KOMBINASI KRIPTOGRAFI DENGAN HILLCIPHER DAN STEGANOGRAFI DENGAN LSB UNTUK KEAMANAN DATA TEKS

Esti Suryani [1)], Titin Sri Martini [2)]
Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Magelang
Telepon (08121554145), (085643705060),
E-mail : suryapalapa@yahoo.com [1)], titinsmartini@yahoo.com[2)]

Abstrak

Jaringan komunikasi seperti internet adalah jaringan yang tidak aman untuk transmisi data, seperti teks video maupun citra digital. Salah satu cara pengamanan data dapat dilakukan dengan mengkombinasikan kriptografi dan steganografi. Tujuannya adalah untuk merahasiakan pesan yang dikirim, yang dapat dilakukan dengan proses kriptografi, serta sekaligus menghindarkan pesan tersebut dari kecurigaan, yang dapat dilakukan dengan proses steganografi.
Pesan yang digunakan dalam makalah ini berupa text. Pada proses kriptografi, pesan yang berupa text tersebut akan dienkrip dengan metode Hill Cipher, dan selanjutnya pesan yang telah terenkrip tersebut akan dilakukan proses steganografi pada citra digital grayscale 8 bit dengan skala 0-255, dengan metode Least Significant Bit (LSB)

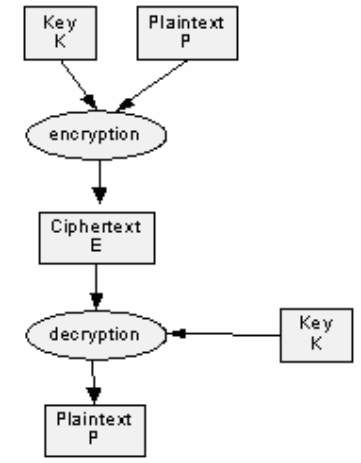
Kata Kunci : Kriptografi, Steganografi, Hill Cipher, Grayscale, Least Significant Bit

PENDAHULUAN

Masalah keamanan menjadi hal penting dalam transmisi data pada jaringan komputer. Untuk mengamankan data digunakan kriptografi, steganografi, atau kombinasi keduanya. Dalam makalah ini akan digunakan kombinasi keduanya.

Kriptografi

Kriptografi: adalah seni dan ilmu untuk menulis rahasia *"The Art of Secreet Writing"*. Tujuannya agar pesan tidak dapat dibaca. Proses yang dilakukan untuk mengamankan sebuah pesan (*plaintext)* menjadi pesan yang tersembunyi *(ciphertext)* disebut dengan **enkripsi** *(encryption)*. *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Proses sebaliknya untuk mengubah *ciphertext* menjadi *plaintext*, disebut **dekripsi** *(decryption)*. Proses kriptografi dapat digambarkan dalam skema gambar 1 berikut



Gambar 1 Proses Kriptografi

Metode kriptografi berdasarkan kunci yang dipakai, dapat dibedakan menjadi dua, yaitu kunci simetris dan kunci asimetris. Dalam makalah ini digunakan metode simetris yaitu Hill Cipher.

Algoritma Enkripsi Hill Cipher

Secara umum tahap-tahap enkripsi Hill Cipher adalah:

1. Korespondenkan abjad dengan numerik

   A⟶0, B⟶1, …, Z ⟶25

2. Buat matriks Kunci berukuran *m* x *m*

$$K_{mxm}=\begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix} \quad (1)$$

3. Matriks K harus berupa matriks yang *invertible*, yaitu memiliki *multiplicative inverse* K^{-1} sehingga $K.K^{-1} = I$
4. Matriks K mempunyai inverse jika determinan matriks $K \neq 0$
5. Jika plaintext $P = p_1 \; p_2 \dots p_n$, plaintext diblok dengan ukuran blok sama dengan ukuran baris atau kolom matriks kunci K, yaitu *m* :

$$P_{qxm}=\begin{bmatrix} p_{11} & p_{12} & \dots & p_{1m} \\ p_{21} & p_{22} & \dots & p_{2m} \\ \dots & \dots & \dots & \dots \\ p_{q1} & p_{q2} & \dots & p_{qm} \end{bmatrix} \quad (2)$$

