Integrasi Kriptografi Algoritma MARS dan Steganografi Metode Least Significant Bit (LSB) dengan Media File Berekstensi *.wav

Alif Mukhron Amar Rizki, Nanang Ismail, Rina Mardiati
Teknik Elektro UIN Sunan Gunung Djati Bandung
alifdudulz@gmail.com, nanang.is@uinsgd.ac.id, rmardiati@uinsgd.ac.id

Abstrak*—Sistem keamanan data yang mengkombinasikan kriptografi dan steganografi sangat diperlukan dalam proses pertukaran pesan/informasi. Hal ini diperlukan karena berkembangnya kejahatan teknologi dengan berbagai teknik interupsi, penyadapan, modifikasi, maupun fabrikasi. Pada penelitian ini digunakan teknik kriptografi dengan algoritma MARS yang dapat menerima kunci yang bervariasi antara 128 – 1248 bit dan diintegrasikan ke dalam steganografi dengan metode Least Significant Bit (LSB) dengan mengganti bit-bit yang tidak terlalu berpengaruh dari berkas audio. Metode ini diharapkan dapat melindungi pesan rahasia secara ganda. Pembangunan aplikasi pada penelitian ini menggunakan software NetBeans dan bahasa pemrograman Java. Aplikasi yang diberi nama StegadulzWav berhasil mengkombinasikan kriptografi dan steganografi baik dalam menanam pesan maupun dalam pengambilan pesan rahasia. Hasil pengujian menunjukkan bahwa semakin kecil ukuran file teks yang digunakan untuk arsip pesan maka semakin baik kualitas stego-audio yang dihasilkan. Nilai MOS (Mean Opinion Score) dari tiga puluh responden berbanding lurus dengan nilai rata-rata Peak Signal to Noise Radio (PSNR) sebesar 42,04 dB yang dapat diterima dengan baik oleh pendengaran manusia*.

Kata kunci; *kriptografi; algoritma MARS, steganografi, Least Significant Bit (LSB); audio*

1. Pendahuluan

Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan/informasi melalui jaringan/internet, sejalan dengan perkembangan kejahatan teknologi dengan berbagai teknik interupsi, penyadapan, modifikasi, maupun fabrikasi. Tanpa adanya jaminan keamanan, orang lain dapat dengan mudah mendapatkan data rahasia yang dikirimkan melalui jaringan/internet.

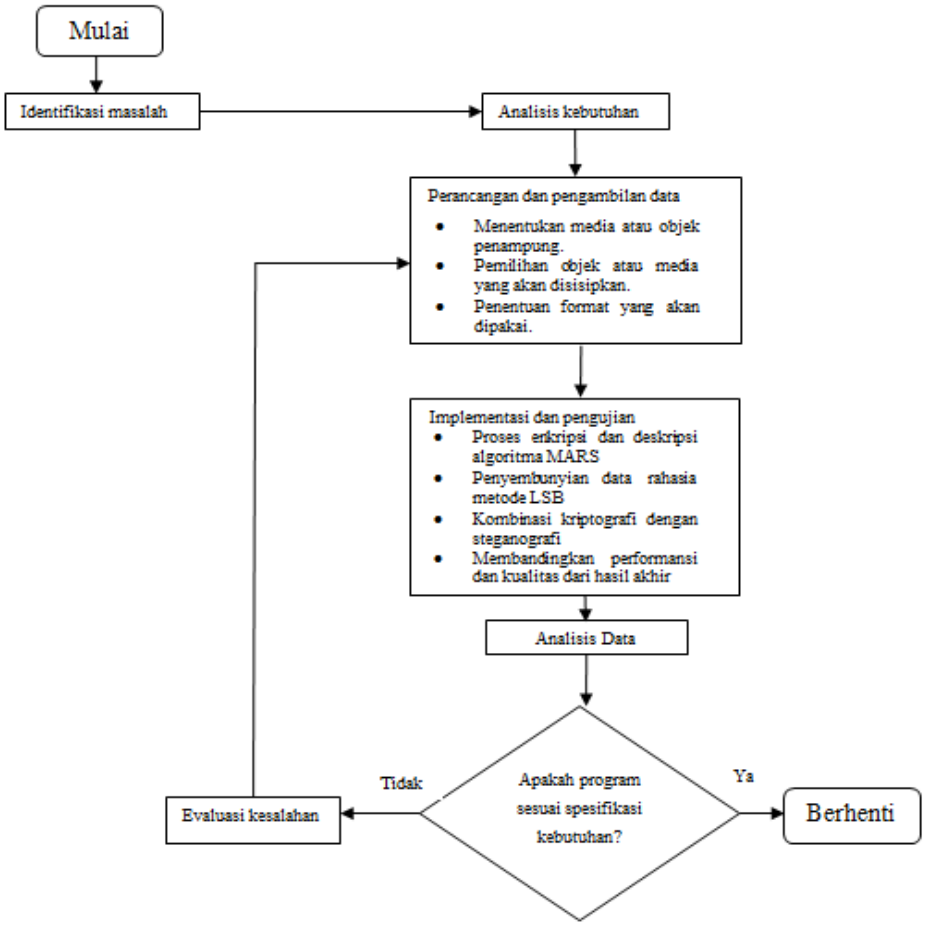
Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari satu tempat ketempat lain[1]. Algoritma kriptografi pun berkembang menjadi algoritma kriptografi yang lebih rumit dan kompleks. Beberapa algoritma yang menjadi kandidat Advanced Encryption Standard (AES) diantaranya Rijndael, RC6, MARS, Twofish dan Serpent. Algoritma MARS memiliki keunggulan yaitu dapat menerima kunci yang bervariasi antara 128 – 1248 bit. Sementara itu Rijndael hanya mampu menerima variasi panjang kunci 128 bit, 192 bit, dan 256 bit[3].

