TEKNIK KEAMANAN DATA MENGGUNAKAN KRIPTOGRAFI DENGAN ALGORITMA VIGENERE CIPHER DAN STEGANOGRAFI DENGAN METODE END OF FILE (EOF)

[1]Patricia Handoko, [2]Aripin, M.Kom
Program Studi Teknik Informatika – S-1
Fakultas Ilmu Komputer
Universitas Dian Nuswantoro, Jl. Nakula 1 No. 5-11, Semarang
[1]111201105900@mhs.dinus.ac.id, [2]arifin@dsn.dinus.ac.id

ABSTRAK

Dengan berkembangan zaman, maka semakin berkembang pula kebutuhan manusia terutama kebutuhan akan informasi. Oleh karena itu maka diperlukanlah suatu pengamanan data yang akan menjamin keamanan dan keutuhan data ketika data tersebut dikirim maupun diterima. Keamanan pengiriman data dapat diselesaikan dengan menggunakan kriptografi. Salah satu algoritma yang dapat digunakan untuk proses kriptografi yaitu dengan menggunakan algoritma Vigenere Cipher. Untuk menyembunyikan data tidaklah cukup hanya dengan proses kriptografi karena akan mengundang kecurigaan pihak lain, maka untuk menutupi kecurigaan tersebut dibutuhkan suatu proses menyisipkan data ke dalam file lain untuk menutupi kecurigaan tersebut. Proses menyisipkan data kedalam file lain lebih kita kenal dengan nama teknik steganografi. Metode End of File dapat menjadi salah satu metode yang dapat digunakan dalam proses Steganografi ini. Hasil dari penelitian ini yaitu menghasilkan aplikasi yang dapat menyembunyikan file dengan baik dan menutup kecurigaan dari pihak lain.

Kata Kunci : penyandian, kriptografi, vigenere cipher, steganografi, end of file

I. PENDAHULUAN

Keamanan data dan informasi merupakan hal sangat penting di era reformasi saat ini. Umumnya, setiap institusi memiliki dokumen-dokumen penting dan bersifat rahasia yang hanya boleh diakses oleh orang tertentu. Sistem informasi yang dikembangkan harus menjamin keamanan dan kerahasiaan dokumen-dokumen tersebut. Namun kendalanya bahwa media-media yang digunakan seringkali dapat disadap oleh pihak lain [**1**].

Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. (*Cryptography is the art and science of keeping messages secure*) "Crypto" berarti "secret" (rahasia)vdan "graphy" berarti "writing" (tulisan). Para pelaku atau praktisi kriptografi disebut *cyrptographers*. Sebuah algoritma kriptografik (*cryptographic algorithm*), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya persamaan kedua matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat [**2**].

Vigenere Cipher adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso. Nama Vigenere sendiri diambil dari seorang yang bernama Blaise de Vigenere. Nama vigenere diambil sebagai namaalgoritma ini karena beliau menemukan kunci yang lebih kuat lagi untuk algoritma ini dengan metode autokey cipher meskipun algoritma dasarnya telah ditemukan lebih dahulu oleh Giovan Battista Bellaso [**3**].

Tetapi pada zaman sekarang ini teknik pengamanan data dengan *kriptografi* masih dirasa kurang. Setelah dilakukan proses enkripsi pada suatu data maka kita perlu menyembunyikan data tersebut di dalam suatu data yang lain sehingga tidak menimbulkan kecurigaan pada pihak-pihak yang tidak berkepentingan. Proses seperti yang disampaikan diatas disebut dengan Steganografi.

Teknik EoF atau End Of File merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini menggunakan cara dengan menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran fileyang telah disisipkan data,sama dengan ukuran file sebelum disisipkan data ditambah denganukuran data yang disisipkan ke dalam file tersebut [**4**].

Berdasarkan masalah tersebut, maka penulis mengusulkan judul penelitian "Teknik Keamanan Data Menggunakan Kriptografi dengan Algoritma Vigenere Chiper dan Steganografi dengan Metode End of File (EoF)" sebagai bahan pertimbangan untuk proses keamanan pada pengiriman data.

