PESAN RAHASIA PADA CITRA DIGITAL DENGAN METODE LSB DAN ENKRIPSI VIGENERE CIPHER

Muhamad Dedi Suryadi[1)]
Zaenal Mutaqin Subekti[2)]

[1), 2)] STMIK Bani Saleh
Jl. Mayor M. Hasibuan No. 68, Bekasi, 17113

E-mail: kangdedi@gmail.com[1)], zaenalmutaqinsubekti.ubl@gmail.com[2)]

ABSTRACT

Confidentiality and security are very important to send a message through the media network or the Internet engineering cryptography and steganography can be used to protect messages sent , the development of cryptographic techniques with algorithms vigenere and integrated into the steganography by the method of least significant bit (lsb) sehigga expected to protect secret message.
This application can only hide text messages on a jpg image , therefore it is necessary for the application development can hide messages in addition to an image into the media such as audio and video.
Keywords : Vigenere , LSB , Cryptography , Steganography , Engineering.

ABSTRAK

Kerahasiaan dan keamanan merupakan hal yang sangat penting dalam mengirim pesan melalui media jaringan atau internet teknik kriptografi dan steganografi dapat digunakan untuk melindungi pesan yang dikirim, pengembangan teknik kriptografi dengan algoritma vigenere dan diintegrasikan kedalam steganografi dengan metode least significant bit (LSB) sehigga diharapkan dapat melindungi pesan rahasia.

Aplikasi ini hanya dapat menyembunyikan pesan teks pada gambar jpg, oleh sebab itu diperlukan pengembangan aplikasi untuk dapat menyembunyikan pesan kedalam media selain gambar seperti audio dan video

Kata kunci: Vigenere, LSB, Kriptografi, Steganografi, Teknik

1. PENDAHULUAN

Teknologi informasi, saat ini sudah berkembang dengan sangat pesat. Hal ini terjadi karena setiap informasi yang

dipertukarkan telah dikemas kedalam bentuk digital, sehingga dapat dengan mudah dipertukarkan melalui berbagai macam media transmisi yang telah tersedia di era digital saat ini. Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual.

Steganografi merupakan salah satu teknik yang digunakan dalam pengamanan informasi, yaitu dengan menyembunyikan informasi ke dalam media digital dengan metode tertentu agar tidak tampak perbedaan secara visual antara *file* asli dengan *file* yang telah disisipi informasi (*stegoimage*) sehingga tidak diketahui oleh steganalis (orang yang dapat memecahkan *stegoimage* tanpa mengetahui kunci yang ada). Data digital yang dapat menjadi tempat/media data yang akan disembunyikan (*stegomedium*) pada steganografi adalah gambar/citra, audio, dan video.

Salah satu metode steganografi adalah *Least Significant Bit* (LSB).Metode modifikasi LSB tergolong metode yang menggunakan teknik substitusi. Metode LSB menyembunyikan data rahasia dalam piksel piksel yang tidak signifikan (*least significant pixel*) dari *stegomedium*. Penelitian yang dilakukan oleh Hartono (2005) didapat kesimpulan bahwa metode LSB baik digunakan sebagai metode steganografi karena memiliki keunggulan yaitu, tidak dibutuhkan citra digital pembanding untuk mengembalikan data, waktu yang dibutuhkan untuk penyembunyian data cepat dan penurunan kualitas citra digital yang dihasilkan relatif kecil.

Berdasarkan uraian diatas, maka rumusan masalah dalam penelitian ini adalah bagaimana menyisipkan pesan kedalam media citra dengan steganografi *Least Significant Bit* (LSB) dan mengamankan pesan *file* txt dan rft dengan kombinasi algoritma kriptografi *vigenere.*

2. IDENTIFIKASI MASALAH

Berdasarkan uraian diatas, maka rumusan masalah dalam penelitian ini adalah bagaimana menyisipkan pesan kedalam media citra dengan steganografi *Least Significant Bit* (LSB) dan mengamankanpesan*file* txt dan rft dengan kombinasi algoritma kriptografi *vigenere.*

3. PENELITIAN TERDAHULU

Truman (2010) meneliti tentang aspek kerahasiaan pada algoritma Vigenère Cipher yang ditinjau berdasarkan kompleksitas algoritma, dan karakteristik penyandian plainteks terhadap cipherteks, menggunakan aplikasi Visual Basic 6. Algoritma Viginère Cipher dapat dipecahkan dengan mudah menggunakan komputer melalui teknik pemecahan analisis frekuensi.

