Prosiding Seminar Ilmu Komputer dan Teknologi Informasi Vol. 1, No. 1, September 2016
ISSN 2540 – 7902

KRIPTOGRAFI PADA FILE AUDIO MP3 MENGGUNAKAN METODE PENGEMBANGAN TRANSPOSISI

Said Fachmi Salim*[,1], Zainal Arifin[2], Dyna Marisa Khairina[3]

[1,2,3]Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Mulawarman
Kampus Gunung Kelua Barong Tongkok Samarinda, Kalimantan Timur
Email: saidfachmi23@gmail.com[1], zainal.arifin@unmul.ac.id[2], dyna.ilkom@gmail.com[3]

ABSTRAK

Metode Transposisi merupakan salah satu teknik enkripsi konvensional (simetri) yang digunakan sejak berabad-abad lalu untuk mengamankan pesan yang dikirimkan kepada orang lain. Pada penelitian ini metode transposisi dikembangkan sehingga implementasinya lebih khusus pada pengacakan file audio dengan format MP3 . Metode ini digunakan untuk melakukan pengacakan bit yang menyusun *frame* secara horizontal dan sesuai dengan kunci simetri untuk melakukan proses enkripsi maupun dekripsi. Penelitian ini bertujuan untuk membuat suatu aplikasi kriptografi yang dapat mengamankan data audio dengan format MP3 menggunakan metode transposisi. Aplikasi ini melakukan proses kriptografi untuk semua file audio dengan format MP3. Kunci bersifat simetri, karakter yang digunakan berupa kunci alfanumerik (a-z,A-Z,0-9) dan spasi, dimana semakin panjang kunci yang digunakan maka audio dengan format MP3 akan semakin tersamarkan. Hasil akhir penelitian ini berupa aplikasi kriptografi pada audio dengan format MP3 dengan metode pengembangan transposisi yang bertujuan untuk menyamarkan data audio dengan format MP3 sehingga informasi rahasia yang terkandung di dalamnya dapat terjaga dan hanya dapat dibaca oleh pengguna yang memiliki kunci kriptografi serta aplikasi tersebut.

Kata kunci : Kriptografi, Audio, MP3, Enkripsi, Dekripsi, Transposisi, Pengembangan Transposisi

1. PENDAHULUAN

Penelitian ini menggunakan file audio dengan format MP3 (*Moving Pictures Experts Group -1* Audio *Layer 3*). Semenjak dikembangkan pada tahun 1993 oleh Karlheinz Brandenburg (Pollak, 2005) File audio dengan format MP3 merupakan file yang paling banyak digunakan dan paling banyak ditemukan dalam kehidupan sehari-hari [1], file audio MP3 paling banyak digunakan dalam industri musik oleh karena itu penulis memilih format MP3 sebagai format audio yang akan digunakan dalan melakukan kriftograpi.

Metode enkripsi yang digunakan untuk pengacakan audio pada *file* MP3 haruslah metode enkripsi yang tidak menambah atau mengurangi data masukan, melainkan menukar posisi [2]. Metode transposisi dipilih dalam penelitian ini karena memenuhi syarat tersebut, metode transposisi yang digunakan dalam penelitian ini telah dikembangkan hingga sesuai untuk berkas audio MP3 baik untuk enkripsi maupun dekripsi.

Metode pengembangan transposisi ini dikembangkan oleh Ahmad Jawahir pada tahun 2015 dan telah diimplementasikan sebelumnya pada *file* audio dengan format MP3 (*MP3eform audio format*), Untuk mengakses berkas MP3 dibutuhkan langkah pembacaan atau penulisan *header* berkas MP3 yang mana langkah ini tidak diperlukan dalam pembacaan MP3, pada *file* audio dengan format MP3 pengacakan dilakukan pada segmen-segmen penyusun bit sedangkan pada file MP3 pengacakan dilakukan pada frame-frame yang menyusun bit data . Tujuan yang ingin dicapai pada penelitian ini adalah membuat suatu aplikasi yang dapat mengamankan *file* dengan format MP3 agar tidak dapat diganggu ataupun diakses oleh pihak yang tidak berhak sehingga keamanan data tetap terjaga dengan batasan :

1. Format *file* audio yang digunakan adalah MP3
2. Proses pengacakan yang dilakukan berdasarkan posisi *byte* pada *frame* yang menyusun audio.
3. Kunci yang dipakai berupa alfanumerik dan simbol (a-z, A-Z, 0-9).
4. Panjang kunci tidak terbatas
5. Hasil *file* yang terenkripsi dan terdeskripsi tetap berformat MP3
6. Tidak ada batasan ukuran maksimal pada *file* MP3
7. Tidak ada batasan byte pada pada *file* audio MP3
8. Kunci bersifat simetris

