ISSN : 2356 – 5195
Online ISSN: 2654 - 8704

Perbandingan Dan Analisa Gambar Pada Steganografi Berdasarkan *MSE* Dan *PSNR*

Bayu Kumoro Yakti*[1], Ragiel Hadi Prayitno[2], Hendra Kusumah[3]
[1,2]Program Studi Teknik Elektro Universitas Gunadarma
E-mail**: *[1]bayuyakti@staff.gunadarma.ac.id,** [2]ragielhp@staff.gunadarma.ac.id,
[3]hendra.kusumah@raharja.info

Abstrak

*Gambar digital adalah gambar dalam bentuk format digital atau media digital seperti hard drive. Gambar digital yang terdiri dari bit (0 atau 1) disebut piksel dan memiliki kapasitas tinggi untuk menyimpan data dan informasi. Keamanan merupakan hal yang penting terutama pada saat mengirim dari data dari satu tempat ke tempat lain. Salah satu cara mengamankan data adalah melalui steganografi. Steganografi merupakan teknik yang digunakan untuk menyembunyikan keberadaan informasi rahasia di dalam suatu objek. Teknik Steganografi menutup dengan sempurna pesan rahasia dalam gambar pembawa dengan keamanan tingkat tinggi. Informasi dan data akan dimanipulasi sehingga tidak dapat dideteksi oleh mata manusia. Format gambar mempengaruhi hasil gambar steganografi. Penelitian ini membandingkan dan menganalisa hasil pengolahan steganografi pada berbagai format gambar digital yang meliputi BMP, PNG, JPEG, dan GIF. Output steganografi yang akan dianalisis adalah MSE dan PSNR. Gambar sampul akan dikonversi menjadi grayscale dengan pesan rahasia berjumlah 58 karakter. Hasil penelitian menunjukkan bahwa format GIF adalah hasil terbaik dengan MSE = 8.697 * 10^{-4} dan PSNR = 78.7369.*

Kata Kunci*— Steganografi, Gambar Digital, MSE, PSNR*

Abstract

*Digital images are images in the form of digital formats or digital media such as hard drives. Digital images consisting of bits (0 or 1) are called pixels and have a high capacity to store data and information. Security is important, especially when sending data from one place to another. One of many methods to secure data is through steganography. Steganography is a technique used to hide the existence of confidential information inside an object. Steganography Technique perfectly closes the secret message in a high-security carrier image. Information and data will be manipulated so that it cannot be detected by the human eye. Image format affects the results of steganographic images. This study compares and analyzes the results of steganographic processing in various digital image formats including BMP, PNG, JPEG, and GIF. Steganographic output to be analyzed is MSE and PSNR. Cover image will be converted to grayscale with a 58-character secret message. The results showed that the GIF format was the best result with MSE = 8,697 * 10-4 and PSNR = 78.7369.*

Keywords*— Steganography, Digital Images, MSE, PSNR*

1. PENDAHULUAN

Internet telah berkembang sedemikian pesat sehingga sebagian besar individu lebih suka menggunakan internet sebagai media utama untuk mentransfer data dari satu ujung dunia ke ujung dunia yang lain. Ada banyak cara untuk mengirimkan data menggunakan internet: melalui

e-mail, *chatting*, *cloud*. Transisi data dibuat sangat sederhana, cepat dan akurat menggunakan internet. Namun, salah satu masalah utama dengan mengirim data melalui internet adalah ancaman keamanan, yaitu data pribadi atau rahasia dapat dicuri atau diretas dengan berbagai cara. Oleh karena itu, sangat penting untuk mempertimbangkan metode yang akan digunakan untuk mengamankan data berikut keluaran data yang ditransmisikan, karena keamanan data tersebut merupakan salah satu faktor terpenting yang perlu diperhatikan dalam proses transfer data.

Keamanan data pada dasarnya berarti perlindungan data dari pengguna atau peretas yang tidak sah dan upaya untuk mencegah modifikasi data. Area keamanan data ini telah mendapatkan banyak perhatian selama periode waktu terakhir karena peningkatan besar dalam kecepatan transfer data melalui internet. Untuk meningkatkan fitur keamanan dalam transfer data melalui internet, banyak teknik telah dikembangkan, seperti Kriptografi, Steganografi, dan watermarking digital. Kriptografi adalah metode untuk menyembunyikan informasi dengan mengenkripsi informasi ke dalam "teks sandi" dan mentransmisikannya ke penerima yang dimaksud, menggunakan kunci yang tidak dikenal. Steganografi memberikan keamanan lebih lanjut dengan menyembunyikan teks sandi menjadi gambar yang tidak nampak atau ke dalam format lain. Kriptografi menggunakan keluaran data yang tidak bisa dibaca. Karena keluaran tersebut, kriptografi mudah dicurigai oleh peretas, sedangkan hasil keluaran steganografi tidak terlihat seperti sandi sehingga steganografi lebih sering dipakai. [1]

