APLIKASI PENYEMBUNYIAN PESAN PADA CITRA DIGITAL DENGAN MENGGUNAKAN METODE KRIPTOGRAFI HILL CIPHER DAN TEKNIK LSB

Ramani Ndruru dan Jeremia Siregar

Mahasiswa Prodi Teknik Inforrmatika Fakultas Tekknologi Industri,
Institut Sains Teknologi TD. Pardede
Dosen Prodi Teknik Informatika Fakultas Teknologi Industri,
Institut Sains Teknologi TD. Pardede
Jl.DR. TD. Pardede. No.8 Medan 20153

Email : ramanindrururanin@mail.com, 2jeremiasiregar@istp.ac.id

ABSTRAK

Penjagaan kerahasiaan pesan dengan cara dienkripsi dengan ilmu kriptografi, membuat pesan menjadi tidak terbaca. Hal ini dapat menimbulkan kecurigaan bahwa pesan yang dikirim merupakan hal yang penting. Agar tidak menimbulkan kecurigaan, maka pesan dapat disembunyikan pada citra, sehingga tidak muncul kecurigaan tersebut awalnya pesan dienkripsi dengan menggunakan metode kriptografi Hill Cipher. Kunci dari Hill Cipiher adalah nilai numerik dalam bentuk matriks K. Proses enkripsi menggunakan matriks K, sedangkan proses dekripsi menggunakan matriks invers dari.

1. PENDAHULUAN

Pada umumnya, pesan dijaga kerahasiaannya dengan cara dienkripsi, sehingga pesan menjadi tidak dapat dibaca. Akan tetapi, pesan yang tidak terbaca (dienkripsi) dapat menimbulkan kecurigaan bahwa pesan yang dikirim merupakan hal yang penting. Agar tidak menimbulkan kecurigaan, maka pesan harus disembunyikan dalam bentuk yang umum, sehingga tidak muncul kecurigaan tersebut. Ilmu yang mempelajari penyembunyian pesan pada citra sehingga pesan menyatu dengan citra tersebut adalah Steganografi. Sedangkan steganografi berasal dari kata "steganos" berarti rahasiadan "graphein" yang berartitulisan.

I.1 Tujuaan dan manfaat

Adapun tujuan dari penulisan skripsi ini adalah mengembangkan suatu aplikasi yang dapat mengenkripsi pesan dengan menggunakan metode Hill Cipher dan menyembunyikan pesan di dalam citra digital dengan teknik LSB sebagai berikut :

2. LANDASAN TEORI

II.1 Citra

seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada suatu media penyimpanan.

II.2 Kriptografi

Kriptografi adalah ilmu yang mempelajari bagaimana suatu pesan atau dokumen kita aman, tidak bisa dibaca oleh pihak yang tidak berhak

ll.3 Hill cipher

Hill cipher termasuk dalam salah satu kriptosistem polialfabetik, artinya setiap karakter alfabet bisa dipetakan ke lebih dari satu macam karakter alfabet. Misalkan m adalah bilangan bulat positif, dan P = C = (Z26).Ide dari Hill cipher adalah dengan mengambil kombinasi linier dari karakter alfabet dalam satu elemen plaintext

Hill Cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi.

Misalkan m = 2, maka dapat ditulis suatu elemen plaintext sebagai x = (x1, x2) dan suatu elemen ciphertext sebagai y = (y1, y2). Di sini, y1, y2 adalah kombinasi linier dari x1 dan x2:
y1 = 11x1 + 3x2
y2 = 8x1 + 7x2
maka dapat ditulis dalam notasi matriks sebagai berikut:

II.4 Stegnogrfi

Steganografi merupakan seni untuk menyembunyikan pesan di dalam media digital sedemikian rupa sehingga orang lain tidak menyadari ada pesan yang disembunyikan di dalam media tersebut.

PEMBAHASAN DAN PERANCANGAN

III.1 Pembahasan

Pembahasan akan mencakup proses proses penyembunyian pesan ke citra dan proses ekstraksi pesan dari citra dengan menggunakan metode kriptografi Hill Cipher dan metode LSB.

III.1.1 Proses Penyembunyian Pesan Ke Citra

Proses penyembunyian pesan ke citra digital dapat dilihat pada gambar III.1 dan melalui dua tahapan, yaitu:
Proses enkripsi pesan dengan menggunakan metode Hill Cipher.

