Vol.3 No.2 Juli-Desember 2017
JESIK
JURNAL ELEKRONIK SISTEM INFORMASI DAN KOMPUTER
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER (STMIK) BINA MULIA

ANALISIS TEKNIK STEGANOGRAFI PADA AUDIO MP3 MENGGUNAKAN METODE PARITY CODING DAN ENKRIPSI CIPHER TRANSPOSITION

Indra Jaya Kusuma[1)]

STMIK Bina Mulia Palu
Website: stmik-binamulia.ac.id

ABSTRAK

Steganografi merupakan seni penyembunyian pesan kedalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu didalam pesan tersebut. Metode steganografi yang digunakan dalam penelitian ini adalah *parity coding*, yaitu menyisipkan pesan/informasi ke dalam media pembawa berupa *file audio* MP3 dengan terlebih dahulu di-enkripsi menggunakan teknik enkripsi kriptografi *cipher* transposisi, yaitu suatu algoritma dengan teknik transposisi huruf-huruf pada *plaintext* dan *chipertext* tetap sama, tetapi urutannya diubah. Hasil pengujian kualitas pada media *audio* MP3 dengan menggunakan data *hexa* menunjukkan bahwa terjadi perubahan pada data *hexa* walaupun tidak signifikan dan perubahan data *hexa* tersebut bersifat fleksibel sama halnya dengan pengujian kualitas menggunakan data spektrum pada *audio* MP3 bahwa terjadi perubahan pada data spektrum namun tidak signifikan. Sedangkan pengujian dari besaran kapasitas baik pada pesan yang disisipkan maupun pada media *audio* MP3 sebagai pembawa pesan tidak berubah atau tetap seperti kapasitas *file* aslinya.

Kata Kunci: *Steganography, Cryptography, MP3*.

1. Pendahuluan

Perkembangan yang pesat dalam proses pengiriman data membawa dampak yang besar, yaitu masalah keamanan data yang dikirim. Untuk itu, tidak memungkinkan untuk dapat mengirimkan data-data penting atau rahasia melalui media-media tersebut secara polos (*plain*). Karena itu harus dilakukan proses pengamanan untuk data yang akan dikirim, salah satunya dengan cara melakukan enkripsi pada data-data tersebut.

Namun, dewasa ini metode tersebut dirasakan masih kurang dalam menjamin keamanan datanya, maka data-data yang telah di-enkripsi akan disembunyikan kedalam data lain yang disebut media pembawa (*carrier*). Metode ini disebut *Steganography*.

Steganography dan *cryptography* merupakan teknik pengamanan data yang mengolah data agar tidak dapat diketahui oleh pihak-pihak yang tidak berwenang untuk membuka data. *Cryptography* merupakan teknik pengacakan data, sedangkan *steganography* merupakan teknik penyembunyian data.

Teknik *steganography* membutuhkan 2 (dua) *property*, yaitu media pembawa dan pesan rahasia. Media pembawa yang umumnya digunakan adalah gambar, suara, video, atau teks. Adapun pesan yang disembunyikan dapat berupa artikel, gambar, daftar barang, kode program, atau pesan lain. Media pembawa *audio* dipilih dalam penelitian ini karena *audio* mempunyai kapasitas yang lebih besar dibandingkan dengan berkas teks maupun gambar dan tidak terlalu rumit jika dibandingkan berkas video.

Penggunaan MP3 sekarang menjadi sangat tinggi karena pada dasarnya sebagian besar manusia akan lebih suka melakukan hal-hal yang dapat menghibur dibandingkan melakukan hal-hal yang statik dan tidak menghibur. Perbedaan ini membuat MP3 lebih dipilih untuk digunakan dalam penelitian ini dibandingkan menggunakan *file* gambar. Dalam melakukan penyembunyian pesan, akan lebih dipilih format yang lebih lumrah digunakan sehingga tidak menimbulkan kecurigaan yang terlalu berlebihan. Penggunaan MP3 sebagai salah satu media *steganography* merupakan suatu langkah yang baik. Hal ini karena lalu lintas pertukaran MP3 di*internet* merupakan suatu hal yang biasa sehingga *steganography* menggunakan MP3 merupakan teknik yang baik untuk mengamankan pesan rahasia melalui media *internet*.