Sistem kriptografi ini dianggap terlalu public karena setiap orang mempunyai kesadaran bahwa pesan yang terlihat memang mengandung suatu kerahasiaan sehingga usaha untuk memecahkan kode enkripsi atau yang dikenal dengan kriptanalisis tidak dapat dihindarkan.
Steganografi muncul dari kekurangan yang dirasakan ada pada kriptografi. Steganografi adalah seni dan ilmu untuk menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui[7]. Salah satu metode steganografi yang sering digunakan adalah Least Significant Bit (LSB). Metode ini diterapkan dengan mengganti bit-bit yang tidak terlalu berpengaruh dari berkas audio dengan bit-bit pesan[9].

Oleh karena itu, pada penelitian ini dilakukan suatu implementasi dengan melakukan kombinasi antara algoritma MARS pada kriptografi dan teknik steganografi dengan metode *Least Significant Bit* (LSB) untuk mendapatkan proteksi ganda yang lebih baik dalam menjaga keamanan dan kerahasiaan data, serta menyembunyikan data dalam sebuah file audio WAV guna melindungi keberadaan data rahasia.

2. Perancangan dan Implementasi Sistem

Tahapan perancangan dan implementasi mengacu pada bagan di bawah ini.



Gambar 1. *Stages of activities*

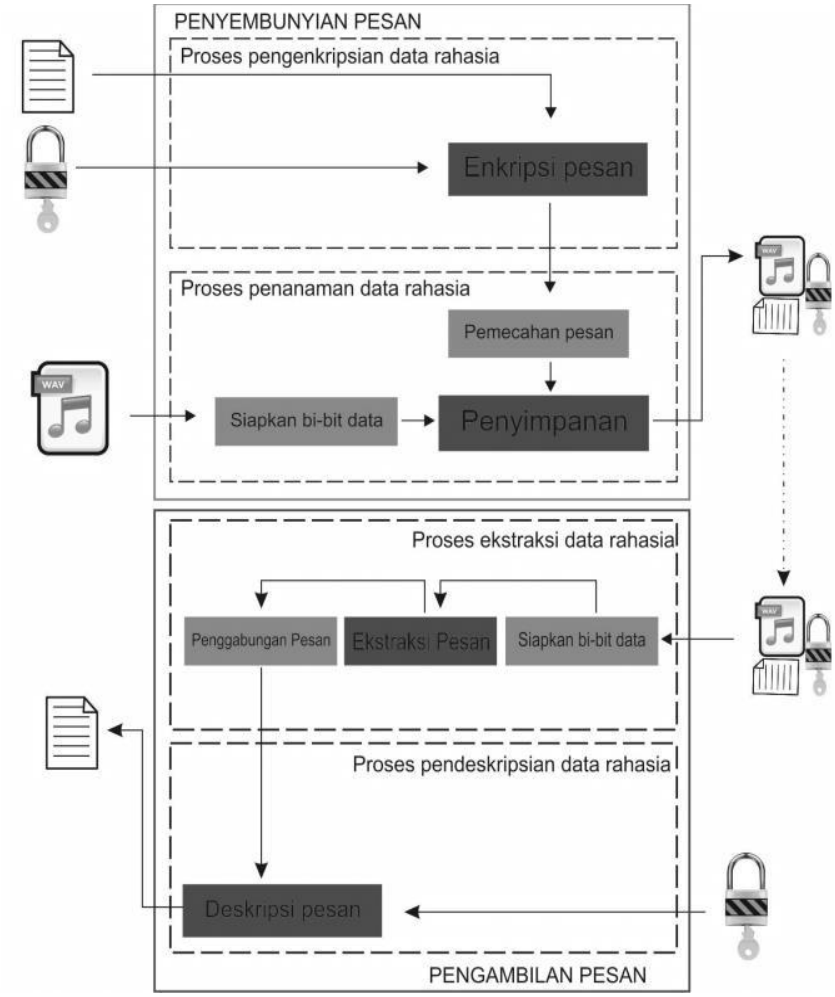
2.1. Analisis Perangkat Lunak

Perangkat lunak yang dibangun merupakan perangkat lunak yang dapat diterapkan baik di desktop maupun laptop, dan memiliki fungsi untuk menyembunyikan pesan ke dalam audio dengan terlebih dahulu melakukan enkripsi terhadap pesan tersebut. Pengguna dapat berinteraksi dengan perangkat lunak melalui antarmuka perangkat lunak. Pengguna dapat memilih audio dimana pesan akan ditanam.