II. DASAR TEORI

A. Kriptografi

Kriptografi merupakan sebuah ilmu yang digunakan untuk menjaga kerahasiaan dari sebuah data, dengan menggunakan metode-metode tertentu sehingga data hanya dapat dibaca oleh orang yang berhak terhadap data tersebut.

Dalam menjaga kerahasiaan data, kriptografi mengubah pesan asli (*plaintext*) menjadi pesan yang disandikan (*ciphertext*), proses ini disebut dengan enkripsi. Kemudian *ciphertext* inilah yang akan dikirim kepenerima, di pihak penerima, penerima mengubah kembali *ciphertext* menjadi *plaintext* agar pesan asli dapat dibaca kembali, proses ini disebut dengan dekripsi.

Kriptografi mempunya 4 tujuan umum [**3**]yaitu;

1. Kerahasiaan

Menjaga isi dari suatu pesan dari siapapun kecuali kepada orang yang memiliki otoritas terhadap data yang disandikan dalam bentuk kunci dekripsi.

2. Integritas Data

Dalam kriptografi akan dilakukan proses pengecekan apakah data yang sampai di penerima merupakan benar data yang pertama kali dikirim oleh pengirim.

3. Autentikasi

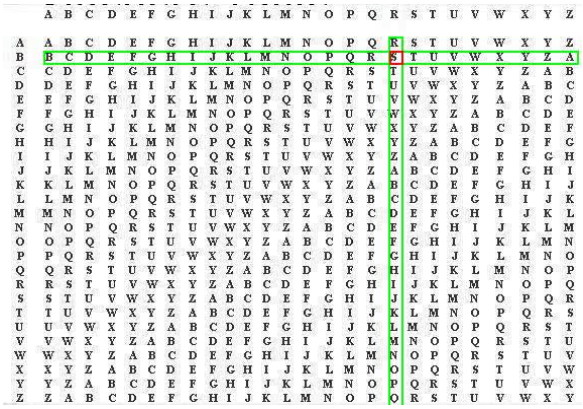
Pada proses autentikasi ini data akan dicek apakah mengalami manipulasi dalam isinya seperti penyisipan, penghapusan dan penggantian data.

4. Non-Repudiasi

Jika seseorang sudah mengirimkan pesan, maka orang tersebut tidak dapat membantah/ menyangkal pengiriman pesan tersebut.

B. Algoritma Vigenere Cipher

Algoritma Vigenere Cipher ini menggunakan bujursangkar Vigenere untuk melakukan enkripsi. Setiap baris di dalam bujursangkar menyatakan huruf-huruf ciphertext yang diperoleh dengan Caesar cipher.Untuk lebih jelasnya perhatikan gambar di bawah ini. Deretan huruf mendatar menunjukkan plaintext, sedangkan huruf menurun menunjukkan kunci.



Gambar 1 : Tabula Recta Algoritma Vigenere Cipher

Pada proses enkripsi Vigenere Cipher ini selain menggunakan Tabula Recta untuk mendapatkan *ciphertext* juga dapat menggunakan rumus berikut [**5**]:

$$Ci = (Pi + Ki) \bmod 26 \quad (1)$$

Sedangkan untuk rumus dekripsi Vigenere Cipher:

$$Pi = (Ci - Ki) \bmod 26 \quad (2)$$

Dimana :

Ci= cipher teks

Pi = plainteks

Ki = kunci

C. Steganografi

Steganografi merupakan seni komunikasi rahasia dengan menyembunyikan pada objek yang tampaknya tidak mencurigakan atau berbahaya. Steganografi berasal dari 2 kata dalam bahasa Yunani yaitu, Steganos, yang berarti tertutup dan Graphia yang berarti menulis. Deskripsi lain yang popular untuk steganografi adalah *Hidden in Plain Sight* yang artinya tersembunyi di depan mata.

Untuk menghasilkan steganografi yang baik ada 3 kriteria yang harus diperhatikan [**6**], yaitu :

1. *Imperceptibility*.

Keberadaaan pesan rahasia tidak bisa dikenali oleh indra manusia. Misalnya, jika *convertext* berupa citra maka penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *covertextnya*.

2. *Fidelity*.