   Plaintext P setelah di blok menjadi berukuran *q* x *m*.
6. Jika pada plaintext, *n* bukan kelipatan *m* maka tambahkan sembarang abjad dalam plaintext sehingga *n* menjadi kelipatan *m*
7. Buat transpose blok matriks P :

$$P^1{}_{mxq} = \begin{bmatrix} p_{11} & p_{21} & \dots & p_{q1} \\ p_{12} & p_{22} & \dots & p_{q2} \\ \dots & \dots & \dots & \dots \\ p_{1m} & p_{2m} & \dots & p_{qm} \end{bmatrix} \quad (3)$$

   Ukuran matriks P^1 adalam *m x q*
8. Kalikan matriks kunci K dengan plaintext transpose dalam modulo 26 berikut:

$$C^1 = K_{mxm} P_{mxn}{}^1$$

$$C^1 = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix} \begin{bmatrix} p_{11} & p_{21} & \dots & p_{q1} \\ p_{12} & p_{22} & \dots & p_{q2} \\ \dots & \dots & \dots & \dots \\ p_{1m} & p_{2m} & \dots & p_{qm} \end{bmatrix}$$

$$C^1 = \begin{bmatrix} c_{11} & c_{21} & \dots & c_{m1} \\ c_{12} & c_{22} & \dots & c_{m2} \\ \dots & \dots & \dots & \dots \\ c_{1q} & c_{2q} & \dots & c_{mq} \end{bmatrix} \quad (4)$$

9. Dihasilkan

$$C = (C^1)^1 = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1q} \\ c_{21} & c_{22} & \dots & c_{2q} \\ \dots & \dots & \dots & \dots \\ c_{m1} & c_{m2} & \dots & c_{mq} \end{bmatrix} \quad (5)$$

10. Ubah hasil step 9 ke dalam abjad menggunakan koresponden abjad dengan numerik pada step 1 sehingga diperoleh *ciphertext*.

Algoritma Dekripsi Hill Cipher

Secara umum tahap-tahap dekripsi Hill Cipher adalah:

1. Korespondenkan abjad dengan numerik

   A⟶0, B⟶1, …, Z ⟶25

2. Ubah ciphertext ke dalam numerik.
3. Kunci yang digunakan untuk mendekrip ciphertext ke plaintext adalah invers dari matriks kunci K_{mxm}
4. Menghitung K^{-1} dengan cara :

   Mencari adjoint matriks K

   Determinan K dalam mod 26

$$K^{-1} = \frac{1}{\det K} adj\,(K),$$

$$\frac{1}{\det K} \text{ dalam mod } 26$$

   Catatan : $\frac{1}{\det K} \bmod 26 = x$

$$(\det K * x) \bmod 26 = 1$$

5. Kalikan inverse matriks kunci dengan ciphertext transpose, diperoleh plaintext transpose

$$P^1 = K^{-1} C^1$$

6. Dari step 5 diperoleh plaintext :

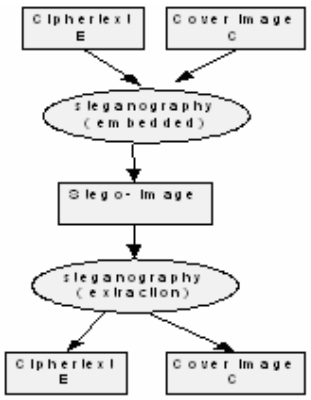
$$P = (P^1)^1$$

7. Korespondensikan abjad dengan numerik hasil step 6 sehingga diproleh plaintext.

Steganografi

Steganografi adalah seni menyembunyikan pesan atau informasi dalam suatu obyek, seperti teks atau image. Tujuannya untuk menghindari kecurigaan.

