# EFISIENSI STEGANOGRAFI AUDIO UNTUK MEYISIPKAN PESAN TEKS DENGAN REKONSTRUKSI IRLS DAN METODE LSB

## *EFFICIENCY OF AUDIO STEGANOGRAPHY TO SEND TEXT MESSAGES WITH IRLS RECONSTRUCTION AND LSB METHODS*

**Ilham Kurnia Eka Saputra**
Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
**ilhamkurnia@telkomuniversity.ac.id**

**Abstrak**

Menyimpan file rahasia atau mengirimkan file yang tanpa terdeteksi keberadaanya saat di transmisikan merupakan kebutuhan yang sekarang paling banyak di cari dan digunakan dalam mengirimkan pesan rahasia yang aman tanpa bisa di ketahuhi dan di serang oleh attacker dan file rahasia tersebut hanya bisa dibuka oleh penerima. Steganografi merupakan sebuah teknik dalam meningkatkan keamanan sebuah data, yaitu dengan melakukan penyisipan sebuah informasi atau pesan rahasia menggunakan sebuah media yang biasanya di sebut dengan host atau carrier atau sampul. di dalam jurnal ini menggunkan metode LSB dan Rekonstruksi IRLS. Pada penelitian kali ini penulis berusaha mendapatkan SNR 40dB atau setara dengan excellent signal (5bars), Character Error Rate (CER) kurang dari 30% dan Bit Error Rate (BER) kurang dari 30% , kita juga akan menguji dengan serangan berupa CS untuk menguji kualitas system apakah pesan akan sangat rusak atau tidak.

**Kata kunci :** *Signal-to-Noise* (SNR), *Iteratively Reweighted Least Square* (IRLS), *Least Significant Bit* (LSB), *character error rate (CER), Bit Error Rate (BER),*.

**Abstract**

Saving secret files or sending files without being detected when being transmitted is a requirement that is now most sought and used in sending secret messages that are safe without being able to be known and attacked by attackers and the secret files can only be opened by the recipient. Steganography is a technique in increasing the security of a data, namely by inserting a secret information or message using a media that is usually called a host or carrier or cover. in this journal using the LSB method and IRLS Reconstruction. In this study the authors tried to get a 40dB SNR or equivalent to excellent signal (5bars), Character Error Rate (CER) of less than 30% and Bit Error Rate (BER) of less than 30%, we will also test with attacks in the form of CS to test the quality of the system whether the message will be very damaged or not.

**Keywords:** *Signal-to-Noise* (SNR), *Iteratively Reweighted Least Square* (IRLS), *Least Significant Bit* (LSB), *character error rate (CER), Bit Error Rate (BER).*

## 1. Pendahuluan

Dalam perkembangan komunikasi digital yang sangat pesat melalui internet membuat akan tiga teknik keamanan yaitu, *watermarking*, kriptografi, dan steganografi. Dalam kriptografi teks polos di konversi menjadi teks sandi yang membuat isi pesan cacat, sementara *watermarking* data akan disisipkan untuk membawa informasi seperti kepemilikan dan hak cipta. Tetapi dalam *watermarking* keberadaan pesan rahasia dapat terdeteksi, yang membuat tingginya minat operator untuk mengungkap pesan rahasi selama transmisi. Oleh karna itu, steganografi merupakan teknik keamanan yang banyak dan dapat diandalkan. Steganografi di jadikan sebagai pelengkap enkripsi, dalam menciptakan keamanan dan ke privasian lebih baik teknik ini dapat di kombinasikan. Media pembawa dalam keadaan saat ini berupa teks, video, gambar, audio, dan datagram dll [1].

Pada penelitian sebelumnya yang berudul *"An Efficient Audio Steganography Technique to Hide Text in Audio"* kelebeihannya menggunakan metode Least Significant Bit (LSB) dan memiliki SNR rata-rata 86,78% tidak ada serangan untuk menguji coba hasil nilai SNR, BER, dan CER setelah serangan [1]. Dalam penelitian "*An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Key"*kelebihannya menggunakan metode metode Least Significant Bit (LSB) dan *Discrete Wavelet Transform* (DWT) yang mana hasilnya memiliki rata-rata SNR 80,75% kekurangannya serangan untuk menguji ketahanan seberapa rusaknya pesan setelah di beri serangan tidak ada di dalamnya [2].

