahami dan tentunya memiliki sifat linieritas (MacWilliams & Sloane, 1977). Salah satu kode linier yang biasa digunakan adalah Kode Hamming. Kode Hamming adalah salah satu kode untuk mengoreksi kesalahan yang dapat terjadi saat data komputer dikirim, dipindahkan, atau disimpan. Kode Hamming [7,4] dan kode Hamming yang diperluas [8,4] merupakan kode Hamming yang sering digunakan.

Kode Hamming juga sering digunakan dalam steganografi, yakni salah satu cabang ilmu penyisipan pesan pada suatu gambar atau media lain. Sebagai contoh, kode Hamming [7,4] digunakan pada proses steganografi dengan melibatkan media berupa video (Mstafa & Elleithy, 2014).

Steganografi dengan melibatkan kode linier pernah juga dibahas oleh Rahman, Khalil, dan Xun Yi (Rahman dkk., 2021). Mereka mengembangkan sebuah pendekatan steganografi biosignal reversibel menggunakan metode koreksi kesalahan berdasarkan kode Golay biner yang diperluas atau *extended Binary Golay Code*. Metode tersebut digunakan untuk mengesktrak pesan rahasia dan merekontruksi biosignal asli agar terhindar dari kerusakan saat dilakukan pengalihdayaan ke *cloud* dan terhindar dari pemangku kepentingan lain.

Pembahasan yang lebih spesifik terkait steganografi dilakukan oleh Subramanian, Elharrouss, Al-Maadeed, dan Bouridane. Mereka mengeksplorasi dan mendiskusikan steganografi dengan berbagai metode *deep learning* atau teknik pembelajaran yang mendalam (Subramanian dkk., 2021). Teknik yang digunakan untuk steganografi pada media gambar dibagi menjadi tiga, yakni metode tradisional, berbasis *Convolutional Neural Network* dan *General Adversarial Network*. Steganografi yang melibatkan kode linier juga dibahas pada (Um dkk., 2020), (P dkk., 2020), (Malathi & Kumar, 2021), (Vien dkk., 2021) dan (Wu dkk., 2020).

Berdasarkan uraian sebelumnya, pada artikel ini diimplementasikan sebuah model penyisipan pesan pada suatu gambar dengan melibatkan kode Hamming yang diperluas atas lapangan biner. Dengan adanya kode tersebut, pesan yang dikirim dapat diperbaiki jika terjadi kesalahan. Selain itu, penyisipan pesan pada gambar dapat mengamankan pesan dari hal-hal yang tidak diinginkan.

METODE

Penelitian ini bertujuan untuk mengetahui penggunaan kode Hamming yang diperluas atau kode Hamming [8,4] pada steganografi dan mengetahui hasil simulasi penyisipan pesan pada gambar dengan melibatkan kode Hamming yang diperluas atas lapangan biner.

Penelitian ini menggunakan metode *Least Significant Bit* (LSB), salah satu algoritma steganografi yang digunakan untuk menyembunyikan pesan rahasia pada suatu media, seperti gambar,

video, atau media lainnya. Informasi rahasia disisipkan pada bit-bit yang tidak terlalu signifikan dalam file media. Prinsipnya, nilai terendah atau *Least Significant Bit* (LSB) biasanya memiliki kontribusi yang paling sedikit dalam menentukan nilai keseluruhan data pada setiap bit data digital (Minarni & Redha, 2020). Media yang digunakan adalah gambar *grayscale* berukuran 360×640 dengan panjang karakter yang disisipkan sebanyak $50, 100, 150, 200, 250$ dan 300 karakter dengan 6 kali percobaan.

Kode Linier

Kode linier yang digunakan dalam artikel ini adalah ruang bagian dari ruang vector $\mathbb{F}_2^n$. Kode linier memiliki beberapa sifat linieritas dan sifat-sifat yang berkaitan dengan ruang bagian pada umumnya (MacWilliams & Sloane, 1977). Sebuah kode linier $[n, k]$ memiliki 2^k anggota yang dinamakan katakode dengan k merupakan dimensi dari kode linier dan n merupakan panjang masing-masing katakode.

Kode Hamming yang Diperluas $[8,4]$

Definisi 1**.** Sebuah kode Hamming biner H_r dengan panjang $n = 2^r - 1$ $(r \geq 2)$ memiliki matriks cek paritas H yang kolom-kolomnya terdapat semua vektor biner bukan nol dengan panjang r. Kode H_r adalah sebuah kode $[\, n, k = 2^r - 1 - r, d = 3\,]$.

