

SIMULASI DAN ANALISIS STEGANOGRAFI CITRA DIGITAL BERDASARKAN PRINSIP LINTASAN KUBUS RUBIK DENGAN KOREKSI KESALAHAN MENGGUNAKAN KODE KONVOLUSI

SIMULATION AND ANALYSIS OF DIGITAL IMAGE STEGANOGRAPHY BASED ON THE PRINCIPLE OF RUBIK'S CUBE TRAILS WITH ERROR CORRECTION USING CONVOLUTION CODES

Fitria Rahma Nur Sulisty¹, Dr. Ir. Bambang Hidayat², Suci Aulia S.T., M.T³

^{1,2}Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

³Prodi D3 Teknik Telekomunikasi, Fakultas Ilmu Terapan, Universitas Telkom

¹itafitriarahma@students.telkomuniversity.ac.id ²bhidayat@telkomuniversity.ac.id

³suciaulia@telkomuniversity.ac.id

Abstrak

Steganografi memiliki tujuan utama agar pesan yang dikirimkan dapat tiba hingga penerima tanpa membuat orang lain mengetahui isi pesan tersebut. Pada tugas akhir ini digunakan metode steganografi kubus rubik yaitu salah satu teknik penetapan posisi pesan *stego* untuk penyisipan pesan teks pada citra digital. Pola pengacakan rubik digunakan sebagai referensi penyisipan pesan teks pada citra digital. Untuk mengurangi *error* pada saat ada gangguan, digunakan metode *error correction* kode konvolusi. Berdasarkan hasil pengujian dari sistem ini, saat tidak diberi gangguan dan pesan rahasia masih dalam batas kapasitas penyisipan didapat nilai BER Odengan nilai PSNR (*Peak Signal to Noise Ratio*) diatas 75dB. Jumlah karakter yang dapat disisipkan pada *cover* saat menggunakan *convolutional code* lebih sedikit bila dibandingkan dengan penyisipan tanpa *convolutional code*. Pengujian sistem menggunakan *noise salt & pepper*, *noise Gaussian*, *noise Poisson*, *noise localvar*, *resize*, *crop*, *rotate*, *brightness*.

Kata kunci : steganografi, citra digital, kubus rubik

Abstract

Steganography has a main purpose that messages sent can arrive to the recipient without making others aware of the contents of the message. This final use steganography rubik's cube methods which is one of the techniques for the determination of position stego message insertion of text messages on the digital image. Rubik shuffling pattern is used as a reference insertion of text messages on the digital image. To reduce the error, convolution code methode used for error correction. Based on the system testing result, when there were disturbances and a secret message is still within the limits of the insertion capacity of BER value 0 obtained with the value of PSNR (Peak Signal to Noise Ratio) above 75dB. The number of characters that can be inserted on the cover when using convolutional code is less compared with the insertion without convolutional code. System attacked using salt & pepper noise, Gaussian noise, Poisson noise, noise localvar, resize, crop, rotate, brightness.

Key : *steganography, digital images, rubik's cube*

1. Pendahuluan

1.1 Latar Belakang

Salah satu cara memberi keamanan pada data yaitu dengan teknik steganografi. Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui [1]. Pesan rahasia pada steganografi dapat berupa pesan tulisan, audio, gambar, atau video yang disisipkan pada media lainnya. Saat ini sudah terdapat banyak metode yang digunakan pada steganografi. Pada penelitian sebelumnya telah dilakukan simulasi metode kubus rubik yang digunakan pada proses enkripsi [2], dan pada penelitian [3], metode steganografi yang digunakan yaitu metode sudoku *puzzle* acak.

Pada tugas akhir ini dilakukan penelitian yang dengan metode kubus rubik ini digunakan untuk menentukan posisi penyisipan pesan rahasia pada citra *cover* digital. Penyisipan pesan rahasia pada citra dilakukan dengan menggunakan metode *Modified Least Significant Bit* (LSB). Untuk menjamin keakuratan data yang diterima di sisi penerima, digunakan teknik deteksi dan koreksi kesalahan dengan kode konvolusi.

Penelitian yang dilakukan pada tugas akhir ini menghasilkan metode steganografi yang berbeda dari yang sudah ada sebelumnya yaitu dengan metode prinsip kubus rubik dan koreksi kesalahan kode konvolusi. Hasil dari proses steganografi yang dilakukan ini memiliki nilai BER 0, PNSR yang lebih besar dari 75dB.