Proses penyisipan dengan menggunakan teknik LSB
K = s

Sebagai contoh, apabila pesan "DESI ESTER" akan disisipkan pada citra digital, maka proses penyisipan ke citra digital adalah sebagai berikut:
Pilih kunci berupa matriks 2x2 yang akan digunakan untuk proses enkripsi. Syaratnya adalah matriks kunci K harus mempunyai determinan sebesar satu, sehingga matriks K mempunyai matriks invers, berupa K-1. Matriks invers K-1 akan digunakan pada proses dekripsi. Sebagai contoh, apabila matriks K yang dipilih adalah :
K = 1767 (digunakan pada proses enkripsi)
1871
Determinan K = (17 x 71) – (67 x 18) = 1. Dengan demikian, K dapat digunakan untuk proses enkripsi, karena mempunyai matriks invers K-1 yang akan digunakan pada proses dekripsi.
K-1 = a2,2-a1,2-a2,1a1,1
modulo 256 (karena terdapat 0-255 karakter di dalam tabel Ascii)
K-1 = 71-67-1817
K-1 = 71189(digunakan pada proses dekripsi)
23817

Proses enkripsi terhadap pesan "DESI ESTER" dengan menggunakan kunci matriks K adalah sebagai berikut:
Dengan demikian, hasil enkripsi dari pesan "DESI ESTER" dengan menggunakan kunci (17 67; 18 71) adalah "ëž_/c"˜.
Selanjutnya, ubah setiap pesan terenkripsi ke biner:
Karakter ke-1, " diubah ke biner = biner(147) = 10010011
Karakter ke-2, ë diubah ke biner = biner(235) = 11101011
Karakter ke-3, ž diubah ke biner = biner(158) = 10011110
Karakter ke-4, _ diubah ke biner = biner(21) = 00010101
Karakter ke-5, / diubah ke biner = biner(47) = 00101111
Karakter ke-6, c diubah ke biner = biner(99) = 01100011
Karakter ke-7, diubah ke biner = biner(127) = 01111111
Karakter ke-8, " diubah ke biner = biner(34) = 00100010
Karakter ke-9, diubah ke biner = biner(11) = 00001011
Karakter ke-10, ˜ diubah ke biner = biner(152) = 10011000
Hasil konversi karakter ciphertext ke biner adalah "10010011 11101011 10011110 00010101 00101111 01100011 01111111 00100010 00001011 10011000". Panjang keseluruhan bit biner = 80.
Tahap berikutnya adalah menyisipkan barisan bit biner dari ciphertext ke citra, dengan menggunakan metode LSB, yaitu dengan mengganti bit paling terakhir dari piksel dengan bit dari ciphertext. Proses penyisipan dapat dilihat pada tabel III.1 berikut.
Metode LSB
Piksel
Citra Asli Bit Cipher Piksel
Hasil Penyisipan

Piksel ke-1:
R = 162 = 10100010
G = 212 = 11010100
B = 117 = 01110101
0 Piksel ke-1:
R = 163 = 10100011
G = 212 = 11010100
B = 116 = 01110100
Piksel ke-2:
R = 10 = 00001010
G = 105 = 01101001
B = 95 = 01011111
0 Piksel ke-2:
R = 11 = 00001011
G = 104 = 01101000
B = 94 = 01011110
Piksel ke-3:
R = 85 = 01010101
G = 195 = 11000011
B = 205 = 11001101
1 Piksel ke-3:
R = 85 = 01010101
G = 195 = 11000011
B = 205 = 11001101
Piksel ke-4:
R = 125 = 01111101
G = 175 = 10101111
B = 245 = 11110101
0 Piksel ke-4:
R = 125 = 01111101
G = 175 = 10101111
B = 244 = 11110100
Piksel ke-5:
R = 20 = 00010100
G = 35 = 00100011
B = 99 = 01100011
1 Piksel ke-5:
R = 21 = 00010101
G = 34 = 00100010
B = 99 = 01100011
Piksel ke-6:
R = 242 = 11110010
G = 212 = 11010100
B = 200 = 11001000
0 Piksel ke-6:
R = 243 = 11110011
G = 213 = 11010101
B = 200 = 11001000

III.1.2 Proses Ekstraksi Pesan Dari

Proses ekstraksi pesan dari citra digital dapat dilihat pada gambar III.2 dan melalui dua tahapan, yaitu: Proses ekstraksi pesan dengan menggunakan teknik LSB.
Proses dekripsi pesan dengan menggunakan metode Hill Cipher.
Masukkan kunci K berupa matriks 2x2 yang akan digunakan untuk proses dekripsi, dan hitung matriks invers K-1 untuk digunakan pada proses dekripsi.
K = 1767 1871
K-1 = a2,2-a1,2 -a2,1a1,1
modulo 256 (karena terdapat 0-255 karakter di dalam tabel Ascii)
K-1 = 71-67-1817
K-1 = 71189 (digunakan pada proses dekripsi)
23817