Berdasarkan latar belakang permasalahan tersebut maka penelitian ini akan menganalisis Teknik *Steganography* pada *audio* MP3 menggunakan metode *Parity Coding* dan Enkripsi *Cipher Transposition***.**

[1)] *Dosen STMIK Bina Mulia Palu*

2. Kerangka Teoritis

2.1 Analisis

Analisis adalah penyelidikan terhadap suatu peristiwa (karangan, perbuatan, dan sebagainya) untuk mengetahui keadaan yang sebenarnya (sebab-musabab, duduk perkaranya, dan sebagainya) [1].

2.2 Steganografi (*Steganography*)

Steganografi merupakan suatu seni penyembunyian pesan kedalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu didalam pesan tersebut. Kata steganografi (*steganography*) berasal dari bahasa Yunani, yaitu *steganos* yang artinya tersembunyi atau terselubung dan *graphein*, yang artinya menulis, sehingga bila digabungkan maka kurang lebih artinya adalah "menulis tulisan yang tersembunyi atau terselubung".

Pada abad 20, teknik steganografi benar-benar mengalami perkembangan. Selama berlangsung perang Boer, Lord Boden Powell (pendiri gerakan kepanduan) bertugas untuk membuat tanda posisi sasaran dari basis artileri tentara Boer. Untuk alasan keamanan, Lord Boden Powell kemudian menggambar peta-peta posisi musuh pada sayap kupu-kupu agar gambar-gambar peta sasaran tersebut terkamuflase.

Adapun Perang Dunia II merupakan periode pengembangan teknik-teknik baru steganografi. Pada awal Perang Dunia II walaupun masih digunakan teknik tinta yang tak terlihat, namun teknik-teknik baru mulai dikembangkan seperti menulis pesan rahasia kedalam kalimat lain yang tidak berhubungan langsung dengan isi pesan rahasia tersebut, kemudian teknik menulis pesan rahasia kedalam pita koreksi karbon mesin ketik, dan juga teknik menggunakan pin berlubang untuk menandai kalimat terpilih yang digunakan dalam pesan. Teknik terakhir adalah *microdots* yang dikembangkan oleh tentara Jerman pada akhir Perang Dunia II.

Dari beberapa contoh dari steganografi konvensional tersebut dapat dilihat bahwa semua teknik steganografi konvensional berusaha untuk merahasiakan suatu komunikasi dengan cara menyembunyikan pesan ataupun mengkamuflase pesan tersebut. Maka sesungguhnya prinsip dasar dalam teknik steganografi lebih dikonsentrasikan pada kerahasiaan komunikasinya, bukan pada datanya [2].

Steganografi membahas bagaimana suatu pesan terentu dapat disisipkan kedalam sebuah berkas media sehingga pihak ketiga tidak menyadarinya. Steganografi memanfaatkan keterbatasan sistem panca indera manusia seperti mata dan telinga. Dengan adanya keterbatasan inilah, metode steganografi ini dapat diterapkan pada berbagai media digital. Hasil keluaran yang dihasilkan dari steganografi ini memiliki bentuk persepsi yang mirip atau bahkan sama dengan bentuk aslinya. tentunya persepsi yang dimaksud disini adalah hanya sebatas kemampuan indera manusia, tetapi tidak oleh komputer atau perangkat pengolah digital lainnya.

Dalam steganografi, proses penyembunyian suatu pesan kedalam media *cover* disebut sebagai penyisipan, sedangkan proses sebaliknya disebut ekstraksi. Penyembunyian data rahasia kedalam media *cover* akan mengubah kualitas media tersebut.

Kriteria yang harus diperhatikan dalam penyembunyian data diantaranya adalah sebagai berikut:

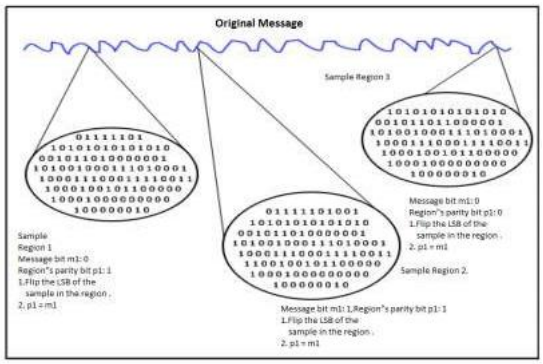
a. *Fidelity*
   Kualitas berkas *cover* tidak jauh berubah setelah penyisipan data rahasia. Berkas *cover* hasil steganografi masih terlihat/terdengar dengan baik. Pengamat tidak akan mengetahui bahwa didalam berkas tersebut terdapat suatu data rahasia.
b. *Recovery*
   Data yang disembunyikan harus dapat diungkapkan/diekstrak kembali. Karena tujuan steganografi adalah untuk penyembunyian informasi, maka sewaktu-waktu informasi yang ada didalam berkas *cover* tersebut harus dapat diambil kembali untuk digunakan lebih lanjut.
c. *Robustness*
   Robustness merupakan salah satu isu desain algoritma steganografi yang utama. Data rahasia yang disisipkan didalam suatu media harus tahan terhadap pengolahan sinyal yang mungkin dilakukan, termasuk konversi *digital-analog* dan *analog-digital*, *linear* dan *non-linear filtering,* maupun kompresi dan perubahan ukuran (*scaling).*
d. *Security*
   Data rahasia harus kebal terhadap deteksi pembajakan dan juga diharapkan bisa menyulitkan dari usaha steganalisis [3].

2.3 *Parity Coding*

Dalam teknik *parity coding*, sinyal dari berkas *audio* dipecah menjadi beberapa *región* yang berbeda dan mengenkripsi setiap *bit* dari pesan rahasia yang ingin disisipkan pada sebuah sampel *región* yang berisi *parity bit*. Apabila *parity bit* dalam *región* yang ditentukan ternyata tidak sesuai dengan *bit* pesan rahasia yang akan dienkripsi, maka prosesnya diganti dengan menukarkan LSB pada salah satu sampel *región*, sehingga si pengirim mempunyai pilihan yang lebih dalam mengenkripsi *bit* pesan rahasia

tersebut dan sinyal *audio* dapat diubah dengan cara yang lebih halus.

Prosedur *parity coding* digambarkan sebagai berikut:



Gambar 1 *Parity Coding Procedure*

Sinyal media yang telah di-*encode* akan dibagi menjadi beberapa *región* yang terpisah dengan ukuran statis. *Parity bit* dari setiap *región* akan dihitung terlebih dahulu untuk disimpan nilainya. *Bit* dari pesan rahasia kemudian akan disisipkan secara merata kedalam *región-región* yang ada. Jika *bit* yang akan dimasukkan kedalam *región* nilainya berbeda, maka susunan dari *bit-bit* LSB harus diubah sedemikian rupa sehingga *parity bit región* nilainya sama dengan *bit* pesan rahasia yang akan disisipkan namun jika nilainya sama *region* tidak diperlu diubah. Kondisi dalam penghitungan *parity bit* adalah *even parity* [4].

2.4 Kriptografi (*Cryptography*)

Cryptography secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita [5]. Selain pengertian tersebut terdapat pula pengertian *cryptography* sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data [6].

Apabila *cryptography* digunakan untuk mengubah dan mengacak pesan menjadi bentuk lain yang tidak bermakna, maka pada *steganography* pesan yang disembunyikan tersebut tetap dipertahankan hanya dalam penyampaiannya disembunyikan dengan berbagai cara pada suatu media penampung. Hal ini karena pesan yang disampaikan secara *cryptography* dapat mencurigakan karena berupa kata-kata acak yang tidak bermakna, sedangkan pesan dalam *steganography* terlihat seperti pesan biasa sehingga tidak mencurigakan [2].

Prinsip-prinsip yang mendasari kriptografi adalah:

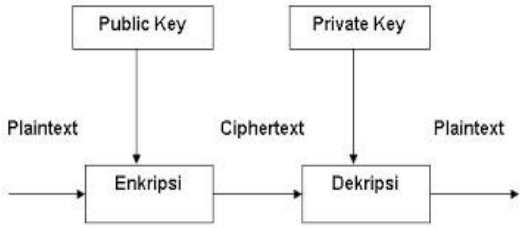
a. *Confidelity* (kerahasiaan), yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima/ pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data sehingga menjadi sulit untuk dibaca dan dipahami.
b. *Data integrity* (keutuhan data), yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
c. *Authentication* (keotentikan), yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
d. *Non-repudiation* (anti-penyangkalan), yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal darinya).