Wildan (2010) meneliti tentang perlindungan pesan rahasia pada citra digital menggunakan metode LSB, dengan algoritma kriptografi Ultra untuk memberikan perlindungan pada pesan yang disisipkan. Kelemahan steganografi

dengan satu lapis kriptografi dapat dengan mudah dipecahkan.

4. METODE PENELITIAN

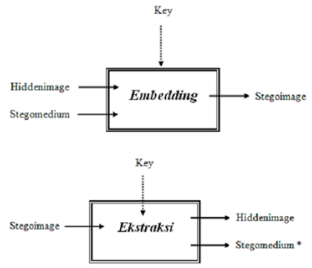
A. Steganografi

Steganografi merupakan seni komunikasi rahasia dengan menyembunyikan pesan pada objek yang tampaknya tidak berbahaya. Keberadaan pesan steganografi adalah rahasia. Istilah Yunani ini berasal dari kata *Steganos*, yang berarti tertutup dan *Graphia*, yang berarti menulis [3].

Steganografi adalah jenis komunikasi yang tersembunyi, yang secara harfiah berarti "tulisan tertutup." Pesannya terbuka, selalu terlihat, tetapi tidak terdeteksi bahwa adanya pesan rahasia. Deskripsi lain yang populer untuk steganografi adalah *Hidden in Plain Sight* yang artinya tersembunyi di depan mata. Sebaliknya, kriptografi adalah tempat pesan acak, tak dapat dibaca dan keberadaan pesan sering dikenal [7].

B. Proses Steganografi

Secara umum, terdapat dua proses didalam steganografi. Yaitu proses embedding untuk menyembunyikan pesan dan ekstraksi untuk mengekstraksi pesan yang disembunyikani. Proses-proses tersebut dapat dilihat pada gambar dibawah ini:



Gambar 1. Proses Steganografi

Gambar 1 atas menunjukkan proses penyembunyian pesan dimana di bagian pertama, dilakukan proses embedding hidden image yang hendak disembunyikan secara rahasia ke dalam stegomedium sebagai media penyimpanan, dengan memasukkan kunci tertentu (key), sehingga dihasilkan media dengan data tersembunyi di dalamnya (stegoimage). Pada Gambar 1 bawah, dilakukkan proses ekstraksi pada stegoimage dengan memasukkan key yang sama sehingga didapatkan kembali hiddenimage. Kemudian dalam kebanyakan teknik steganografi, ekstraksi pesan tidak akan mengembalikan stegomedium awal persis sama dengan stegomedium setelah dilakukan ekstraksi bahkan sebagian besar mengalami kehilangan. Karena saat penyimpanan pesan tidak dilakukan pencatatan kondisi awal dari stegomedium yang digunakan untuk menyimpan pesan [3].

C. Least Significant Bit

Strategi penyembunyian data citra yang digunakan untuk menyisipkan citra kedalam media citra adalah dengan metode Least Significant Bit (LSB). Dimana bit data citra akan digantikan dengan bit paling rendah dalam media citra. Pada file

citra 24 bit setiap piksel pada citra terdiri dari susunan tiga warna, yaitu merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (1 byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Informasi dari warna biru berada pada bit 1 sampai bit 8, dan informasi warna hijau berada pada bit 9 sampai dengan bit 16, sedangkan informasi warna merah berada pada bit 17 sampai dengan bit 24.

