STEGANOGRAFI TEKS PADA CITRA DIGITAL MENGGUNAKAN METODE BRAILLE DAN METODE PEMILIHAN PIKSEL LSB

TEXT STEGANOGRAPHY IN DIGITAL IMAGES USING THE BRAILLE METHOD AND THE METHOD OF SELECTING PIXELS LSB

Elyza Dilla Susanti[1], Dr.Ir.Bambang Hidayat,DEA[2], Nur Andini,ST,.MT[3]
[123] Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]elyzadilla@students.telkomuniversity.ac.id, [2]bhidayat@telkomuniversity.ac.id,
[3]nurandini@telkomuniversity.ac.id

ABSTRAK

Perkembangan teknologi saat ini telah berkembang pesat. Salah satunya teknologi internet yang sudah sangat mendunia memberi fasilitas dan kemudahan untuk berkirim informasi atau bertukar data. Semua orang bebas untuk mengaksesnya. Seiring berkembangnya teknologi internet, menyebabkan munculnya kejahatan yang disebut dengan "CyberCrime" atau kejahatan melalui jaringan Internet. Sehingga perlu teknik untuk menjaga keamanan dan kerahasiaan informasi atau data yang dikirimkan. Salah satunya dengan teknik Steganografi. Steganografi adalah teknik yang digunakan untuk menyembunyikan informasi rahasia dalam sebuah media informasi sehingga data yang dikirimkan tidak dapat diidentifikasi oleh pihak yang tidak berhak. Steganografi punya beberapa metode, yang sering digunakan adalah metode LSB. Metode LSB adalah metode menyembunyikan pesan rahasia dengan menyisipkan pada bit rendah atau bit yang paling kanan (LSB) pada data piksel yang menyusun file tersebut. Pada tugas akhir ini diterapkan metode braille untuk meningkatkan keandalan LSB dengan cara menyisipkan pesan rahasia dengan masukkan berupa teks yang dikonversikan dalam bilangan biner 6 bit. Kemudian hasilnya dianalisis perubahan citra sebelum disisipi pesan rahasia dan sesudah disisipi pesan rahasia dengan membandingkan nilai MSE, PSNR, BER, CER dan MOS. Setelah dilakukan pengujian sistem diperoleh nilai rata-rata PSNR=125,899dB dan MSE=0,221, BER=0 dan nilai CER=0 ini berarti tidak ada bit pesan dan karakter yang eror setelah diekstraksi. Sedangkan hasil penilaian MOS sekitar 4,48-4,76 pada skala 1-5 dari 30 orang responden.

Kata kunci : **Steganografi, metode braille, LSB, MSE, PSNR, BER, CER, MOS**

ABSTRACT

The current technological development has been growing rapidly. One of these internet technologies are already very global provide facilities and services to send information or exchange data. Everyone is free to access. As the development of Internet technology, led to the emergence of a crime called "cybercrime" or crime through the internet network. So it is necessary techniques to maintain security and confidentiality of information or data transmitted. One of them with Steganography technique. Steganography is a technique used to hide secret information in an information media that transmitted data can not be identified by unauthorized parties. Steganography had some method, which is often used is the method of LSB. LSB method is a method of hiding a secret message by inserting the low bit or bits (LSB)right on the data pixels that make up the file.In this final project applied braille method to improve the reliability of LSB for inserting secret messages with input text converted into binary number 6 bits. . Results are then analyzed image changes before and after the secret message embedding by comparing the value of PSNR, MSE, BER,CER and MOS. Once done testing the system retrieved the average value PSNR= 125,899dB, MSE=0,221, BER = 0 and the value of CER = 0 this means no bit error messages and characters that once extracted. While the results of the assessment of the MOS about 4,48-4,76 on scale 1-5 *from 30 respondents.*