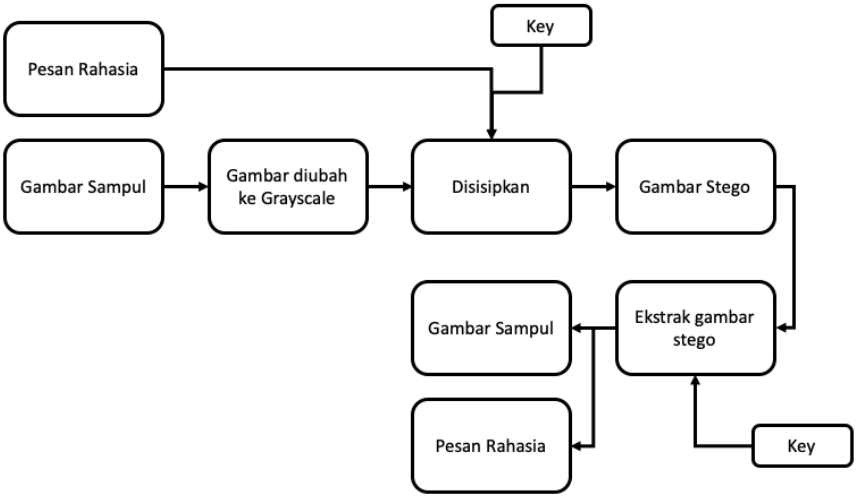
Steganografi merupakan metode data pesan rahasia yang disisipkan pada data sampul. Sehingga steganografi mempunyai dua input yaitu data pesan rahasia dan data sampul. Pesan rahasia dapat berupa teks, gambar, suara atau video [2]. Data sampul dapat juga berupa hal yang sama dengan pesan rahasia yaitu berupa teks, gambar, suara atau video. Pada sistem steganografi, data pesan rahasia dan data sampul dapat dilakukan dengan data yang berbeda-beda seperti: pesan rahasia teks disisipkan pada data sampul gambar, pesan rahasia audio disisipkan pada data sampul gambar, pesan rahasia gambar disisipkan ke data sampul gambar dan seterusnya. Pada penelitian ini, input yang dipakai adalah pesan rahasia berupa teks dan gambar sebagai sampul. Format pada gambar (Contoh: PNG, JPG, BMP) mempengaruhi hasil output dari steganografi, karena data gambar sebelum dan sesudah disisipkan oleh pesan rahasia akan berbeda [3].

Tujuan dari penelitian ini adalah membandingkan output metode steganografi pada format gambar yang berbeda, merujuk pada penelitian [4], [5], [6]. Pada penelitian ini, data yang akan disisipkan memiliki pesan rahasia yang sama. Gambar sampul pada penelitian ini menggunakan gambar yang sama, namun dengan format yang berbeda-beda. Penelitian menggunakan software MATLAB 2019a untuk menjalankan program steganografi dan software GIMP 2.10 untuk mengkonversi data gambar sampul ke berbagai format.

2. METODE PENELITIAN

Bab ini akan membahas tahap-tahap yang akan dilakukan pada penelitian ini. Berikut adalah tahap yang akan dilakukan.

ISSN : 2356 – 5195
Online ISSN: 2654 - 8704



Gambar 1. Flow penelitian

Berdasarkan gambar 1 diatas, input pada penelitian ini adalah pesan rahasia berupa teks dan gambar sampul dengan berbagai format. Pada pesan rahasia, tiap karakter pada pesan diubah menjadi 8 bit ASCII untuk penyisipan. Berikut adalah tabel ASCII yang digunakan:

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Gambar 2. Tabel ASCII [7]

Berdasarkan gambar 2 diatas, karakter yang digunakan adalah karakter "!" dengan desimal 33 sampai dengan karakter "~" dengan desimal 126. Karakter pada ASCII tersebut akan diubah ke nilai desimal dan diubah lagi ke nilai biner untuk disisipkan pada gambar. Sebagai contoh, jika pesan rahasia yang dipakai adalah 'bayu' maka hasil desimal yang didapat adalah 98 97 121 117. Kemudian, nilai desimal tersebut diubah menjadi biner, maka hasil yang didapat adalah 01100010 01100001 01111001 01110101. Masing-masing karakter akan diubah menjadi biner sehingga pesan rahasia yang awalnya berjumlah 4 karakter berubah menjadi 32 data biner (jumlah karakter dikali 8). Karena jumlah biner yang cukup banyak, pada penelitian ini pesan rahasia dibatasi menjadi 25 karakter sehingga nilai biner maksimal yang didapat adalah 200 data. Karena ukuran data tersebut, ukuran minimal gambar yang dipakai pada penelitian ini berukuran 200 piksel.

Setelah proses pesan rahasia diubah menjadi bit selesai, dilanjutkan dengan proses gambar sampul. Gambar sampul yang dipakai adalah gambar RGB seperti pada gambar 3.

Gambar 3. Lena

Dari gambar RGB tersebut diubah menjadi gambar grayscale sehingga mempunyai nilai 0 sampai 255 dimana nilai 0 adalah warna hitam dan nilai 255 adalah warna putih. Gambar grayscale memakai 8bit integer [3]. Dari hasil nilai gambar sampul (grayscale) tersebut, gambar dijadikan matriks 1 baris. Kemudian dilanjutkan proses penyisipan.

Pada proses penyisipan, keluaran yang dihasilkan adalah gambar stego. Gambar stego akan dikirimkan kepada penerima. Pada proses penyisipan dibutuhkan key untuk pengirim pesan dan penerima pesan. Key penyisipan pada penelitian ini adalah berupa kondisi. Kondisi tersebut adalah:

- Jika bit pesan ‘1’ dan piksel gambar sampul ‘ganjil’ maka piksel gambar sampul tetap nilainya atau tidak berubah dan menjadi gambar stego
- Jika bit pesan ‘0’ dan piksel gambar sampul ‘genap’ maka piksel gambar sampul tetap nilainya atau tidak berubah dan menjadi gambar stego
- Jika bit pesan ‘1’ dan piksel gambar sampul ‘genap’ maka piksel gambar sampul nilainya ditambah 1 dan mejadi gambar stego
- Jika bit pesan ‘0’ dan piksel gambar sampul ‘ganjil’ maka piksel gambar sampul nilainya dikurang 1 dan mejadi gambar stego

Proses ekstraksi key pesan pada gambar stego dilakukan dengan mengambil bentuk angka pada piksel gambar secara satu per satu. Jika piksel dari gambar stego adalah ‘ganjil’ maka bit pesan adalah ‘1’. Jika piksel dari gambar stego adalah ‘genap’ maka bit pesan adalah ‘0’. Setelah didapat bit pesan, data dikelompokkan per 8bit kemudian diubah kembali ke desimal dan selanjutnya diubah kembali lagi ke dalam bentuk huruf. Setelah semua format diproses dengan steganografi, dilakukan perbandingan gambar sampul dan gambar stego memakai metode MSE dan PSNR.