Untuk menjelaskan metode ini, digunakan citra digital sebagai stegomedium. Pada setiap byte terdapat bit yang tidak signifikan. Misalnya pada byte 00011001, maka bit LSB-nya adalah 1. Untuk melakukan penyisipan pesan, bit yang paling tepat untuk diganti dengan bit pesan adalah bit LSB, sebab pengubahan bit tersebut hanya akan mengubah nilai byte-nya menjadi satu lebih tinggi atau satu lebih rendah. Sebagai contoh, urutan bit berikut ini menggambarkan 3 piksel pada stegomedium 24-bit.

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

Pesan yang akan disisipkan adalah karakter A yang nilai biner-nya adalah 01000001 (ASCII), maka akan dihasilkan stegoimage dengan urutan bit sebagai berikut:

(00100110 11101001 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

Terlihat hanya tiga bit rendah yang berubah (bit dengan garis bawah), untuk mata manusia maka tidak akan tampak perubahannya. Secara rata-rata dengan metode ini hanya setengah dari data bit rendah yang berubah, sehingga bila dibutuhkan dapat digunakan bit rendah kedua bahkan ketiga [8].

D. Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik – teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data,serta otentikasi [9].

E. Vigenere Chiper

Vigenere Cipher atau biasa di sebut *vigenere* termasuk dalam *cipher* abjad majemuk (*Polyalphabetic Substitution Cipher*) yang dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigenere pada abad 16 (tahun 1586, meskipun Giovan Batista Belaso telah menggambarkannya pertama kali pada tahun 1553 seperti ditulis dalam bukunya *La Cifra Del sig.* Giovan Batistan Belaso.

Vigenere Cipher dipublikasikan pada tahun 1586, tetapi algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya *Cipher* tersebut kemudian dinamakan *Vigenere Cipher*.*Cipher* ini berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19. *Vigenere Cipher* Digunakan oleh Tentara Konfiderasi pada perang Sipil America (*American Civil War*).Perang sipil terjadi setelah *Vigenere Cipher* berhasil dipecahkan. *Vigenere Cipher* adalah algoritma menyandikan teks alfabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kata kunci

Teknik untuk menghasilkan *ciphertext* bisa dilakukan menggunakan substitusi

angka maupun bujur sangkar *vigènere*. Teknik susbtitusi *vigenere* dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser.

Alfabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Nilai Vigenere	0	1	2	3	4	5	6	7	8	9	10	11	12

Alfabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Nilai Vigenere	13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 2. Langkah Mencari Chipertext

Gambar 2.3 merupakan langkah untuk mencari ciphertext yaitu dengan substitusi angka, dimana huruf A memiliki nilai 0, B memiliki nilai 1 , dan seterusnya. Rumus dalam algoritma *vigenere* (Cahyadi, 2012) :

Enkripsi:

Ci = (Pi+Ki) mod 26…….(1)

Dekripsi:

Pi = (Ci – Ki) mod 26 ; *untukCi* >= *Ki* …….. (2)

Pi = (Ci + 26 – Ki) mod 26 ; *untukCi* <= *Ki* …….. (3)

Keterangan:

Ci = Nilai desimal karakter *ciphertext* ke-i
Pi = Nilai desimal karakter *plaintext* ke-i
Ki = Nilai desimal karakter kunci ke-i

Sebagai contoh jika *plaintext* adalah "AKU" :

Plaintext : AKU
Kunci : YOU
Ciphertext : YYO

Kemudian akan dilakukan tahap dekripsi dengan menggunakan rumus (2) atau (3).

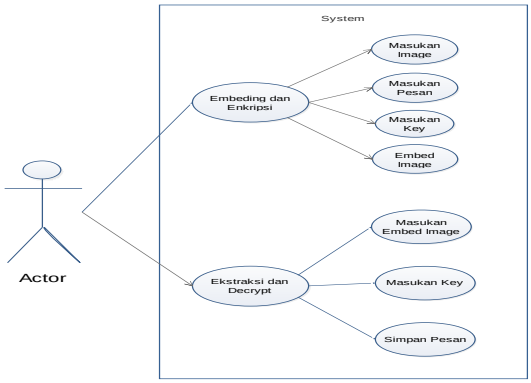
Proses dekripsi merupakan pengembalian *plaintext* ke C*iphertext*

5. PEMBAHASAN

A. Pemodelan dengan use case diagram

Pemodelan adalah penggambaran dari suatu sistem yang akan dibuat (Whiten, et al. 2007). Dalam pemodelan akan menunjukkan spesifikasi dari sistem yang akan di buat.