- *Requirement Specification*: Dalam pembuatan aplikasi, spesifikasi dasar PC yang diperlukan, antara lain:
  - CPU Pentium 300 megahertz (MHz) processor
  - Memory 64 megabytes (MB) dari RAM
  - Display Super VGA (800 x 600)
  - Keyboard dan Mouse atau beberapa perangkat penunjuk kompatibel lainnya.
  - Perangkat lunak minimum sistem operasi Windows Xp dan Java oracle.

ISSN (e): 2540-9123
ISSN (p): 2502-1982

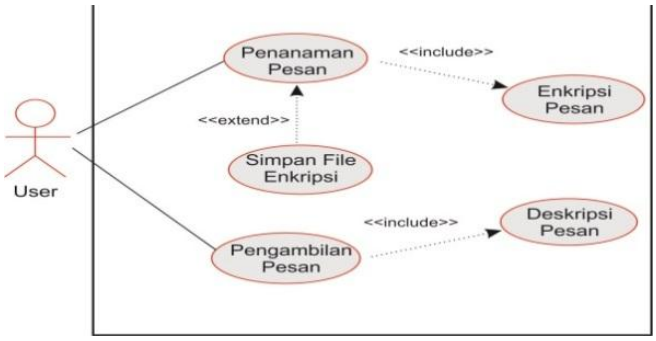
- Arsitektur Perangkat Lunak: Arsitektur perangkat lunak yang dibangun pada penelitian ini memiliki 2 buah modul utama yang diilustrasikan pada Gambar 2.



Gambar 2. *Software arhitecture*

2.2. *Use case* Model

Diagram *Use case* digunakan untuk memberikan gambaran fungsionalitas perangkat lunak. Perangkat lunak ini memiliki 5 buah *Use case*.



Gambar 3. *Use case diagram of system*

Use case ‘enkripsi pesan’ menunjukan fungsi pembacaaan data pesan, validasi ukuran pesan terhadap berkas audio dan proses enkripsi pesan sebelum disembunyikan. *Use case* ‘penanaman pesan’ digunakan untuk memasukkan informasi pesan ke dalam berkas audio. *Use*

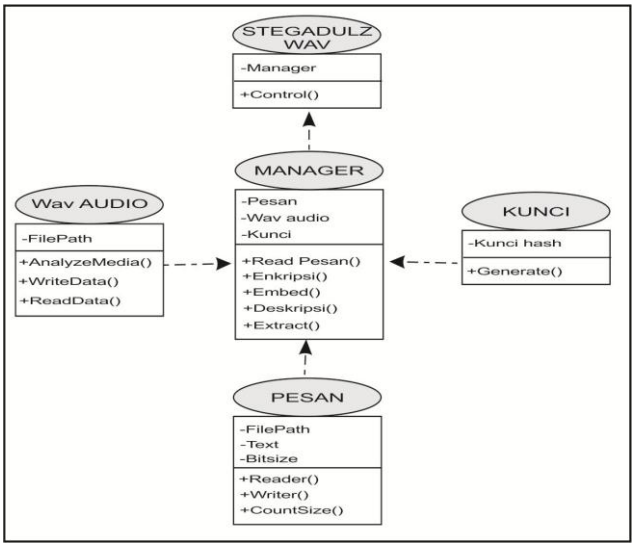
ISSN (e): 2540-9123
ISSN (p): 2502-1982

case ‘simpan file enkripsi’ digunakan untuk menyimpan file enkripsi pesan secara terpisah. Ketiga *Use case* ini hanya digunakan pada saat penyembunyian pesan.

Use case pengambilan pesan digunakan untuk mengambil kembali pesan yang disembunyikan, lalu *Use case* deskripsi pesan melakukan proses deskripsi untuk membentuk kembali pesan rahasia yang asli. Kedua *Use case* ini hanya digunakan pada proses pengambilan pesan.