2.1. Literature Review

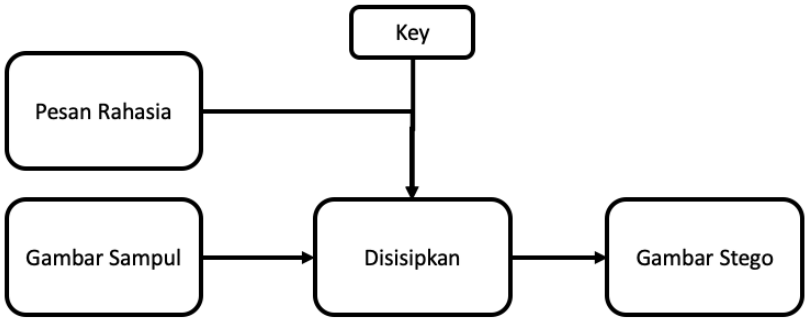
Pada sub bab ini akan dibahas literatur yang berhubungan dengan penelitian ini. Literatur yang dibahas menyangkut penelitian-penelitian sebelumnya yang berkaitan dengan penelitian yang akan dilakukan. Berikut adalah literatur yang akan dibahas:

- Steganografi
- Gambar Digital
- Perbandingan BMP dan JPEG sesuai dengan penelitian [4]
- Perbandingan PNG dan JPEG sesuai dengan penelitian [5]
- Perbandingan GIF dan JPEG sesuai dengan penelitian [6]

2.1.1. Steganografi

Steganografi berasal dari kata Yunani yang berarti tulisan tersembunyi. Kata "steganos" yang berarti "tertutup" dan "grafis" yang berarti "menulis". Dengan demikian, steganografi bukan hanya seni menyembunyikan data tetapi juga menyembunyikan fakta transmisi data rahasia. Steganografi menyembunyikan data rahasia di file lain sedemikian rupa sehingga hanya penerima yang mengetahui keberadaan pesan. Pada zaman kuno, data dilindungi dengan menyembunyikannya di belakang lilin, menulis tabel, perut kelinci atau pada kulit kepala budak. Tetapi hari ini sebagian besar orang mengirimkan data dalam bentuk teks, gambar, video, dan audio melalui media. Untuk pengiriman data rahasia secara aman, objek multimedia seperti audio, video, dan gambar digunakan sebagai sumber sampul untuk menyembunyikan data. [2]

Pada penelitian ini, steganografi yang digunakan adalah steganografi gambar atau penyisipan dimana pesan rahasia berbentuk teks disisipkan pada gambar. Berikut adalah dasar alur diagram dari steganografi:



Gambar 4. Diagram steganografi

Berdasarkan gambar 4 diatas, dasar steganografi terdiri dari 2 input yang berupa Gambar sampul dan pesan rahasia, dan output berupa Gambar stego.

2.1.2. Gambar Digital [3]

Ada sejumlah jenis file gambar digital yang tersedia saat ini. Jenis file gambar yang paling umum digunakan adalah JPEG, GIF, PNG dan BMP. Jenis file gambar didasarkan pada teknik kompresi yang digunakan untuk mengurangi ukuran file gambar. Gambar dalam berbagai jenis file mungkin berbeda warna, jika warna telah digunakan. Gambar dalam bentuknya yang paling sederhana mungkin hanya mengandung dua intensitas, misalnya, hitam dan putih, dan hanya membutuhkan 1 bit untuk mewakili intensitas pada setiap piksel.

- Portable Network Graphics (PNG): Format ini tidak memiliki format penyimpanan dan menggunakan pola pada gambar untuk mengompres gambar. Kompresi dalam file PNG merupakan gambar yang tidak dikompresi atau identik dengan gambar aslinya. Format ini memakai gambar berbasis palet yaitu 24 bit untuk RGB dan 32 bit untuk ARGB di mana A adalah singkatan dari alpha channel dari gambar. Format ini dirancang khusus untuk penggunaan internet sehingga tidak mendukung model warna lain selain RGB. Format ini menggunakan kompresi lossless, sehingga memberikan gambar nyata setelah setiap kompresi. Berikut adalah bentuk umum PNG: [5]
    - Algoritma Kompresi Lossless digunakan.
    - Memakai RGB yang berlaku.

- Memakai 24 atau 32 bit untuk gambar.

- Graphical Interchange Format (GIF): GIF adalah format file gambar yang biasa digunakan untuk gambar di web dan sprite pada software. Berbeda dengan format gambar JPEG, GIF menggunakan kompresi lossless yang tidak menurunkan kualitas gambar. Namun, GIF menyimpan data gambar menggunakan warna yang diindeks, yang berarti gambar GIF standar dapat mencakup maksimal 256 warna. Karena GIF hanya berisi 256 warna, GIF tidak ideal untuk menyimpan foto digital, seperti yang ditangkap dengan kamera digital. Bahkan ketika menggunakan palet warna khusus dan menerapkan *dithering* untuk menghaluskan gambar, foto yang disimpan dalam format GIF sering terlihat kasar dan tidak realistis. Oleh karena itu, format JPEG, yang mendukung jutaan warna, lebih umum digunakan untuk menyimpan foto digital. GIF lebih cocok untuk tombol dan spanduk di situs web, karena jenis gambar ini biasanya tidak memerlukan banyak warna. Namun, sebagian besar pengembang web lebih suka menggunakan format PNG karena mendukung rentang warna yang lebih luas dan menyertakan saluran alfa yang memungkinkan gambar tunggal dengan transparansi untuk berbaur dengan warna latar halaman web. Namun, baik JPEG maupun PNG tidak mendukung animasi, sehingga GIF animasi tetap populer di web. [6]