Mutu *stegomedium* tidak berubah banyak akibat penyisipan. Misalnya, jika *convertext* berupa citra maka penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *covertextnya*.

3. *Recovery*.

Pesan yang disembunyikan harus dapat dikenali kembali. Karena tujuan steganografi adalah *data hiding*, maka sewaktu-waktu pesan rahasia di dalam *stegotext* harus dapat diambil kembali untuk digunakan.

D. Metode End Of File

Teknik EOF atau End Of File merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini menggunakan cara dengan menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran file yang telah disisipkan data,sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam file tersebut.

Proses yang terjadi dalam penyisipan pesan dengan metode EoF adalah dengan mengubah pesan menjadi kode desimal, dapatkan nilai atau letak pixel terakhir dari citra, berikan sebuah tanda pengenal *start* dari pesan dan tambahkan kode desimal dari pesan.

Pada proses pengungkapan pesan, maka proses yang diperlukan adalah mengenali letak tanda pengenal dan

mengambil nilai desimal dari pesan rahasia serta terakhir mengubah nilai desimal menjadi sebuah pesan [**4**].

III. METODE PENELITIAN

A. Metode Pengumpulan Data

Dalam penelitian ini data yang digunakan merupakan data sekunder.Penulis meperoleh data dari telaah pustaka dan artikel-artikel yang penulis dapat dari pustaka yang mendukung, informasi dari internet, dan jurnal-jurnal.

B. Metode Pengembangan Sistem

Rapid Aplication Development (RAD) adalah sebuah metode pengembangan software yang diciptakan untuk menekan waktu yang dibutuhkan untuk mendesain serta mengimplementasikan sistem informasi sehingga dihasilkan siklus pengembangan yang sangat pendek.

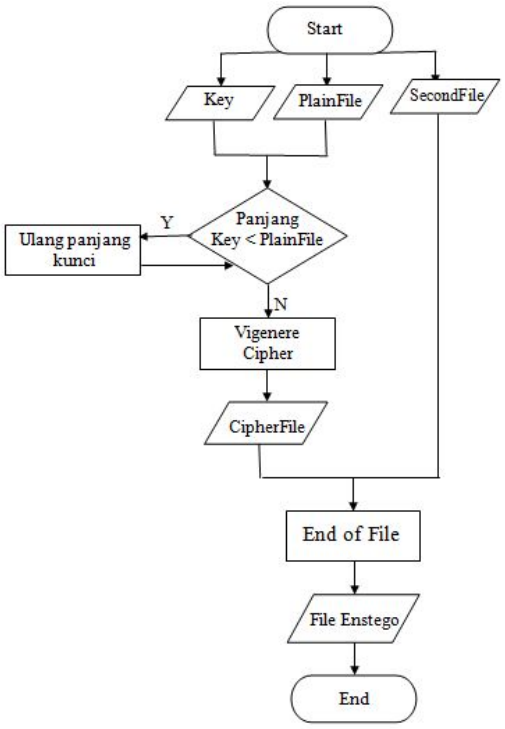
Model RAD ini merupakan adaptasi dari model sekuensial linier dimana perkembangan yang cepat dicapai dengan menggunakan pendekatan kontruksi berbasis komponen. Sehingga, jika kebutuhan dipahami dengan baik, proses RAD memungkinkan developer menciptakan sistem fungsional yang utuh dalam periode waktu yang sangat pendek (± 60 sampai 90 hari).

Berikut ini adalah kelebihan metodologi RAD [**7**]:

1. Penghematan waktu dalam keseluruhan fase projek dapat dicapai.
2. RAD mengurangi seluruh kebutuhan yang berkaitan dengan biaya projek dan sumberdaya manusia.
3. RAD sangat membantu pengembangan aplikasi yang berfokus pada waktu penyelesaian projek.
4. Sudut pandang user disajikan dalam akhir baik melalui fungsi-fungsi atau antarmuka pengguna.
5. RAD menciptakan rasa kepemilikan yang kuat di antara seluruh pemangku kebijakan projek.