Berikut adalah komponen yang digunakan dalam bidang kriptografi:

a. Algoritma, merupakan himpunan aturan matematis yang digunakan dalam enkripsi dan deskripsi.
b. *Plaintext* (M), adalah pesan yang hendak dikirimkan (berisi data asli).
c. *Ciphertext* (C), adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
d. Enkripsi (fungsi E), adalah proses pengubahan *plaintext* menjadi *ciphertext*.
e. Dekripsi (fungsi D), adalah kebalikan dari enkripsi, yakni mengubah *ciphertext* menjadi *plaintext* sehingga berupa data awal/asli.
f. Kunci, adalah suatu bilangan yang dirahasiakan, yang digunakan dalam proses enkripsi dan dekripsi.
g. Kriptologi, merupakan studi tentang kriptografi dan kriptanalisis.
h. Kriptanalisis, merupakan aksi memecahkan mekanisme kriptografi dengan cara menganalisisnya untuk menemukan kelemahan dari suatu algoritma kriptografi sehingga akhirnya dapat ditemukan kunci atau teks asli.

Kriptografi itu sendiri terdiri dari dua proses utama, yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijalaskan diatas, proses enkripsi mengubah *plaintext* menjadi *ciphertext* (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti.

Proses enkripsi dan dekripsi dalam kriptografi digambarkan sebagai berikut:



Gambar 2 Diagram Proses Enkripsi dan Dekripsi

2.5 Kriptografi *Cipher Transposition*

Pada teknik *cipher* transposisi, huruf-huruf yang ada didalam *plaintext* dan *ciphertext* tetap sama, tetapi urutannya diubah. Dengan kata lain, teknik ini melakukan *transpose* terhadap rangkaian karakter yang ada didalam suatu teks. Nama lain untuk metode ini adalah permutasi, karena *transpose* setiap karakter didalam teks sama dengan mempermutasikan karakter-karakter tersebut.

Teknik *cipher* transposisi memiliki banyak varian algoritma, diantaranya adalah *column transposition cipher*. Untuk mempermudah pemahaman, berikut ini Peneliti menampilkan contoh proses enkripsi *column transposition cipher* dengan *plaintext* sebagai berikut:

THEQUICKBROWNFOXJUMPSOVERTHE
LAZY DOG

Untuk mengenkripsi pesan, *plaintext* ditulis secara horizontal dengan lebar kolom tetap, misal selebar 6 karakter (kunci k = 6) sehingga pesan menjadi:

THEQUI
CKBROW
NFOXJU
MPSOVE
RTHELA
ZYDOGX

Penambahan karakter X merupakan tambahan sebagai persyaratan bahwa jumlah karakter merupakan kelipatan dari jumlah huruf kunci. Selanjutnya *ciphertext* dapat dibaca secara vertikal atau kolom per kolom, sehingga pesan berubah menjadi:

TCNMRZ HKFPTY EBOSHD QRXOEO
UOJVLG IWUEAX

Untuk mendekripsi pesan tersebut, panjang *ciphertext* dibagi dengan kunci.

Pada contoh ini, panjang *ciphertext* yaitu 36 karakter dibagi 6 untuk mendapatkan jumlah kolom yaitu 6. Algoritma dekripsi identik dengan algoritma enkripsi. Jadi untuk contoh ini, *ciphertext* dalam baris-baris selebar 6 karakter menjadi:

TCNMRZ HKFPTY EBOSHD QRXOEO
UOJVLG IWUEAX

Dengan membaca setiap kolom maka dapat memperoleh pesan semula, yaitu:

THEQUICKBROW
NFOXJUMPSOVERTHELAZYDOG

2.6 *Audio* MP3

MPEG-1 *audio layer* III atau yang lebih dikenal dengan MP3, adalah salah satu dari pengkodean dalam *digital audio* dan juga merupakan format kompresi *audio* yang memiliki sifat "menghilangkan". Istilah menghilangkan yang dimaksud adalah kompresi *audio* kedalam format MP3 menghilangkan aspek-aspek yang tidak signifikan pada pendengaran manusia untuk mengurangi besarnya *file audio*.

