

APLIKASI PENYEMBUNYIAN PESAN PADA CITRA DIGITAL DENGAN MENGGUNAKAN METODE KRIPTOGRAFI *HILL CIPHER* DAN TEKNIK *LEAST SINGNIFICANT BIT*

Riesman Hulu¹, Swingly Purba², Rikardo Hotman Siahaan³

Prodi Teknik Informatika, Fakultas Teknologi Industri
Institut Sains Dan Teknologi TD Pardede, Jl. DR. TD. Pardede No.8 Medan 20153

E-Mail:

riesmanhulu@gmail.com^{1*}, swinglypurba@istp.ac.id², ricardoricardo3010@gmail.com³

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 Cipher 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 citra dengan menggunakan teknik *Least Significant Bit* (LSB). Aplikasi hasil rancangan dapat digunakan untuk menyembunyikan pesan pada citra digital dengan menggunakan teknik LSB dan pengamanan pesan menggunakan metode kriptografi *Hill Cipher*.

Kata kunci : Enkripsi, Dekripsi, Hill Cipher, LSB

ABSTRACT

Maintaining message confidentiality by encrypting it with cryptography renders it unreadable. This can raise suspicions that the message being sent is important. To avoid suspicion, the message can be hidden in the image, thus preventing such suspicion. Initially, the message is encrypted using the Hill Cipher cryptography method. The key to the Hill Cipher is a numeric value in the form of a matrix K. The encryption process uses the matrix K, while the decryption process uses the inverse matrix of K. Therefore, to ensure that K has an inverse, the determinant of K must be equal to one. The resulting encrypted message is then hidden in the image using the Least Significant Bit (LSB) technique. The designed application can be used to hide messages in digital images using the LSB technique and secure messages using the Hill Cipher cryptography method.

Keywords: Enkripsi, Dekripsi, Hill Cipher, LSB

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. 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. Pada prosesnya, pesan dienkripsi terlebih dahulu dengan menggunakan metode kriptografi dan hasil enkripsi disisipkan pada citra, sehingga tidak menimbulkan kecurigaan terhadap keberadaan pesan rahasia. Salah satu metode kriptografi yang dapat digunakan adalah metode *Hill Cipher*. Metode ini termasuk salah satu sistem kripto polialfabetik, yang berarti setiap karakter alfabet bisa dipetakan ke lebih dari satu macam karakter. *Hill Cipher* ditemukan oleh Lester S. Hill. Ide dari *Hill Cipher* adalah dengan mengambil m kombinasi linear dari m karakter alfabet dalam satu elemen teks-asli sehingga dihasilkan m alfabet karakter dalam satu elemen teks-asli. Secara umum, matriks kunci K berukuran $m \times m$ sebagai kunci, hasil enkripsi ditulis sebagai $y = x.K$. Teks kode diperoleh dari teks-asli dengan cara transformasi linear. Untuk melakukan dekripsi, menggunakan matriks invers K^{-1} , proses dekripsi dilakukan dengan rumus $x = y.K^{-1}$. Dekripsi hanya mungkin dilakukan jika K memiliki inversi, dan suatu matriks K memiliki inversi jika dan hanya jika determinannya tidak sama dengan nol [ARI08]. Setelah pesan dienkripsi dengan menggunakan metode *Hill Cipher*, maka hasil enkripsi disisipkan pada citra dengan menggunakan ilmu steganografi. Di dalam steganografi, teknik yang paling umum digunakan adalah penyisipan bit pesan pada bit terakhir pada media gambar, atau yang dikenal dengan teknik LSB (*Least Significant Bit*). 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 teknik LSB, dan

didekripsi dengan menggunakan kunci yang sama pada saat proses enkripsi dengan menggunakan metode *Hill Cipher*.

Berdasarkan uraian di atas maka penulis ingin membuat tugas akhir dengan judul “Aplikasi Penyembunyian Pesan pada Citra Digital dengan Menggunakan Metode Kriptografi *Hill Cipher* dan Teknik *Least Significant Bit*”.

