Available *online* at : http://bit.ly/InfoTekJar

InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan

ISSN (Print) 2540-7597 | ISSN (Online) 2540-7600

Data Mainig

Studi Penyisipan Pesan Teks Terenkripsi Dalam Citra Digital Dengan Menggunakan Algoritma Vigenere Cipher dan Steganografi Least Significant Bit

Aulia Ihsan

Universitas Deli Sumatera

KEYWORDS

Pesan; Vigenere Cipher; LSB;

CORRESPONDENCE

Phone: 0857-6208-7269

E-mail: auliaichsan15@gmail.com

A B S T R A C T

Pesan merupakan salah satu media komunikasi antar satu individu ke individu lain. Pesan memiliki keragaman, mulai dari pesan yang bersifat umum dan pesan yang bersifat rahasia. Kerahasiaan yang terdapat dalam suatu pesan merupakan salah satu hal yang harus dijaga keamanannya sehingga pihak lain yang tidak memiliki otoritas untuk mengetahui kerahasiaan tersebut tidak dapat membukanya. Maka dari itu, muncul suatu teknik untuk mengenkripsi suatu pesan dengan algoritma kriptografi vigenere cipher. Suatu algoritma yang sulit untuk ditebak plaintextnya bahkan dikriptanalisis ciphertextnya. Tak hanya itu, pesan (plaintext) yang telah dienkripsi dengan vigenere cipher, ciphertextnya akan disisip ke dalam citra digital dengan metode steganografi LSB sehingga pesan rahasia (plaintext) akan tetap secure.

PENDAHULUAN

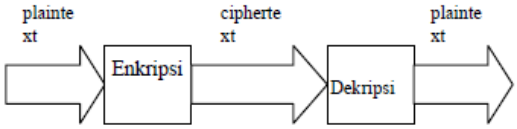
Mengirim pesan dengan aman merupakan satu hal yang harus dikedepankan untuk dilakukan demi menjaga kerahasiaan yang terdapat di dalam pesan. Salah satu cara untuk menjaga keamanan dan kerahasiaan pesan tersebut adalah dengan cara mengenkripsi pesan tersebut dengan metode atau teknik yang telah ada sejak zaman dahulu dan masih diterapkan sampai dengan sekarang. Metode atau teknik tersebut disebut kriptografi. Kriptografi merupakan teknik untuk mengubah pesan asli (plaintext) menjadi pesan tersandi (ciphertext) sehingga menjadi bentuk pesan yang tidak bisa dimengerti. Di dalam paper ini, penulis menggunakan algoritma kriptografi vigenere cipher untuk mengenkripsi pesan teks (plaintext) menjadi pesan tersandi (ciphertext) dengan menggunakan kunci (key) tertentu. Kemudian untuk lebih menjaga keamanan pesan teks tersebut, ciphertext tersebut disisipkan ke dalam citra digital dengan menggunakan steganografi LSB. Steganografi LSB merupakan metode steganografi dimana penyisipan pesan disisip pada setiap bit terakhir pada citra digital.

Kriptografi

Kriptografi pada awalnya merupakan ilmu dan seniuntuk menjaga kerahasiaan pesan dengan caramenyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kemudian seiring dengan berkembangnya kriptografi yaitu kriptografi tidak lagi sebatas mengenkripsikan pesan, tetapi jugamemberikan aspek keamanan yang lain sepertiserangan dari kriptanalisis. Karena itu pengertiankriptografi pun berubah menjadi ilmu sekaligus seniuntuk menjaga keamanan pesan.Kriptografi selain menyandikan pesan jugamenyediakan beberapa aspek keamanan. Berikutaspek keamanan kriptografi :

- Kerahasiaan (confidentiality), layanan yangdigunakan untuk menjaga isi pesan dari siapapunyang tidak berhak untuk membacanya.
- Integritas data (*data integrity*), layanan yangmenjamin bahwa pesan masih asli/utuh ataubelum pernah dimanipulasi selama pengiriman.
- Otentikasi (*authentication*), layanan yang untukmengidentifikasi kebenaran pihak-pihak yangberkomunikasi (*user authentication*) dan untukmengidentifikasi kebenaran sumber pesan (*dataorigin authentication*).
- Nirpenyangkalan (*non-repudiation*), layananuntuk mencegah entitas yang berkomunikasimelakukan penyangkalan, yaitu pengirim pesanmenyangkal melakukan pengiriman ataupenerima pesan menyangkal telah menerimapesan.