2.3. Software Design

1) Class Design: Perangkat lunak ini mempunyai dua buah modul, yaitu modul penyembunyian pesan dan modul pengambilan pesan. Namun dalam implementasinya kedua modul ini dilakukan pada sebuah kelas yang berfungsi sebagai manager.



Gambar 4. *Classes diagram*

2) Interface Design: Pada saat aplikasi dijalankan, maka jendela yang terbuka pertama kali adalah flash dan setelah itu akan terbuka antarmuka aplikasi. Antarmuka ini akan menjadi jendela utama dari perangkat lunak yang akan dibangun. Pengguna akan memasukkan masukan dan mengklik tombol atau radio button untuk menghasilkan perintah yang diinginkan. Antarmuka ini dirancang sesederhana mungkin, agar pengguna tidak kesulitan dalam menggunakannya.

2.4. *Software Implementation*

Jendela yang terbuka saat pertama kali aplikasi di jalankan adalah flash berisi logo aplikasi StegadulzWAV.

Menu encode menjadi jendela utama dengan lima tombol klik dan satu tombol check box. Gambar 5 menunjukan menu encode aplikasi StegadulzWAV setelah flash.

ISSN (e): 2540-9123
ISSN (p): 2502-1982

Gambar 5. *Encode menu of StegadulzWAV*

3. Pengujian Sistem

3.1. Perancangan Kasus Uji

Rancangan kasus uji dibuat agar pengujian dapat terstruktur sehingga diharapkan dapat muncul rekomendasi mengenai tata cara serta kondisi pemakaian perangkat lunak agar memberikan kualitas kinerja yang optimal.

1) Truth Testing Cases of Software: Kasus uji ini dibuat untuk membuktikan kebenaran dan kesesuaian antara perangkat lunak yang dibangun dengan spesifikasi kebutuhannya. Rancangan uji kebenaran perangkat lunak sebagai berikut :

a) Penyisipan berkas data teks ke dalam berkas audio WAV.
b) Ekstraksi sebuah berkas audio WAV yang telah disisipi data untuk mendapatkan berkas data yang *valid*.
c) Penyimpanan keluaran berkas *stego-audio* WAV setelah disisipi berkas data rahasia.

2) Performance Testing Cases of Software: Pengujian kinerja perangkat lunak dilakukan dengan variasi ukuran berkas data dan variasi ukuran dari berkas penampung WAV. Pengujian ini dilakukan untuk mengetahui kualitas berkas WAV serta mengetahui waktu penyembunyian dan pengambilan data rahasia.

3) Data Pengujian

Tabel 1 menunjukkan berkas penampung audio yang digunakan dalam pengujian perangkat lunak *StegadulzWAV*.

Tabel 1. *File data of Media*

No	Nama *File*	Ukuran *File (bytes)*	Desibel (dB)
1	Bismillah.wav	235,978	-18,92
2	Deteksi.wav	1575,296	-6,62
3	Melodi.wav	4138,600	-5,16

ISSN (e): 2540-9123
ISSN (p): 2502-1982

Tabel 2 menunjukkan berkas teks yang digunakan dalam pengujian perangkat lunak *StegadulzWAV*.

Tabel 2. *File Data of Teks*

No	Nama *File*	Ukuran
1	Kata mutiara.txt	95
2	Kisah_teladan.txt	220,860
3	Pengenalan sentral trunk EWSD.doc	1358,848

3.2. Testing

1) Software Truth Testing: Pengujian kebenaran perangkat lunak dilakukan dengan menjalankan aplikasi *StegadulzWAV*. Pengujian yang dilakukan adalah sebagai berikut:

a) Penyembunyian sebuah pesan ke dalam sebuah berkas audio WAV dilakukan sebagai berikut :

1. Masukkan berkas penampung WAV.
2. Masukkan berkas data yang akan disisipkan.
3. Masukkan kunci.
4. Lakukan proses penyembunyian pesan.

b) Pengambilan sebuah pesan dari dalam sebuah berkas *stego-audio* WAV dilakukan sebagai berikut :

1. Masukkan berkas *stego-audio* WAV.
2. Masukkan kunci.
3. Lakukan proses pengambilan pesan.

Tabel 3 menunjukan ringkasan hasil pengujian fungsionalitas perangkat lunak.

Tabel 3. Ringkasan Hasil Pengujian Kebenaran Perangkat Lunak

No	Pengujia	Kriteria	Ket
1	Proses penanaman dan enkripsi pesan.	Aplikasi mengeluarkan *file audio* berisi pesan yang sudah di enkripsi.	Berhasil
2	Proses pengambilan dan deskripsi pesan	Aplikasi mengeluarkan pesan dari *stego-audio* dan mendeskripsikan pesan sehingga sama dengan pesan asli	Berhasil
3	Proses penyimpanan pesan yang terenkrips	Aplikasi menyimpan pesan terenkripsi dan *stego-audio* secara terpisah	Berhasil

2) Software Performance Testing: Pengujian kinerja perangkat lunak diukur dari :

a) Waktu penyembunyian dan pengambilan berkas data.
b) Ukuran berkas audio asli dengan ukuran berkas *stego-audio*
c) Kualitas berkas audio WAV yang telah disisipi berkas data.