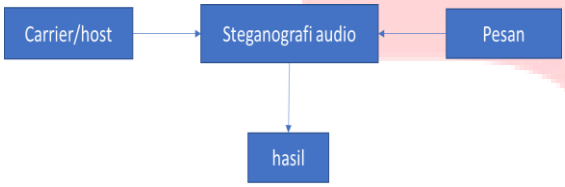
Pada penelitian kali ini akan membuat sebuah analisis terhadap audio steganografi menggunakan metode LSB dan rekonstruksi IRLS yang di dalammnya akan di beri serangan berupa CS dan membandingkan ketika sebelum di beri serangan dengan sesudah di beri serangan juga memiliki nilai SNR, BER, dan CER yang tidak jauh berbeda atau secret message yang tidak terlalu rusak. Maka dari

itu pada tugas akhir ini akan membantu orang orang yang ingin memiliki atau membutuhkan keamanan dan privasi dalam pengiriman sebuah pesan berupa text sehingga lebih nyaman dan merasa aman dalam pengiriman sebuah pesan dan terhindari dari hacker hacker saat proses transmisi

## 2. Dasar Teori /Material dan Metodologi/perancangan

### 2.1 Steganografi

Steganografi merupakan sebuah teknik dalam meningkatkan keamanan sebuah data, yaitu dengan melakukan penyisipan sebuah informasi atau pesan rahasia menggunakan sebuah media yang biasanya di sebut dengan host atau carrier atau sampul. Banyak bermacam macam media digital yang dapat dijadikan sebagai host atau tuan rumah, diantaranya adalah video, gambar, teks, audio, IP datagram, dan lain sebagainya [3].




**Gambar 2.1** proses steganografi

Dalam meningkatkan keamanan dalam kerahasiaan dan bisa meningkatkan kapasitas ukuran file yang membuat efisien, dapat di gunakan teknik *Compressive Sampling* (CS) di dalam steganografi[9]. Dengan persamaan rumus ;

$$fs \geq 2Xfmaks \qquad (2.1)$$

Salah satu metode yang bisa di aplikasikan dalam steganografi yaitu dalam menembunyinkan informasi di dalam audio, ini yang membuat steganografi dapat di implementasikan di dalam berbagai metode. Cara yang sering di gunakan atau paling umum dengan menyisipkan bit dari informasi tersebut pada *Least Signification Bit (LSB)* dari audio yang disisipkan per bitnya[10].

Algoritma Rivest Shamir Adleman (RSA) merupakan proses penyandian kunci asimetrik (*asimmetric key)*. Proses perumusan ini didasari pada landasan Teorama Euler, agar dapat menghasilkan kunci pribadi maupun kunci umum yang saling berkaitan, walaupun saat proses enkripsi dan deskripsi menngunakan unci yang berbeda tetapi hasilnya akan selalu tetap benar, baik kunci umum mau pun kunci pribadi yang di gunakan dalam RSA merupakan suatu bilangan prima, dan untuk menghindari usaha pemecahan teks rahasia menggunakan bilangan prima yang besar, karena semakin susah untuk mencari bilangan besar sebagai faktornya maka dari itu kunci di anjurkan untuk menggunakan bilangan primana yang besar [4].