2. Dasar Teori

2.1 Steganografi

Steganografi berasal dari Bahasa Yunani, yaitu “*steganos*” dan “*graphein*” yang berarti “*covered writing* (tulisan tersembunyi)”. Steganografi merupakan ilmu dan seni menyembunyikan pesan rahasia sehingga keberadaan pesan tidak terdeteksi oleh indera manusia [1]. Pada steganografi, bentuk pesan rahasia yang dikirim banyak macamnya, seperti teks, citra, dan lain sebagainya, sedangkan media yang digunakan sebagai *cover* atau media untuk menyembunyikan data dapat berupa teks, audio, citra digital, atau video.

2.2 Citra Digital^[6]

Citra digital adalah gambar dua dimensi yang bisa ditampilkan pada layar komputer sebagai himpunan/diskrit nilai digital yang disebut pixel/picture elements. Pada citra digital, tiap pixel memiliki koordinat tersendiri, dan memiliki nilai yang bervariasi. Nilai tersebut akan menentukan warna yang muncul pada layar. Tiap warna merupakan kombinasi dari tiga warna dasar yaitu merah, hijau, dan biru (*Red, Green, Blue* – RGB).

Suatu citra dapat didefinisikan sebagai fungsi $f(x,y)$ berukuran M baris dan N kolom, dengan x dan y adalah koordinat spasial, dan amplitudo f di titik koordinat (x,y) dinamakan intensitas keabuan dari citra pada titik tersebut. Apabila nilai x , y , dan nilai amplitudo f secara keseluruhan berhingga (*finite*) dan bernilai diskrit maka dapat dikatakan bahwa citra tersebut adalah citra digital.

2.3 Metode berdasarkan Prinsip Kubus Rubik^[8]

Pada tugas akhir ini, kubus rubik yang akan dijadikan acuan yaitu rubik $4 \times 4 \times 4$. Metode kubus rubik dijadikan sebagai penentu posisi bit-bit pesan rahasia pada citra (*cover*). Kubus rubik akan diputar-putar sehingga posisi rubik berubah, posisi perubahan tersebut yang akan menjadi acuan posisi penyisipan bit pesan rahasia. Persamaan kubus rubik yang dipakai yaitu sebagai berikut.

$$f_{i,j,k} = \{16, 33, 49, 65, 81\} ; i = 1,2,3, \dots, 8 \quad (2.1)$$

2.4 Modified Least Significant Bit (MLSB)

Modified LSB merupakan salah satu teknik yang digunakan pada steganografi paling sederhana yang bekerja pada domain spasial. Pada metode ini, bit-bit data rahasia disimpan pada bit LSB citra. Bit pesan rahasia akan disisipkan dengan syarat nilai MSB dari piksel tersebut bernilai 1. Contoh MSB dan LSB yaitu pada *byte* 01001011, angka bit 0 (pertama, digarisbawahi) merupakan bit MSB, sedangkan angka bit 1 (terakhir, digarisbawahi) merupakan bit LSB.

2.5 Kode Konvolusi^{[4][7]}

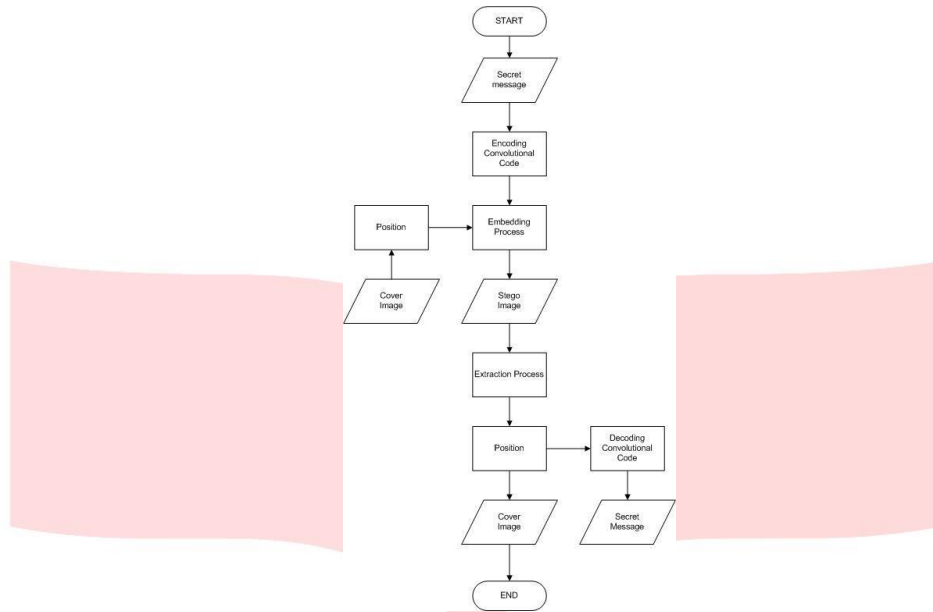
Kode konvolusi terdiri dari satu set rangkaian bilangan biner yang dihasilkan dari *encoder* konvolusi. Pada teori, urutan kode konvolusi memiliki durasi yang tak terhingga. Pada pelaksanaannya, kondisi kode konvolusi yaitu secara berkala dipaksa untuk sebuah kondisi yang sudah diketahui dan rangkaian kode dihasilkan dari sebuah cara penghalang. Kode konvolusi non-rekursif yaitu dimana tidak terdapat umpan balik pada kode konvolusi tersebut.