Proses menyandikan plainteks menjadi cipherteks disebut dengan Enkripsi. Sementara prosesmengembalikan cipherteks menjadi plainteks semula disebut dedngan Dekripsi. Kunci adalah parameter yang digunakan untuk transformasi dekripsi danenkripsi. Berikut adalah gambaran tentang hubunganEnkripsi dan Dekripsi :



Gambar1. Gambaran Enkripsi dan Dekripsi

Fungsi enkripsi *E* memetakan *P* ke *C*, *E*(*P*) = *C*
Fungsi dekripsi *D* memetakan *C* ke *P*, *D*(*C*) = *P*

Dengan demikian, fgngsi enkripsi dan dekripsi harusmemenuhi sifat: *D*(*E*(*P*)) = *P* [1]

Vigenere Cipher

Sandi Vigenere adalah metode menyandi teks alphabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Sandi Vigenere merupakan bentuk sederhana dari sandi polialfabetik. Kelebihan sandi ini dibanding sandi Caesar dan sandi mono alfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi. Giovan Batista Belaso menjelaskan metode ini dalam buku La cifra del. Sig. Giovan Batista Nelaso (1553) dan disempurnakan oleh diplomat Perancis Blaise de Vigenere pada tahun 1586. Pada abad ke19 banyak orang yang mengira vigenere adalah penemu sandi ini, sehingga sandi ini dikenal sebagai “sandi Vigenere”. Sandi ini dikenal dengan luas karena cara kerjanya mudah dimengerti dan dijalankan dan bagi para pemula sulit dipecahkan[2]

Pengembangan dari algoritma Vigenere cipher untuk penyandian image dilakukan dengan menggunakan formula Vigenere cipher dengan menggunakan nilai basis modulo 256 sesuai dengan intensitas warna padaimage. Kunci-kunci tersebut disebut dengan Vigenere table. Atau dapat juga dihitung dengan formula berikut :

Ci = pi + k (i mod m) (mod 26)
Pi = ci + k (i mod m) (+ 26)
Keterangan :

m = panjang karakter kunci
i = posisi huruf dalam angka
k = nilai kunci

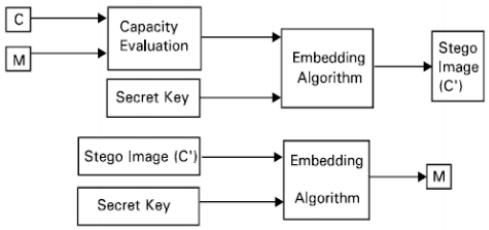
A	B	C	D	E	F	G
0	1	2	3	4	5	6
H	I	J	K	L	M	N
7	8	9	10	11	12	13
O	P	Q	R	S	T	U
14	15	16	17	18	19	20
V	W	X	Y	Z		
21	22	23	24	25		

Tabel 1. Posisi Huruf dalam Angka

Steganografi

Steganografi adalah suatu seni untukmenyembunyikan suatu data, di mana data tersebut disembunyikan ke dalam suatumedia berupa teks, audio danimageyangtampak biasa saja sehingga tidak akan menimbulkan banyak perhatian dari pihak yang tidak dikehendaki[3].
Beberapa istilah dalam steganografi yaitu :

- Embedded messege (hiddentext) yaitu pesan yang disembunyikan didalam covertext.
- Cover object (covertext) yaitu pesan yang digunakan untuk menyembunyikan embedded messege
- Stegotext adalah pesan yang sudah berisi pesan embedded messege
- Stegokey merupakan kunci yang digunakan untuk menyisipkan pesan dan ekstrasi pesan dari stegotext[3].