Kode Hamming adalah kode *single-error-correcting* yang sempurna (MacWilliams & Sloane, 1977). Kode ini adalah salah satu pendeteksi kesalahan yang mampu mendeteksi beberapa kesalahan, namun hanya mampu mengoreksi satu kesalahan. Berdasarkan Teorema Koreksi dan Deteksi (MacWilliams & Sloane, 1977), maka kode Hamming yang memiliki $d = 3$ dapat mengoreksi $\frac{1}{2}(3-1) = 1$ kesalahan.

Kode Hamming yang digunakan pada artikel ini adalah kode Hamming yang diperluas $[8, 4]$ dengan matriks pembangun G, yakni

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Pertama, pesan (m_1, m_2, m_3, m_4) dengan panjang k bit $(k = 4)$ dikodekan dengan menambah 4 bit paritas (p_1, p_2, p_3, p_4) sehingga katakode yang terbentuk adalah kombinasi seperti $(m_1, m_2, m_3, m_4, p_1, p_2, p_3, p_4)$

Kode Hamming adalah kode linier yang memiliki dua matriks yakni matriks cek paritas H dan matriks pembangun G yang berfungsi pada proses enkode dan dekode. Pada proses enkode, setiap pesan (m_1, m_2, m_3, m_4) akan dikalikan dengan

matriks pembangun G dengan penggunaan modulo 2 . Hasil yang terbentuk adalah katakode X yang terdiri dari 8 bit.

Katakode tersebut akan digunakan untuk penyisipan pesan. Berikut adalah model Enkode menggunakan Kode Hamming yang diperluas $[8,4]$.

$$X = M\,G$$

dengan

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Tahap dekode bertujuan untuk mendeteksi pesan yang diterima. Pesan tersebut dikalikan dengan transpose dari matriks cek paritas H dengan modulo 2. Berikut adalah model dekode menggunakan Kode Hamming yang diperluas $[8,4]$.

$$\boldsymbol{Z} = XH^{tr}$$

dengan

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Hasil dari sebuah vektor $Z\,(z_1, z_2, z_3)$ harusnya berisi (000) jika tidak ada kesalahan dari pesan. Sebaliknya, maka hal ini membutuhkan proses pengoreksian kesalahan.

Contoh 1. Asumsikan bahwa diketahui sebuah pesan $M_1\,(1,0,1,1)$ dan kode Hamming yang diperluas $[8,4]$, proses enkode dan dekode seperti berikut;

1. Pada tahap enkode, hitung $X = M_1\,G$, diperoleh sebuah katakode $X = 10110100$.
2. Pada tahap dekode, untuk memperoleh pesan yang benar maka vektor Z harus nol. Asumsi yang pertama misal diperoleh $X = 10110100$ tanpa ada kesalahan, maka Z akan menjadi (000) yang artinya tidak terdapat kesalahan pada pesan.
3. Asumsi yang kedua saat pesan yang diterima terdapat kesalahan, namun pada penelitian ini diasumsikan bahwa semua pesan yang diterima tidak terdapat kesalahan sehingga tidak membutuhkan asumsi yang kedua ini.