3. Perancangan Sistem

Steganografi terdiri dari dua proses, yaitu proses penyisipan (*embedding*) yang dilakukan di sisi pengirim dan ekstraksi (*extraction*) yang dilakukan di sisi penerima.

Di sisi pengirim, pesan rahasia (*secret message*) akan disisipkan ke dalam *cover* yang berupa citra digital RGB. Hasil dari *cover* yang telah disisipi pesan rahasia yaitu *stego image*. Untuk pengujian akan dilakukan pada *stego image* dengan menggunakan beberapa serangan (*attack*) seperti noise. Kemudian di sisi penerima, *stego image* yang telah diserang (*attack*) akan diekstraksi agar pesan rahasia (*secret message*) dapat dipisahkan dari *cover image* yang tidak disisipi pesan rahasia.

Diagram alir sistem steganografi berdasarkan prinsip kubus rubik dapat dilihat pada gambar 1 berikut.



Gambar 1. Diagram Alir Sistem Steganografi secara Umum

4. Pengujian Sistem

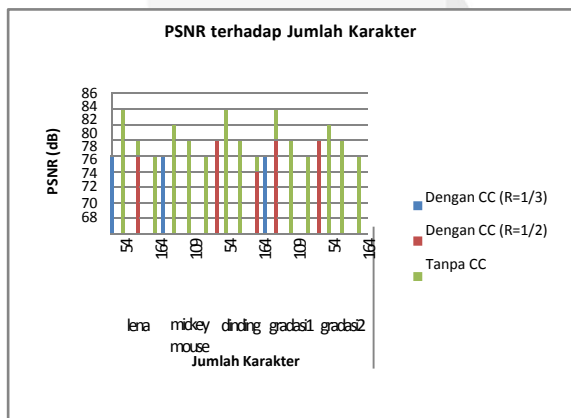
4.1 Analisis Pengaruh Ukuran Citra Cover dan Penggunaan Convolutional Code terhadap Kapasitas Penyisipan Pesan

Tabel 1. Kapasitas Maksimum Penyisipan Pesan

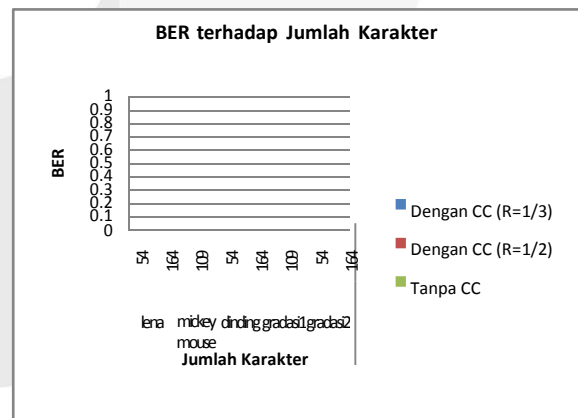
Citra	Jumlah Karakter Maksimum		
	Dengan CC (R=1/3)	Dengan CC (R=1/2)	Tanpa CC
lena	4439	6659	13319
mickey mouse	13956	20934	41868
dinding	14802	22203	44406
gradasi1	2126	3190	6380
gradasi2	1514	2271	4543

Pada tabel 1 di atas, dapat dilihat bahwa semakin besar ukuran citra, maka kapasitas pesan yang dapat disisipkan semakin bertambah pula. Pengaruh dari penggunaan convolutional code (cc) yaitu jumlah karakter yang dapat disisipkan lebih sedikit dibandingkan dengan penyisipan tanpa cc.