Ekstraksi panjang pesan dari piksel terakhir citra, yaitu 80 bit biner.
Ekstraksi bit biner dari citra dengan menggunakan metode LSB, yaitu mengambil bit paling terakhir dari citra, seperti terlihat pada tabel III.2.
Tabel III.2 Proses Ekstraksi dengan Metode LSB
Piksel Citra Asli Bit Cipher
Piksel ke-1:
R = 163 = 10100011
G = 212 = 11010100
B = 116 = 01110100
Piksel ke-2:
R = 11 = 00001011
G = 104 = 01101000
B = 94 = 01011110
Piksel ke-3:
R = 85 = 01010101
G = 195 = 11000011
B = 205 = 11001101
Piksel ke-4:
R = 125 = 01111101
G = 175 = 10101111
B = 244 = 11110100
Piksel ke-5:
R = 21 = 00010101
G = 34 = 00100010
B = 99 = 01100011
Piksel ke-6:
R = 243 = 11110011
G = 213 = 11010101
B = 200 = 11001000

Lakukan hingga 80 bit pesan terekstraksi dengan benar.
Hasil ekstraksi barisan bit biner adalah "10010011 11101011 10011110 00010101 00101111 01100011 01111111 00100010 00001011 10011000".
Ubah setiap 8 bit biner ke bentuk desimal.
Karakter ke-1, 10010011 = 147 karakter "
Karakter ke-2, 11101011 = 235 karakter ë
Karakter ke-3, 10011110 = 158 karakter ž
Karakter ke-4, 00010101 = 21 karakter _
Karakter ke-5, 00101111 = 47 karakter /
Karakter ke-6, 01100011 = 99 karakter c
Karakter ke-7, 01111111 = 127 karakter
Karakter ke-8, 00100010 = 34 karakter
"Karakter ke-9, 00001011 = 11 karakter
Karakter ke-10, 10011000 = 152 karakter ˜
Proses dekripsi dengan menggunakan kunci (71 189; 238 17), sbb;
Hasil ekstraksi pesan dari citra digital adalah "DESI ESTER". Pesan hasil ekstraksi sama dengan pesan asli.

III.2 Perancangan

Proses perancangan aplikasi penyembunyian pesan pada citra digital dengan menggunakan metode Hill Cipher dan teknik Least Significant Bit, menggunakan bahasa pemrograman Microsoft Visual Basic .Net.

III.3 Form Penyembunyian Pesan

Form ini berfungsi untuk menyembunyikan pesan pada citra digital sebagai berikut ;

III.3 Form Ekstraksi Pesan

Form Ekstraksi berfungsi untuk mengekstraksi pesan dari citra digital. Pada form ini, user dapat memilih citra yang telah disisipkan oleh pesan pada form Penyembunyian Pesan, lalu memasukkan kunci berupa matriks 2x2 yang akan digunakan untuk mengekstrak pesan dari citra.

Apabila matriks kunci K yang digunakan sama dengan saaat proses penyisipan, maka pesan akan terekstraksi dengan benar. Dalam hal ini, matriks kunci yang digunakan adalah matriks invers dari K, yaitu K-1 yang akan dihitung secara otomatis oleh aplikasi dan digunakan untuk proses dekripsi dari ciphertext hasil ekstraksi. Form ini juga dapat menampilkan langkah- dari proses ekstraksi pesan:

III.4 Form About

Form ini berfungsi untuk menampilkan identitas dari mahasiswa penyusun tugas akhir dan sekaligus pembuat aplikasi. Rancangan form dapat dilihat pada gambar berikut.

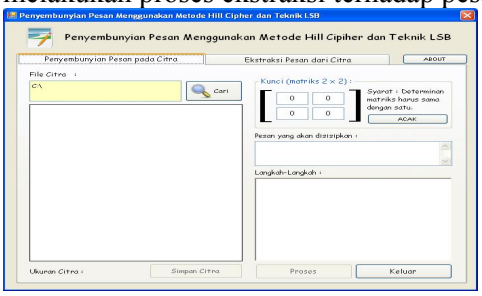
ALGORITMA DAN IMPLEMENTASI

IV.1 Algoritma

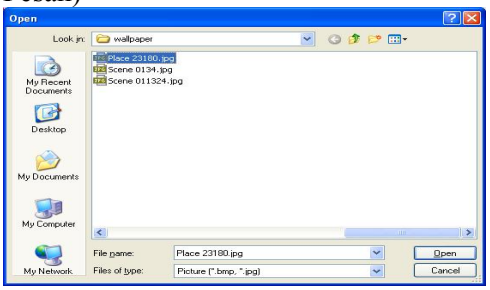
Algoritma utama yang digunakan pada aplikasi penyembunyian pesan pada citra digital ini adalah : Algoritma Penyembunyian Pesan Algoritma Ekstraksi Pesan