2. LANDASAN TEORI

2.1 Kriptografi

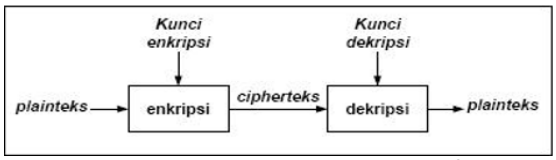
Penyandian merupakan salah satu alternatif atau cara untuk mengamankan atau menjaga suatu kerahasiaan data atau gambar. Seni dan ilmu untuk

*Corresponding Authors
Email : saidfachmi23@gmail.com

ISSN 2540 – 7902

menyandikan atau menjaga keamanan atau serta kerahasiaan pesan disebut kriptografi [3]

Kriptografi juga dapat diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentikasi data, dengan kata lain kriptografi digunakan untuk menjamin keleluasaan pribadi dan pembuktian keaslian pesan dalam berkomunikasi [4]. Kriptografi mengatasi masalah keamanan data dengan menggunakan kunci, yang dalam hal ini algoritma tidak dirahasiakan lagi, tetapi kunci harus tetap dijaga kerahasiaannya. Kunci (*key*) adalah parameter yang digunakan untuk transformasi *enciphering* dan *deciphering*. Kunci biasanya berupa *string* atau deretan bilangan. Dengan menggunakan K, maka fungsi enkripsi dan dekripsi dapat ditulis sebagai skema pada gambar 1 :



Gambar 1. Alur Skema Kriptografi

2.2 Metode Penyandian Transposisi

Teknik transposisi pada dasarnya adalah membuat *ciphertext* dengan menggantikan posisi objek-objek *plaintext* tanpa menggantikan objek *plaintext* tersebut [4], jadi pada teknik transposisi ini tidak diperlukan karakter lain. Pada teknik transposisi ini pembuatan *ciphertext* dilakukan dengan pembacaan nilai matrix pada kolom per kolom sesuai dengan kunci yang digunakan

2.3 Metode Penyandian Transposisi Pengembangan

Enkripsi berkas menggunakan subtitusi dan pergeseran bit telah sering dilakukan, terhadap berkas audio namun bukan dengan mengacak isi berkas, melainkan melalui pengacakan suara. Metode enkripsi yang digunakan haruslah metode enkripsi yang tidak menambah atau mengurangi data masukan, melainkan menukar posisi [2]. Metode transposisi dipilih dalam penelitian ini karena memenuhi syarat tersebut.

Tabel 1. Transposisi Baris

Kunci	4	3	1	5	2	6
Plaintext	S	a	Y	A	S	E
	D	a	N	G	B	E
	L	a	J	A	R	K
	R	i	P	T	O	G
	R	a	F	I	Y	Z

Metode pengembangan transposisi dikembangkan hingga sesuai untuk berkas audio. Baik untuk enkripsi maupun dekripsi, data suara berkas audio dibagi menjadi segmen-segmen, diindekskan dalam bentuk array dan kemudian posisi indeks diacak menggunakan metode transposisi. Kunci yang digunakan akan mempengaruhi hasil pengacakan posisi indeks. Hasil keluaran dibentuk dengan menyusun ulang data mengikuti indeks-indeks dari hasil pengacakan posisi menggunakan metode transposisi. Jika kunci yang digunakan untuk dekripsi tidak sama dengan kunci yang digunakan saat enkripsi, maka suara terdengar tidak seperti aslinya, kecuali kunci yang digunakan memiliki order yang sama. Langkah pertama yang harus dilakukan sebelum memulai membentuk tabel transposisi adalah membuat 105ector yang menunjukkan urutan panjang baris atau kolom. Hal ini dilakukan karena pada metode transposisi yang dikembangkan ini, terdapat sel tabel yang dilangkahi, jadi ada kemungkinan beberapa baris atau kolom yang tidak utuh. Nilai m dan n harus ditentukan terlebih dahulu sebelum membentuk 105ector tersebut. Nilai m dicari dengan menggunakan algoritma

2.4 Berkas MP3

MP3 adalah pengembangan dari teknologi sebelumnya sehingga dengan ukuran yang lebih kecil dapat menghasilkan kualitas yang setara dengan kualitas CD , spesifikasi dari layer-layer sebagai berikut :