Sejarah MP3 dimulai dari tahun 1991 saat proposal dari Phillips (Belanda), CCET (Perancis), dan Institut Für Rundfunktechnik (Jerman) memenangkan proyek untuk DAB (*Digital Audio Broadcast*). Produk mereka seperti Musicam (akan lebih dikenal dengan *layer* 2) terpilih karena kesederhanaan, ketahanan terhadap kesalahan, dan perhitungan komputasi yang sederhana untuk melakukan pengkodean yang menghasilkan keluaran yang memiliki kualitas tinggi. Pada akhirnya ide dan teknologi yang digunakan tersebut dikembangkan menjadi MPEG-1 *audio layer* 3.

Dengan demikian, MP3 merupakan pengembangan dari teknologi sebelumnya sehingga dengan ukuran yang lebih kecil dapat menghasilkan kualitas yang setara dengan kualitas CD.

2.7 Steganografi pada *Audio*

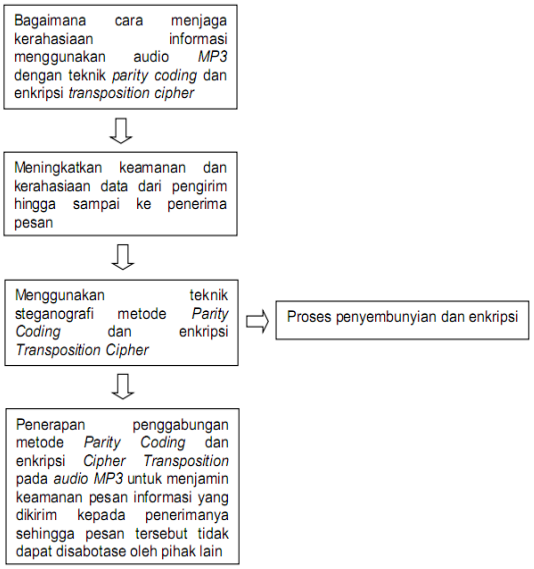
Penyembunyian data pada *audio* merupakan teknik yang paling menantang pada steganografi ini. Hal ini disebabkan *Human Auditory System* (HAS) memiliki jangkauan yang dinamis. HAS memiliki kemampuan mendengar lebih dari satu sampai satu miliar, dan jangkauan frekuensi lebih dari satu hingga seribu.

Auditory System ini juga sangat peka pada gangguan suara (*noise*) yang paling halus sekalipun. Sedikit saja terdapat gangguan pada sebuah berkas *audio* maka dengan mudah akan terdeteksi. Satu-satunya kelemahan yang terdapat pada HAS dalam membedakan suara adalah kenyataan bahwa suara keras dapat menenggelamkan suara pelan.

Terdapat dua konsep yang harus dipertimbangkan sebelum memilih metode mana yang akan dipakai, yaitu format *digital audio* dan media transmisi dari *audio* [7].

3. Metode Penelitian

Berdasarkan referensi diatas maka model penelitian ini digambarkan sebagai berikut:



Gambar 3 Model Penelitian

Penelitian ini termasuk jenis penelitian deskriptif yaitu penelitian yang dimaksudkan untuk menyelidiki keadaan, kondisi, situasi, peristiwa, dan hal-hal lain, yang hasilnya dipaparkan dalam bentuk deskriptif laporan penelitian [8].

Untuk memperoleh data-data yang dibutuhkan dalam penelitian ini, digunakan teknik sebagai berikut:

a. Studi Pustaka, yaitu mencari, mengumpulkan, dan mempelajari data-data yang berhubungan dengan penelitian ini.
b. Eksperimen, yaitu suatu percobaan yang dirancang khusus guna membangkitkan data yang diperlukan untuk menjawab pertanyaan penelitian [9].

