P-ISSN : 2580-4316
E-ISSN : 2654-8054
https://doi.org/10.37817/ikraith-informatika.v11i1

PERANGKAT LUNAK PENYEMBUNYIAN PESAN PADA CITRA DIGITAL DENGAN MENGGUNAKAN METODE KRIPTOGRAFI *HILL CIPHER* DAN TEKNIK *LEAST SIGNIFICANT BIT*

Pallentino Rossy Damanik[1], **Swingly Purba**[2], **Melva Pangaribuan**[3]

Jurusan Teknik Informatika, ISTP Medan

Email : [1] pallentinodamanik@gmail.com [2]Swingly.Purba@gmail.com
[3]melpangrib@gmail.com

ABSTRAK

Penjagaan kerahasiaan pesan dengan cara dienkripsi dengan ilmu kriptografi, membuat pesan menjadi tidak terbaca. Hal ini pesan 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 K.

Dengan demikian, untuk memastikan bahwa K memiliki invers, maka determinan dari K harus sama dengan satu. Kemudian hasil enkripsi berupa pesan teracak disembunyikan ke teknik dan pengamanan pesan menggunakan metode kriptografi *Hill Ciper*.

Kata Kunci : *Kripto Grafi, Hill Cipher, LSB*

https://doi.org/10.37817/ikraith-informatika.v11i1
P-ISSN : 2580-4316
E-ISSN : 2654-8054

ABSTRACT

Encrypting messages to ensure confidentiality renders them unreadable, which can arouse suspicion that the transmitted message contains important information. To avoid such suspicion, the message can be hidden within an image.

Initially, the message is encrypted using the Hill Cipher method. The key for the Hill Cipher is a numerical value represented as a matrix, K. The encryption process utilizes matrix K, while the decryption process employs the inverse of matrix K; consequently, to ensure K is invertible, its determinant must equal one.

The resulting encrypted (scrambled) message is then embedded

developed application enables the hiding of messages within digital images using the LSB technique, while securing the messages via the Hill Cipher method.

Keywords : *Cryptograpyh, Hill Cipher, LSB*

P-ISSN : 2580-4316
E-ISSN : 2654-8054
https://doi.org/10.37817/ikraith-informatika.v11i1

1. PENDAHULUAN

Kerahasiaan pesan merupakan bagian dari ilmu kriptografi. 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.

Pada prosesnya, pesan dienkripsi terlebih dahulu dengan menggunakan metode kriptografi dan hasil enkripsi disisipkan pada citra, sehingga tidak menimbulkan kecurigaan terhadap keberadaan pesan rahasia. *Hill Cipher*

Dengan menggunakan teknik LSB, maka citra hasil steganografi tidak akan berbeda jauh dengan citra aslinya secara kasat mata, karena bit yang berubah adalah bit yang terakhir. Untuk mengekstrak pesan, maka *ciphertext* diekstrak dari citra dengan menggunakan metode *Hill Cipher*.

2. RUMUSAN MASALAH

Maka yang menjadi Permasalahanya adalah bagaimana merancang perangkat lunak yang dapat melakukan enkripsi terhadap pesan dengan menggunakan metode *Hill Cipher* dan menyisipkan hasil enkripsi pada citra digital dengan menggunakan teknik LSB

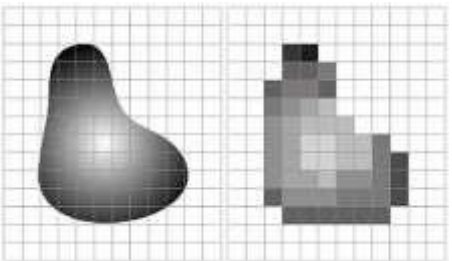
3. BATASAN MASALAH

1. *Input* aplikasi adalah:
   a. Gambar sebagai media penyimpan pesan, memiliki ekstension *.jpg dan *.bmp, dan dibatasi berukuran maksimal 1024 x 768 piksel.
   b. Pesan rahasia, dengan panjang maksimum dibatasi 1000 karakter.
   c. Kunci, merupakan matriks numerik dibatasi berukuran 2 x 2.
2. Proses yang dilakukan adalah:
   a. Proses penyisipan pesan.
   b. Proses ekstraksi pesan.
3. *Output* aplikasi adalah pesan yang terkandung di dalam citra.
4. Aplikasi dapat menampilkan perhitungan dari metode yang digunakan.
5. Pesan dienkripsi dengan menggunakan metode *Hill Cipher* dan LSB