Keywords ***: Steganography, braille method, LSB, BER, CER, MSE, PSNR, MOS***

1. Pendahuluan

Perkembangan teknologi digital saat ini sudah sangat pesat sehingga memudahkan orang untuk berkomunikasi. Teknologi yang sering digunakan adalah teknologi internet. Saat ini Internet sudah menjadi bagian dari kehidupan masyarakat di dunia dengan memanfaatkan internet orang-orang dapat saling bertukar informasi atau data sampai berbagai belahan dunia. Informasi yang ditukarkan berupa informasi digital yang berupa teks, citra, audio, dan video. Seiring berkembangnya teknologi internet, menyebabkan munculnya kejahatan yang disebut dengan "CyberCrime" atau kejahatan melalui jaringan Internet. Untuk itu, semakin berkembangnya teknologi digital seharusnya diikuti dengan perkembangan pengamanan. Salah satu solusi untuk mengatasi masalah tersebut dengan menggunakan teknik steganography yang dalam bahasa yunani berarti "pesan tersembunyi" (covered writing) dalam menjaga keamanan data. Teknik steganografi adalah teknik menyembunyikan pesan rahasia dalam pesan/media lain sehingga keberadaan data rahasia tidak diketahui oleh pihak yang tidak berhak. Banyak metode steganografi yang dikembangkan, yang paling sederhana adalah metode penyisipan Least Significant Bit (LSB). Metode LSB adalah metode menyembunyikan pesan rahasia pada bit rendah atau bit yang paling kanan (LSB) pada data piksel yang menyusun file tersebut. Dalam tugas akhir ini akan membahas simulasi steganografi teks ke dalam media (cover) berupa citra digital menggunakan metode LSB Braille. Pada penelitian yang telah dilakukan sebelumnya, metode LSB Braille yang digunakan hanya menyisipkan 1 bit pesan rahasia pada layer biru dan dilakukan pengujian dengan parameter peak signal-to-noise ratio (PSNR) dan Maximum Hiding Capacity (MHC). Hasilnya metode LSB Braille lebih efisien dan dapat meningkatkan nilai PSNR dan MHC [1].

2. Dasar Teori

A. Steganografi

Steganografi merupakan seni untuk menyembunyikan pesan di dalam media digital sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu pesan di dalam media tersebut. Kata steganografi (*steganography*) berasal dari bahasa Yunani *steganos* yang artinya "tersembunyi/terselubung" dan *graphein* "menulis" sehingga kurang lebih artinya "menulis (tulisan) terselubung" [6].

Ada beberapa hal yang harus diperhatikan dalam penyembunyian data, yaitu [6] :

1. *Fidelity* : Mutu citra penampung data tidak jauh berubah. Setelah terjadi penambahan pesan rahasia, *stego-data* masih terlihat dengan baik
2. *Robustness* : Pesan yang disembunyikan harus tahan (*robust*) terhadap berbagai operasi manipulasi yang dilakukan pada *stego-data.*
3. *Recovery* : Data yang disebunyikan harus dapat diungkapkan kembali (*recovery*).

B. Citra Digital

Citra digital dapat didefinisikan sebagai fungsi 2 variabel f(x,y) dimana x dan y merupakan koordinat spasial dan nilai f(x,y) menunjukkan nilai intensitas citra suatu titik. Teknologi dasar untuk menciptakan dan menampilkan warna pada citra digital berdasarkan pada penelitian bahwa sebuah warna merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau dan biru *(Red, Green, Blue* – RGB) [5].

C. Citra BMP (Bitmap)

Format BMP mempunyai kelebihan dari segi kualitas gambar, yaitu tidak dimampatkan *(uncompressed)* sehingga tidak ada informasi yang hilang. Dalam tugas akhir ini, akan digunakan format citra digital Bitmap sebagai citra *cover* [5].

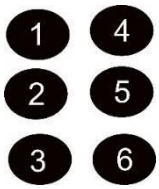
D. Least Significant Bit

Metode *Least Significant Bit* (LSB) merupakan metode penyisipan steganografi yang paling sederhana bekerja pada domain spasial. Penyisipan pesan dilakukan dengan cara mengganti bit-bit citra cover dengan bit-bit data rahasia.Pada susunan bit dalam sebuah *byte* (1 *byte* = 8 bit), ada bit yang paling berarti (*Most significant bit* atau MSB) dan bit yang paling kurang berarti (*Least Significant Bit* atau LSB). Sebagai contoh byte 11011010, angka 1 (pertama digaris bawahi) adalah MSB dan angka bit 0 (terakhir digaris bawahi) adalah bit LSB [4].