- Joint Picture Experts Group (JPG atau JPEG): Format ini adalah format yang dioptimalkan untuk foto dan gambar nada kontinu yang berisi sejumlah besar warna. File JPEG dapat mencapai rasio kompresi tinggi dengan tetap menjaga kualitas gambar yang jelas. Perlu diingat bahwa JPEG adalah format file gambar terkompresi. Gambar JPEG tidak terbatas pada jumlah warna tertentu, seperti gambar GIF sehingga menjadi format terbaik untuk mengompresi gambar foto. Meskipun gambar JPEG dapat menampung data gambar berwarna dan beresolusi tinggi, format ini bersifat lossy [4], yang berarti kualitas akan menurun ketika gambar dikompresi ke ukuran yang lebih kecil. Jika gambar dikompresi terlalu banyak, grafik menjadi terasa "tersumbat" dan beberapa detail akan hilang. Seperti GIF, JPEG adalah format lintas platform, yang berarti file yang sama akan terlihat sama di Mac dan PC. File JPEG memungkinkan hanya 8 - 24-bit warna yang diindeks.

- Bitmapped Image (BMP) adalah format eksklusif tanpa kompresi yang ditemukan oleh Microsoft. File BMP berisi data grafik raster yang tidak tergantung pada perangkat layar. Hal ini berarti file gambar BMP dapat dilihat tanpa adaptor grafis. Gambar BMP umumnya tidak terkompresi atau dikompresi dengan metode kompresi lossless. File dapat menyimpan gambar digital dua dimensi dengan monokrom dan warna. Format ini mendukung berbagai kedalaman warna, saluran alfa, profil warna dan kompresi data opsional. Namun, hal ini merupakan keuntungan untuk menyembunyikan data tanpa menimbulkan kecurigaan. Untuk memahami bagaimana gambar bitmap dapat digunakan untuk menyembunyikan data, format file harus terlebih dahulu dijelaskan. File bitmap dapat dipecah menjadi dua blok utama, header dan data. Header, yang terdiri dari 54 byte, dapat dipecah menjadi dua sub-blok. Format ini diidentifikasi sebagai Header Bitmap, dan Informasi Bitmap. Gambar yang kurang dari 16bit memiliki sub-blok tambahan dalam header yang diberi label Palet Warna. Berikut adalah bentuk umum format BMP. [4]

    - Format bitmap yang dapat dikompresi, atau dikompres dengan RLE
    - Dalam 1-bit hitam dan putih.

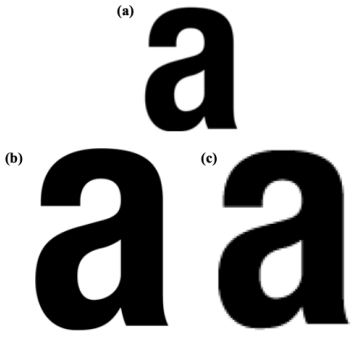
- Grayscale 8-bit.
- Warna RGB 16-, 24- atau 32-bit. - atau warna indeks 4- atau 8-bit.
- File BMP tidak mendukung warna CMYK.
- Transparansi didukung untuk piksel individual seperti dalam GIF

Berkenaan dengan cara penyimpanannya, gambar digital dapat diklasifikasikan ke dalam dua kategori yaitu:

- Gambar raster atau Bitmap
- Gambar vektor.

Gambar bitmap atau raster adalah array persegi panjang dari nilai sampel atau piksel. Gambar-gambar ini memiliki jumlah piksel yang tetap. Dalam pembesaran gambar raster, interpolasi matematis diterapkan. Format gambar umum BMP, GIF, PNG dan JPEG adalah format gambar bitmap atau raster.

Di sisi lain, gambar vektor disimpan dalam bentuk garis dan kurva matematika. Informasi seperti panjang, warna, ketebalan. disimpan dalam bentuk vektor. Gambar-gambar ini dapat ditampilkan dalam ukuran dan resolusi apa pun. Gambar vektor cocok untuk ilustrasi, gambar seni dan font. Perbedaan dalam pembesaran gambar vektor dan gambar raster dapat diamati pada Gambar 5. Penurunan kualitas karena pembesaran terlihat jelas pada batas-batas karakter yang disimpan dalam format raster.



Gambar 5. (a) Gambar (b) gambar a diperbesar dalam format vektor (c) gambar a diperbesar dalam format raster

2.1.3. Perbandingan Steganografi dalam format BMP dan JPEG [4]

Peneliti [4] melakukan penelitian dengan membandingkan steganografi dengan format BMP dan JPEG. Peneliti memakai metode steganografi *Least Significant Bit* (LSB) dimana pesan dijadikan bit dan masing-masing bit tersebut disisipkan pada bit gambar yang paling kecil atau paling kanan pada tiap piksel gambar tersebut.

Berikut adalah hasil dan perbandingan format BMP dan JPEG yang didapat peneliti:

Tabel 1. Perbandingan format BMP dan JPEG dalam LSB steganografi (Tinggi = 2, Sedang = 1, Rendah = 0)

Parameter	BMP	JPEG
Efisiensi penyisipan	2	1
Jumlah data yang disisipkan	2	0

Deteksi steganalisis	0	1
Persentase Distorsi gambar yang dihasilkan	2	1
Kekuatan melawan manipulasi gambar	0	1
Gambar stegano tidak terlihat sudah disisipkan	2	2
Kekuatan melawan serangan statistik	0	1
Kapasitas muatan	2	1
File tidak mencurigakan	0	2

Dalam gambar jenis BMP, tipe data yang dapat disematkan berukuran besar dan gambar tidak terdistorsi karena kemampuan gambar jenis ini untuk membawa jumlah data tanpa terdeteksi. Gambar jenis JPEG memiliki resistensi yang rendah terhadap serangan statistik dan serangan manipulasi, juga mudah terdistorsi ketika disisipkan data, sehingga data menjadi dapat ditemukan.