Penilaian kualitas berkas audio WAV tersebut dilakukan melalui dua hal, yaitu :

a) Penilaian subjektif dengan cara mendengarkan suara hasil pemutaran berkas audio WAV dan menilai dengan *Mean Opinion Score* (MOS).

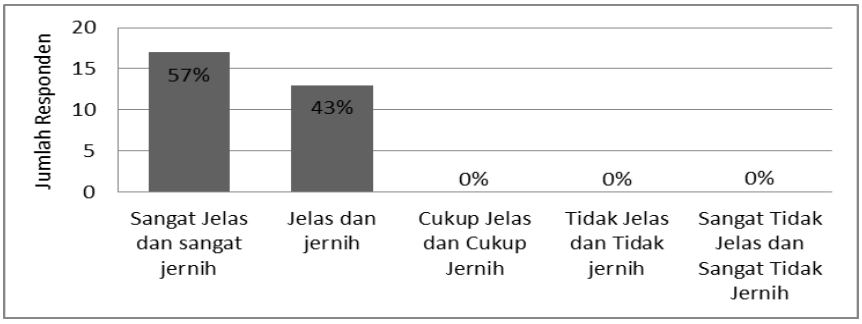
ISSN (e): 2540-9123
ISSN (p): 2502-1982

b) Menghitung nilai PSNR (*Peak Signal to Noise Ratio*). Nilai PSNR dalam satuan desibel (dB) dihitung dengan rumus :

$$PSNR = 10\log_{10}\left(\frac{P_1^2}{P_1^2 + P_0^2 - 2P_1P_0}\right) \qquad (1)$$

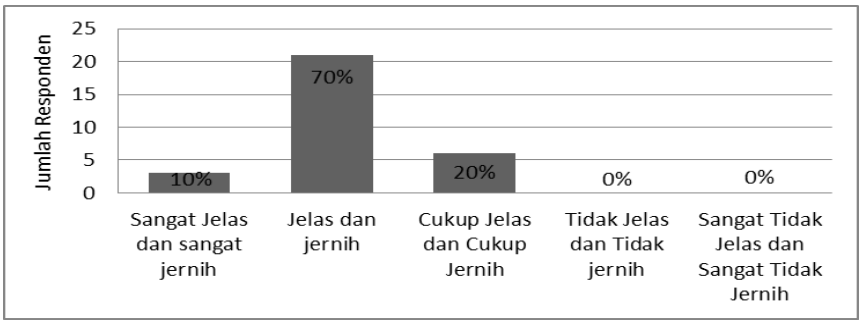
dimana P_0 menyatakan kekuatan sinyal awal dan P_1 menyatakan kekuatan sinyal setelah disisipi data. P_0 dan P_1 diukur dalam satuan desibel (dB).

Dari hasil pengujian kinerja perangkat lunak didapat bahwa *file* audio masukan dengan *file* keluaran memiliki ukuran yang sama, ini berarti proses metode LSB (*Least Significant Bit*) telah berhasil dilakukan.



Gambar 6. Perbandingan audio bismillah dengan kata mutiara

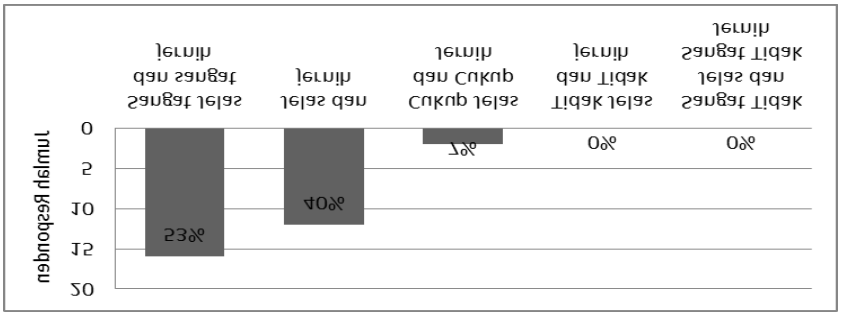
Hasil perbandingan audio bismillah dengan kata mutiara adalah sebesar 17 orang memilih nilai MOS 5 (sangat jelas dan sangat jernih) sedangkan 13 orang memilih nilai MOS 4 (jelas dan jernih), ini berarti kualitas perbandingan suara bismillah dan kata mutiara masih sangat baik dengan nilai MOS rata-rata 4,63.