E. Metode Braille

Braille merupakan metode membaca dan menulis untuk orang buta yang dikembangkan oleh Louis Braille (1809–1852). Sistem Braille menggunakan enam titik yang disusun secara sistematis dengan dua

kolom dari tiga titik, yang dikenal sebagai sel Braille. Enam titik tersebut menjadi dasar braille. Dengan ketentuan, titik-titik di kolom kiri diberi nomor 1, 2 dan 3 dari atas ke bawah dan titik-titik di kolom kanan diberi nomor 4, 5 dan 6 dari atas ke bawah. Keenam titik sel Braille dikonfigurasi dalam 64 kemungkinan kombinasi (termasuk spasi yang tidak memiliki titik) [1].



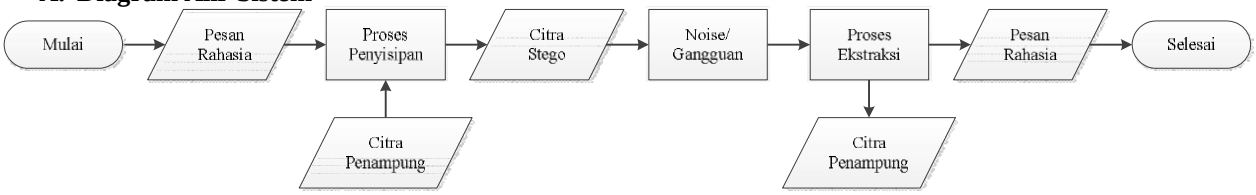
Gambar 1. Kerangka Abjad Braille

Tabel 1. Karakter Braille yang Direpresentasikan 6 bit

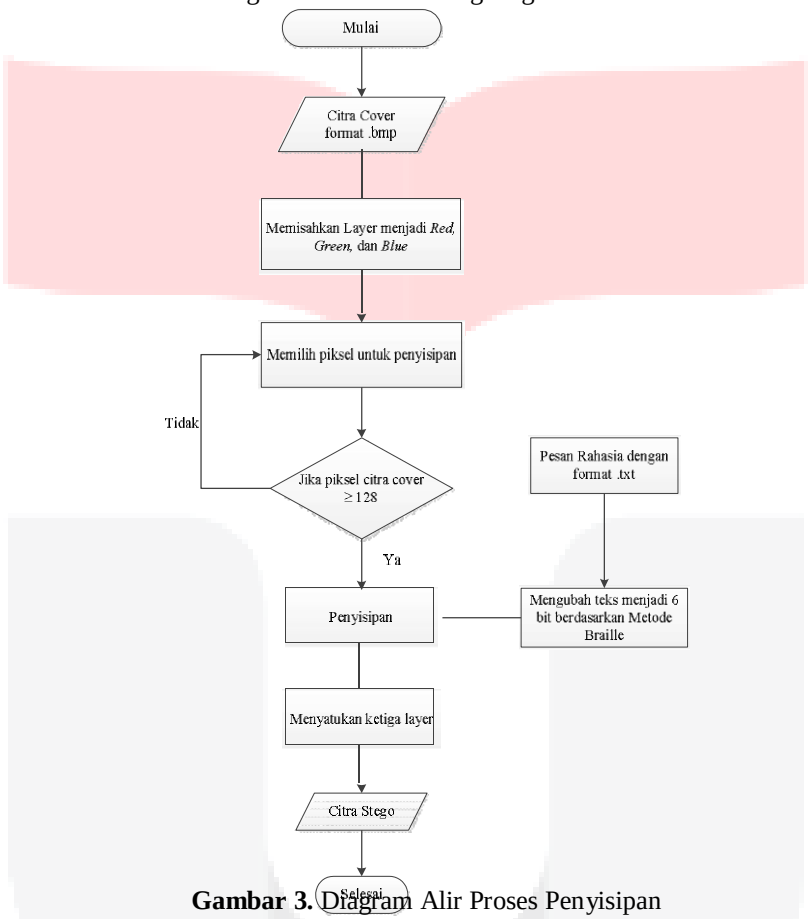
Char	Black Dots Index in Cell	Binary Representation						Char	Black Dots Index in Cell	Binary Representation					
		1st	2nd	3rd	4th	5th	6th			1st	2nd	3rd	4th	5th	6th
a	1	1	0	0	0	0	0	6	1,2,4,6	1	1	0	1	0	1
b	1, 2	1	1	0	0	0	0	7	1,2,4,5,6	1	1	0	1	1	1
c	1, 4	1	0	0	1	0	0	8	1,2,5,6	1	1	0	0	1	1
d	1, 4, 5	1	0	0	1	1	0	9	2,4,6	0	1	0	1	0	1
e	1, 5	1	0	0	0	1	0	0	1,2,3,4,5,6	1	1	1	1	1	1