C. Pemodelan Proses

Berikut ini merupakan pemodelan proses yang penulis ajukan:

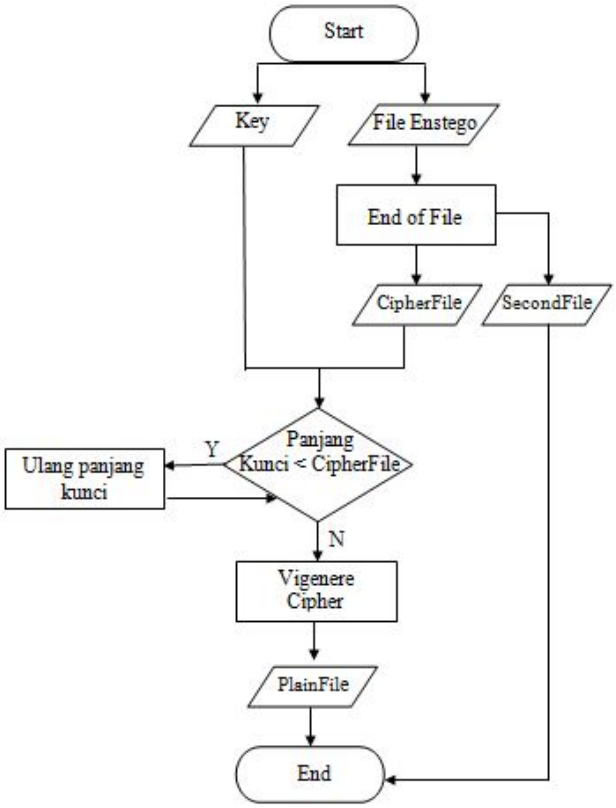


Gambar 2 : Pemodelan Proses Enstego

Pemodelan proses untuk proses Enstego yaitu mempunyai 3 buah inputan awal yaitu key, PlainFile dan SecondFile, kemudian key dan PlainFile akan terlebih dahulu melewati proses enkripsi dengan metode Vigenere Cipher. Pada proses enkripsi ini panjang key harus sama dengan panjang PlainFile, jika panjang kunci lebih kecil dari PlainFile maka akan terjadi pengulangan key sampai panjang key sama dengan panjang PlainFile. Setelah PlainFile berhasil terenkripsi maka diperolehlah CipherFile. Kemudian proses selanjutnya yaitu menyisipkan CipherFile ke dalam SecondFile dengan masuk ke pemrosesan steganografi dengan metode End of File, dengan metode End of File ini maka CipherFile akan disisipkan ke bagian paling akhir dari SecondFile, dan selesailah proses Enstego dan diperolehlah File Enstego.

Pemodelan Proses untuk proses Destego yaitu memiliki 2 inputan awal yaitu key dan CipherFile. Terlebih dahulu File Enstego melewati proses steganografi dengan metode End of File untuk memisahkan CipherFile dan SecondFile. Setelah proses steganografi berhasil maka, akan di dapatkan 2 file yaitu CipherFile dan SecondFile.

CipherFile akan diproses lagi dengan proses dekripsi dengan metode Vigenere Cipher. Pada proses dekripsi ini panjang key harus sama dengan panjang CipherFile, selain itu key yang digunakan harus sama dengan key yang digunakan saat proses enkripsi. Jika panjang key lebih pendek dari panjang CipherFile maka akan terjadi pengulangan panjang key sampai semua CipherFile berhasil terdekripsi. Kemudian setelah proses dekripsi berhasil maka, selesailah proses destego dan diperolehlah PlainFile kembali.



Gambar 3 : Pemodelan Proses Destego

IV. HASIL PENELITIAN

Pada penelitian ini penulis mencoba menggabungkan file-file dengan jenis file yang tidak hanya 1 format file melainkan dengan banyak jenis format file. Hal tersebut penulis lakukan karena penulis ingin menguji file dengan format apa saja yang dapat digunakan untuk aplikasi SteganoKrip ini.

Dari penelitian ini penulis memperoleh hasil penelitian berdasarkan pengamatan mata manusia untuk melihat perbedaan antara file asli dan file yang telah disisipi oleh file lain dan hasil penelitian berupa ukuran file yang berubah antara file asli dan file yang telah disisipi oleh file lain.