4.2 Analisis Pengaruh Jumlah karakter dan Penggunaan Convolutional Code terhadap PSNR Citra Stego dan BER Pesan Terekstraksi



Gambar 2. Pengaruh Jumlah Karakter pada Nilai PSNR



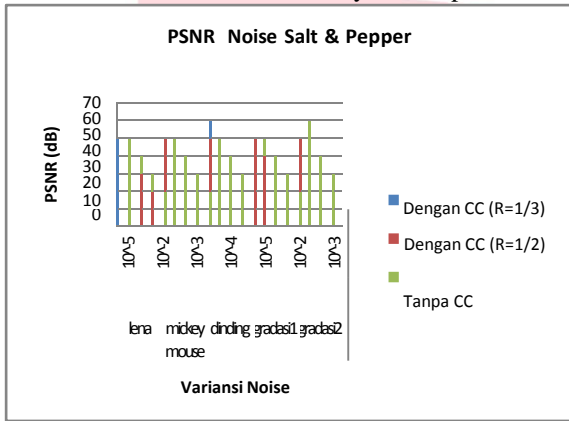
Gambar 3. Pengaruh Jumlah Karakter pada Nilai BER

Pengaruh dari jumlah karakter terhadap nilai PSNR berdasarkan gambar 2 yaitu semakin banyak jumlah karakter pesan rahasia yang disisipkan maka nilai PSNR menjadi semakin kecil. Hal tersebut terjadi karena semakin banyak pesan yang disisipkan, maka nilai piksel citra yang berubah menjadi semakin banyak. Pengaruh dari ukuran citra yaitu semakin besar ukuran citra maka nilai PSNR akan semakin besar pula.

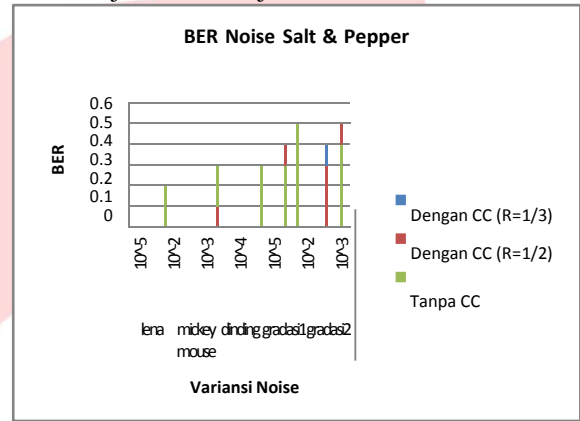
Pada gambar 3 dapat dilihat bahwa nilai BER tetap 0 dengan jumlah karakter yang disisipkan hingga 164 karakter. Hal ini menunjukkan bahwa jumlah karakter 164 masih dapat disisipkan pada citra dan dapat diekstraksi dengan sempurna. Pesan tersebut dapat terekstraksi sempurna pada lima citra yang diujikan.

4.3 Analisis Pengaruh Noise Salt and Pepper dan Penggunaan Convolutional Code terhadap PSNR Citra Stego dan BER Pesan Terekstraksi

Berdasarkan gambar 4 dapat dilihat bahwa pengaruh *noise salt and pepper* yaitu semakin besar variansi *noise salt and pepper* maka nilai PSNR menjadi semakin kecil. Hal tersebut terjadi karena semakin besar variansi *noise* maka semakin banyak nilai piksel citra yang diubah menjadi merah, hijau, atau biru.



Gambar 4. Pengaruh Noise Salt & Pepper Pada nilai PSNR Citra



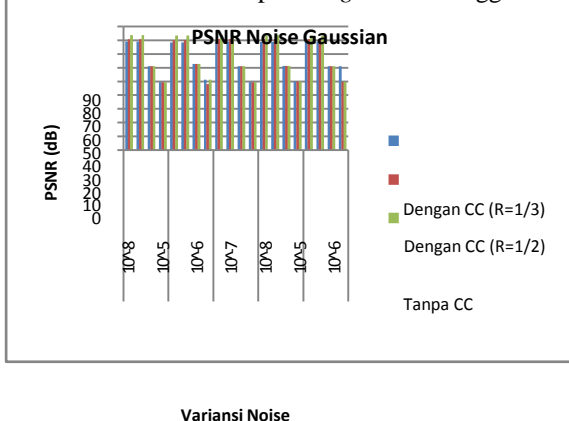
Gambar 5. Pengaruh Noise Salt & Pepper Pada nilai BER Citra

Saat variansi *noise* semakin besar, nilai BER menjadi semakin besar pula, seperti terlihat pada gambar 5. Pada citra lena.bmp, sistem memiliki ketahanan terhadap *noise salt and pepper* hingga variansi *noise* 10⁻⁴. Pada citra mickey mouse.bmp dan dinding.bmp, sistem memiliki ketahanan terhadap *noise salt and pepper* hingga variansi *noise* 10⁻³. Pada citra gradasi1.bmp, sistem memiliki ketahanan terhadap *noise salt and pepper* hingga variansi *noise* 10⁻⁴. Sedangkan pada citra gradasi2.bmp, sistem tahan terhadap *noise gaussian* hingga variansi *noise* 10⁻⁵.