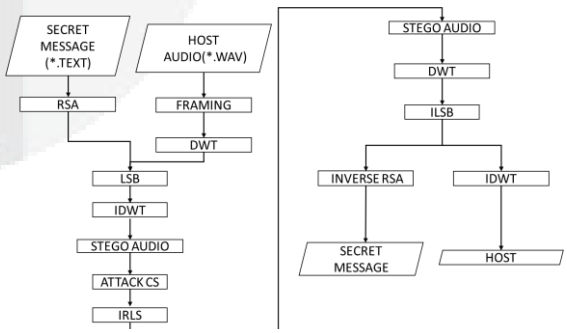
Enkripsi: $E_e\,(m) = c = m^e \; mod \; n$ (2.2)

Dekripsi: $D_d\,(c) = m = c^d \; mod \; n$ (2.3)

Pada sistem Steganografi Audio untuk mengirimkan pesan rahasia berupa teks melalui audio steganografi, juga di dalam tugas akhir ini menggunkan metode LSB dan Rekonstruksi IRLS. Pada penelitian kali ini penulis berusaha mendapatkan SNR 40dB atau setara dengan excellent signal (5bars), Character Error Rate (CER) kurang dari 30% dan Bit Error Rate (BER) kurang dari 30% , kita juga akan menguji dengan serangan berupa CS untuk menguji kualitas system apakah pesan akan sangat rusak atau tidak.

### 2.2 Desain Sistem

Dalam merancang sebuah sistem dibutuhkan rancangan sistem yang terstruktur untuk mempermudah merealisasikan sistem yang dibuat. di rancang sebuah sistem agar audio dapat mengirimkan sebuah pesan rahasia yang mana tidak dapat di deteksi atau diketahuhi oleh orang lain, kecuali hanya penerimanya saja yang memiliki kunci untuk membuka pesan rahasia tersebut, yang mana proses ini di sebut audio steganografi yang menggunkan rekrontruksi IRLS dan metode LSB, yang mana ketahanan dan kekuatannya untuk di ketahuhi isi dari audio steganograginya akan di uji coba kan, agar membuktikan bahwa audio steganografi merupakan salah satu tempat atau wadah pengiriman pesan rahasia berupa text yang aman




**Gambar 2.2** Diagran Blok Sistem

Gambar 2.2 menjelaskan proses sistem dari dari audio steganografi yaitu pertama tuliskan secret message yang ingin anda sisipkan lalu enkripsi pesan menjadi cipher text yang sudah di beri publik key, setelah itu pilih audio dengan genre yang diinginkan lalu di framing untuk penempatan audionya setelah itu di DWT agar saat sinyal yang di ubah bisa kembalikan seperti semula, setalh itu host audio

disisipkan pesan yang sudah di RSA dengan menggunakan LSB lalu di IDWT untuk mengembalikan sinyal seperti semula maka jadi lah stego audio yang belum diberi serangan. Audio steganografi diberi serangan berupa CS dengan menggunkan rekonstruksi IRLS dengan measurement rate yang berbeda beda maka jadi lah audio steganografi yang suda diberi serangan, setelah itu di DWT kembali untuk mengambil atau memisahkan pesan rahasia dengan host berupa audio

**Gambar 2.3** Diagram alr perancangan system radar

text berbentuk cipher text akan di buka dengan menggunakan private key maka akan terbuka secret message yang di sisipkan

### 2.3. Parameter Performasi Sistem

Untuk mengetahuhi kualitasnya system akan di uji oleh beberapa parameter. Parameter tersebut antara lain:

1. *Bit Error Rate* (BER)

Untuk mengukuran secara objectif kita menggunkan parameter BER. Nilai BER yang semakin kecil menunjukkan semakin bagus kualitas system transmisi tersebut. Dituliskan sebagai berikut rumus BER[5].

$$BER = \frac{Jumlah\ bit\ error}{jumlah\ bit\ keseluruhan}\ 100\% \quad (2.4)$$

Jika nilai BER 30% maka masih dapat di toleransi. Jika lebih dari 30% maka pesan sudah terlalu rusak untuk dapat dikenali lagi[6].