Alur Program Enkode dan Penyisipan Pesan

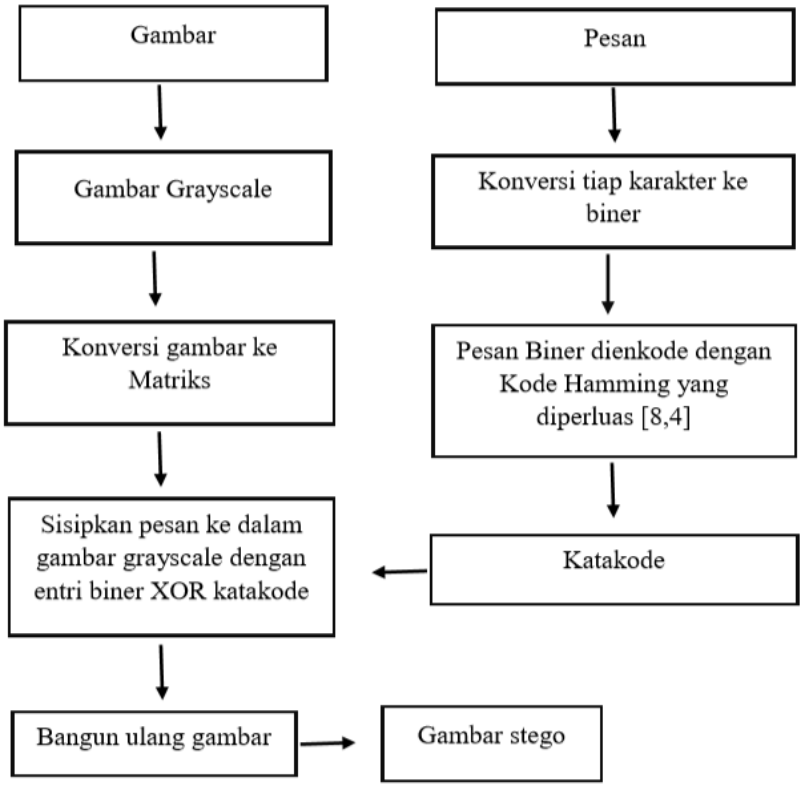
Alur program enkode dan penyisipan pesan pada media gambar digital sebagai berikut:

1. Menerima masukan pesan yang akan disisipkan.
2. Konversi pesan menjadi bilangan biner dengan panjang 8 bit.
3. Pada tahap ini akan dilakukan proses enkode menggunakan kode Hamming yang diperluas $[8,4]$ dengan matriks cek paritas H dan matriks pembangun

G. Kode ini memiliki jarak minimum $d = 3$, dapat mendeteksi 2 kesalahan dan mengoreksi 1 kesalahan dengan laju informasi $\frac{1}{2}$. Bilangan biner yang terbentuk akan dibagi menjadi 2 bagian dan asumsikan sebagai M_1 dan M_2 . Gunakan Persamaan $X = M\,G$ untuk menghasilkan katakode. Dalam hal ini, 1 karakter akan menjadi 2 katakode.

4. Pada tahap ini akan dilakukan proses penyisipan pesan menggunakan LSB pada media gambar grayscale. 2 Katakode akan disisipkan pada setiap baris dari gambar grayscale secara berdampingan. XOR katakode dengan elemen pada gambar. Hasilnya akan menggantikan posisi elemen tersebut.
5. Bangun ulang gambar yang sudah tersisipkan pesan (gambar stego)

Secara umum, alur program enkode dan penyisipan pesan dapat dilihat pada Gambar 2.



Gambar 2. Alur Program Enkode dan Penyisipan Pesan

Alur Program Ekstraksi dan Dekode Pesan

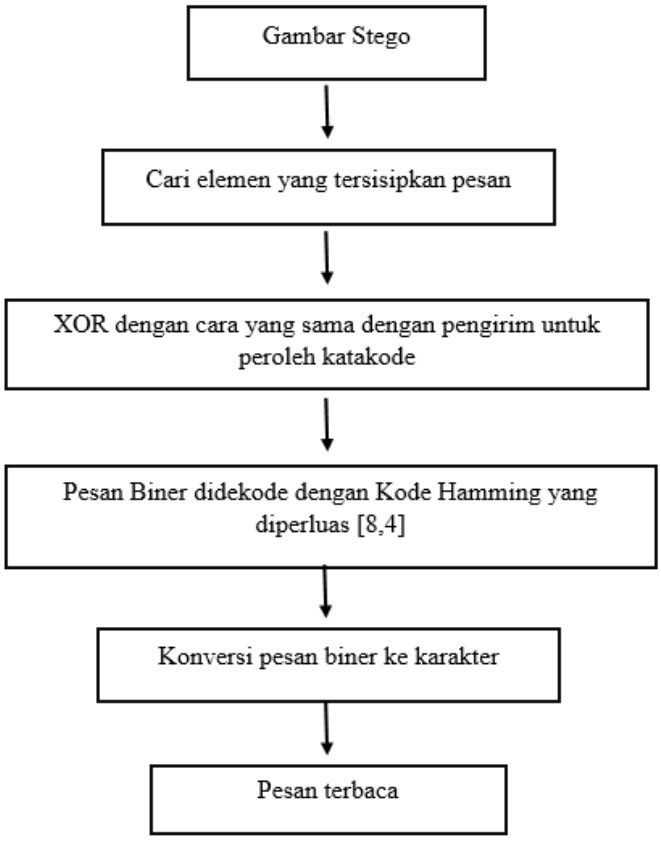
Alur program ekstraksi pesan dari gambar stego dan dekode pesan:

1. Cari elemen dari matriks gambar stego yang tersisipkan pesan.
2. Dengan asumsi penerima juga memiliki gambar *grayscale*, XOR

elemen tersebut dengan elemen pada gambar grayscale pada posisi yang sama. Hasilnya akan diperoleh 2 katakode.