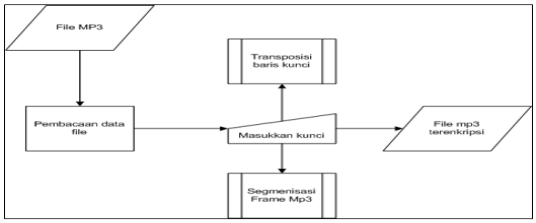
Layer 1 : Paling baik pada 384 kbit/s.
Layer 2 : Paling baik pada 256…384 kbit/s, sangat baik pada 224 – 256 kbit/, baik pada 192 – 224 kbit/s.
Layer 3 : paling baik pada 224 – 320 kbit/s, sangat baik pada 192 – 224 kbit/s, baik pada 128 – 192 kbit/s

File MP3 terdiri dari bagian-bagian kecil yang disebut *frame*. Biasanya tiap frame dapat berdiri sendiri, tiap frame memilik header yang berisi informasi frame tersebut [5]. Pada *file* MP3 frame bisa merupakan bagian yang saling bergantung namun untuk memotong *file* mp3 bisa dilakukan dimana saja selama masih dalam batasan frame

3. HASIL DAN PEMBAHASAN

3.1 Proses Enkripsi Transposisi

Pada gambar 2 dijelaskan alur intruksi dari proses enkripsi pada file audio dengan format mp3

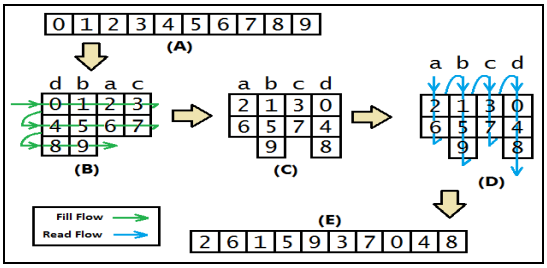


Gambar 2. Flowchart proses Enkripsi

ISSN 2540 – 7902

Pada *chiper* transposisi, huruf-huruf di dalam plainteks tetap sama, hanya saja urutannya diubah. Dengan kata lain, algoritma ini melakukan *transpose* terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (*scrambling*) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut. Pada sistem yang dibuat, transposisi dilakukan sebanyak 1 kali yaitu transposisi baris

Setelah audio berubah menjadi pecahan maka proses selanjutnya yaitu melakukan proses enkripsi menggunakan Metode Pengembangan Transposisi berdasarkan baris secara horizontal sesuai dengan kunci yang dimasukkan pengguna. Kunci yang dapat digunakan oleh pengguna yaitu alfanumerik (a-z, A-Z, 0-9) . Semakin banyak dan rumit kunci yang dimasukkan maka posisi *frame* akan semakin teracak dan hasil enkripsi semakin tersamarkan



Gambar 3. Proses Transposisi Baris

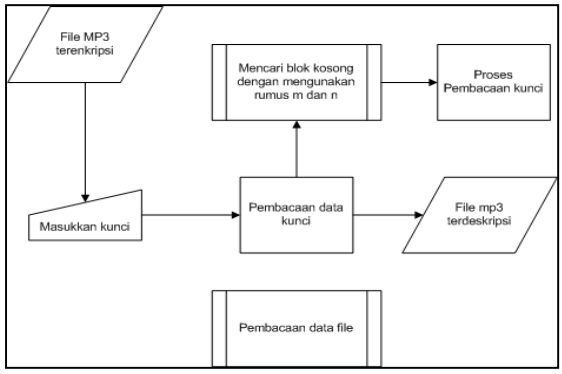
Pada gambar 3 dijelaskan awal proses transposisi dihitung panjang frame lalu diacak berdasarkan panjang kunci yang ditransposisikan secara baris. Kebalikan dari proses enkripsi, proses dekripsi dimulai dengan pembacaan berkas MP3 terenkripsi menggunakan pembaca MP3 dan kemudian kunci yang sama dengan yang digunakan saat proses enkripsi dimasukkan. Setelah itu, preproses segmen dilakukan untuk memisahkan segmen suara yang akan diacak dan sisa segmen yang tidak terpakai. Segmen suara kemudian dikembalikan berdasarkan baris kemudian Hasil pengacakan ini kemudian digabungkan kembali dengan segmen sisa dan kemudian dituliskan menjadi berkas MP3.