2. Signal to Noise Rasio (SNR)

Untuk mengukur kualitas audio secara objectif digunakan salah satu parameter yaitu SNR. SNR merupakan nilai yang menyatkan rasio antara daya sinyal audio yang telah disisipi steganografi terhadap daya noise. Nilai SNR lebih dari 20 dB merupakan nilai yang baik. Semakin besar nilai SNR, maka steganografi pada audio tidak dapat dirasakan oleh indra pendengaran manusia atau dengan demikian audio steganografi semakin tidak terdengan atau *imperceptible.* Persamaan SNR bias di hitung dengan[7].

$$SNR = 10 \log_1 0 \frac{\sum n[x_0(n)]^2}{\sum n[x_0(n) - x_w(n)]^2} \quad (2.5)$$

Keterangan:

3. *Character Error* Rate (CER)

*Character Error Rate* merupakan parameter pengujian yang dipakai untuk mengukur tingkat akurasi data hasil proses ekstraksi dari pesan yang telah disisipkan pada host audio dengan menghitung presentase perbandingan jumlah karakter yang salah satu error dari hasil ekstraksi dengan jumlah 21 karakter keseluruhan sebelum dilakukan ekstraksi, secara matematis, dapat dihitung dengan[8].

$$CER = \frac{jumlah\ karakter\ yang\ salah}{jumlah\ karakter\ keseluruhan}\ X\ 100\% \quad (2.6)$$

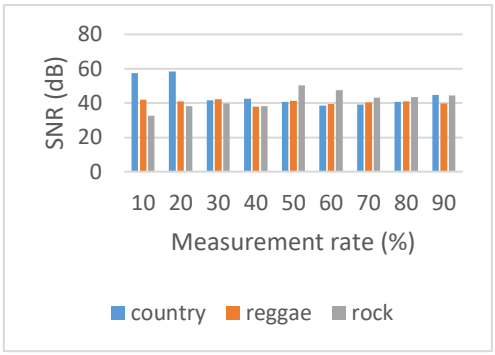
## 3. Pembahasan

### 3.1. Hasil pengujian sistem Steganografi Audio

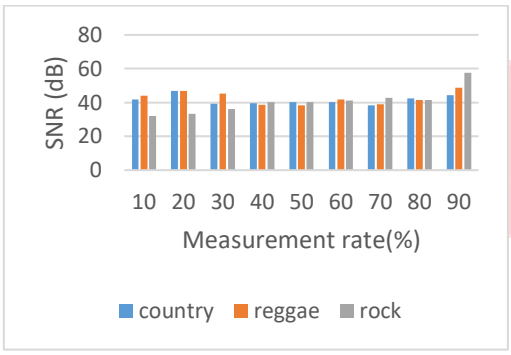
Pada penelitian Tugas Akhir ini, dilakukan proses analisis pada efisiensi steganografi audio menggunakan metode LSB dan Rekonstruksi IRLS, yang mana akan di beri measurement rate terhadap audio yang sudah disisipkan pesan dan dilakukan analisis terhadap parameter SNR, BER dan CER.

### 3.2. Hasil pengukuran parameter SNR

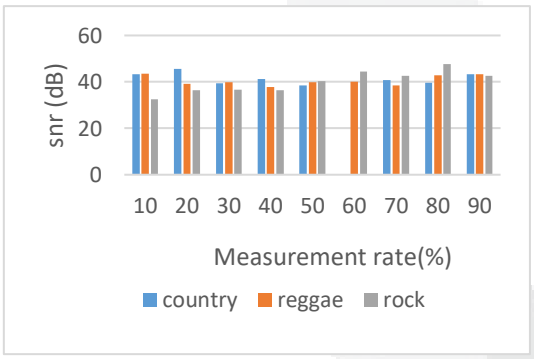
Gambar 3.1 menunjukkan hasil analisis SNR setelah serangan yang mana memiliki nilai yang berbeda dengan sebelum di berikan serangan, pada proses ini memiliki nilai SNR terbesar ada pada genre country saat di beri serangan measurement rate sebesar 20% yaitu 58,3424 dB dan memiliki nilai SNR terkecil pada genre rock saat di beri serangan measurement rate sebesar 10% yaitu 32,5004 dB. Didalam Gambar 3.2 menjelaskan hasil analisis pengujian kedua SNR di dapatkan nilai tertinggi yaitu pada genre rock yang mana pada measurement rate 90% dengan nilai 57,5864 dB dan memiliki nilai SNR kecil pada genre rock pada measurement rate 10% dengan nilai 31,951 dB. Gambar 3.3 menunjukan hasil pengujian ketiga SNR setelah serangan yang mana memiliki nilaiyang berbeda dengan pengujian sebelumnya , pada proses ini memiliki nilai SNR paling besar pada genre rock dengan measurement rate 80% dengan nilai 47,7515 dB dan memiliki nilai SNR paling rendah juga ada pada genre rock dengan measurement rate 10% 32,6065 dB. Gambar 3.4 menunjukan hasil pengujian ketiga SNR setelah serangan yang mana memiliki nilaiyang berbeda dengan pengujian sebelumnya , pada proses ini memiliki nilai SNR paling besar pada genre rock dengan measurement rate 40% dengan nilai 47,8623 dB dan memiliki nilai SNR paling rendah juga ada pada genre rock dengan measurement rate 10% dengan nilai 31,7173 dB