   Eksperimen dilakukan dengan langkah-langkah sebagai berikut [10]:

   1. Melakukan kajian secara induktif yang berkait erat dengan permasalahan.
   2. Mengidentifikasi dan mendefinisikan masalah.
   3. Melakukan studi literatur dari sumber yang relevan, memformulasikan hipotesis penelitian, menentukan variabel penelitian, serta merumuskan definisi operasional dan definisi istilah.
   4. Membuat rencana penelitian yang mencakup:
      a) Mengidentifikasi variabel luar yang tidak diperlukan tetapi mungkin dapat mengkontaminasi proses eksperimen.
      b) Menentukan cara mengontrol.
      c) Memilih rancangan penelitian yang tepat.
      d) Menentukan populasi serta memilih sampel dan sejumlah subjek penelitian.
      e) Membagi subjek kedalam kelompok kontrol maupun kelompok eksperimen.
      f) Membuat dan memvalidasi instrumen penelitian serta melakukan studi pendahuluan agar diperoleh instrumen penelitian yang memenuhi syarat untuk mengambil data yang diperlukan
      g) Mengidentifikasi prosedur pengumpulan data dan menentukan hipotesis.

Adapun perangkat pendukung yang digunakan pada penelitian ini terdiri dari:

a. Perangkat keras (*hardware*), yaitu laptop atau *personal computer* (pc).
b. Perangkat lunak (*software*), yaitu sistem operasi *windows*, *Cryptool2*, *mp3stegz*, *spectrum analyzer*, dan *HxD*.

4. Hasil Penelitian

Pada penelitian ini Peneliti akan melakukan hasil analisa enkripsi kriptografi berupa teks dengan teknik *cipher transposition*, uji kualitas dan kapasitas *audio* MP3 sebagai media pembawa pesan, serta melakukan penggujian kapasitas pesan yang disisipkan.

4.1 Enkripsi Pesan *Cryptography Cipher Transposition*

Pesan yang akan digunakan dalam penelitian ini adalah pesan teks. Pesan teks ini kemudian akan dienkripsi terlebih dahulu menggunakan metode *cipher transposition*.

Contoh pesan yang dienkripsi dalam penelitian ini adalah:

PASCASARJANASISTEMKOMPUTERSTM
IKHANDAYANIMAKASSAR

Untuk mengenkripsi pesan, *plaintext* ditulis secara horizontal dengan lebar kolom tetap, yaitu selebar 8 karakter (kunci *k*=8) sehingga menjadi:

PASCASAR JANASIST EMKOMPUT
ERSTMIKH ANDAYANI MAKASSAR
XXXXXXXX XXXXXXXX

Dengan demikian dapat dituliskan sebagai berikut:

PASCASAR
JANASIST
EMKOMPUT
ERSTMIKH
ANDAYANI
MAKASSAR
XXXXXXXX
XXXXXXXX

Penambahan karakter X merupakan tambahan sebagai persyaratan bahwa jumlah karakter merupakan kelipatan dari jumlah huruf kunci.

Selanjutnya *ciphertext* dapat dibaca secara vertikal atau kolom per kolom, sehingga menjadi:

PJEEAMXX AAMRNAXX SNKSDKXX
CAOTAAXX ASMMYSXX SIPIASXX
ASUKNAXX RTTHIRXX

Untuk mendekripsi pesan, panjang *ciphertext* tersebut dibagi dengan kunci yang digunakan. Pada penelitian ini, panjang *ciphertext* adalah 64 karakter yang dibagi dengan kunci 8 untuk mendapatkan jumlah kolom, yaitu 8.

Algoritma dekripsi identik dengan algoritma enkripsi. Jadi, untuk penelitian ini, *ciphertext* dalam baris-baris selebar 8 karakter menjadi:

PJEEAMXX
AAMRNAXX
SNKSDKXX
CAOTAAXX
ASMMYSXX
SIPIASXX
ASUKNAXX
RTTHIRXX

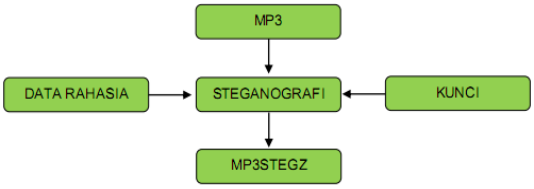
Dengan membaca setiap kolom maka dapat diperoleh pesan semula, yaitu:

PASCASARJANASISTEMKOMPUTERSTM
IKHANDAYANIMAKASSAR

4.2 Penyisipan Pesan *Steganography Parity Coding*

Penyembunyian pesan dilakukan dengan mengganti *bit-bit* yang ada didalam *audio* MP3 dengan *bit-bit* pesan. *Bit* yang cocok untuk diganti adalah *bit-bit* yang kurang penting pada *audio* data yang ada di setiap *frame*-nya. Keuntungan inilah yang dimanfaatkan dalam proses penyembunyian pesan, karena telinga manusia tidak dapat membedakan perubahan suara.