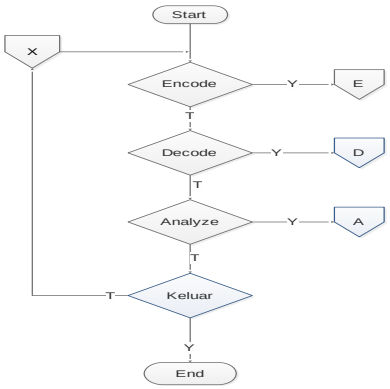
Use case menunjukkan gambaran umum dari suatu sistem yang akan dibuat. *Use case* digunakan untuk menyusun sesuatu dalam bentuk model



Gambar 3. Use case diagram

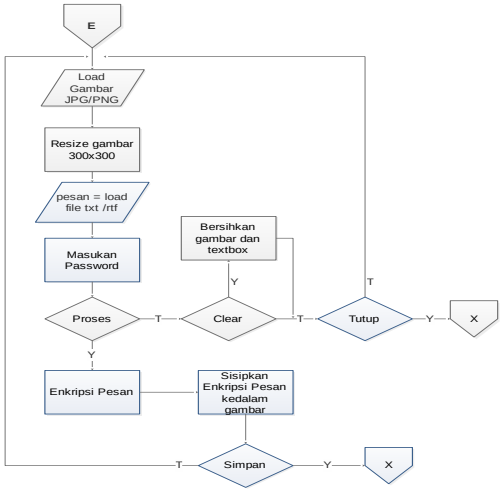
B. *Flowcart* menu utama

Flowchart menu utama dapat dilihat seperti gambar berikut :



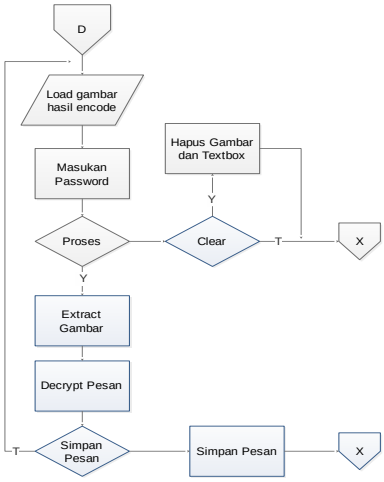
Gambar 3. Flowcart menu utama

C. Flowcart encode



Gambar 4. Flowcart encode

D. Flowcart decode



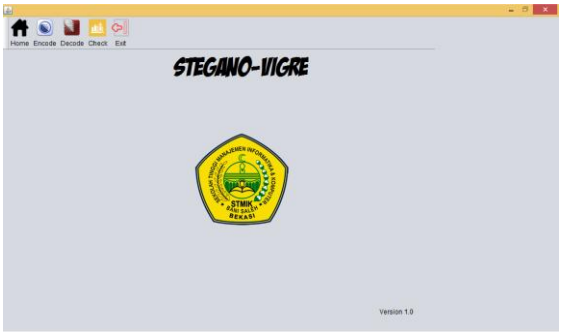
Gambar 4. Flowcart decode

E. Implementasi

Implementasi sistem kombinasi kriptografi dan steganografi diprogram dengan bahasa pemrograman Java, dan diberi nama aplikasi "StegoVigre". Implementasi ini dilakukan pada laptop dengan sistem operasi Windows 8.1 Profesional, Processor Intel ® Dual Core CPU 1.6 GHz, harddisk 320 GB, dan RAM 2 GB.