f	1, 2, 4	1	1	0	1	0	0	,	2	0	1	0	0	0	0
g	1, 2, 4, 5	1	1	0	1	1	0	;	2,3	0	1	1	0	0	0
h	1, 2, 5	1	1	0	0	1	0	:	2,5	0	1	0	0	1	0
i	2, 4	0	1	0	1	0	0	.	2,5,6	0	1	0	0	1	1
j	2, 4, 5	0	1	0	1	1	0	?	2,6	0	1	0	0	0	1
k	1, 3	1	0	1	0	0	0	!	3,4,5,6	0	0	1	1	1	1
l	1, 2, 3	1	1	1	0	0	0	'	3	0	0	1	0	0	0
m	1, 3, 4	1	0	1	1	0	0	-	3,6	0	0	1	0	0	1
n	1, 3, 4, 5	1	0	1	1	1	0	"	4	0	0	0	1	0	0
o	1, 3, 5	1	0	1	0	1	0	&	1,2,3,4,6	1	1	1	1	0	1
p	1, 2, 3, 4	1	1	1	1	0	0	[	1,2,3,5,6	1	1	1	0	1	1
q	1, 2, 3, 4, 5	1	1	1	1	1	0	@	2,3,4,6	0	1	1	1	0	1
r	1, 2, 3, 5	1	1	1	0	1	0	]	2,3,4,5,6	0	1	1	1	1	1
s	2, 3, 4	0	1	1	1	0	0	+	2,3,5	0	1	1	0	1	0
t	2, 3, 4, 5	0	1	1	1	1	0	=	2,3,5,6	0	1	1	0	1	1
u	1, 3, 6	1	0	1	0	0	1	<	2,3,6	0	1	1	0	0	1
v	1, 2, 3, 6	1	1	1	0	0	1	*	3,5	0	0	1	0	1	0
w	2, 4, 5, 6	0	1	0	1	1	1	>	3,5,6	0	0	1	0	1	1
x	1, 3, 4, 6	1	0	1	1	0	1	/	3,4	0	0	1	1	0	0
y	1, 3, 4, 5, 6	1	0	1	1	1	1	)	3,4,5	0	0	1	1	1	0
z	1, 3, 5, 6	1	0	1	0	1	1	-	3,4,6	0	0	1	1	0	1
1	1, 6	1	0	0	0	0	1	(	4,5	0	0	0	1	1	0
2	1, 2, 6	1	1	0	0	0	1	$	4,5,6	0	0	0	1	1	1
3	1, 4, 6	1	0	0	1	0	1	%	4,6	0	0	0	1	0	1
4	1, 4, 5, 6	1	0	0	1	1	1	Space	Empty Cell	0	0	0	0	0	0
5	1, 5, 6	1	0	0	0	1	1								