Tabel 2. Tabel susunan Kunci

Susunan kunci enkripsi	Fa 1	Do 2	Mi 3	Si 4	Do 5	Sol 6	Re 7	Re 8	La 9	Mi 10
Hasil Dekripsi	5 Do	8 Re	3 Mi	1 Fa	6 Sol	9 La	4 Si	2 Do	7 Re	10 Mi

3.2 Proses Deskripsi Transposisi

Proses dekripsi merupakan kebalikan dari proses enkripsi. Proses dekripsi dimulai dengan pembacaan berkas MP3 terenkripsi menggunakan pembaca MP3 dan kemudian kunci yang sama dengan yang digunakan saat proses enkripsi dimasukkan. Setelah itu, preproses segmen dilakukan untuk memisahkan segmen suara yang akan diacak dan sisa segmen yang tidak terpakai. Segmen suara kemudian diacak berdasarkan baris Hasil pengacakan ini kemudian digabungkan kembali dengan segmen sisa dan kemudian dituliskan menjadi berkas MP3.



Gambar 4. Flowchart Proses Deskripsi

Pada Gambar 4 Langkah pertama yang harus dilakukan sebelum membentuk tabel transposisi adalah membuat vektor yang menunjukkan urutan panjang baris baris. Hal ini dilakukan karena pada metode transposisi yang dikembangkan ini, terdapat sel tabel yang dilangkahi, jadi ada kemungkinan beberapa baris yang tidak utuh. Nilai m dan n harus ditentukan terlebih dahulu sebelum membentuk vektor tersebut. Nilai m dicari dengan menggunakan algoritma teks berikut :

Setelah menemukan nilai m, maka nilai n kemudian dapat ditemukan dengan menggunakan perhitungan berikut :

```
m = 1
While(True)
If m x Length(Key) >= Length(Data) Then
Break
End If
m = m + 1
Loop
```

Setelah menemukan nilai m, maka nilai n kemudian dapat ditemukan dengan menggunakan perhitungan berikut : n = Length(Data) - ((m - 1) x Length(Key)

Setelah segmen diacak, baik itu pada proses enkripsi maupun dekripsi, langkah penyatuan segmen dan sisa bit harus dilakukan. Sisa bit yang telah dipisahkan sebelumnya digabungkan kembali. Hasil

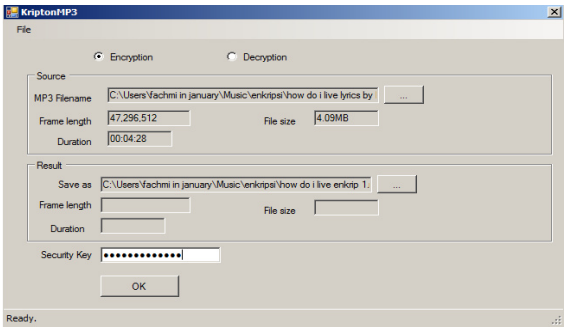
ISSN 2540 – 7902

penggabungan ini kemudian ditulis ke dalam berkas MP3 menggunakan MP3 *writer*.

3.3 Implementasi Sistem

Program dibuat menggunakan bahasa pemrograman C#.

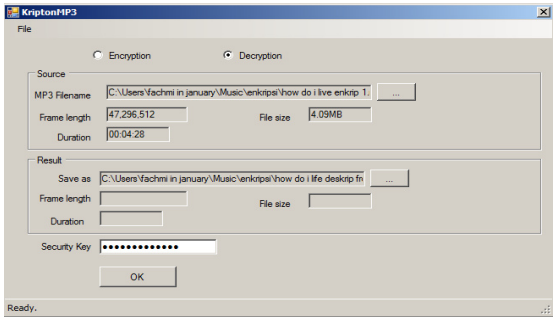
Enkripsi



Gambar 5. Interface Enkripsi

Pilih proses Encryption seperti pada gambar 5 diatas , pilih berkas MP3 yang akan dienkripsi setelah itu akan muncul informasi data file MP3 tersebut Antara lain : ukuran, panjang frame, dan durasi. Masukkan password dan lokasi tempat menyimpan hasil enkripsi, klik tombol "OK"

Deskripsi

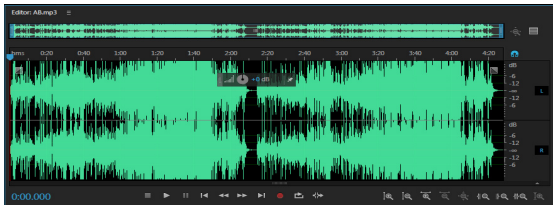


Gambar 6. Interface Deskripsi

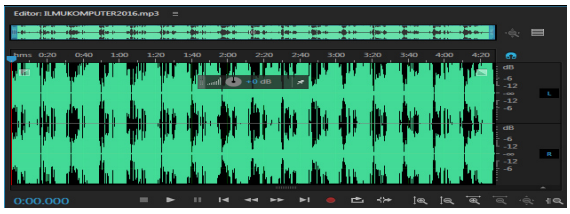
Pada gambar 6, Tahapan menjalankan proses dekripsi tak jauk berbeda dengan proses enkripsi yang membedakan yaitu pemilihan menu proses dari enkripsi jadi deskripsi.