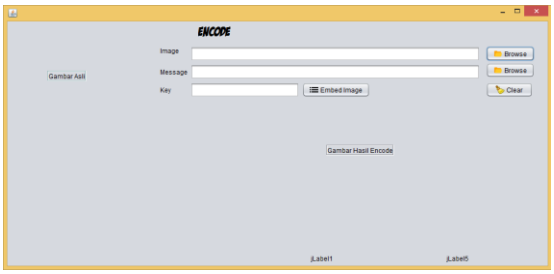
Aplikasi ini terbagi dalam dua bagian, yaitu Enkripsi dan Dekripsi. Enkripsi digunakan oleh pengguna yang ingin mengirimkan pesan secara rahasia yang disembunyikan dalam sebuah gambar bitmap (stego), sedangkan dekripsi digunakan oleh pengguna yang menerima gambar stego berisi pesan rahasia.

1. Tampilan form utama



Gambar 5. Tampilan form utama

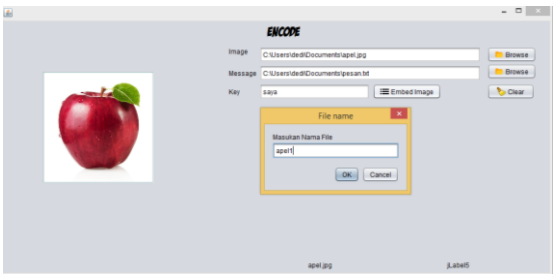
2. Tampilan menu *Encode*



Gambar 6. Form *encode*

menunjukan proses embedding data kedalam citra image. Mula-mula user akan memilih image sebagai cover medium (Gambar 5). Setelah itu user akan memilih pesan yang akan disisipkan kedalam cover medium.

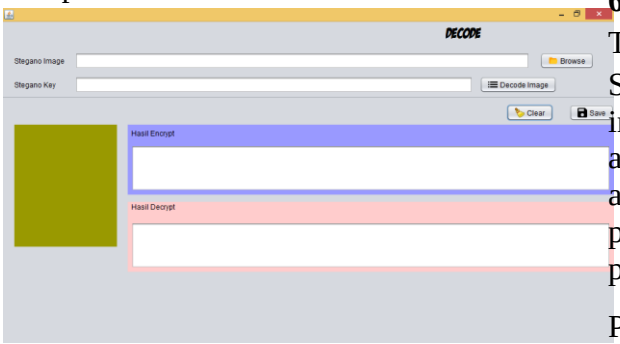
3. Proses Embeding



Gambar 7. Proses *embeding*

Gambar 7 menunjukan proses embedding antara cover image dan pesan rahasia. Setelah itu user akan diminta memasukan nama file hasil dari proses embedding ini, Jika proses embedding berhasil, makan akan muncul pesan bahwa proses embedding sudah berhasil

4. Tampilan menu Decode

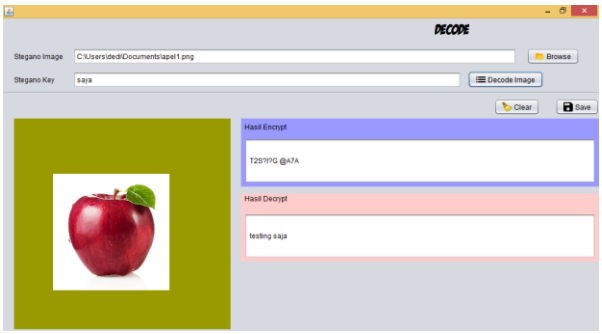


Gambar 8. Form decode

Gambar 8 menunjukan Form untuk proses Decode. Pertama-tama user akan mencari stego image dengan mengklik tombol browse, sehingga tampak gambar 8 untuk mencari dimana lokasi stego image yang akan di ekstraksi.