TABEL I

HASIL PENELITIAN BEDASARKAN GAMBAR

No	PlainFile	SecondFile	File Enstego	File Destego
1				
2				
3				
4				
5				

Pada hasil nomor 1 PlainFile merupakan file dengan format .xls dan merupakan file yang akan disisipkan pada SecondFile. File tersebut memiliki ukuran sebesar 514 KB. Sedangkan pada kolom Secondfile, masih pada hasil nomor 1, merupakan gambar dengan format .jpg dan merupakan gambar yang akan digunakan untuk menampung PlainFile. File tersebut memiliki ukuran sebesar 762 KB. Kemudian hasil dari penggabungan kedua file tersebut dapat dilihat pada kolom File Enstego. Pada hasil no 1 dapat dilihat bahwa tidak ada perbedaan gambar antara file yang belum dan yang sudah disisipi oleh file yang lain. Dengan tidak adanya perbedaan tersebut maka akan menghilangkan

kecurigaan bahwa file tersebut mengandung file pesan yang disembunyikan.

Pada hasil nomor 3 menunjukkan bahwa PlainFile merupakan file dengan format .mp3 yang memiliki ukuran file sebesar 3.36 MB yang akan disisipkan ke SecondFile yang merupakan file dengan format .pptx yang memiliki ukuran file sebesar 326 KB. Setelah kedua file tersebut melewati proses enstego menggunakan aplikasi SteganoKrip maka File Enstego yang muncul yaitu file yang tidak dapat terbaca oleh Microsoft Power Point, tetapi pesan yang terdapat didalamnya tidak rusak dan dapat terbaca lagi setelah dilakukan proses destego dengan aplikasi SteganoKrip.

Pada hasil nomor 5, penggabungan PlainFile dengan format .txt dan SecondFile dengan format .docx juga menghasilkan File Enstego dengan format .docx yang tidak dapat dibuka, tetapi ketika File Enstego diproses kembali dengan proses destego untuk mendapatkan PlainFile maka PlainFile yang disembunyikan pun tetap berhasil didapatkan dan tidak merusak PlainFile tersebut.

Pada kolom yang paling kanan merupakan hasil dari proses Destego. Dari hasil tersebut dapat diketahui bahwa pesan yang disembunyikan dapat dikembalikan lagi seperti pesan yang belum dienkripsi dan tidak mengalami kerusakan apapun sehingga file yang disembunyikan dapat dipergunakan seperti semestinya.

Penulis juga mendapatkan hasil pengukuran berdasarkan besar kecilnya ukuran file :

Pada tabel II menunjukkan bahwa aplikasi SteganoKrip ini dapat menyembunyikan pesan dengan semua jenis format file. Penulis mencoba menggunakan file dengan format .xls, .jpg, .pptx, .pdf, .mp3, .txt dan .docx untuk menguji aplikasi SteganoKrip yang telah penulis selesaikan.

Dari penelitian yang telah penulis lakukan didapatkan hasil bahwa penggabungan dari kedua file yaitu PlainFile dan SecondFile akan memperbesar ukuran SecondFile sebesar ukuran PlainFile.

TABEL II

HASIL PENELITIAN BEDASARKAN UKURAN FILE

No	PlainFile	Ukuran	SecondFile	Ukuran	Ukuran File Enstego
1	C:\Users\Public\Pictures\Sample Pictures\STO 2013 02 27.xls	514 KB	C:\Users\Public\Pictures\Sample Pictures\Koala.jpg	762 KB	1.24 MB
2	C:\Users\Public\Pictures\Sample Pictures\TA.pptx	326 KB	C:\Users\Public\Pictures\Sample Pictures\Ujian_TOEFL_BK.pdf	49.2 KB	375 KB
3	C:\Users\Public\Pictures\Sample Pictures\tulus-sepatu.mp3	3.36 MB	C:\Users\Public\Pictures\Sample Pictures\TA.pptx	326 KB	3.68 MB
4	C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg	757 KB	C:\Users\Public\Pictures\Sample Pictures\a.txt	3.52 KB	761 KB
5	C:\Users\Public\Pictures\Sample Pictures\coding.txt	814 bytes	C:\Users\Public\Pictures\Sample Pictures\BAB I.docx	17.7 KB	18.5 KB

Dapat dilihat pada tabel II no 1, PlainFile dengan ukuran file sebesar 514 KB disisipkan kedalam SecondFile dengan ukuran file sebesar 762 KB akan menghasilkan File Enstego dengan ukuran file sebesar 1.24 MB yang merupakan penggabungan ukuran file antara PlainFile dengan SecondFile.