4. LANDASAN TEORI

Citra adalah suatu gambaran, kemiripan, atau imitasi dari suatu objek. Citra sebagai keluaran suatu sistem perekaman data dapat bersifat optik berupa foto, bersifat analog berupa sinyal-sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada suatu media penyimpanan

Terdapat II.1

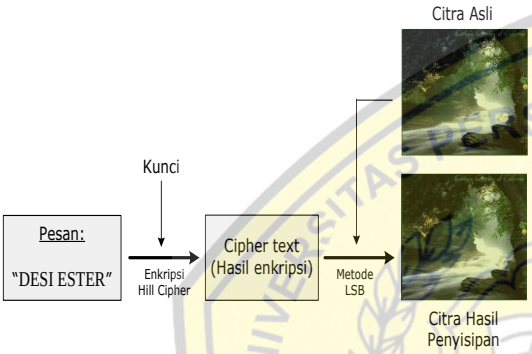


(a) (b)

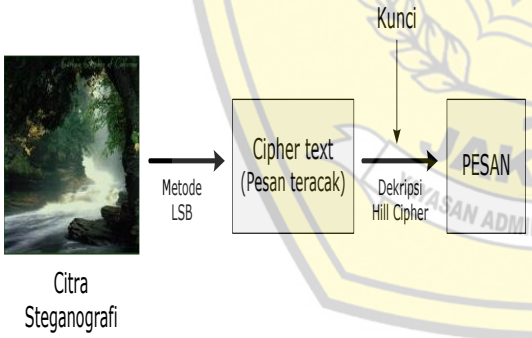
II.1 Contoh Citra (a) Citra Analog, (b) Citra Digital

https://doi.org/10.37817/ikraith-informatika.v11i1
P-ISSN : 2580-4316
E-ISSN : 2654-8054

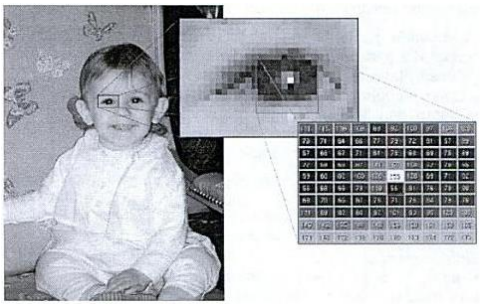
Dari sensor ini berupa arus yang besarnya sebanding dengan intensitas cahaya yang mengenainya. Arus tersebut kemudian dikonversi menjadi data digital dan dikirimkan ke unit penampil atau unit pengolah lainnya. Secara keseluruhan, hasil keluaran sistem pencitraan berupa citra digital. Proses akuisisi dapat dilihat pada gambar II.2



Gambar II.2 Proses Penyembunyian Pesan Pada Citra Digital



Gambar II.3 Sistem Koordinat Citra



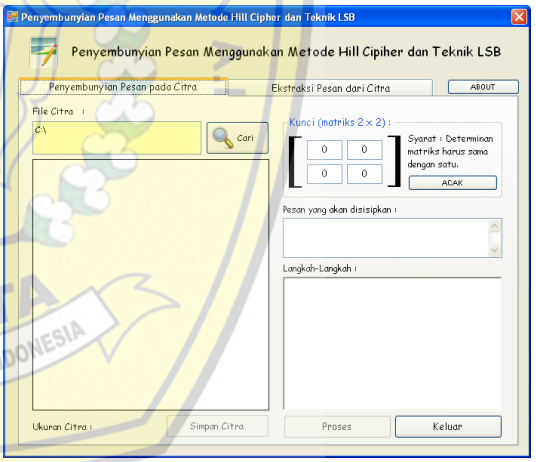
Gambar II.4 Contoh Citra Grayscale dan Nilai Intensitas pada Area Cropping

5. METODOLOGI PENELITIAN

Pembahasan akan mencakup proses proses penyembunyian pesan ke citra dan proses ekstraksi pesan dari citra dengan kriptografi dan metode LSB