Peneliti [4] memakai banyak parameter dalam perbandingannya sehingga perbedaan kelebihan dan kekurangan dari setiap format sangat jelas. Tetapi, peneliti[4] tidak menjelaskan secara detail bagaimana cara mendapatkan hasil tersebut.

2.1.4. Perbandingan Steganografi dalam Format PNG dan JPEG

Peneliti [5] melakukan penelitian dengan membandingkan steganografi dengan format PNG dan JPEG. Peneliti memakai metode steganografi *Least Significant Bit* (LSB).

Berikut adalah hasil dan perbandingan format PNG dan JPEG yang didapat peneliti:

Tabel 2. Perbandingan format PNG dan JPEG dalam LSB Steganografi

Parameter	PNG	JPEG
Efisiensi penyisipan	Tinggi	Sedang
Jumlah data yang disisipkan	Sedang	Rendah
Deteksi steganalisis	Sedang	Sedang
Persentase Distorsi gambar yang dihasilkan	Sedang	Sedang
Kekuatan melawan manipulasi gambar	Sedang	Tinggi
Gambar stegano tidak terlihat sudah disisipkan	Sedang	Sedang
Kekuatan melawan serangan statistik	Rendah	Rendah
Kapasitas muatan	Rendah	Rendah
File tidak mencurigakan	Rendah	Rendah

Metode LSB tidak efektif dalam kasus JPEG karena data yang dimanipulasi saat kompresi bersifat lossy. Sedangkan untuk gambar PNG, LSB sederhana dapat efektif tanpa kehilangan data akibat kompresi. Selain itu, keduanya memiliki kapasitas penyimpanan dan kualitas gambar yang hampir setara dari gambar akhir. Peneliti [5] tidak menjelaskan data

output hasil penelitiannya dan tidak melakukan perbandingan kualitas gambar setelah disisipkan dan sebelum disisipkan.

2.1.5. Perbandingan Steganografi dalam format GIF dan JPEG

Pada penelitian [6] ini, teknik LSB diimplementasikan pada gambar GIF dan JPEG. Melalui pengukuran kualitas dengan komputasi RMSE, SNRrms, SNRpeak, dan MAE, ditemukan bahwa LSB pada JPEG lebih baik daripada LSB pada GIF. Ukuran data yang disematkan dalam format gambar GIF lebih kecil dari ukuran data yang disematkan dalam format gambar JPEG.

Ketika jumlah data yang disembunyikan bertambah pada gambar GIF, gambar sampul menjadi terdistorsi, membuat keberadaan data yang disematkan menjadi terdeteksi.

Pada penelitian ini, peneliti [6] tidak menjelaskan hasil dari perbandingan kedua format tersebut.

2.1.6. MSE dan PSNR

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum sinyal yang diukur dengan jumlah noise yang mempengaruhi sinyal. PSNR biasanya diukur dalam desibel (db). PSNR digunakan untuk membandingkan kualitas gambar sampul sebelum dan sesudah pesan dimasukkan. Untuk menentukan PSNR, nilai MSE (Mean Square Error) harus ditentukan terlebih dahulu.

MSE adalah nilai kesalahan rata-rata antara gambar asli dan gambar manipulasi (dalam kasus steganografi; MSE adalah nilai kesalahan rata-rata antara gambar sampul dan gambar stego). PSNR sering dinyatakan dalam skala logaritmik dalam desibel (dB). Nilai PSNR yang turun di bawah 30 dB menunjukkan kualitas yang relatif rendah, di mana distorsi akibat penyisipan terlihat jelas. Namun, kualitas gambar stego yang tinggi terdapat pada nilai 40dB ke atas. [8]

Dalam tampilan biasa, nilai terbaik dalam gambar menunjukkan bahwa mata manusia hampir tidak mengenali gambar asli dan gambar steganografi. Nilai PSNR yang lebih tinggi berarti memiliki kemiripan yang lebih dekat antara hasil rekonstruksi dan gambar asli. PSNR didefinisikan sebagai:

$$\text{PSNR} = 10 \log_{10} \left(\frac{C^2_{max}}{MSE}\right) \quad (1)$$

Semakin rendah MSE, semakin rendah kesalahan yang dihasilkan. Di mana MSE dinyatakan sebagai:

$$\text{MSE} = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2 \quad (2)$$

3. HASIL DAN PEMBAHASAN

Pada bab ini, akan dijelaskan hasil dari penelitian yang dilakukan. Objek yang akan dibandingkan dalam penelitian ini adalah format gambar dengan metode yang sama seperti yang dijelaskan pada bagian II. hal-hal yang akan dibandingkan dan dianalisa adalah:

- Format BMP, PNG, JPEG, GIF pada gambar sampul dan gambar steganografi

- Memakai pesan yang sama
- Memakai gambar yang sama

Gambar sampul yang dipakai berukuran 512x512 piksel. Dalam piksel tersebut dapat menampung 64 karakter pesan, dimana tiap karakter akan dikonversi menjadi 8bit biner sehingga 64 * 8 = 512, sesuai dengan piksel gambar.

Pesan rahasia yang dipakai adalah pesan teks yang berjumlah 58 karakter yaitu: “How razorback-jumping frogs can level six piqued gymnasts!”. Pesan teks tersebut dipilih karena kalimat tersebut terdiri dari 26 alfabet.