3. Proses dekode sama dengan pada Contoh 1. Pada simulasi ini, diasumsikan bahwa tidak ada kebisingan atau kesalahan pada pesan. Sehingga hasil dekode adalah (000), artinya tidak ada kesalahan pesan.
4. Karakter pesan diperoleh dari 4 bit pertama dari tiap katakode pada setiap baris. Gabungkan 4 bit dari katakode tersebut untuk menjadi bilangan biner dengan panjang 8 bit pada setiap baris.
5. Ubah bilangan biner menjadi karakter dan susun menjadi sebuah pesan yang diterima.

Secara umum, alur program ekstraksi dan dekode pesan dapat dilihat pada Gambar 3.



Gambar 3. Alur Program Ekstraksi dan Penyisipan Pesan

HASIL DAN PEMBAHASAN

Perancangan simulasi data sesuai dengan alur program pada Gambar 2 dan

3. Kode yang digunakan adalah kode Hamming yang diperluas $[8,4]$ atas $\mathbb{F}_2$ atau $GF(2)$. Data yang digunakan adalah teks yang akan disisipkan pada sebuah gambar. Teks pesan yang dikonversi ke bentuk bilangan biner menggunakan Tabel *American Standard Code for Information Interchange* (ASCII) seperti pada Gambar 4.

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[END OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Gambar 4. American Standard Code for Information Interchange (ASCII)

Gambar yang digunakan sebagai tempat penyisipan pesan adalah gambar grayscale. Gambar dalam Python adalah list 2 dimensi yang elemen-elemennya adalah bilangan bulat $0,\cdots,255$. Untuk memanipulasi gambar, digunakan modul Python yaitu OpenCV (http://opencv.org) yang sudah tersedia pada *Google Colab*.

Dari program simulasi yang sudah dijalankan, dapat diperoleh gambar steganografi, *Pick Signal to Noise Rasio* (PSNR), dan waktu komputasi.

Hasil Gambar Steganografi

Gambar grayscale yang digunakan berukuran 360×640. Sehingga ada batasan dalam menentukan panjang pesan pada simulasi. Banyaknya karakter pesan yang dapat diterapkan pada gambar berukuran 360×640 ini harus kurang dari baris matriks gambar grayscale, yakni 359. Panjang karakter yang digunakan pada program simulasi adalah $50, 100, 150, 200, 250$ dan 300 karakter dengan 6 kali percobaan. Gambar di bawah ini adalah Gambar grayscale yang digunakan pada simulasi ini.

Focus **ACT**ion **O**f **R**esearch **M**athematic
Volume 6, No. 02, July – December, 2023
Page 112-124

ISSN: 2655-3511 (print)
ISSN: 2656-307X (online)
DOI:10.30762/f_m.v6i2. 1678

Gambar 5. Grayscale

Berdasarkan proses enkode dan penyisipan pesan pada Gambar 5, diperoleh gambar-gambar hasil steganografi sesuai dengan banyaknya karakter (N) yang disisipkan, sebagai berikut.

N = 50, PSNR = 56.760 dB

N = 100, PSNR = 55.349 dB

N = 150, PSNR = 54. 218 dB

N = 200, PSNR = 53.307 dB

N = 250, PSNR = 52.750 dB

N = 300, PSNR = 52.022 dB

Gambar 6. Hasil Steganografi

Focus **ACT**ion **O**f **R**esearch **M**athematic
Volume 6, No. 02, July – December, 2023
Page 112-124

ISSN: 2655-3511 (print)
ISSN: 2656-307X (online)
DOI:10.30762/f_m.v6i2. 1678

Pick Signal to Noise Rasio (PSNR)