2. TINJAUAN PUSTAKA

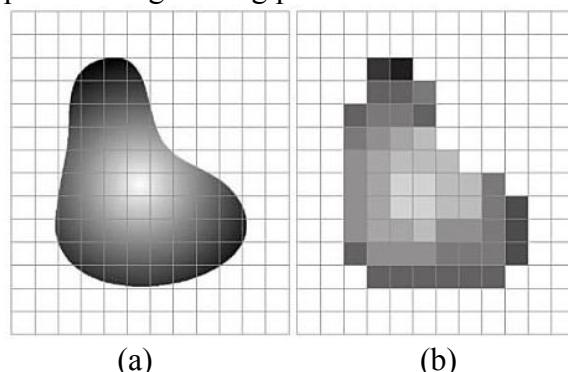
2.1. Citra

Citra adalah suatu representasi (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.

2.2. Citra Analog dan Citra Digital

Citra analog merupakan citra yang bersifat kontinu, seperti gambar pada monitor televisi, foto sinar-X, foto yang tercetak di kertas foto, lukisan, pemandangan alam, hasil CT scan, gambar-gambar yang terekam pada pita kaset, dan lain sebagainya. Citra analog tidak dapat direpresentasikan dalam komputer, sehingga tidak bisa diproses di komputer secara langsung.

Sedangkan, pengertian citra digital adalah citra yang dapat diolah oleh komputer. Yang disimpan pada komputer adalah angka-angka yang menunjukkan besar intensitas pada masing-masing piksel tersebut.

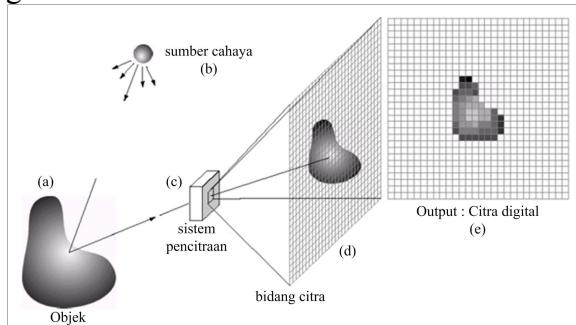


Gambar 2. 1 Contoh Citra (a) Citra Analog, (b) Citra Digital

2.3 Proses Akuisisi Citra

Proses akuisisi citra digital dapat dijelaskan sebagai berikut Ada sebuah objek yang akan diambil gambarnya untuk dijadikan citra digital. Sumber cahaya diperlukan untuk menerangi objek, yang berarti ada intensitas cahaya (*brightness*) yang diterima oleh objek. Oleh objek, intensitas cahaya ini sebagian diserap dan sebagian lagi dipantulkan ke lingkungan sekitar objek.

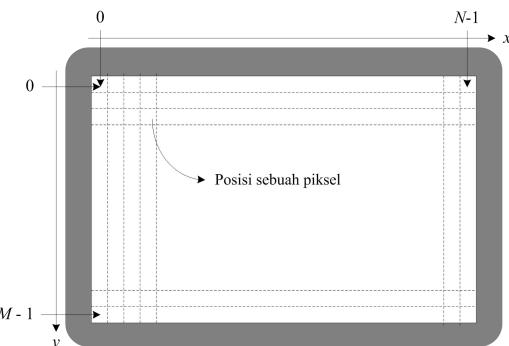
Proses akuisisi citra dapat dilihat pada gambar berikut.



Gambar 2. 2 Proses Akuisisi Citra Digital (a) objek, (b) sumber cahaya, (c) sistem pencitraan (imaging), (d) bidang citra, (e) citra digital

2.4 Representasi Citra Digital

Citra digital dibentuk oleh kumpulan titik yang dinamakan piksel (*pixel* atau *picture element*). Setiap piksel digambarkan sebagai satu kotak kecil. Setiap piksel mempunyai koordinat posisi. Sistem koordinat pada suatu citra digital berukuran $M \times N$ ditunjukkan pada gambar II.3 berikut.