Berikut adalah algoritma yang dipakai penulis:

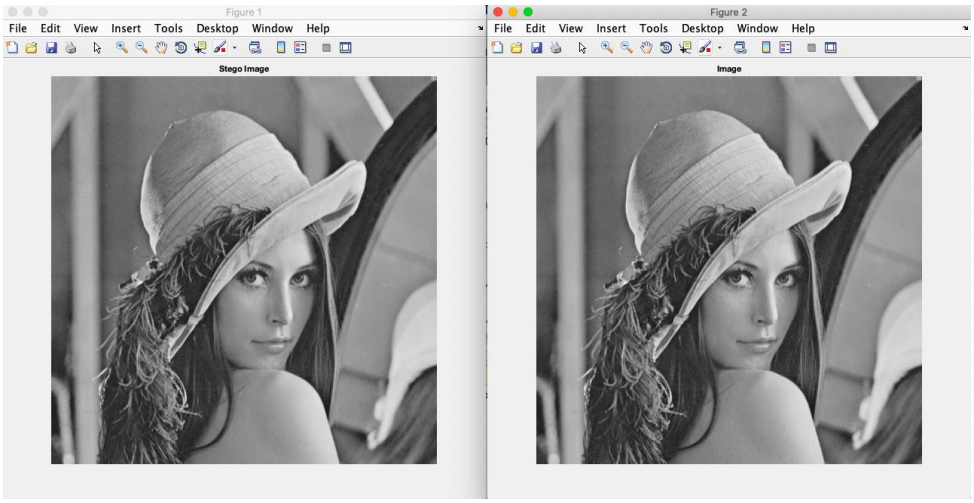
1. Menulis pesan dan deklarasi sebagai string
2. Mengubah pesan menjadi 8bit biner
3. Membaca gambar sampul
4. Mengubah gambar sampul menjadi grayscale
5. Mengubah gambar sampul tersebut menjadi matriks 1 baris
6. Membaca bit pesan dan piksel pada gambar
7. Untuk proses enkripsi, lakukan kondisi IF pada tiap piksel dan bit pesan
    a. Jika jika piksel citra 0 atau genap dan bit pesan 1 maka piksel citra lama +1
    b. Jika piksel citra 1 atau ganjil dan bit pesan 0 maka piksel citra lama -1
    c. Jika kondisi tidak memenuhi, proses dilanjutkan
8. Matriks gambar baris dikembalikan ke matriks semula
9. Cetak gambar sampul dan gambar stego
10. Untuk proses dekripsi, lakukan kondisi if pada tiap piksel dan bit pesan
    a. Jika citra stego 0 atau genap maka bit pesannya 0
    b. Jika citra stego 1 atau ganjil maka bit pesannya 1
    c. Jika kondisi tidak memenuhi, proses dilanjutkan
11. Membaca per 8bit yang didapat
12. Ubah bit tersebut ke desimal kemudian ke string
13. Cetak pesan
14. Hitung MSE dan PSNR
15. Selesai

Subbab selanjutnya membahas hasil penelitian berdasarkan algoritma tersebut.

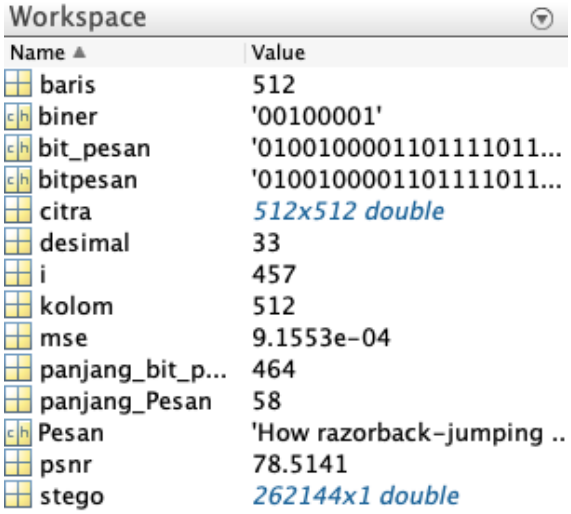
3. 1. Steganografi pada BMP

Berikut adalah hasil gambar sampul dan gambar stego pada gambar lena.bmp

ISSN : 2356 – 5195
Online ISSN: 2654 - 8704



Gambar 6. Perbandingan gambar Stego dan gambar sampul pada format .bmp



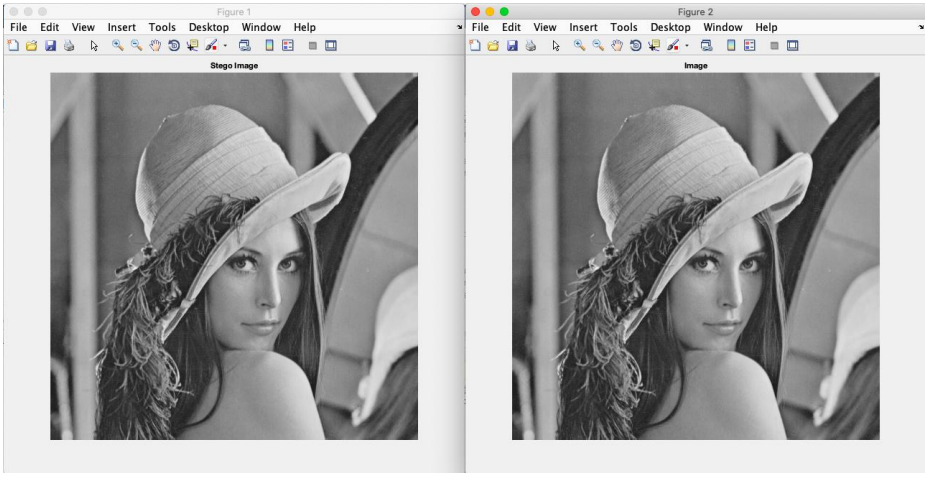
Gambar 7. hasil pada MATLAB

Gambar 6 merupakan hasil gambar stego (kiri) dan gambar sampul (kanan) yang sudah diproses. Gambar 7 merupakan hasil input dan output pada MATLAB. Pada gambar 7 diatas, ditampilkan hasil MSE dan PSNR. Hasil MSE yang didapat adalah 9,155 * 10^{-4}. Hasil PSNR yang didapat adalah 78,5141.