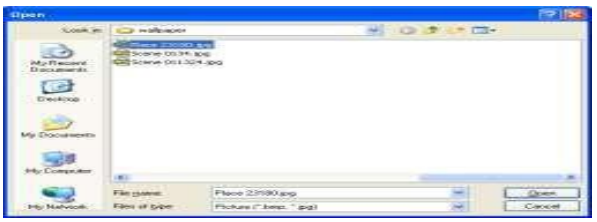
utama yang digunakan pada aplikasi ini adalah:

1. Penyembunyian Pesan
2. Algoritma Ekstraksi Pesan
3. Pada saat aplikasi dijalankan, *form* Utama akan tampil seperti terlihat Form untuk menyembunyikan pesan dan tab untuk melakukan proses ekstraksi terhadap pesan.



Gambar IV.1 Form Utama (Tab Penyembunyian Pesan)

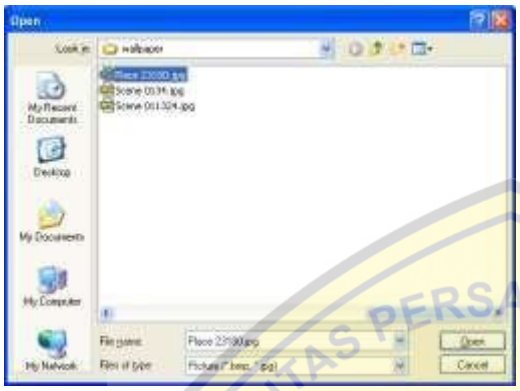
Tekan tombol ”cari” untuk mrmbuka *file* citra sebagai media penyembunyian pesan.



Gambar IV.2 Kotak Dialog Open File

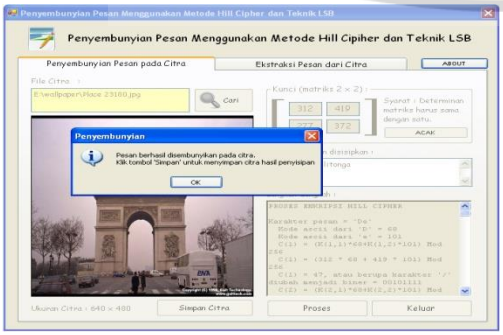
P-ISSN : 2580-4316
E-ISSN : 2654-8054
https://doi.org/10.37817/ikraith-informatika.v11i1

Tekan tombol “Open” dan gambar akan ditampilkan pada form Utama



Gambar Utama (Tab Penyembunyian Pesan)

Masukkan pesan rahasia yang ingin disembunyikan pada citra (sebagai contoh: „Desi Ester Silitonga“ dan masukkan matriks kunci yang akan digunakan untuk proses enkripsi *Hill Cipher*. Syarat pemilihan matriks kunci adalah bahwa matriks harus memiliki determinan sebesar satu, sehingga matriks memiliki dapat proses Proses IV.4



Gambar IV.4 Proses Penyembunyian Pesan

Selanjutnya, klik “Simpan Citra” hasil steganografi yang telah disisipkan rahasia.

Untuk melakukan proses ekstraksi citra, klik pada tab “Ekstraksi Pesan”, lalu pilih citra yang telah disisipkan pesan, masukkan kunci yang sama dengan kunci pada saat penyembunyian pesan, dan pesan rahasia akan terekstrak seperti terlihat



Gambar IV.5 Proses Ekstraksi Pesan

DAFTAR PUSTAKA

[ARI08] Ariyus, D., Pengantar Ilmu Kriptografi, PenerbitAndi, Yogyakarta.

[KUR04] Kurniawan, J., Kriptografi,Keamanan *Internet* dan Jaringan Komunikasi, Informatika, Bandung.

P-ISSN : 2580-4316
E-ISSN : 2654-8054

[MUN06] Munir, R., Kriptografi, Informatika, Bandung.

[SAD12] Sadikin,R., Kriptografi untuk Keamanan Jaringan, Penerbit Andi, Yogyakarta.

[SCH96] Schneier, B., Applied Crytography, Second Edition, John Willey and Sons Inc.

[SUT09] Sutoyo, T, **Teori Pengolahan Citra Digital**, Penerbit Andi, Yogyakarta.

http://en.wikipedia.org/wiki/Hill_cipher

http://practicalcryptography.com/ciphers/classical-era/hill/