Proses steganografi dapat digambarkan dalam skema gambar 2 berikut :



Gambar 2 Proses steganografi

Teknik yang digunakan :

- Spasial Domain
  Memodifikasi langsung nilai *byte* dari *cover-object* (nilai *byte* dapat merepresentasikan intensitas/warna *pixel* atau amplitudo). Metode spasial domain ada 2, yaitu LSB (Least Significant Bit) dan MSB (Most Significant Bit)
- Transform Domain
  Memodifikasi hasil transformasi sinyal dalam ranah frekuensi. Sinyal dalam ranah spasial/waktu diubah ke ranah frekuensi dengan menggunakan transformasi seperti:
  - DCT (Discrete Cosine Transform)
  - DFT (Discrete Fourier Transform)
  - DWT (Discrete Wavelet Transform)

Penyisipan pesan dilakukan pada koefisien transformasi. Dalam makalah ini teknik steganografi menggunakan LSB.

LSB (Least Significant Bit) Embedding Process

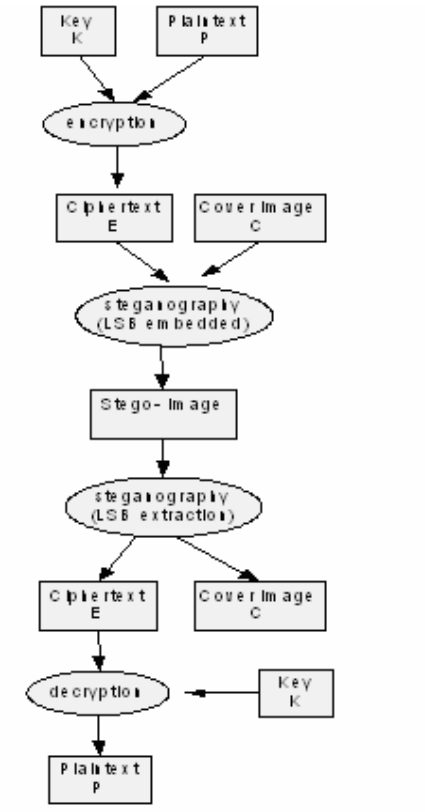
Least Significant Bit adalah salah satu metode untuk menyembunyikan pesan dalam media digital dengan cara menyisipkan pesan tersebut pada satu bit paling kanan ke pixel file obyek.
Berikut ini penyisipan data pada file citra bitmap greyscale 8 bit per pixel dengan skala 0 sampai 255, atau dengan format biner 00000000 sampai 11111111.
Misalnya pixel-pixel citra yang akan digunakan sebagai wadah (cover image) adalah :
(01001101 00101110 10101110 10001010
10101111 10100010 00101011 10101011)
untuk menyisipkan karakter ‘A’ (01000001), maka pixel-pixel cover image tersebut akan berubah menjadi :
(0100110**0** 0010111**1** 1010111**0** 1000101**0**
1010111**0** 1010001**0** 0010101**0** 1010101**1**)
Perubahan yang tidak significant ini tidak akan terdeteksi oleh mata manusia.

LSB (Least Significant Bit) Extracing Process

Proses ekstraksi dilakukan dengan 2 tahap. Pertama untuk memperoleh ciphertext diambil bit-bit paling belakang dari stego image. Kedua, untuk memperoleh cover image, tambahkan satu bit paling belakang pada pixel-pixel sisa tahap pertama dengan bit yang sama dengan bit paling belakang cover image.
Dari proses penyisipan karakter ‘A’ diperoleh stego imege
(0100110**0** 0010111**1** 1010111**0** 1000101**0**
1010111**0** 1010001**0** 0010101**0** 1010101**1**)
Dengan mengambil bit-bit paling belakang dari stego image tersebut maka diperoleh karakter ‘A’ **(01000001)** dan pixel-pixel sisa tahap pertama cover image
(0100110**?** 0010111**?** 1010111**?** 1000101**?**
1010111**?** 1010001**?** 0010101**?** 1010101**?**)
Menggunakan tahap kedua diperoleh cover image berikut :
(01001101 00101110 10101110 10001010
10101111 10100010 00101011 10101011)