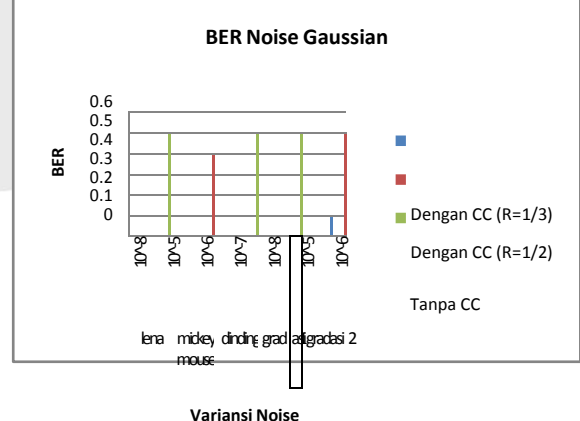
Nilai BER saat menggunakan *convolutional code* lebih kecil daripada saat *convolutional code* tidak digunakan. Semakin kecil *rate* dari *convolutional code* mengakibatkan semakin kecil nilai BER. Citra yang memiliki ketahanan paling tinggi terhadap *noise salt and pepper* yaitu citra mickey mouse.bmp dan dinding.bmp. Sedangkan citra yang memiliki ketahanan paling rendah terhadap *noise salt and pepper* yaitu citra gradasi2.bmp.

4.4 Analisis Pengaruh Noise Gaussian dan Penggunaan Convolutional Code terhadap PSNR Citra Stego dan BER Pesan Terekstraksi

Pengaruh *noise gaussian* pada nilai PSNR yaitu semakin besar variansi *noise* mengakibatkan nilai PSNR semakin kecil. Hal tersebut dapat dilihat pada gambar 6. Sedangkan untuk BER tanpa menggunakan *convolutional code* memiliki nilai yang lebih besar dibandingkan saat menggunakan *convolutional code*. Semakin kecil *rate convolutional code* maka kemampuan koreksi error menjadi semakin besar, seperti terlihat pada gambar 7. Sistem ini tahan terhadap *noise gaussian* hingga variansi *noise* 10⁻⁷.

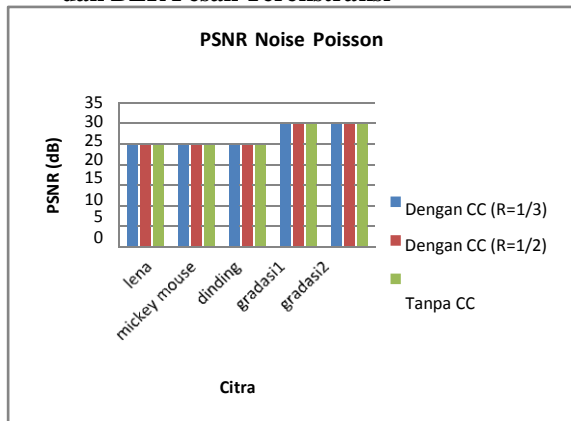


Gambar 6. Pengaruh Noise Gaussian Pada nilai PSNR Citra

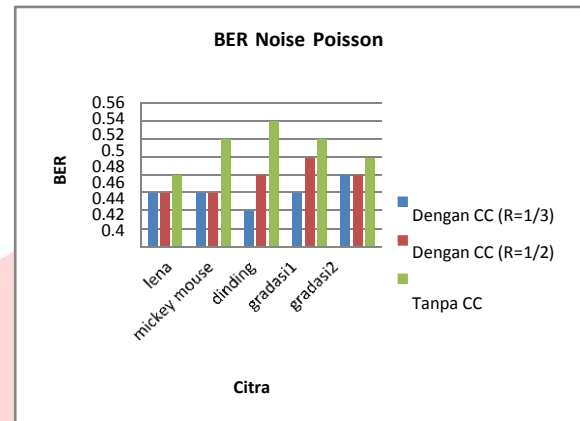


Gambar 7. Pengaruh Noise Gaussian Pada nilai BER Citra

4.5 Analisis Pengaruh Noise Poisson dan Penggunaan Convolutional Code terhadap PSNR Citra Stego dan BER Pesan Terekstraksi