Gambar 2.2 Bagan Proses Penyembunyian dan Pengembalian Data [4]

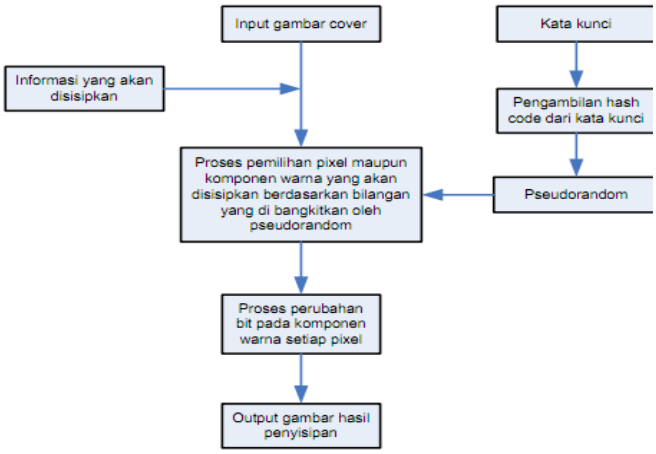
Proses penyembunyian data pada metode steganography adalah salah satu bagian yang memegang peranan penting di dalam proses secara keseluruhan dimana pada bagian ini, penyembunyian data yang merupakan inti dari metode steganography dilakukan. Pada proses penyembunyian data ini diperlukan ketepatan dalam perhitungan bit–bit warna serta bit–bit data karena jika terjadi sedikit kesalahan saja pada perhitungan maka akan berakibat pada rusaknya data yang dikirimkan sehingga data tidak akan dapat dikembalikan ke dalam bentuksemula. Selain itu ukuran keberhasilan pada metode steganography juga dipengaruhi oleh proses penyembunyian data dimana hasil dari proses penyembunyian data yang berupa stego image haruslah menyerupai gambar asli (cover image) sehingga tidak terjadi kecurigaan dari pihak lain yang melihatnya. Selain itu faktor efisiensi data juga perlu dipertimbangkan dalam penyembunyian data sehubungan dengan perbandingan besarnya data yang disembunyikan dengan kualitas stego image yang dihasilkan (semakin besar

data yang disembunyikan maka kualitas stego image yang dihasilkan semakin rendah). Besar data yang dapat dihasilkan oleh metode steganography secara umum mencapai sekitar 5 hingga 10 persen dari ukuran file citra digital[4]

Least Significant Bit

Teknik Steganografi dengan menggunakan metode modifikasi Least Significant Bit(LSB) adalah teknik yang paling sederhana, pendekatan yang sederhana untuk menyisipkan informasi di dalam suatu citra digital (medium cover). Mengkonversisuatu gambar dari format GIF atau BMP, yang merekonstruksi pesan yang sama dengan aslinya (lossless compression) ke JPEG yang lossy compression, dan ketika dilakukan kembali akan menghancurkan informasi yang tersembunyi dalam LSB[2].

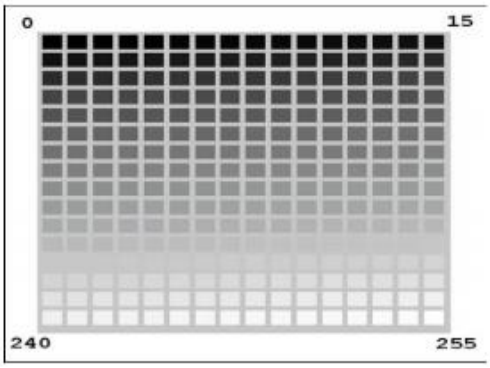
Teknik LSB mengubah bit-bit pada gambar cover secara linier sesuai dengan urutan warna komponen dan urutan pixel, dengan begitu attacker/cracker dapat dengan mudah mengeluarkan kembali pesan rahasia yang telah disisipkan pada gambar. Untuk mencegah hal-hal tersebut maka digunakan kata kunci dan penempatan bit-bit yang random pada gambar[5]



Gambar 3.1 Diagram Blok Proses Encoding Random LSB [5]

Proses Penyisipan Pesan dengan Algoritma LSB

Menyisipkan suatu pesan (*embedded messege)* pada sebuah citra digital ditentukan dengan pola nilai RGB citra tersebut.