3. Perancangan Sistem

A. Diagram Alir Sistem



Gambar 2. Diagram Alir Sistem Steganografi secara Umum

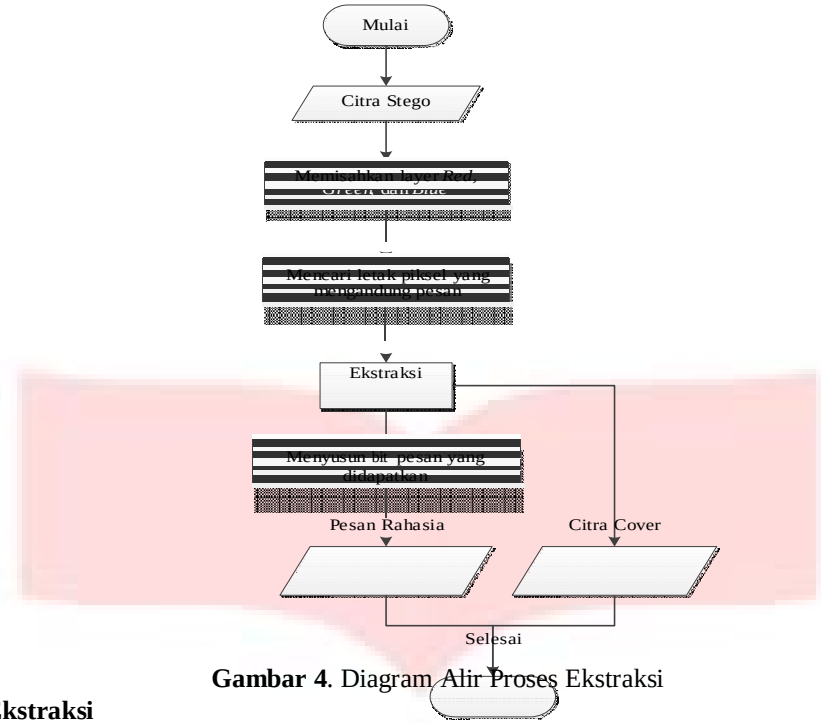


Gambar 3. Diagram Alir Proses Penyisipan

B. Proses Penyisipan

Proses penyisipan steganografi dapat dijelaskan sebagai berikut

1. Citra *cover* yang digunakan sebagai media penyisipan berupa citra berformat .bmp
2. Pisahkan setiap layer pada citra *cover* menjadi leyer R(merah), G(hijau), dan B(Biru)
3. Tentukan posisi piksel yang akan disisipkan pesan. Letak piksel yang memungkinkan disisipi pesan harus lebih besar atau sama dengan 128 piksel.
4. Pesan rahasia dalam bentuk teks dan diubah menjadi bentuk 6 bit berdasarkan metode braille
5. Proses penyisipan dilakukan menggunakan metode LSB dengan cara mengganti bit terakhir cover dengan bit pesan rahasia. Penyisipan pesan dimulai dari layer merah, jika posisi pada layer merah tidak cukup menampung seluruh bit pesan, penyisipan dilanjutkan di layer hijau selanjutnya layer biru.
6. Citra yang sudah disisipkan pesan dilakukan serangan/gangguan berupa *noise* gaussian, *noise* salt & pepper, *resize*, dan *cropping.*
7. Setelah diberikan serangan/gangguan gabungkan kembali setiap layer yang telah disisipi pesan menjadi citra stego berformat .bmp



Gambar 4. Diagram Alir Proses Ekstraksi

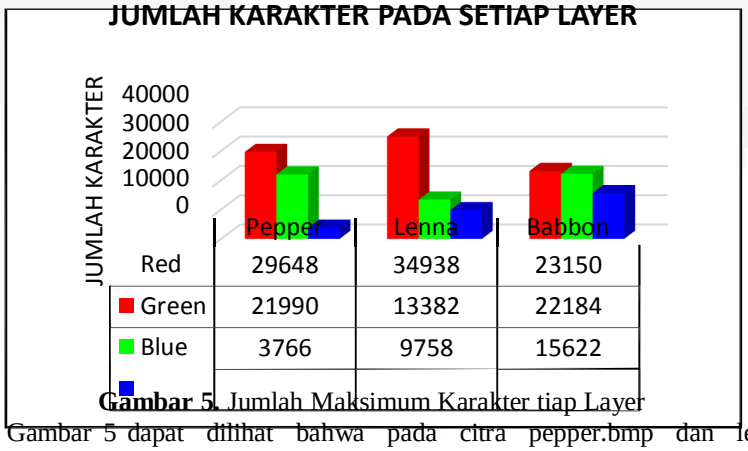
C. Proses Ekstraksi

Proses penyisipan steganografi dapat dijelaskan sebagai berikut

1. Penerima menerima citra stego dari pengirim, lalu pisahkan setiap layer pada citra stego menjadi layer R (merah), G(hijau), dan B(Biru).
2. Setelah layer dipisahkan maka tentukan lokasi piksel yang telah disisipi pesan.
3. Ekstraksi citra stego tersebut untuk mendapatkan citra cover dan pesan rahasia. Dengan mengambil nilai bit pada kolom ke 8 dari setiap baris yang sesuai dengan letak piksel yang disisipi sehingga jumlah bit sama dengan jumlah bit pesan yang disisipkan.
4. Susun bit-bit yang telah diambil menjadi pesan rahasia. Pada proses ekstraksi selain menghasilkan pesan rahasia juga menghasilkan citra cover yang digunakan.