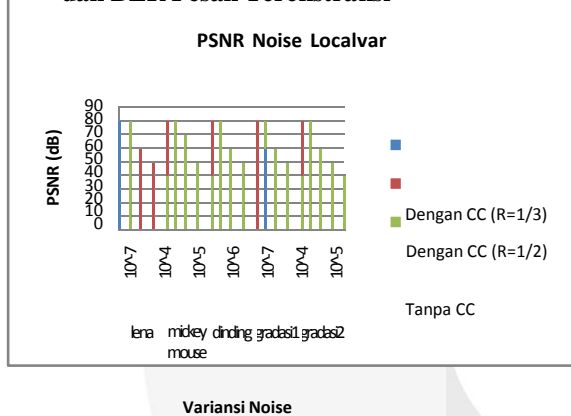
Gambar 8. Pengaruh *Noise Poisson* Pada nilai PSNR Citra



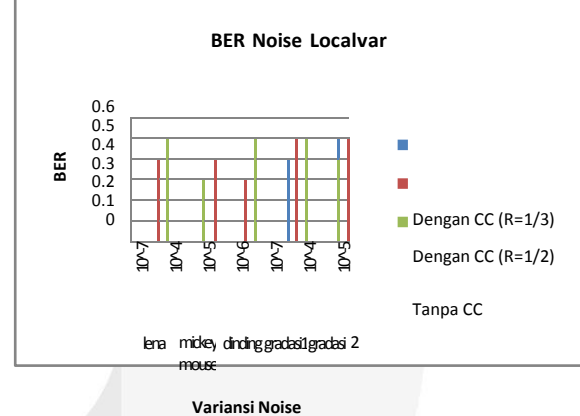
Gambar 9. Pengaruh *Noise Poisson* Pada nilai BER Citra

Berdasarkan gambar 8, pengaruh *noise poisson* terhadap PSNR bergantung pada citra yang digunakan. Nilai PSNR paling kecil yaitu saat menggunakan citra dinding.bmp. Untuk nilai BER dapat dilihat pada gambar 4.15. Kemampuan koreksi *convolutional code* dengan rate 1/3 lebih baik dibandingkan dengan *convolutional code* dengan rate 1/2. Hasil tersebut dapat dilihat pada gambar 9.

4.6 Analisis Pengaruh Noise Localvar dan Penggunaan Convolutional Code terhadap PSNR Citra Stego dan BER Pesan Terekstraksi



Gambar 10. Pengaruh *Noise Localvar* Pada nilai PSNR Citra

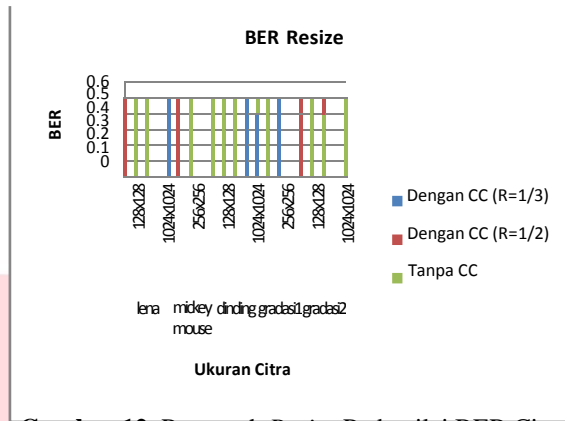


Gambar 11. Pengaruh *Noise Localvar* Pada nilai BER Citra

Pada gambar 10 dapat dilihat pengaruh *noise localvar* terhadap nilai PSNR. Semakin besar variansi *noise localvar* maka nilai PSNR akan semakin kecil. Sedangkan untuk BER dapat dilihat pada gambar 11, saat menggunakan *convolutional code* nilai BER lebih kecil daripada saat tidak menggunakan *convolutional code*. *Convolutional code* dengan rate 1/3 memiliki nilai BER lebih kecil daripada *convolutional code* dengan rate 1/2 karena semakin kecil nilai *rate* maka kemampuan koreksi menjadi semakin besar.