3.4 Pengujian Sistem

Pengujian Berdasarkan Panjang Kunci



Gambar 7. Pengujian menggunakan panjang 4 char



Gambar 8. Pengujian menggunakan panjang 16 char

Pada hasil pengujian berdasarkan panjang kunci dapat kita liat perbedaan pada gambar 7 dan gambar 8, dimanapanjang kunci dihitung berdasarkan panjang karakter yang digunakan.

Pengujian berdasarkan data file

Pengujian selanjutnya dilakukan berdasarkan pada perubahan apa saja yang terjadi pada file yang telah dienkripsi

Tabel 3. Perbandingan perubahan data file

Parameter	Ukuran	Durasi	*Sample rate*	format	*Bit Depth*
Source File	4.190 KB	00:04:28.120	44100 Hz	MP3	32
Result File	4.190 KB	00:04:28.120	44100 Hz	MP3	32

Berdasarkan tabel 3 diatas dapat disimpulkan bahwa proses kriptografi file MP3 dengan menggunakan metode pengebangan transposisi hanya mengubah posisi dari isi *chipper audio* maupun *frame audio* dari file MP3 tersebut tanpa mempengaruhi nilai dari data format dan data file tersebut

Pengujian Waktu Proses Enkripsi dan Dekripsi

Berdasarkan 2 pengujian sebelumnya, pengujian dilakukan dengan melihat. Pengujian selanjutnya dilakukan untuk melihat waktu yang dibutuhkan dalam melakukan proses enkripsi maupun proses dekripsi berdasarkan durasi dan panjang *frame* dari *file* MP3.

Tabel 4. Perbandingan panjang waktu proses

No	Durasi MP3	Panjang Frame	Panjang Kunci	Waktu Proses	
				Enkripsi	Dekripsi
1	00:51:48	548.352.000	15	1,88 sec	1,6 sec
2	00:05:17	56.107.008	15	0,25 sec	0,23 sec
3	03:03:18	1,939,465,728	15	7,18 sec	6,65 sec

ISSN 2540 – 7902

Berdasarkan tabel 4 diatas pengujian waktu proses melakukan proses enkripsi dan dekripsi menggunakan metode pengembangan transposisi, maka dapat dilihat bahwa lama waktu yang dibutuhkan untuk melakukan proses enkripsi maupun dekripsi berbanding lurus dengan durasi dan panjang frame yang menyusun MP3. Jadi semakin panjang frame dan durasi audio maka proses enkripsi dan dekripsi juga semakin lama.

4. Kesimpulan dan Saran

4.1 Kesimpulan

Kesimpulan yang dapat diambil berdasarkan penelitian mengenai Kriptografi Video menggunakan metode Transposisi antara lain :

1. Aplikasi kriptografi pada file audio MP3 menggunakan metode pengembangan transposisi dilakukan dengan melakukan pengacakan *frame* penyusun audio, secara horizontal.
2. Berdasarkan penelitian diketahui bahwa lama proses untuk melakukan proses kriptografi file audio MP3 menggunakan metode pengembangan transposisi ditentukan oleh panjang *frame* , dan durasi audio.
3. Semakin panjang kunci yang digunakan maka hasil kriptografi akan semakin tersamarkan.

4.2 Saran

Berdasarkan kesimpulan yang ada dari Kriptografi video menggunakan metode Transposisi memiliki beberapa keunggulan serta kelemahan. Oleh karena itu penulis memiliki beberapa saran untuk pengembangan program selanjutnya antara lain:

1. Dibutuhkan suatu metode yang dapat melakukan kriptografi pada audio dengan jenis format yang lain.
2. Dibutuhkan pengembangan aplikasi kedepannya dalam versi *mobile.*

5. DAFTAR PUSTAKA

[1] Adriansyah Y, 2010. "*Simple Audio Cryptography*", Institute Teknologi Bandung Indonesia.

[2] Jawahir Ahmad , Haviluddin. "*An audio encryption using transposition method", International Journal of Advances in Intelligent Informatics* ISSN: 2442-6571 Vol 1 No 2, July 2015, pp. 98-106.

[3] Kurniawan, Y. 2004. *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Bandung : Penerbit Informatika

[4] Munir, Rinaldi. Kriptografi. 2006. Bandung: Penerbit Informatika. Universitas Mulawarman. Samarinda

[5] Pollak l., "Audio Compression Using Wavelet Techniques", Electrical and Computer Engineering Purdue University, 2005.