3. 2. Steganografi pada PNG

Berikut adalah hasil gambar sampul dan gambar stego pada gambar lena.png

ISSN : 2356 – 5195
Online ISSN: 2654 - 8704



Gambar 8. Perbandingan Gambar stego dan gambar sampul pada format .png

Workspace

Name	Value
baris	512
biner	'00100001'
bit_pesan	'0100100001101111011...
bitpesan	'0100100001101111011...
citra	*512x512 double*
desimal	33
i	457
kolom	512
mse	9.1553e-04
panjang_bit_p...	464
panjang_Pesan	58
Pesan	'How razorback-jumping ..
psnr	78.5141
stego	*262144x1 double*

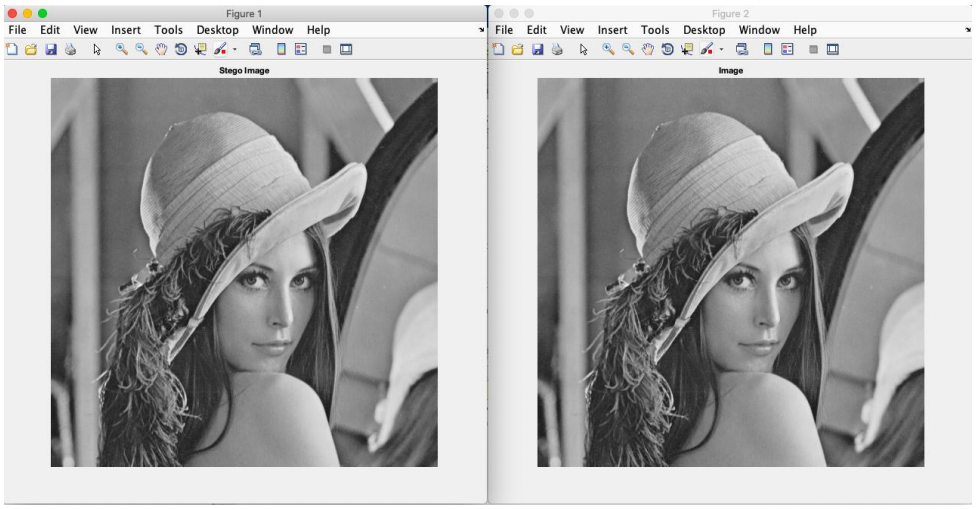
Gambar 9. hasil pada MATLAB

Gambar 8 merupakan hasil gambar stego (kiri) dan gambar sampul (kanan) yang sudah diproses. Gambar 8 merupakan hasil input dan output pada MATLAB. Pada gambar 7 diatas, ditampilkan hasil MSE dan PSNR. Hasil MSE yang didapat adalah 9,155 * 10^{-4}. Hasil PSNR yang didapat adalah 78,5141.

3. 3. Steganografi pada JPEG

Berikut adalah hasil gambar sampul dan gambar stego pada gambar lena.jpeg

ISSN : 2356 – 5195
Online ISSN: 2654 - 8704



Gambar 10. Perbandingan gambar stego dan gambar sampul pada format jpg

Workspace

Name	Value
baris	512
biner	'00100001'
bit_pesan	'0100100001101111011...
bitpesan	'0100100001101111011...
citra	*512x512 double*
desimal	33
i	457
kolom	512
mse	8.8882e-04
panjang_bit_p...	464
panjang_Pesan	58
Pesan	'How razorback-jumping ..
psnr	78.6426
stego	*262144x1 double*

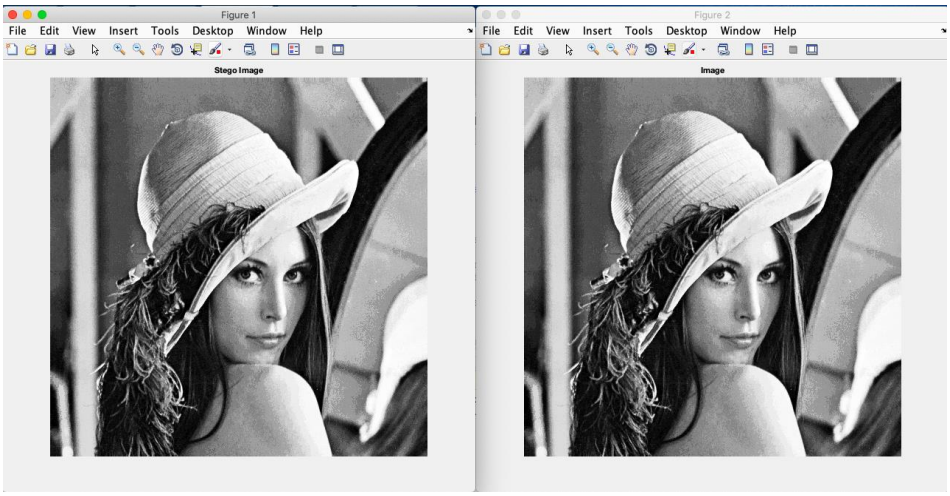
Gambar 11. hasil pada MATLAB

Gambar 10 merupakan hasil gambar stego (kiri) dan gambar sampul (kanan) yang sudah diproses. Gambar 8 merupakan hasil input dan output pada MATLAB. Pada gambar 11 diatas, ditampilkan hasil MSE dan PSNR. Hasil MSE yang didapat adalah 8,888 * 10^{-4}. Hasil PSNR yang didapat adalah 78,6426.