Selanjutnya user akan melakukan proses ekstraksi dengan mengklik tombol decode image. Jika proses ekstraksinya berhasil, maka akan muncul keterangan bahwa proses ekstraksi sudah berhasil

Isi pesan sudah di enkripsi dan di embed kedalam media citra, akan muncul pada textbox, begitu juga pesan aslinya setelah melalui proses enkripsi pesan seperti pada gambar 9



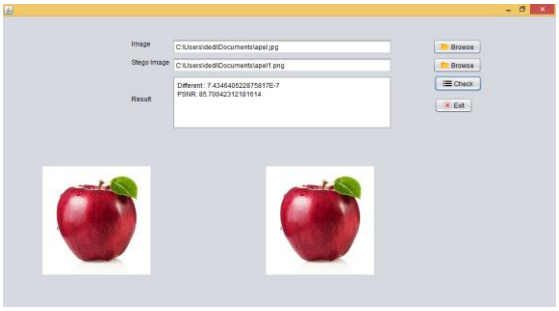
Gambar 9. Stego Image, pesan enkripsi dan pesan asli

6. HASIL PENGUJIAN

Tampilan Menu Analize

Setelah proses embedding dan extracting image dilakukan, langkah berikutnya adalah membandingkan hasil antara citra asli dengan stego image. Apakah ada perbedaan yang cukup significant dari proses embedding ini.

Pada form ini ditampilkan selisih antar pixel atara citra asli dengan stego image dan mencari nilai psnr (*Peak Signal to Noise Ratio)* seperti pada gambar 10



Gambar 10. perbandingan stego image dengan citra asli

7. KESIMPULAN DAN SARAN

1. Kesimpulan
   Dengan melakukan kombinasi antara algoritma kriptografi dan algoritma steganografi pesan lebih terjamin kerahasiaanya dengan ketentuan *cover image* harus memenuhi syarat untuk dimodifikasi. Perangkat lunak yang dibangun berjalan dengan baik sesuai dengan fungsi-fungsi yang dibutuhkan dalam melakukan proses enkripsi dan penyisipan pesan sekaligus proses ekstraksi dan dekripsi pesan.

2. Saran
   Untuk penelitian selanjutnya kombinasi algoritma *Least Significant Bit* (LSB) dan algoritma kriptografi vigenere dan dapat dilakukan dengan menambah file yang lain misalnya pdf atau .doc dan wadah penampung juga bisa menggunakan media lain seperti audio ataupun video. Perlunya mengkombinasikan algoritma-algoritma lain dalam kriptografi dan steganografi untuk memeberikan keamanan ganda pada pesan. Misalnya algoritma DSA (*Digital Signature Algorithm*) pada Kriptografi dan *Algorithms andTransformation* pada stegaografi. Ataupun juga dapat mengkombinasikan tiga algoritma agar pesan lebih bisa terjamin kerahasiaannya.

8. DAFTAR PUSTAKA

[1] Aditya, Y., Pratama, A. & Nurlifa, A. 2010. Studi Pustaka Untuk Steganografi Dengan Beberapa Metode. *Prosiding Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010)*, pp. G-32-G-35

[2] Ariyus, D. 2009. Keamanan Multimedia. Yogyakarta: Andi Offset. Basuki, A., Jozua F., Palandi dan Fatchurrochman. 2005. Pengolahan Citra Digital Menggunakan Visual Basic. Jakarta: Penerbit Graha Ilmu.

[3] Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J. dan Kalker, T. 2008. Digital Watermarking and Steganography.2nd Edition. Burlington: Morgan Kaufmann

[4] Cahyadi, T. 2012. Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra JPEG.*Jurnal Transient* 1(4): 281-288.

[5] Kekre, H. B., Athawale, A. dan Halarnkar, P. N. 2008. Increased Capacity of Information Hiding in LSB's Method for Text and Image. *International Journal of Electrical, Computer, and Systems Engineering* **2**(4): 246 – 251.

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

[7] Kipper, G. 2004.*Investigator's Guide to Steganography.*Washington: Auerbach.

[8] Lestriandoko, N. H. 2006. *Pengacakan Pola Steganografi untuk Meningkatkan Keamanan Penyembunyian Data Digital*. http://journal.uii.ac.id/index.php/ Snati/article/view/1538/1313. Diakses tanggal 30 Mei 2010.

[9] Munir, R. 2006. Kriptografi.Penerbit Informatika Bandung. Bandung.