5. Hasil Pengujian

A. Analisis Jumlah Karakter Maksimum



Gambar 5. Jumlah Maksimum Karakter tiap Layer

Berdasarkan Gambar 5 dapat dilihat bahwa pada citra pepper.bmp dan lenna.bmp memiliki kapasitas tampung karakter untuk layer red lebih besar dari kedua layer lainnya. Hal ini dikarenakan jika dilihat kedua citra tersebut memiliki kombinasi warna kemerah-merahan lebih mencolok. Sedangkan pada citra baboon.bmp memiliki kapasitas tampung karakter untuk layer red, green dan blue memiliki nilai yang hampir sama. Hal itu terjadi karena pada citra baboon.bmp memiliki kombinasi warna merah, hijau dan biru yang hampir merata.

B. Analisis Pengaruh Banyak Pesan Rahasia pada Citra Cover

Tabel 2. Jumlah Karakter terhadap Persentase Penyisipan Total Kapasitas Pesan

Jenis Citra	25% penyisipan	50% penyisipan	75% penyisipan	100% penyisipan
Pepper.bmp	13851	27702	41553	55404
Lenna.bmp	14520	29039	43559	58078
Baboon.bmp	15239	30478	45717	60956

Tabel 3. Hasil Ekstraksi Pesan Tanpa Gangguan

Jenis Penyisipan	Pepper.bmp				Lenna.bmp				Baboon.bmp			
	CER	BER	MSE	PSNR	CER	BER	MSE	PSNR	CER	BER	MSE	PSNR
25% penyisipan	0	0	0,052	140,329	0	0	0,056	139,708	0	0	0,058	139,228
50% penyisipan	0	0	0,105	133,354	0	0	0,111	132,81	0	0	0,117	132,323
75% penyisipan	0	0	0,158	129,286	0	0	0,167	128,743	0	0	0,175	128,262
100% penyisipan	0	0	0,210	126,435	0	0	0,222	125,869	0	0	0,233	125,394

Pada Tabel 3 dapat dilihat bahwa hasil ekstraksi pesan tanpa adanya gangguan memiliki nilai CER dan BER sama dengan 0 ini berarti tidak ada karakter dan bit yang eror setelah diekstraksi. Karakter dan bit pesan yang dikirim oleh pengirim dapat diterima sempurna oleh penerima. Dapat dilihat semakin banyak karakter yang disisipkan pada citra maka semakin tinggi nilai MSE karena nilai eror antara citra cover dan stego semakin besar. Sedangkan nilai PSNR semakin tinggi karena semakin buruk kualitas citra tersebut.

C. Analisis Citra Stego ketika diberi Gangguan

- Gangguan *noise* gaussian pada citra stego

Tabel 4. Hasil Ekstraksi Pesan dengan Gangguan *noise* Gaussian

	Variance	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09	0,1
Baboon.bmp	CER	0,9848	0,9848	0,9849	0,9852	0,9855	0,9865	0,9866	0,9869	0,9875	0,9882
	BER	0,5046	0,5062	0,5098	0,5125	0,5150	0,5171	0,5182	0,5226	0,5240	0,5256
	MSE	625,235	1211,8	1747,22	2250,81	2715,52	3161,03	3566,87	3949,15	4301,74	4634,79
	PSNR	46,444	39,827	36,168	33,635	31,758	30,239	29,031	28,013	27,158	26,412

Pada Tabel 4 dapat dilihat bahwa semakin besar nilai *variance noise* gaussian maka semakin banyak jumlah *noise* yang tersebar dalam citra sehingga membuat nilai BER, CER dan MSE semakin tinggi sedangkan nilai PSNR semakin kecil karena kualitas citra menjadi menurun.