Gambar 7. Perbandingan audio bismillah dengan kisah teladan

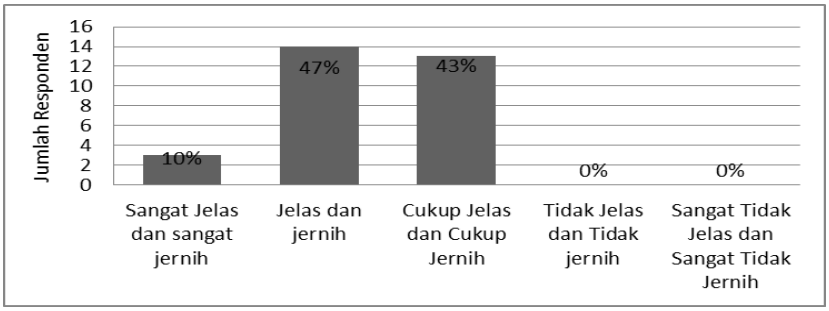
Hasil perbandingan audio bismillah dengan kisah teladan adalah sebesar 3 orang memilih nilai MOS 5 (sangat jelas dan sangat jernih) sedangkan 21 orang memilih nilai MOS 4 (jelas dan jernih) dan 6 orang memilih nilai MOS 3 (cukup jelas dan cukup jernih). Kualitas perbandingan suara bismillah dan kisah teladan masih baik dengan nilai MOS rata-rata 3,94.

ISSN (e): 2540-9123
ISSN (p): 2502-1982



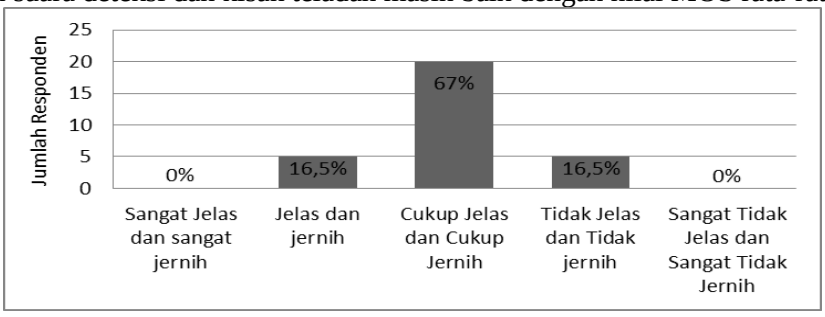
Gambar 8. Perbandingan audio deteksi dengan kata mutiara

Hasil perbandingan audio deteksi dengan kata mutiara adalah sebesar 16 orang memilih nilai MOS 5 (sangat jelas dan sangat jernih) sedangkan 12 orang memilih nilai MOS 4 (jelas dan jernih) dan 2 orang memilih nilai MOS 3 (cukup jelas dan cukup jernih). Kualitas perbandingan suara deteksi dan kata mutiara masih sangat baik dengan nilai MOS rata-rata 4,47.



Gambar 9. Perbandingan audio deteksi dengan kisah teladan

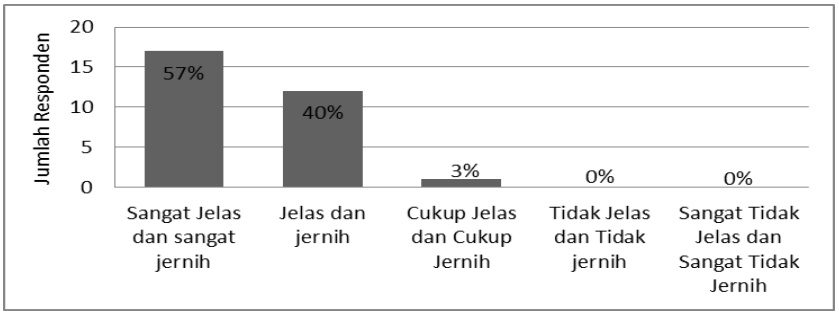
Hasil perbandingan audio deteksi dengan kisah teladan adalah sebesar 3 orang memilih nilai MOS 5 (sangat jelas dan sangat jernih) sedangkan 14 orang memilih nilai MOS 4 (jelas dan jernih) dan 13 orang memilih nilai MOS 3 (cukup jelas dan cukup jernih). Kualitas perbandingan suara deteksi dan kisah teladan masih baik dengan nilai MOS rata-rata 3,63.