Gambar 3.2 Skema Pola Nilai RBG Citra Digital [4]

Misalkan sebuah karakter “D” akan disisipkan ke sebuah citra digital dengan nilai RGB :

$$\begin{bmatrix} 255 & 153 & 0 \\ 255 & 0 & 13 \\ 17 & 0 & 210 \end{bmatrix}$$

Matriks nilai RGB

$$\begin{bmatrix} 11111111 & 10011010 & 00000000 \\ 11111111 & 00000000 & 00001101 \\ 00010001 & 00000000 & 11010010 \end{bmatrix}$$

Matriks RGB setelah dikonversi ke biner

Prosesnya yaitu :

- Ubah karakter D menjadi bilangan decimal kemudian konversi ke bilangan biner (berdasarkan pada table ASCII) D = 68 (dec) = 01000100 (biner)
- Sisipkan tiap bit biner ke dalam matriks citra pada bit terakhir

$$\begin{bmatrix} 1111111\mathbf{0} & 1001101\mathbf{1} & 0000000\mathbf{0} \\ 1111111\mathbf{0} & 0000000\mathbf{0} & 0000110\mathbf{1} \\ 0001000\mathbf{0} & 0000000\mathbf{0} & 11010010 \end{bmatrix}$$

Terdapat perubahan pada bit terakhir tiap matriks RGB (biner) yang telah disisip karakter D. Hasil konversi ke nilai RGB kembali sebagai berikut :

$$\begin{bmatrix} 254 & 154 & 0 \\ 254 & 0 & 13 \\ 16 & 0 & 210 \end{bmatrix}$$

Hasil konversi nilai RGB dari biner

Karakter D merupakan embedded messege dan citra yang digunakan untuk menyisipkan karakter D tersebut merupakan covertext

PENGUJIAN DAN ANALISIS

Pada tahap pengujian dan analisis ini, penulis akan mengenkripsi sebuah pesan rahasia yang kemudian hasil *ciphertext*nya akan disisipkan ke media citra.

Plaintext = K I L L J O H N
Key = L O N D O N

Ciphertext :

- Atur kesejajaran antara plaintext dan kunci

K	I	L	L	J	O	H	N
L	O	N	D	O	N	L	O

- Ubah tiap karakter plaintext dan kunci menjadi nilai posisi alphabet , kemudian jumlahkan tiap nilai posisi plaintext ke nilai kunci

10	18	11	11	9	14	7	13
11	14	13	3	14	13	11	14
21	**22**	**24**	**14**	**23**	**27**	**18**	**27**

- Setelah mendapatkan hasil penjumlahan, tiap nilai posisi dimodulokan dengan 26

Nilai	**Mod 26**	**Hasil**	**Konversi Ke Karakter (Ciphertext)**
21		21	V

22	22	W
24	24	Y
14	14	O
23	23	X
27	1	A
18	18	S
27	1	A

Kemudian ubah kembali tiap karakter ciphertext menjadi bilangan decimal kemudian dikonversikan ke bilangan biner (berdasarkan pada table ASCII)

Karakter	Decimal	Biner
V	86	01010110
W	87	01010111
Y	89	01011001
O	79	01001111
X	88	01011000
A	65	01000001
S	83	01010011
A	65	01000001

Hasil konversi tiap karakter pesan rahasia yang telah terenkripsi ke dalam bentuk bilangan biner.

Tahap selanjutnya, input sebuah citra digital dengan ekstensi JPEG atau JPG lalu ubah file citra tersebut ke dalam bentuk matriks.

Gambar 2. Citra JPEG

Ubah citra JPEG tersebut kedalam bentuk matriks biner.

x Matriks 8 (Nilai RGB)

Matriks 8 (RGB)

255	154	0	13	15	123	0	5
255	17	1	6	210	14	15	20
0	6	7	254	127	30	24	0
5	0	112	14	1	110	210	200
3	120	1	8	168	0	0	22
0	15	14	25	0	0	25	20
0	10	0	0	14	20	200	25
0	15	25	0	0	0	0	0

Hasil konversi ke bilangan biner

11111	01101	00000	00001	00001	01010	00000	00000
111	100	000	101	111	011	000	101
11111	00010	00000	00000	11010	00001	00001	00010
111	001	001	100	010	110	111	100
00000	00000	00000	11111	01111	00011	00011	00000
000	110	111	110	111	110	000	000
00000	00000	01110	00001	00000	01101	11010	11001
101	000	000	110	001	110	010	000
00000	01111	00000	00001	10101	00000	00000	00011
011	000	001	000	000	000	000	000
00000	00001	00001	00011	00000	00000	00011	00010
000	111	110	001	000	000	001	100
00000	00001	00000	00000	00001	00010	11001	00011
000	010	000	000	110	100	000	001
00000	00001	00011	00000	00000	00000	00000	00000
000	111	001	00	000	000	000	000