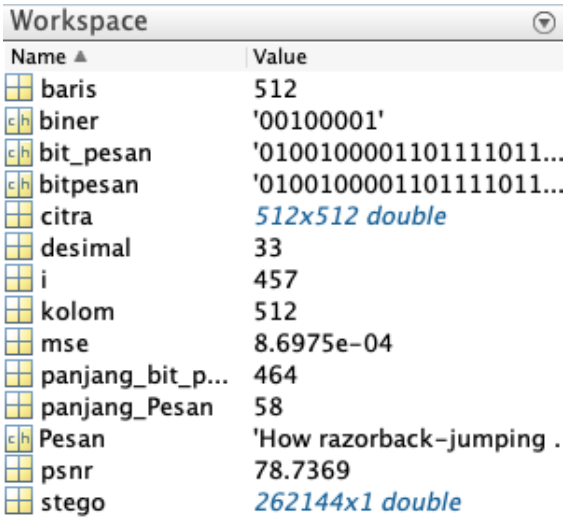
3. 4. Steganografi pada GIF

Berikut adalah hasil gambar sampul dan gambar stego pada gambar lena.jpeg

ISSN : 2356 – 5195
Online ISSN: 2654 - 8704



Gambar 12. perbandingan gambar stego dan gambar sampul pada format .gif



Gambar 13. Hasil pada MATLAB

Gambar 12 merupakan hasil gambar stego (kiri) dan gambar sampul (kanan) yang sudah diproses. Gambar 8 merupakan hasil input dan output pada MATLAB. Pada gambar 13 diatas, ditampilkan hasil MSE dan PSNR. Hasil MSE yang didapat adalah 8,697 * 10^{-4}. Hasil PSNR yang didapat adalah 78,7369.

3. 5. Perbandingan metode pada format

Table dibawah merupakan ringkasan dari penelitian yang sudah dilakukan:

Tabel 3. Perbandingan hasil format

No.	Format	MSE	PSNR
1	BMP	9,155 * 10^{-4}	78,5141
2	PNG	9,155 * 10^{-4}	78,5141
3	JPEG	8,888 * 10^{-4}	78,6426
4	GIF	8,697 * 10^{-4}	78,7369

Bersdasarkan hasil penelitian yang sudah dilakukan, hasil steganografi pada format BMP dan PNG mempunyai hasil yang sama yaitu MSE = 9,155 * 10^{-4} dan PSNR = 78,5141. Hasil tersebut dikarenakan kedua format merupakan kompresi lossless atau tidak dikompresi sehingga

hasil kedua format yang dikeluarkan sama. Hasil terbaik ada pada format GIF dengan MSE = 8,697 * 10^{-4} dan PSNR = 78,7369. Pada penelitian ini, GIF merupakan format terbaik karena pada penelitian ini kompresi yang dilakukan bersifat lossless dan warna yang digunakan adalah grayscale. dapat dilihat pada gambar 12, warna pada format GIF lebih gelap karena format tersebut memakai bit yang lebih sedikit sehingga pada saat penyisipan perbedaanya tidak terlalu terlihat dibanding format yang lain.

4. KESIMPULAN

Pada penelitian ini telah dilakukan pengolahan steganografi pada format gambar yang berbeda-beda dengan pesan yang sama. Format yang digunakan adalah BMP, PNG, JPEG dan GIF. Format GIF merupakan format terbaik dengan MSE = 8,697 * 10^{-4} dan PSNR = 78,7369. Format tersebut mempunyai output terbaik karena pada penelitian ini warna yang digunakan adalah grayscale. Warna pada format GIF lebih gelap karena format tersebut memakai bit yang lebih sedikit sehingga pada saat penyisipan perbedaanya tidak terlalu terlihat dibanding format lain. Dalam penelitian lebih lanjut dapat dilakukan penyisipan dengan gambar berwarna atau RGB dan menambah variasi pada ukuran gambar dan jumlah pesan yang disisipkan.

5. SARAN

Penelitian ini dapat dilakukan penambahan variasi gambar atau ukuran gambar yang berbeda-beda untuk mendapatkan variasi output untuk dianalisa.

DAFTAR PUSTAKA

[1] I. Nehra, "Review Paper On Image Based Steganography," in *International Journal of Scientific & Engineering Research*, 2015.

[2] J. Kour, "Steganography Techniques A Review Paper," in *International Journal of Emerging Research in Management &Technology*, 2014.

[3] V. Tyagi, Understanding Digital Image Processing, Research Gate, 2018.

[4] E. E. A. b. Elgabar, "Comparison of LSB Steganography in BMP and JPEG Images," in *International Journal of Soft Computing and Engineering*, 2013.

[5] B. Sinha, "Comparison of PNG & JPEG Format for LSB Steganography," in *International Journal of Science and Research*, 2015.

[6] E. J. A. R. AL-TAEE, "Comparison Study of LSB Steganography for JPEG and GIF Images," in *EUROPEAN ACADEMIC RESEARCH*, 2015.

[7] Ezoic, "ASCII Table and Description," Ezoic Inc, [Online]. Available: http://www.asciitable.com/. [Accessed 16 Maret 2020].

[8] R. Kumar, "A Real Time Approach to Compare PSNR and MSE Value of Different Original Images and Noise (Salt and Pepper, Speckle, Gaussian) Added Images," in *International Journal of Latest Technology in Engineering, Management & Applied Science*, 2018.