Kombinasi Kriptografi dan Steganografi

Kombinasi Kriptografi dengan metode Hill cipher dan Steganografi dengan metode LSB dapat digambarkan dalam skema gambar 3 berikut :



Gambar 3 Proses kriptografi-stegangrafi

IMPLEMENTASI

Skema proses kriptografi dan steganografi dapat dilihat pada gambar 3, contoh penerapannya diberikan sebagai berikut :

Proses Enkripsi

Pesan yang digunakan adalah TRUELOVE NEVERDIE dengan kunci adalah

$K = \begin{bmatrix} 3 & 3 & -1 \\ 1 & 6 & 3 \\ 2 & -4 & 1 \end{bmatrix}$. Proses enkripsinya :

a) Pesan atau plaintext yaitu TRUELOVENEVERDIE diubah ke bentuk numerik, di peroleh :

T	R	U	E	L	O	V	E	N	E	V	E	R	D	I	E
19	17	20	4	11	14	21	4	13	4	21	4	17	3	8	4

b) Karena banyaknya abjad dalam plaintext yaitu 16 bukan kelipatan dari ukuran kolom matriks kunci yaitu 3 maka tambahkan sembarang abjad dalam plaintext sehingga *k* menjadi kelipatan m. Dalam Implementasi ini ditambahkan abjad Y dan Z.

c) Buatlah plaintext dalam bentuk blok dengan ukuran blok sama dengan ukuran kolom matriks kunci yaitu 3, sehingga plaintext menjadi:

$$P = \begin{bmatrix} T & R & U \\ E & L & O \\ V & E & N \\ E & V & E \\ R & D & I \\ E & Y & Z \end{bmatrix}$$

d. Buat P transpose :

$$P^1 = \begin{bmatrix} T & E & V & E & R & E \\ R & L & E & V & D & Y \\ U & O & N & E & I & Z \end{bmatrix}$$

e. Korespondensikan hasil d dengan numerik, sehingga diperoleh :

$$P^1 = \begin{bmatrix} 19 & 4 & 21 & 4 & 17 & 4 \\ 17 & 11 & 4 & 21 & 3 & 24 \\ 20 & 14 & 13 & 4 & 8 & 25 \end{bmatrix}$$

f. Kalikan matriks kunci K dengan plaintext transpose dalam modulo 26 berikut:

$$C^1 = K.P^1$$

$$C^1 = \begin{bmatrix} 3 & 3 & -1 \\ 1 & 6 & 3 \\ 2 & -4 & 1 \end{bmatrix} \begin{bmatrix} 19 & 4 & 21 & 4 & 17 & 4 \\ 17 & 11 & 4 & 21 & 3 & 24 \\ 20 & 14 & 13 & 4 & 8 & 25 \end{bmatrix}$$

$$= \begin{bmatrix} 88 & 31 & 62 & 71 & 52 & 59 \\ 181 & 112 & 84 & 142 & 59 & 223 \\ -10 & -22 & 39 & -72 & 30 & -63 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 10 & 5 & 10 & 19 & 0 & 7 \\ 25 & 8 & 6 & 12 & 7 & 15 \\ 16 & 4 & 13 & 6 & 4 & 15 \end{bmatrix}$$

g. Ubah hasil step f ke dalam abjad menggunakan koresponden abjad dengan numerik pada step a sehingga diperoleh *ciphertext* :

$$C^1 = \begin{bmatrix} K & F & K & T & A & H \\ Z & I & G & M & H & P \\ Q & E & N & G & E & P \end{bmatrix}$$

h. Diperoleh ciphertext :

$$C = (C^1)^1 = \begin{pmatrix} K & Z & Q \\ F & I & E \\ K & G & N \\ T & M & G \\ A & H & E \\ H & P & P \end{pmatrix}$$

j. Ciphertext C = KZQFIEKGNTMGAHEHPP

Proses Dekripsi

a. Matriks Kunci $K = \begin{bmatrix} 3 & 3 & -1 \\ 1 & 6 & 3 \\ 2 & -4 & 1 \end{bmatrix}$

b. Mencari invers matriks K, dengan cara :