Dapat dilihat pada tabel 4.2 no 2, SecondFile dengan ukuran file sebesar 49.2 KB dapat menampung dan penyembunyikan PlainFile yang memiliki ukuran file lebih besar yaitu 326 KB. Jadi SecondFile yang digunakan sebagai penampung pesan tersembunyi tidak harus memiliki ukuran file yang lebih besar dari pada pesan yang disembunyikan (PlainFile).

V. KESIMPULAN

A. Kesimpulan

Dari hasil perancangan dan pembuatan aplikasi SteganoKrip dengan Kriptografi menggunakan Vigenere Cipher dan Steganografi dengan metode End of File, maka didapatkan hasil sebagai berikut :

1. Dari hasil percobaan yang telah dilakukan aplikasi ini dapat menyembunyikan file dengan baik dan menutup kecurigaan dari pihak lain.

2. Pada proses dekripsi dapat mengembalikan file yang disembunyikan dengan baik dan tidak merusak file tersebut.
3. Penggabungan dari 2 file tersebut memperbesar ukuran file yang dihasilkan dari proses SeganoKrip ini, dikarenakan penggabungan ukuran dari masing-masing file tersebut.
4. Untuk hasil yang maksimal sebaiknya SecondFile merupakan file *image*.
5. File yang ukurannya lebih kecil dapat menampung file yang ukurannya lebih besar.

B. Saran

Saran yang dapat digunakan untuk tahap pengembangan dari aplikasi SteganoKrip ini yaitu :

1. Aplikasi ini membutuhkan besarnya kinerja komputer sesuai dengan besarnya file yang akan diproses. Semakin besar ukuran file yang akan diproses maka semakin besar kinerja komputer yang dibutuhkan.
2. Pada Message Box ditambahkan nama file dan tempat penyimpanan file yang telah berhasil melewati proses Enstego maupun Destego.
3. Sebaiknya ditambahkan menu seperti *Guiding Instruction* untuk mempermudah user mengoperasikan aplikasi SteganoKrip ini.

VI. DAFTAR PUSTAKA

[1] Muhammad Fairuzabadi, "Implemetasi Kriptografi Klasik menggunakan Borland Delphi," *Jurnal Dinamika Informatika*, pp. 65-78, September 2010.

[2] Jati Sasongko, "Pangamanan Data Informasi menggunakan Kriptografi Klasik," *DINAMIK*, vol. X, no. 3, pp. 160-167, September 2005.

[3] Ahmad Pudoli, Akbar Muchbarak, Farham Harvianto, and Sutrisno Hadi, "Keamanan Data Pada File Excel Dengan Menggunakan Vigenere Chipper," Mei 2014.

[4] Harianto Antonio, "Studi Perbandingan Enkripsi Steganografi Dengan Menggunakan Metode Least Significant Bit Dan End Of File," *Program Studi Teknik Informatika Jurusan Teknik Elektro Fakultas Teknik Universitas Tanjungpura*, 2013.

[5] Tri Cahyadi, "Implementasi Steganografi LSB dengan Enkripsi Vigenere Cipher Pada Citra JPEG," *Transient*, vol. 1, no. 4, December 2012.

[6] Renaldi Munir, *Diktat Kuliah Studi Teknik Informatika, Institut Teknologi Bandung*. Bandung, 2006.

[7] G.M Marakas, *System Analysis Design: an Active Approach*. New York: Mc.Graw-Hill, 2006.

[8] Naila Fithria, *Jenis-Jenis Serangan Terhadap Kritografi*, 2007.

[9] Dony Ariyus, *Keamanan Multi Media*. Yogyakarta, 2009.

[10] J.E Kendall and K.E Kendall, *Analisis dan Perancangan Sistem*. Jakarta, Indonesia: Indeks, 2010.