- Gangguan *noise* salt & pepper pada citra stego

Tabel 5. Hasil Ekstraksi Pesan dengan Gangguan *Noise* Gaussian

	Variance	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09	0,1
Baboon.bmp	CER	0,9664	0,9675	0,9685	0,9687	0,9705	0,9720	0,9732	0,9736	0,9744	0,9757
	BER	0,4688	0,4718	0,4731	0,4745	0,4766	0,4780	0,4799	0,4815	0,4832	0,4858
	MSE	194,269	389,978	581,742	769,894	965,926	1172,52	1361,54	1553,77	1747,56	1954,45
	PSNR	58,1328	51,1644	47,165	44,3627	42,0944	40,1561	38,6616	37,3409	36,1655	35,0466

Pada tabel 5 dapat dilihat bahwa nilai CER, BER, dan MSE semakin meningkat karena nilai *variance noise* salt & pepper semakin ditingkatkan. Namun nilai PSNR semakin menurun karena kualitas citra menjadi buruk ketika *variance noise* salt & pepper besar.

- Gangguan *resize* pada citra stego

Tabel 6. Hasil Ekstraksi Pesan dengan Gangguan *Resize*

	Piksel	0,5	0,75	1,25
Baboon.bmp	CER	0,9999	0,9911	0,9972
	BER	0,9969	0,7206	0,9170
	MSE	0,169	0,215	0,252
	PSNR	128,613	126,218	124,609

Pada Tabel 6 dapat dilihat bahwa ketika dilakukan *resize* sebesar 0,5 piksel didapatkan nilai CER sebesar 0,999 dan nilai BER sebesar 0,9969 menunjukkan bahwa hampir semua bit dan karakter yang diterima tidak dapat diekstraksi sempurna. Kemudian nilai PSNR terbaik yaitu 128,613dB dan nilai MSE terkecil sebesar 0,169 terjadi ketika dilakukan *resize* sebesar 0,5 piksel.

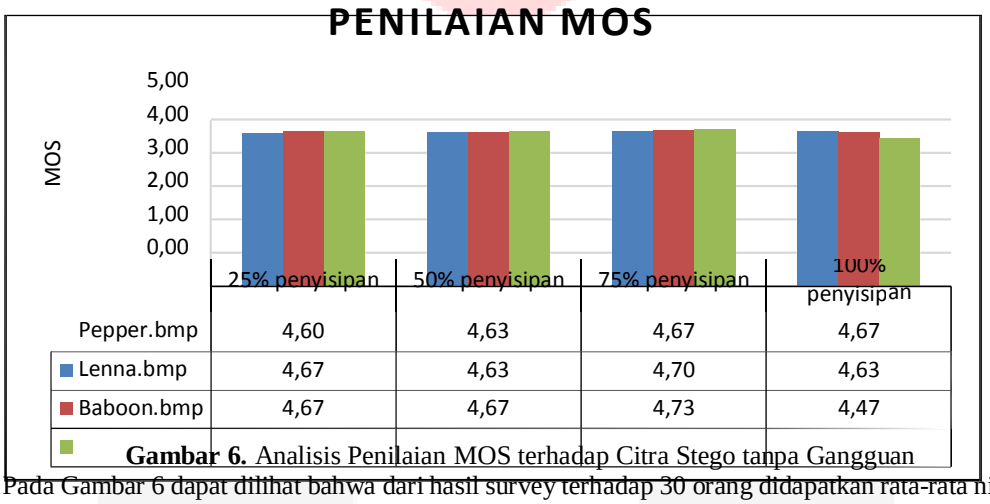
- Gangguan *cropping* pada citra stego

Tabel 7. Hasil Ekstraksi Pesan dengan Gangguan *Cropping*

Baboon.bmp	Piksel	10	20	30	40	50	60	70	80	90	100
	CER	0,968	0,971	0,973	0,976	0,976	0,978	0,980	0,982	0,984	0,985
	BER	0,503	0,542	0,578	0,609	0,638	0,670	0,699	0,724	0,751	0,776
	MSE	0,23499	0,23594	0,23706	0,24096	0,244983	0,247744	0,250258	0,252794	0,259115	0,26605
	PSNR	125,308	125,267	125,22	125,056	124,891	124,779	124,678	124,498	124,33	124,066

Pada Tabel 7 dapat dilihat bahwa semakin besar nilai piksel yang dicropping maka semakin banyak piksel yang hilang. Dapat dilihat bahwa nilai tertinggi pada CER sebesar 0,985, nilai BER sebesar 0,776 dan nilai MSE sebesar 0,26605 terjadi pada saat dilakukan *cropping* sebesar 100 piksel. Nilai PSNR terbesar sebesar 125, 308 ketika dilakukan *cropping* sebesar 10 piksel kualitas citra masih bagus karena hanya sedikit piksel yang hilang.