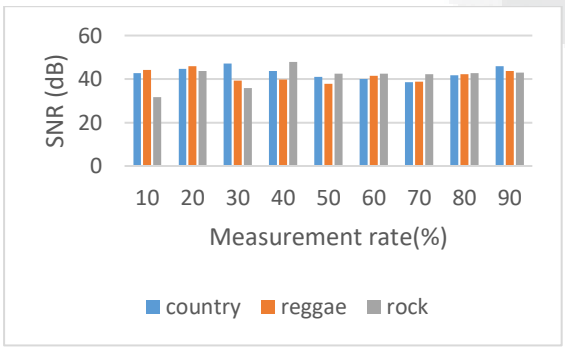

**Gambar 3.1** Hasil analisis pertama




**Gambar 3.2** Hasil analisis kedua



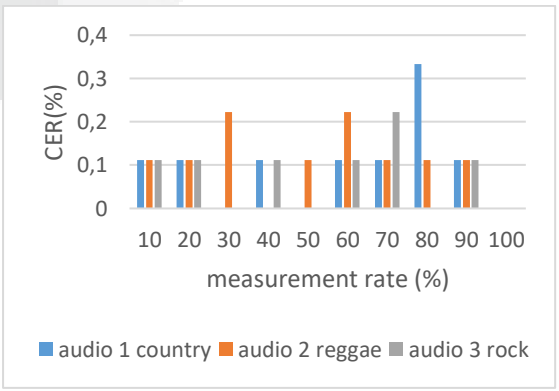

**Gambar 3.3** Hasil analisis ketiga



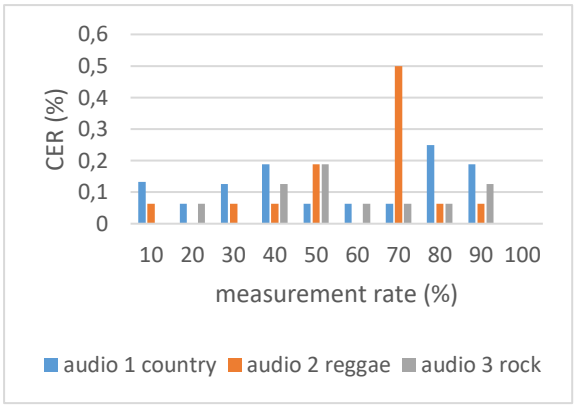

**Gambar 3.6** Hasil Analisis keempat

### 3.3. Hasil pengukuran parameter CER

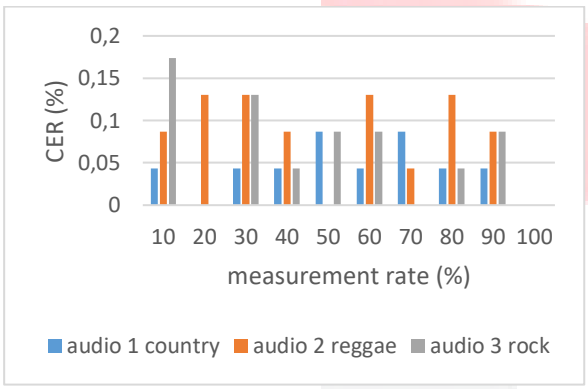
Pada gambar 3.7 diatas dilakukan pengujian pertama dengan memasukkan secret message "Fakultas" pada tiga genre yang berbeda dan juga percentage yang berbeda. Dari ketiga genre tersebut didapatkan nilai rata-rata cer yang bagus pada genre reggae yaitu 0,077777 atau sama dengan 8% dan kurang bagus pada genre rock 0,111111 atau sama dengan 10%. Dari tabel 4.12 menunjukkan bahwa nilai. gambar 3.8 dilakukan pengujian kedua yang mana memasukkan secret message brupa "Fakultas Teknik" pada tiga genre yang berbeda dan juga percentage yang berbeda-beda. Dari ketiga genre tersebut di dapatan nilai rata-rata cer yang bagus pada genre reggae yaitu 0,06875 atau setara dengan 7% dan genre yang kurang bagus ada pada genre country 0,1133333 atau setara dengan 10%. Dari gambar 3.8 menunjukkan bahwa pengujian pertama dan kedua nilai cer bagus dan kurang bagus pada genre yang sama. Pada gambar 3.9 dilakukan pengujian ketiga yang mana memasukkan secret message brupa "Fakultas Teknik Elektro" pada tiga genre yang berbeda dan juga percentage yang berbeda-beda. Dari ketiga genre tersebut di dapatan nilai rata-rata cer yang bagus pada genre country yaitu 0,0434783 atau setara dengan 4%, dan nilai cer yang kurang bagus ada pada genre rock yaitu 0,0826088 atau setara dengan 9%. Maka rata-rata cer yang baik dan kurang baik pada pengujian ketiga berbeda dengan rata-rata pengujian pertama dan kedua.Dan pada gambar 3.10 dilakukan pengujian keempat yang mana memasukkan secret message brupa "Fakultas Teknik Elektro Telkom" pada tiga genre yang berbeda dan juga percentage yang berbeda-beda. Dari ketiga genre tersebut di dapatan nilai rata-rata cer yang bagus pada genre reggae 0,04 atau setara dengan 4 % pada genre country dan rock lah nilai c er kurang bagus yaitu 0,05 atau setara 5%. Pada pengujian ini tiap genre memiliki nilai rata-rata cer yang hampir sama