- Mencari adjoint matriks K, diperoleh :

$$adj(K) = \begin{bmatrix} 18 & 1 & 15 \\ 5 & 5 & -10 \\ -16 & 18 & 15 \end{bmatrix}$$

Mencari determinan matriks K dalam mod 26, diperoleh 7

$$\frac{1}{\det K} \bmod 26 = x$$
$$(\det K * x) \bmod 26 = 1$$
$$(7 * x) \bmod 26 = 1$$
$$x = 15$$

Dicari Invers matriks K :

$$K^{-1} = 15 \begin{bmatrix} 18 & 1 & 15 \\ 5 & 5 & -10 \\ -16 & 18 & 15 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 10 & 15 & 17 \\ 23 & 23 & 6 \\ 20 & 10 & 17 \end{bmatrix}$$

c. Mencari plaintext transpose :

$$P^1 = K^{-1}C^1$$

$$P^1 = \begin{bmatrix} 10 & 15 & 17 \\ 23 & 23 & 6 \\ 20 & 10 & 17 \end{bmatrix} \begin{bmatrix} 10 & 5 & 10 & 19 & 0 & 7 \\ 25 & 8 & 6 & 12 & 7 & 15 \\ 16 & 4 & 13 & 6 & 4 & 15 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 747 & 238 & 411 & 472 & 173 & 550 \\ 901 & 323 & 446 & 749 & 185 & 596 \\ 722 & 248 & 481 & 602 & 138 & 545 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 19 & 4 & 21 & 4 & 17 & 4 \\ 17 & 11 & 4 & 21 & 3 & 24 \\ 20 & 14 & 13 & 4 & 8 & 25 \end{bmatrix}$$

d. Dari step c diperoleh :

$$P = (P^1)^1 = \begin{bmatrix} 19 & 17 & 20 \\ 4 & 11 & 14 \\ 21 & 4 & 13 \\ 4 & 21 & 4 \\ 17 & 3 & 8 \\ 4 & 24 & 25 \end{bmatrix}$$

e. Ubah hasil step d ke dalam abjad menggunakan koresponden abjad dengan numerik sehingga diperoleh *plaintext* :

$$P = \begin{bmatrix} T & R & U \\ E & L & O \\ V & E & N \\ E & V & E \\ R & D & I \\ E & Y & Z \end{bmatrix}$$

f. Diperoleh *plaintext* :
TRUELOVENEVERDIE

PENUTUP

Kesimpulan

- Semakin besar ukuran matriks kunci, maka semakin sulit Hill Cipher dipecahkan.
- Metode LSB mudah diimplementasikan dan tidak mengakibatkan perubahan yang signifikan pada cover image dari image aslinya.

Saran

- Hill Cipher dapat dimodifikasi dengan Chaining Hill Cipher dengan menambahkan karakter spasi, koma dan titik.
- Metode kriptografi dapat menggunakan kunci asimetrik
- Metode steganografi dapat menggunakan transform domain, yaitu DCT, DFT, atau DWT.

DAFTAR PUSTAKA

[1] Stinson, D.R., 1995, Cryptography Theory and Practice, CRC Press Boca Raton London Tokyo
[2] Widyanarko, A., Studi dan Analisi Mengenai Hill Cipher, Teknik Kriptanalisis dan Upaya penanggulangannya, Program Studi Teknik Informatika Institut Teknologi Bandung.
[3] Duraiswamy, K., and Rani, U.R., Security Thorough Obscurity, Sri Sarada College For Women
[4] Hakim, M.A., Studi dan Implementasi Steganografi Metode LSB dengan Preprocessing Kompresi Data dan Ekspansi Wadah, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung
[5] Rafferty, C., 2005, Steganography & Steganalysis of Images Msc Comms Sys Theory 2005