IV.2 Implementasi

Pada saat aplikasi dijalankan, form Utama akan tampil seperti terlihat pada gambar IV.1 berikut. Form ini berisi tab untuk menyembunyikan pesan dan tab untuk melakukan proses ekstraksi terhadap pesan.

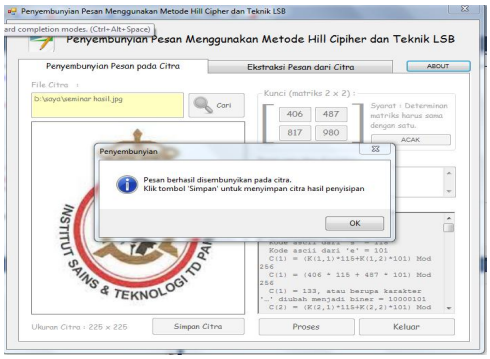


Gambar IV.1 Form Utama (Tab Penyembunyian Pesan)

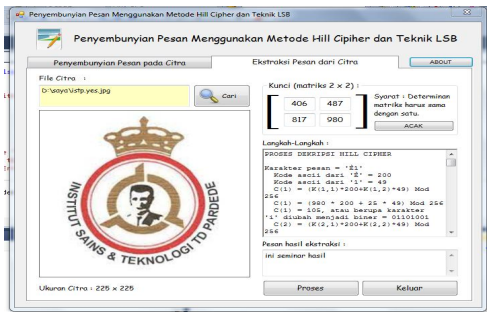


Gambar IV.2 Kotak Dialog Open File

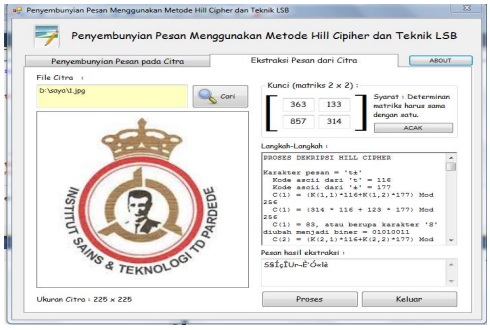
Gambar IV.3 Tampilan Gambar Form Utama (Tab Penyembunyian Pesan)



Gambar IV.4 Proses Penyembunyian Pesan



Gambar IV.5 Proses Ekstraksi Pesan



Gambar IV.6 Proses Ekstraksi Pesan dengan Kunci yang Salah

KESIMPULAN DAN SARAN

V.1 Kesimpulan

Setelah menyelesaikan perancangan aplikasi penyembunyian pesn pada citra digital dengan menggunakan metode kriptografi Hill Cipher dan teknik Least Significant Bit, penulis menarik kesimpulan sebagai berikut:

Aplikasi hasil rancangan dapat digunakan untuk menyembunyikan pesan pada citra digital dengan menggunakan teknik LSB dan pengamanan pesan menggunakan metode kriptografi Hill Ciper.

V.2 Saran

Beberapa saran yang dapat diberikan untuk pengembangan perangkat lunak lebih lanjut:

Aplikasi dapat dikembangkan sehingga dapat menyembunyikan file pada citra, seperti: file dokumen dan file office.

Aplikasi dapat ditambahkan algoritma kompresi untuk memperkecil ukuran pesan / file yang akan disisipkan pada citra

DAFTAR PUSTAKA

[ARI]Ariyus, D., Pengantar IlmuKriptografi, Penerbit Andi, Yogyakarta.

[KUR]Kurniawan, J., Kriptografi, Keamanan Internet dan Jaringan Komunikasi, Informatika, Bandung.

[MUN]Munir, R., Kriptografi, Informatika, Bandung.

[SAD]Sadikin, R., Kriptografi untuk Keamanan Jaringan, Penerbit Andi, Yogyakarta.[SCH]Schneier, B., Applied Crytography, Second Edition, John Willey and Sons Inc.

[SUT]Sutoyo, T, Teori Pengolahan Citra Digital, Penerbit Andi, Yogyakarta.

http://en.wikipedia.org/wiki/Hill_cipherhttp://practicalcryptography.com/ciphers/classical-era/hill/