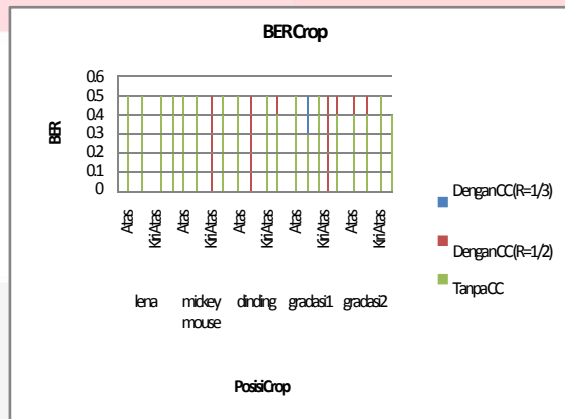
4.7 Analisis Pengaruh Resize dan Penggunaan Convolutional Code terhadap BER Pesan Terekstraksi

Pengaruh *resize* terhadap BER yaitu bergantung dari ukuran citra stego dan perubahan ukurannya seperti terlihat pada gambar 12. Saat penyisipan menggunakan *convolutional code* maupun tidak menggunakan *convolutional code* tidak memiliki pola yang pasti dan tidak ada yang lebih unggul. Hal ini dikarenakan saat citra mengalami perubahan ukuran, nilai piksel pun ikut mengalami perubahan, namun perubahan nilai piksel tersebut terjadi secara acak. Nilai BER bergantung pula pada citra yang digunakan. Sistem ini tidak dapat menahan serangan *resize*.



Gambar 12. Pengaruh *Resize* Pada nilai BER Citra

4.8 Analisis Pengaruh *Crop* dan Penggunaan *Convolutional Code* terhadap BER Pesan Terekstraksi

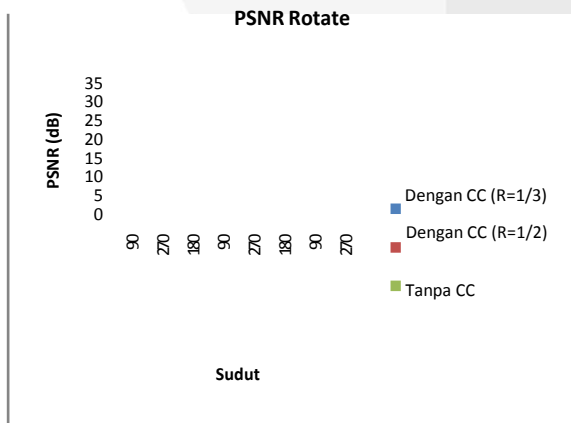


Gambar 13. Pengaruh *Crop* Pada nilai BER Citra

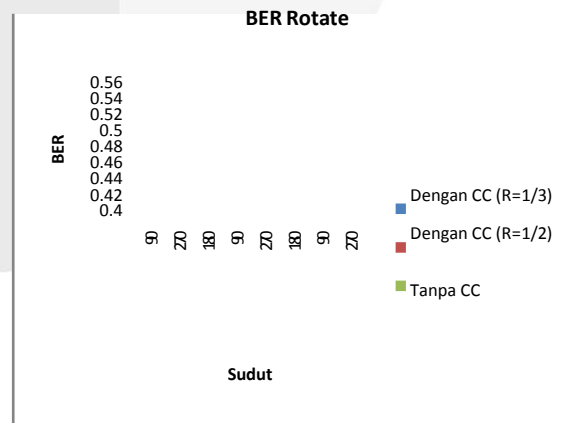
Nilai BER saat dilakukan *crop* yaitu bergantung dari posisi citra tersebut dipotong. Bila citra yang dipotong yaitu di posisi pesan rahasia tersebut disisipkan, maka nilai BER menjadi semakin kecil. Namun bila citra dipotong di posisi dimana pesan rahasia tidak disisipkan, maka nilai BER menjadi lebih besar. Hal tersebut dapat dilihat pada gambar 13. Namun pada citra gradasi 1.bmp dan gradasi 2.bmp tidak memiliki ketahanan terhadap *crop*.

4.9 Analisis Pengaruh *Rotate* dan Penggunaan *Convolutional Code* terhadap PSNR Citra Stego dan BER Pesan Terekstraksi

Pengaruh *rotate* terhadap nilai PSNR bergantung pada citra yang digunakan, seperti terlihat pada gambar 14. Pada citra dinding.bmp, gradasi1.bmp, dan gradasi2.bmp nilai PSNR paling kecil terjadi saat citra diputar dengan sudut 180°. Sedangkan pada citra lena.bmp nilai PSNR hampir sama walau sudut putar citra berbeda, dan pada citra mickey mouse.bmp nilai PSNR paling besar terjadi saat citra diputar dengan sudut 180°.