Proses yang penyembunyian pesan didalam *audio* MP3 tersebut digambarkan sebagai berikut:

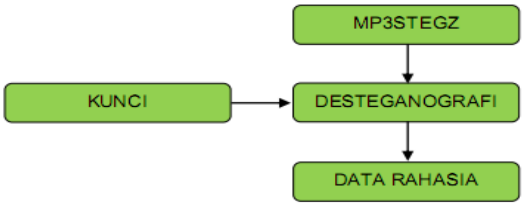


Gambar 4 Blok Diagram Steganografi

4.3 Teknik Pengungkapan Pesan *Desteganography*

Pesan yang telah disembunyikan didalam *audio* MP3 penampung dapat dibaca kembali melalui proses desteganografi, yaitu proses kebalikan dari steganografi.

Proses desteganografi seperti yang dapat dilihat pada gambar dibawah ini:



Gambar 5 Blok Diagram Desteganografi

4.4 Pembahasan

4.4.1 Analisa Uji Kualitas Data *Hexa*

Analisa hasil uji kualitas menggunakan data *hexa* pada media *audio* MP3 Avril Lavigne dengan judul lagu Complicated dapat dibadingkan sebagai berikut:

a. Sebelum disisip pesan

Data *hexa audio* MP3 sebelum disisipkan pesan sebagai berikut:

```
00000120  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000130  FF FF FF FF FF FF FF FF FF FF FB 72 50 86 80 01
00000140  20 00 4B 80 00 00 00 00 00 09 70 00 00 00 00 00
00000150  01 2E 00 00 00 00 00 00 25 C0 00 00 00 FF FF FF
00000160  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

Gambar 6 Data *Hexa* Sebelum Disisipi Pesan

b. Setelah disisip pesan

Data *hexa audio* MP3 setelah disisipkan pesan sebagai berikut:

```
00000120  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000130  FF FF FF FF FF FF FF FF FF FF FB 72 50 86 80 01
00000140  20 00 4B 80 00 00 00 00 00 09 70 00 00 00 00 00
00000150  01 2E 00 00 00 00 00 00 25 C0 00 00 00 58 58 58
00000160  58 36 38 23 2E 74 78 74 20 00 FF FF FF FF FF FF
```

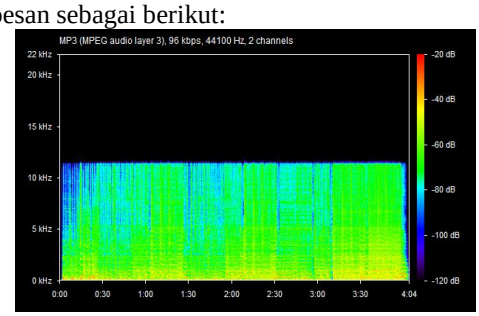
Gambar 7 Data *Hexa* Setelah Disisipi Pesan

4.4.2 Analisa Uji Kualitas Data Spektrum

Analisa hasil uji kualitas menggunakan data spektrum pada media *audio* MP3 Avril Lavigne judul lagu Complicated dapat dibandingkan sebagai berikut:

a. Sebelum disisip pesan

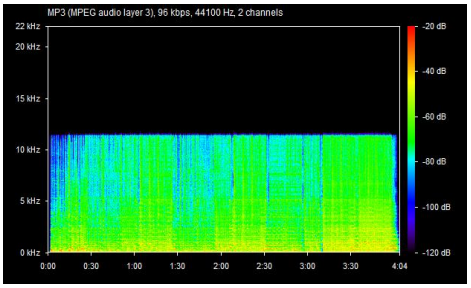
Data spektrum *audio* MP3 sebelum disisipkan pesan sebagai berikut:



Gambar 8 Data *Spektrum* Sebelum Disisipi Pesan

b. Setelah disisip pesan

Data spektrum *audio* MP3 sebelum disisipkan pesan sebagai berikut:



Gambar 9 Data *Spektrum* Setelah Disisipi Pesan

4.4.3 Analisa Uji Kapasitas Pesan Rahasia (*.txt*)

Analisa hasil uji kapasitas pesan rahasia (*.txt*), baik sebelum dilakukan penyisipan maupun setelah dilakukan penyisipan pada media pembawa (*carrier*) berjenis *audio* MP3 dapat dijelaskan pada tabel dibawah ini:

Tabel 1 Hasil Uji Kapasitas Pesan Rahasia (*.txt*)

File Pesan (.txt)	File Audio (MP3)	Stegano	Destegano	Keterangan
Pesan Rahasia	Avril (complicated)	73 bytes	73 bytes	Tetap

4.4.4 Analisa Uji Kapasitas Media Pembawa Pesan (MP3)

Analisa hasil uji kapasitas *audio* MP3 sebagai media pembawa (*carrier*) pesan rahasia, baik sebelum dilakukan penyisipan maupun setelah dilakukan penyisipan pesan rahasia (*.txt*) dapat dijelaskan pada tabel dibawah ini:

Tabel 2 Hasil Uji Kapasitas Media Pembawa Pesan (MP3)

File Audio (MP3)	Kapasitas	File (.txt)	Kapasitas	mp3stegz	Ket
Avril (complicated)	2790000 bytes	Pesan Rahasia	73 bytes	2790000 bytes	Tetap

5. Penutup

Berdasarkan hasil analisa uji kualitas dan uji kapasistas yang dilakukan dalam penelitian menunjukkan beberapa hal, yaitu penyembunyian/ penyisipan pesan rahasia pada *audio* MP3 dengan menggunakan metode *parity coding* dapat dilakukan namun perlu diperhatikan bahwa besaran kapasitas pesan rahasia yang disisipkan harus lebih kecil dari kapasitas media pembawa pesan *audio* MP3.

Adapun pengujian kualitas pada media *audio* MP3 menggunakan data *hexa* menunjukkan bahwa terjadi perubahan pada data *hexa* walaupun tidak signifikan, dan perubahan pada data *hexa* tersebut bersifat fleksibel. Pada pengujian kualitas menggunakan data spektrum pada *audio* MP3 menunjukkan bahwa terjadi perubahan pada data spektrum namun juga tidak signifikan.

Sedangkan pengujian dari besaran kapasitas, baik pada pesan yang disisipkan maupun pada media *audio* MP3 sebagai pembawa pesan tidak berubah atau tetap seperti pada kapasitas *file* aslinya.

Untuk itu, penelitian selanjutnya dapat melengkapi hasil penelitian ini dengan menambah jenis *file* yang dapat disisipkan dan dikembangkan hingga proses mendekripsikan pesan.

Daftar Pustaka

[1] Suharso dan Ana Retnoningsih. 2005. *Pengertian Analisis*. KBBI: Departemen Pendidikan Nasional.

[2] Johnson, Neil F., D. Zoran, and J. Sushil. 2002. *Information Hiding: Stteganography And Watermarking - Attacks And Countermeasures*. USA: Kluwer Academic Publishers.

[3] Nurrachman, Hilman. 2013. *Analisis dan Implementasi Steganografi Menggunakan Audio MP3 Dengan Metode Parity Coding*. Bandung: Universitas Widyatama.

[4] Malviya, Swati, Manish Saxena, and Dr. Anubhuti Khare. 2012. *Audio Steganography by Different Methods*. International Journal Of Emerging Technology And Advanced Engineering Volume 2 Issue 7. ISSN 2250-2459). Website:Www.Ijetae.Com.

[5] Schneier, B. 1996. *Applied Cryptography*. New York: Wiley.

[6] Menezes, A., P. Oorshcot, and S. Vanstone. 1997. *Handbook Of Applied Cryptography*. Boca Raton FL: CRC Press.

[7] Bender, Walter, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. 1996. *Techniques For Data Hiding*. IBM Systems Journal, Volume 35 No.3 and 4 Pp.313-336.

[8] Arikunto, Suharsimi. 2009. *Prosedur Penelitian; Suatu Pendekatan Praktik*. Edisi Revisi 6. Jakarta: Rhineka Cipta.

[9] Margono. 2005. *Pengertian Penelitian Eksperimental*. http:/metodepenelitian/ navelsblog.html.

[10] Sukardi. 2003. *Langkah-Langkah Penelitian Eksperimental*. http:/metodepenelitian/ navelsblog.html