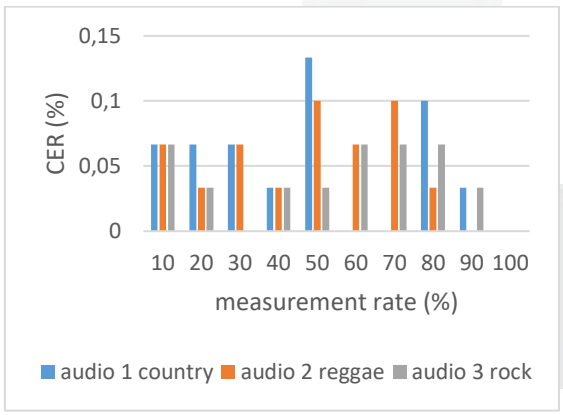

**Gambar 3.7** Hasil analisis pertama




**Gambar 3.8** Hasil analisis kedua



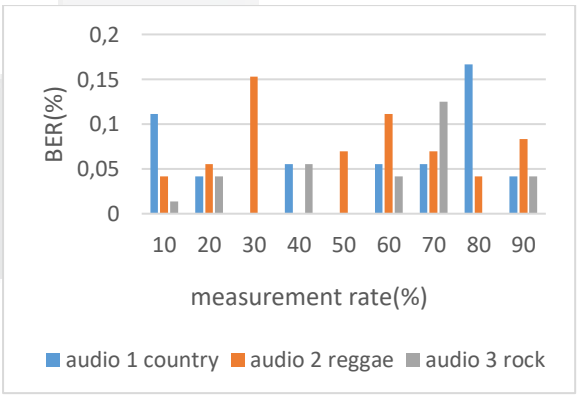

**Gambar 3.9** Hasil analisis ketiga



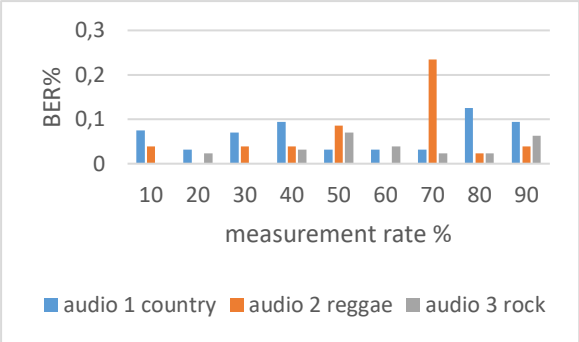

**Gambar 3.10** Hasil Analisis keempat

### 3.5. Hasil pengukuran parameter BER

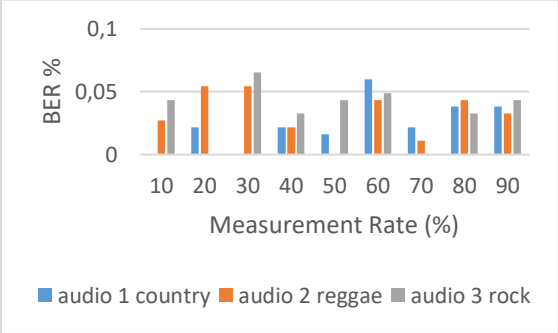
Pada gambar 3.11 diatas dilakukan pengujian pertama dengan memasukkan secret message "Fakultas" pada tiga genre yang berbeda dan juga percentage yang berbeda. Dari ketiga genre tersebut didapatkan nilai rata-rata ber yang bagus pada genre reggae yaitu 0,0319445 ata sama dengan 3% dan kurang bagus pada genre country 0,0527779 atau sama dengan 5%. Dari tabel menunjukkan bahwa nilai ber akan berbeda beda dan tidak monoton naik maupun turun yang tergantung oleh percentage nya. Pada gambar 3.12 dilakukan pengujian kedua yang mana memasukkan secret message brupa "Fakultas Teknik" pada tiga genre yang berbeda dan juga percentage yang berbeda-beda. Dari ketiga genre tersebut di dapatan nilai rata-rata ber yang bagus pada genre reggae yaitu 0,0273438 atau setara dengan 3% dan genre yang kurang bagus ada pada genre country 0,0582813 atau setara dengan 