Kemudian sisipkan setiap bit karakter ciphertext ke dalam setiap bit akhir matriks citra dengan kunci **logika OR** dimana :

Input		Output (F)
A	B	
0	0	0
0	1	1
1	0	1
1	1	1

Hasil penyisipan pesan terenkripsi (*embedded messege*) ke citra digital (*covertext*) dengan metode *least significant bit (lsb)* yaitu :

11111	01101	00000	00001	00001	01010	00000	00000
111	101	000	101	111	011	001	101
11111	00010	00000	00000	11010	00001	00001	00010
111	001	001	101	010	111	111	101
00000	00000	00000	11111	01111	00011	00011	00000
000	111	111	111	111	110	000	001
00000	00000	01110	00001	00000	01101	11010	11001
101	001	000	110	001	111	011	001
00000	01111	00000	00001	10101	00000	00000	00011
011	001	001	001	001	000	000	000
00000	00001	00001	00011	00000	00000	00011	00010
000	111	110	001	000	000	001	100
00000	00001	00000	00000	00001	00010	11001	00011
000	011	000	001	110	100	001	001
00000	00001	00011	00000	00000	00000	00000	00000
000	111	001	000	000	000	000	001

Setelah mendapatkan stegotext diatas, kembalikan format citra yang berupa bilangan biner kembali ke bilangan nilai RGB.

x Matriks 8 (Nilai RGB)

Matriks 8 (RGB)

255	155	0	13	15	123	1	5
255	17	1	7	210	15	15	21
0	7	7	255	127	30	24	1
5	1	112	14	1	111	211	201
3	120	1	9	169	0	0	22
0	15	14	25	0	0	25	20
0	11	0	1	14	20	201	25
0	15	25	0	0	0	0	1

Pesan yang tenkripsi dengan algoritma *vigenere cipher* telah disisipkan ke dalam sebuah citra digital dengan algoritma *least significant bit* dan menghasilkan stegotext dalam bentuk citra digital (*stegotext*).

KESIMPULAN

Penggunaan *vigenere cipher* untuk mengenkripsi suatu pesan sangat efektif lebih aman dan sulit untuk dikriptanalisis karena *vigenere cipher* merupakan salah satu algoritma kriptografi klasik yang pemecahan kuncinya masih tergolong sukar. Ditambah lagi hasil enkripsi data dengan *vigenere cipher* di*embedded* ke dalam suatu citra digital dengan algoritma steganografi least significant bit (l*sb*). Yang hasilnya sisipannya akan menjadi sangat secure. Karena jika seorang kriptanalis mengkriptanalisis file citra tersebut seperti dicompressatau dilakukan pengeditan pada file citra (*stegotext*) tersebut, maka

posisi matriks didalamnya akan berubah dan pesan yang disisipkan akan hancur dan akan tidak terbaca bahkan sulit untuk dimengerti saat hasil ekstrasi pesan (*embedded messege*) telah didapatkan.

Disini membuktikan bahwa penggunaan *vigenere cipher* dikombinasikan dengan *lsb*akan sangat aman dan pesan akan sulit untuk diketahui.

REFERENSI

[1] Munir, Rinaldi. *Belajar Ilmu Kriptografi*. Penerbit Andi. Yogyakarta. 2008.

[2] Cahyadi, T. *Implementasi Steganografi LSB Dengan Enkripsi Vigenere Chiper Pada Citra JPEG*. Jurnal Transient 1(4) : 282-288. 2012

[3] Ibrahim A. and Zabian A. *Algorithm for Text Hiding in Digital Image for information Security. International Journal of Computer Science and Network Security*.9(6):262–268.2009

[4] Noertjahyana, Agustinus and Gunadi, Kartika. *Aplikasi Metode Steganography Pada Citra Digital Dengan Menggunakan Metode Lsb (Least Significant Bit).* Jurnal SIFO Mikroskil, 13 (2). pp. 113-122. ISSN 1412-0100. 2012

[5] Gozali, Ferrianto and Edang Juana, Thamrin Hartono. *Image Steganography Using Randomized Least Significant Bit For Multimedia Messaging Application*. Electrical Eengineering Department, Faculty of Industrial Technology, Trisakti University Jakarta. 2014