D. Analisis Penilaian MOS



Gambar 6. Analisis Penilaian MOS terhadap Citra Stego tanpa Gangguan

Pada Gambar 6 dapat dilihat bahwa dari hasil survey terhadap 30 orang didapatkan rata-rata nilai MOS dari ketiga citra dari rentang 4,47 – 4,73 pada skala 1-5. Hal ini menunjukkan bahwa secara kasat mata citra cover terlihat sangat mirip dengan citra stego.

E. Kesimpulan

Dari hasil perancangan dan pengujian sistem steganografi teks pada citra digital menggunakan metode Braille dan pemililah piksel LSB dapat disimpulkan bahwa sistem dapat melakukan proses penyisipan dan ekstraksi dengan baik, panjang pesan yang dapat disisipkan bergantung pada ukuran citra cover dan kepadatan piksel. Berdasarkan penilaian secara objektif ketika citra stego tidak diberi serangan nilai BER sebesar 0 dan nilai CER sebesar 0 ini berarti tidak ada bit pesan dan karakter yang eror setelah diekstraksi dan memiliki nilai rata-rata PSNR sebesar 125,899dB dan MSE sebesar 0,221 pada karakter maksimum yang dapat disisipkan. Saat sistem steganografi disisipkan karakter penuh dan diberikan serangan *noise* gaussian mempunyai nilai rata-rata BER sebesar 0,5156, CER sebesar 0,9861, nilai MSE sebesar 2816,4165 dan nilai PSNR sebesar 32,8682 dB. Saat diberikan serangan *noise* salt & pepper mempunyai nilai rata-rata BER sebesar 0,4773, nilai CER sebesar 0,9710, nilai MSE sebesar 1069,16 dan nilai PSNR sebesar 43,0290 dB. Saat sistem steganografi diberikan serangan *resize* mempunyai nilai rata-rata BER sebesar 0,8782, nilai CER sebesar 0,9961, nilai MSE sebesar 0,2118 dan nilai PSNR sebesar 126,48 dB. Saat diberikan serangan *cropping* mempunyai nilai rata-rata BER sebesar 0,649, nilai CER sebesar 0,977, nilai MSE sebesar 0,247 dan nilai PSNR sebesar 124,80 dB. Berdasarkan hasil pengujian sistem steganografi ini tidak tahan terhadap serangan *noise* gaussian dan salt & pepper serta serangan *resize* dan *cropping.* Karena hasil pesan setelah diekstraksi berbeda dengan pesan asli. Berdasarkan penilaian subjektif dari hasil pengamatan oleh 30 orang responden nilai MOS diantara 4,47 –

4,73 pada skala 1-5 yang menunjukkan bahwa hasil citra stego terlihat mirip dengan citra cover sehingga tidak ada yang menduga bahwa di dalam citra tersebut terdapat pesan rahasia.

Daftar Pustaka

[1]. Ali, Abdelmgeid Amin dan Saad, Hussien Seddik. 2013 *Image Steganography Technique By Using Braille*. International Journal of Image Processing (IJIP).7, (1).
[2]. Andrian, Yudhi. (2013). *"Perbandingan Metode LSB, LSB+1, dan MSB pada Steganografi Citra Digital"*. Prosiding SNIf. Medan.
[3] Munir, Rinaldi. (2004). Pengolahan Citra Digital dengan Pendekatan Algoritmik. Bandung: Informatika.
[4] Munir, Rinaldi. (2006). Kriptografi, Bandung: Informatika.
[5] Putra, Darma. (2010). *Pengolahan Citra Digital*, Yogyakarta: Andi.
[6] Sutoyo, T. et al. (2009). Teori Pengolahan Citra Digital, Yogyakarta: Andi.