Gambar 10. Perbandingan audio deteksi dengan EWSD

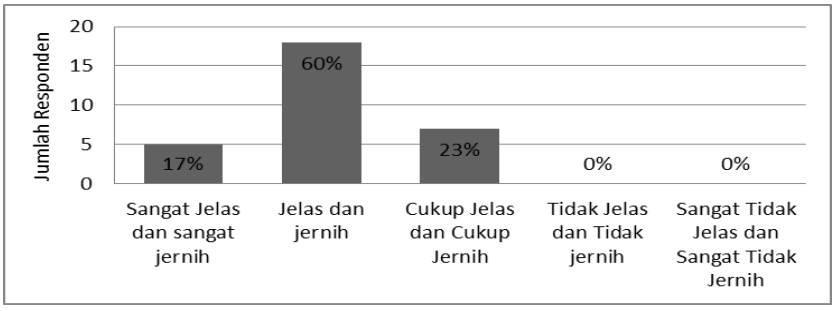
Hasil perbandingan audio deteksi dengan EWSD adalah sebesar 5 orang memilih nilai MOS 4 (jelas dan jernih) sedangkan 20 orang memilih nilai MOS 3 (cukup jelas dan cukup jernih) dan 5 orang memilih nilai MOS 2 (tidak jelas dan tidak jernih). Kualitas perbandingan suara deteksi dan EWSD masih cukup baik dengan nilai MOS rata-rata 3,13.

ISSN (e): 2540-9123
ISSN (p): 2502-1982



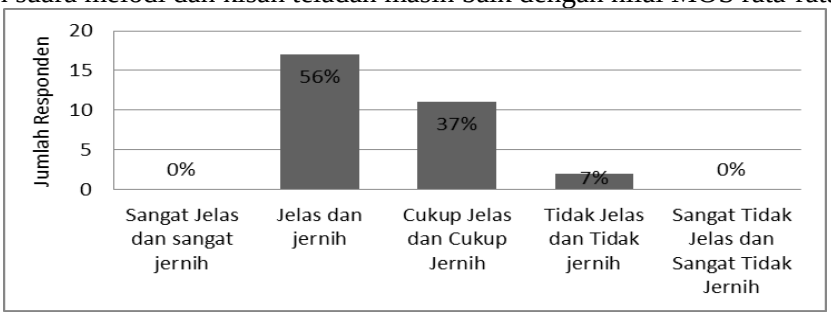
Gambar 11. Perbandingan audio melodi dengan kata mutiara

Hasil perbandingan audio melodi dengan kata mutiara adalah sebesar 17 orang memilih nilai MOS 5 (sangat jelas dan sangat jernih) sedangkan 12 orang memilih nilai MOS 4 (jelas dan jernih) dan 1 orang memilih nilai MOS 3 (cukup jelas dan cukup jernih). Kualitas perbandingan suara melodi dan kisah teladan masih sangat baik dengan nilai MOS rata-rata 4,63.



Gambar 12. Perbandingan audio melodi dengan kisah teladan

Hasil perbandingan audio melodi dengan kisah teladan adalah sebesar 5 orang memilih nilai MOS 5 (sangat jelas dan sangat jernih) sedangkan 18 orang memilih nilai MOS 4 (jelas dan jernih) dan 7 orang memilih nilai MOS 3 (cukup jelas dan cukup jernih). Kualitas perbandingan suara melodi dan kisah teladan masih baik dengan nilai MOS rata-rata 4,00.



Gambar 13. Perbandingan audio melodi dengan EWSD

Hasil perbandingan audio melodi dengan EWSD adalah sebesar 17 orang memilih nilai MOS 4 (jelas dan jernih) sedangkan 11 orang memilih nilai MOS 3 (cukup jelas dan cukup jernih) dan 2 orang memilih nilai MOS 2 (tidak jelas dan tidak jernih). Kualitas perbandingan suara melodi dan EWSD masih cukup baik dengan nilai MOS rata-rata 3,13.

Nilai PSNR (*Peak Signal to Noise Ratio*) rata-rata 42,04 dB dikatakan sangat baik karena nilai lebih besar dari 30 dB dapat diterima dengan baik oleh pendengaran manusia. Terdapat satu *file* yang tidak terenkripsi karena *file* penampung lebih kecil dari *file* teks.

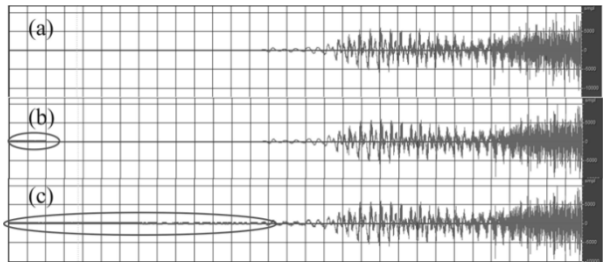
3.3. Analisis Hasil

ISSN (e): 2540-9123
ISSN (p): 2502-1982

Berdasarkan hasil pengujian, dapat dilihat bahwa *StegadulzWAV* yang dibuat sudah sesuai dengan spesifikasi kebutuhan perangkat lunak yang telah dipaparkan sebelumnya.