6%. Dari gambar 3.12 menunjukkan bahwa pengujian pertama dan kedua nilai ber bagus dan kurang bagus pada genre yang sama. Pada gambar 3.13 dilakukan pengujian ketiga yang mana memasukkan secret message brupa "Fakultas Teknik Elektro" pada tiga genre yang berbeda dan juga percentage yang berbeda-beda. Dari ketiga genre tersebut di dapatan nilai rata-rata ber yang bagus pada genre country yaitu 0,0233696 atau setara dengan 2%, dan nilai ber yang kurang bagus ada pada genre reggae yaitu 0,0353261 atau setara dengan 4%. Maka rata-rata ber yang baik dan kurang baik pada pengujian ketiga berbeda dengan rata-rata pengujian pertama dan kedua. Dan pada gambar 3.14 dilakukan pengujian keempat yang mana memasukkan secret message brupa "Fakultas Teknik Elektro Telkom" pada tiga genre yang berbeda dan juga percentage yang berbeda-beda. Dari ketiga genre tersebut di dapatan nilai rata-rata ber yang bagus pada genre rock 0,0175 atau setara dengan 2 % tetapi genre reggae juga memiliki nilai ber sebesar 2 % dengan nilai 0,0191667, dan pada genre country lah nilai ber kurang bagus yaitu 0,023333 atau setara 2%. Pada pengujian ini semua genre memiliki percentage yang sama semua tetapi memiliki nilai yang berbeda dikit saja.