Pick Signal to Noise Rasio atau PSNR adalah sebuah pengukuran yang menunjukkan seberapa besar skema peningkatan dapat mengatasi efek kebisingan (Roopaei dkk., 2016). PSNR digunakan untuk melihat perbandingan nilai gambar dengan gambar yang sudah tersisipkan pesan atau kebisingan. Satuan dari PSNR adalah decibel (dB). PSNR didefinisikan dengan

$$PSNR = 10 \log 10 \left(\frac{C_{max}^2}{MSE}\right)$$

dengan

C_{max} : $nilai\ maksimum\ pixel$

MSE : $Mean\ Square\ Error$

Mean Square Error (MSE) sering digunakan sebagai ukuran tingkat keakuratan untuk gambar dan video (Keleş dkk., 2021). Namun, nilainya bergantung pada skala atau rentang yang dinamis dari gambar maupun video yang digunakan. MSE didefinisikan sebagai berikut (Sajati, 2018).

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{i=0}^{n-1} [I(i,j) - K(i,j)]^2$$

dengan

m, n : lebar, tinggi citra yang diamati

$I(i,j)$: nilai piksel asli pada koordinat (i,j)

$K(i,j)$: nilai piksel gambar yang tersisipkan pesan pada koordinat (i,j)

Berdasarkan simulasi yang sudah dilakukan, nilai PSNR setiap gambar steganografi diperoleh sebagaimana pada Tabel 1.

Berdasarkan nilai PSNR yang ditunjukkan pada Tabel 1, kualitas gambar yang dihasilkan masih sangat baik. Nilai PSNR yang tinggi menunjukkan bahwa kualitas gambar yang direkonstruksi memiliki nilai MSE yang kecil (Subramanian dkk., 2021).

Tabel 1. PSNR Setiap Gambar Steganografi

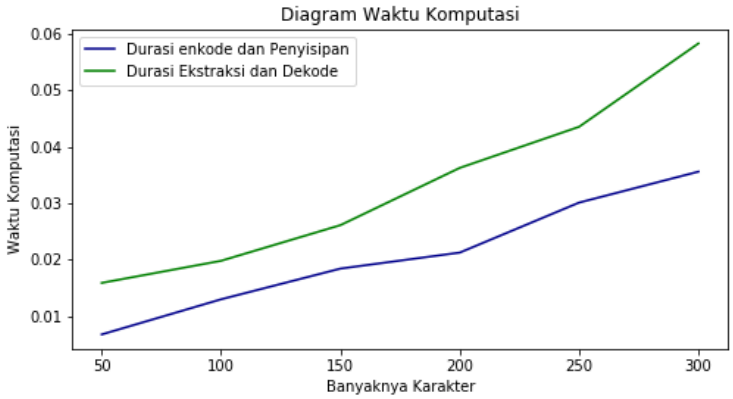
Gambar	Banyaknya karakter yang disisipkan (N)	PSNR
Stego 1	50	56.760 dB
Stego 2	100	55.349 dB
Stego 3	150	54. 218 dB
Stego 4	200	53.307 dB
Stego 5	250	52.750 dB
Stego 6	300	52.022 dB

Focus **ACT**ion **O**f **R**esearch **M**athematic
Volume 6, No. 02, July – December, 2023
Page 112-124

ISSN: 2655-3511 (print)
ISSN: 2656-307X (online)
DOI:10.30762/f_m.v6i2. 1678

Waktu Komputasi

Waktu komputasi diperoleh dari keseluruhan program simulasi yang dijalankan untuk setiap percobaan. Diagram waktu komputasi dengan satuan detik dapat dilihat di Gambar 7.



Gambar 7. Waktu Komputasi

Berdasarkan Gambar 7, dapat disimpulkan bahwa semakin banyak karakter yang disisipkan maka semakin membutuhkan waktu untuk komputasi program.

KESIMPULAN

Berdasarkan simulasi diperoleh beberapa kesimpulan, yakni pengkodean menggunakan kode Hamming yang diperluas [8,4] dapat digunakan pada proses steganografi, hasil gambar steganografi tidak jauh berbeda dari gambar asli *grayscale*, pesan yang disisipkan dapat terbaca dengan benar dengan batas banyak karakter kurang dari baris matriks gambar grayscale, dan banyak karakter yang disisipkan berbanding lurus dengan perubahan gambar dan waktu komputasi yang dibutuhkan.