Pengujian kinerja perangkat lunak menunjukkan hasil yang memuaskan. Keberhasilan perangkat lunak dalam melakukan teknik gabungan steganografi dan kriptografi dalam penyembunyian pesan atau ekstraksi pesan, berjalan sesuai dengan fungsinya masing-masing. Parameter yang menentukan kualitas dari *stego-audio* yang dihasilkan adalah ukuran dari arsip pesan yang ingin ditanamkan.

Pada pengujian kualitas audio subjektif dan nilai PSNR, dihasilkan kesimpulan bahwa semakin besar pesan yang disembunyikan pada media yang sama, maka semakin kecil nilai PSNR yang didapat sehingga kualitas dari *stego-audio* semakin menurun. Dapat dianalisis juga bahwa ada keterkaitan nilai objektif PSNR dengan nilai subjektif. Tapi terkadang nilai ini bisa berubah tergantung dari penyebaran frame dan kecocokannya dengan panjang bit pesan. Jika bit pesan bisa tersebar merata sesuai jumlah frame maka nilai PSNR yang didapat cenderung naik.



Gambar 14. Perbandingan audio melodi dengan kisah teladan

Gambar 15, menunjukan sinyal asli dari *file* bismillah.wav yang memiliki besar *file* 235 *byte*s (a) tidak berbeda jauh dengan sinyal yang telah disisipi oleh pesan sebesar 95 *byte*s (b) sedangkan jika dibandingkan dengan sinyal yang telah disisipi oleh pesan sebesar 230 *byte*s (c) terlihat perbedaan yang signifikan.

Penentuan ukuran *file* pesan yang sangat berbeda jauh dengan ukuran *file* penampung audio akan menentukan kualitas dari *stego-audio* yang dihasilkan. Pada Gambar 4.9 terlihat sinyal (b) yang memiliki noise sedikit karena hanya disisipi pesan sebesar 95 *byte*s, sedangkan sinyal (c) memiliki banyak noise setelah disisipi pesan sebesar 230 *byte*s. Maka semakin besar *file* yang disisipi semakin banyak noise yang dihasilkan dan mempengaruhi kualitas audio menjadi tidak jernih. Kecepatan proses penyembunyian dan pengambilan pesan juga tergantung pada besarnya media steganografi yang digunakan. Hal ini dikarenakan proses penyembunyian membutuhkan pembacaan media secara menyeluruh terlebih dahulu untuk menganalisis struktur berkas audio tersebut.

Panjang kata sandi (pass*word*) juga menentukan lama dan kecepatan proses penyembunyian dan pengambilan pesan. Keamanan pesan yang disisipkan ke dalam WAV dengan aplikasi *StegadulzWAV* ini akan semakin meningkat. Hal ini dikarenakan pesan yang disisipkan dalam keadaan terenkripsi, serta *file* WAV yang dijadikan sebagai penampung pesan tidak mengundang kecurigaan karena tidak mengalami perubahan berarti yang dapat dipersepsi manusia.

4. Kesimpulan dan Saran

4.1. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa:

1. Perangkat lunak yang mengimplementasikan teknik penggabungan kriptografi dengan steganografi pada berkas WAV berhasil dibangun.
2. Algoritma MARS memiliki performansi yang baik karena dalam sistem gabungan ini kontribusi waktu yang diberikan terhadap proses keseluruhan tidak signifikan/relatif lebih kecil dibanding proses-proses yang lain.

ISSN (e): 2540-9123
ISSN (p): 2502-1982

3. Penentuan parameter ukuran arsip pesan dan ukuran arsip penampung akan berpengaruh pada performansi *StegadulzWAV*.
4. Nilai rata-rata PSNR menunjukan 42,04 dB dapat diterima dengan baik oleh pendengaran manusia dan nilai PSNR cenderung menurun dengan bertambahnya ukuran pesan yang disembunyikan.

4.2. Saran

Beberapa saran untuk pengembangan alat kedepannya adalah sebagai berikut:

1. Perlu dilakukan pengembangan untuk meningkatkan kapasitas penyembunyian bit-bit pesan serta analisis lebih lanjut dalam implementasi teknik steganografi pada format audio lainnya seperti OGG, WMA, M4A, ACC.
2. Perlu dilakukan pengujian terhadap *stego-audio*, apakah dapat bertahan terhadap steganalisis dengan metode tertentu.
3. Program dapat dikembangkan tidak hanya suara digital sebagai berkas penampungnya tetapi dapat juga berupa media teks, media citra, media video, ataupun data digital lainnya.

Daftar Pustaka

[1] G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)
[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
[3] I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.
[4] K. Elissa, "Title of paper if known," unpublished.
[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.
[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.