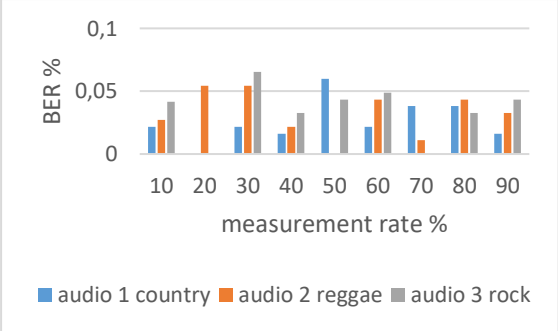

**Gambar 3.11** Hasil analisis pertama




**Gambar 3.12** Hasil analisis kedua




**Gambar 3.13** Hasil analisis ketiga




**Gambar 3.14** Hasil analisis keempat

## 1. Kesimpulan

Setelah dilakukan pengujian dan analisis terhadap sistem yang telah dibuat maka dapat ditarik kesimpulan sebagai berikut: Proses *Audio Steganography* menggunakan metode penyisipan LSB dapat terealisasikan dan dapat di implementasikan dengan sangat baik dan menghasilkan nilai rata rata SNR 99,52381dB, CER 0, dan BER 0.Proses *Audio Steganography* setelah di beri Measurement Rate memiliki nilai SNR rata-rata diatas 40dB .Proses *Audio Steganography* setelah di beri Measurement Rate memiliki nilai BER rata-rata dibawah 30 % yang menunjukkan BER cukup baik. Proses *Audio Steganography* setelah di beri Measurement Rate memiliki nilai CER rata-rata dibawah 30% yang menunjukkan pesan tidak terlalu rusak. Waktu yang di butuhkan untuk measurement rate tiap persentagenya berbeda beda dan berubah ubah walaupun tidak jauh berbeda

**Daftar Pustaka:**

[1] Rajiput, Shital P.; Adhitya, Krishnakant P.; Patnaik, Girish K. *An Efficient Audio Steganography Technique to Hide Text in Audio*. *International Conference on Computing, Communication, Control and Automation (ICCUBEA)*. IEEE,. p. 1-6, 2017

[2] MELIGY, Ali M.; NASEF, Mohammed M.; EID, Fatma T. An efficient method to audio steganography based on modification of least significant bit technique using random keys. *International Journal of Computer Network and Information Security*, , 7.7: 24. 2015.

[3] TAYEL, Mazhar; GAMAL, Ahmed; SHAWKY, Hamed. A proposed implementation method of an audio steganography technique. In: *2016 18th International Conference on Advanced Communication Technology (ICACT)*. IEEE, p. 180-184 , 2016.

[4] Gintang, Albert; Isnanto, R. Rizal; Windasari, Ike Pertiwi. Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi dan Sistem Komputer*, 3.2: 253-258, 2015.

[5] RAFRASTARA, Fauzi Adi, et al. Image Steganography using Inverted LSB based on 2 nd, 3 rd and 4 th LSB pattern. In: *2019 International Conference on Information and Communications Technology (ICOIACT)*. IEEE, p. 179-184, 2019.

[6] KORDOV, Krasimir; STOYANOV, Borislav. Least Significant Bit Steganography using Hitzl-Zele Chaotic Map. *International Journal of Electronics and Telecommunications*, , 63.4: 417-422, 2017.

[7] ANWAR, Mohamad; SAROSA, Moechammad; ROHADI, Erfan. Audio Steganography Using Lifting Wavelet Transform and Dynamic Key. In: *2019 International Conference of Artificial Intelligence and Information Technology (ICAIIT)*. IEEE, p. 133-137, 2019.

[8] Karah, Ali AH; Kayhan, Sema K. Watermarked Compressive Sensing Measurements Reconstructed by the Greedy Algorithms. *International Journal of Computer Theory and Engineering*, 7.3: 219, 2015

[9] ARIF, Muhammad Husnul; FANANI, Ahmad Zainul. Kriptografi Hill Cipher dan Least

Significant Bit untuk Keamanan Pesan pada Citra. *CSRID (Computer Science Research and Its Development Journal)*, 8.1: 60-72, 2016,.

[10] MUSTAFA, Mahmoud, et al. A Novel Enhanced LSB Algorithm for High Secure Audio Steganography. In: *2018 10th Computer Science and Electronic Engineering (CEEC)*. IEEE, p. 125-130, 2018