Penelitian ini menggunakan pengkodean dengan kode Hamming yang diperluas [8,4] dan gambar digital sebagai media penyisipan pesan. Untuk penelitian selanjutnya, diharapkan dapat menggunakan jenis kode dan media penyisipan pesan lainnya.

UCAPAN TERIMA KASIH

Penulis pertama dan kedua mengucapkan terima kasih kepada juri kegiatan Lomba Pemodelan Tingkat Nasional dari Universitas Mulawarman. Artikel ini merupakan perbaikan karya yang disampaikan saat lomba tersebut.

DAFTAR PUSTAKA

Keleş, O., Yılmaz, M. A., Tekalp, A. M., Korkmaz, C., & Dogan, Z. (2021). *On the Computation of PSNR for a Set of Images or Video* (arXiv:2104.14868). arXiv. http://arxiv.org/abs/2104.14868

MacWilliams, F. J., & Sloane, N. J. A. (1977). *The Theory of Error-Correcting Codes* (Vol. 16).

Malathi, P., & Kumar, T. G. (2021). An efficient data hiding technique in image using binary Hamming code along with particle swarm optimisation. *International Journal of Intelligent Systems Technologies and Applications*, *20*(2), 167. https://doi.org/10.1504/IJISTA.2021.119048

Minarni, M., & Redha, R. (2020). Implementasi Least Significant Bit (LSB) dan Algoritma Vigenere Chiper pada Audio Steganografi. *Jurnal Sains dan Teknologi: Jurnal Keilmuan dan Aplikasi Teknologi Industri*, *20*(2), 168. https://doi.org/10.36275/stsp.v20i2.268

Mstafa, R. J., & Elleithy, K. M. (2014). A highly secure video steganography using Hamming code (7, 4). *IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014*, 1–6. https://doi.org/10.1109/LISAT.2014.6845191

Nurhadi. (2022). Inilah 7 Kaus Dugaan Kebocoran Data Pribadi Sepanjang 2022, (Online), (https://nasional.tempo.co/read/1632043/inilah-7-kasus-dugaan-kebocoran-data-pribadi-sepanjang-2022), diakses 08 September 2022

P, M., M, A. S., Paliwal, A., & T, G. K. (2020). Maximizing the Embedding Efficiency Using Linear Block Codes in Spatial and Transform Domains. *Procedia Computer Science*, *167*, 302–312. https://doi.org/10.1016/j.procs.2020.03.227

Rahman, M. S., Khalil, I., & Yi, X. (2021). Reversible Biosignal Steganography Approach for Authenticating Biosignals Using Extended Binary Golay Code. *IEEE Journal of Biomedical and Health Informatics*, *25*(1), 35–46. https://doi.org/10.1109/JBHI.2020.2988449

Riyanto, M. Z. (2020). Kode Linear untuk Deteksi dan Koreksi Kesalahan

Penulisan dalam Huruf Hijaiyah. *JURNAL FOURIER*, *9*, 49–58. https://doi.org/10.14421/fourier.2020.92.49-58

Roopaei, M., Eghbal, M. K., Shadaram, M., & Agaian, S. (2016). Noise-Free Rule-Based Fuzzy Image Enhancement. *Electronic Imaging*, *28*(13), 1–5. https://doi.org/10.2352/ISSN.2470-1173.2016.13.IQSP-225

Sajati, H. (2018). The Effect of Peak Signal to Noise Ratio (PSNR) Values on Object Detection Accuracy in Viola Jones Method. *Conference SENATIK STT Adisutjipto Yogyakarta*, *4*. https://doi.org/10.28989/senatik.v4i0.139

Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image Steganography: A Review of the Recent Advances. *IEEE Access*, *9*, 23409–23423. https://doi.org/10.1109/ACCESS.2021.3053998

Um, L. E., Jouhari, H., García-Planas, M. I., & Souidi, E. M. (2020). *Convolutional Codes and Steganography under Linear Systems Theoretical Point of View*. *22*.

Vien, Q.-T., Nguyen, T. T., & Nguyen, H. X. (2021). Deep-NC: A secure image transmission using deep learning and network coding. *Signal Processing: Image Communication*, *99*, 116490. https://doi.org/10.1016/j.image.2021.116490

Wu, X., Yang, C.-N., & Liu, Y.-W. (2020). A general framework for partial reversible data hiding using hamming code. *Signal Processing*, *175*, 107657. https://doi.org/10.1016/j.sigpro.2020.107657