Gambar 14. Pengaruh *Rotate* Pada nilai PSNR Citra

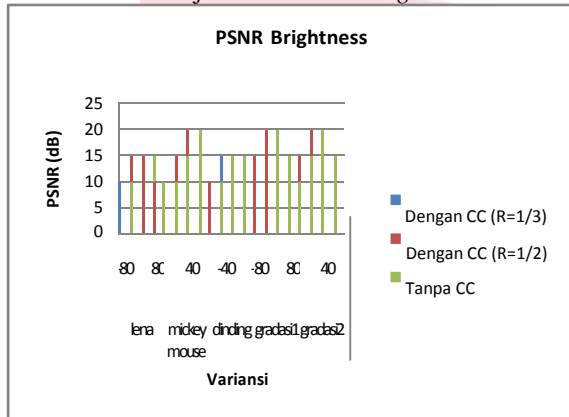


Gambar 15. Pengaruh *Rotate* Pada nilai BER Citra

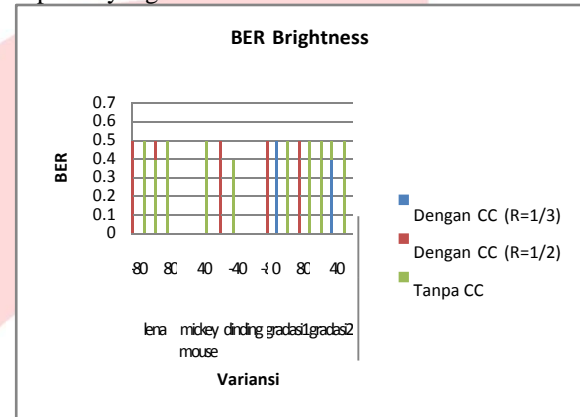
Nilai BER berdasarkan gambar 15 dapat dilihat bahwa citra yang digunakan mempengaruhi hasil yg didapat. Nilai BER yang konstan didapat saat citra digunakan yaitu mickey mouse.bmp, sedangkan pada citra lainnya nilai BER tidak memiliki pola yang pasti. Pada citra mickey mouse.bmp, nilai BER paling kecil didapat saat digunakan *convolutional code* dengan *rate* 1/3.

4.10 Analisis Pengaruh *Brightness* dan Penggunaan *Convolutional Code* terhadap PSNR Citra Stego dan BER Pesan Terekstraksi

Berdasarkan gambar 16 berikut, nilai PSNR akan semakin besar saat diberi nilai *brightness* yang mendekati 0. Hal tersebut terjadi karena saat *brightness* mendekati 0, nilai piksel yang diubah tidak terlalu besar.



Gambar 16. Pengaruh *Brightness* Pada nilai PSNR Citra



Gambar 17. Pengaruh *Brightness* Pada nilai BER Citra

Untuk nilai BER dapat dilihat dari gambar 17. Nilai BER bergantung pada citra yang digunakan. Pada citra mickey mouse.bmp, saat citra diberi *brigtness* dengan nilai -80 dan -40, pesan rahasia dapat terekstraksi dengan sempurna. Sedangkan pada citra dinding.bmp, pesan rahasia dapat terekstraksi dengan sempurna saat diberi *brightness* dengan nilai 40 dan 80. Pada citra yang lainnya pesan rahasia tidak dapat diekstraksi dengan sempurna saat diberi *brightness*.

Daftar Pustaka:

- [1] Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Penerbit Informatika.
- [2] Tampubolon, Fressilya Caroline. 2014. *Simulasi dan Analisis Steganografi Citra Digital Menggunakan Metode Sudoku Puzzle Acak dan Kode BCH*. Bandung: Universitas Telkom.
- [3] Raniprima, Savierda. 2014. *Simulasi dan Analisis Steganografi Citra Digital dengan Enkripsi Berdasarkan Prinsip Kubus Rubik*. Bandung: Universitas Telkom.
- [4] Morelos, Robert H. and Zarogaza. 2006. *The Art of Error Correcting Coding*. Southern Gate, Chicester: John Wiley & Sons, Ltd.
- [5] Moreira, Jorge Castiñeira and Farrell, Patrick Guy. 2006. *Essentials of Error-Control Coding*. Southern Gate, Chicester: John Wiley & Sons, Ltd.
- [6] Putra, Darma. 2010. *Pengolahan Citra Digital*. Yogyakarta: Andi.
- [7] Wibisono, Gunawan dan Sari, Lydia. 2011. *Teknik Pengodean Sistem Komunikasi Dijital*. Bandung: Rekayasa Sains.
- [8] Amirtharajan, Rangarajan etc. 2013. *Rubik's Cube: A Way for Random Image Steganography*. Tamil Nadu, India : SASTRA University.