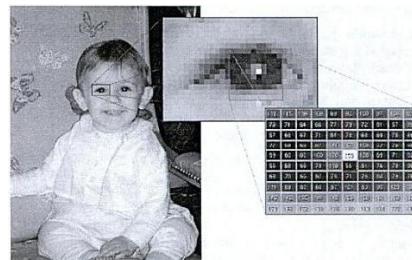


Gambar 2. 3 Sistem Koordinat Citra

Citra digital yang berukuran $M \times N$ lazim dinyatakan dengan matriks yang berukuran M baris dan N kolom sebagai berikut:

$$f(x, y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0, N-1) \\ f(1,0) & f(1,1) & \dots & f(1, N-1) \\ \vdots & \vdots & \ddots & \vdots \\ f(M-1,0) & f(M-1,1) & \dots & f(M-1, N-1) \end{bmatrix}$$

Nilai pada suatu irisan antara baris dan kolom pada posisi (x, y) disebut dengan *picture elements*, *image elements*, *pels*, atau *pixels*. Istilah terakhir (*pixel*) paling sering digunakan pada citra digital. Gambar II.4 menyajikan contoh dari suatu citra digital (*citra grayscale*), dengan nilai intensitas dari citra pada area tertentu.



Gambar 2. 4 Contoh Citra Grayscale dan Nilai Intensitas pada Area Cropping

2.5 Jenis Citra

a. Citra Biner

Citra biner adalah citra digital yang hanya memiliki dua kemungkinan nilai piksel, yaitu hitam dan putih. Citra biner disebut juga sebagai citra B&W (*black and white*) atau citra monokrom. Hanya dibutuhkan 1 bit untuk mewakili nilai setiap piksel dari citra biner.

b. Citra Grayscale

Citra *grayscale* merupakan citra digital yang hanya memiliki satu nilai kanal pada setiap pikselnya, dengan kata lain nilai bagian Red = Green = Blue. Nilai tersebut digunakan untuk menunjukkan tingkat intensitas.

c. Citra Warna (8 bit)

Setiap piksel dari citra warna 8 bit hanya diwakili oleh 8 bit dengan jumlah warna maksimum yang dapat digunakan adalah 256 warna.

Tabel 2. 1 Format Citra Warna 8 bit

Bit-7	Bit-6	Bit-5	Bit-4	Bit-3	Bit-2	Bit-1	Bit-0
R	R	R	G	G	G	B	B

d. Citra Warna (16 bit)

Citra warna 16 bit (biasanya disebut sebagai citra *highcolor*) dengan setiap pikselnya diwakili dengan 2 byte *memory* (16 bit). Warna 16 bit memiliki 65.536 warna.

Tabel 2. 2 Format Citra Warna 16 bit

Bit-15	Bit-14	Bit-13	Bit-12	Bit-11	Bit-10	Bit-9	Bit-8	Bit-7	Bit-6	Bit-5	Bit-4	Bit-3	Bit-2	Bit-1	Bit-0
R	R	R	R	R	G	G	G	G	G	G	B	B	B	B	B

e. Citra Warna (24 bit)

Setiap piksel dari citra warna 24 bit diwakili dengan 24 bit sehingga total 16.777.216 variasi warna.

f. Format File Citra

Format *file* citra standar yang digunakan saat ini terdiri dari beberapa jenis. Format-format ini digunakan dalam menyimpan citra dalam sebuah *file*. Setiap format memiliki karakteristik masing-masing. Berikut adalah penjelasan beberapa format citra yang umum digunakan saat ini:

- Bitmap (*.bmp)

Format .bmp adalah format penyimpanan standar tanpa kompresi yang umum dapat digunakan untuk menyimpan citra biner hingga citra warna. Format ini terdiri dari beberapa jenis yang setiap jenisnya ditentukan dengan jumlah bit yang digunakan untuk menyimpan sebuah nilai piksel.

- JPEG (.jpg)

Format .jpg adalah format yang sangat umum digunakan saat ini, khususnya untuk transmisi citra. Format ini digunakan untuk menyimpan citra hasil kompresi dengan metode JPEG.

- Graphics Interchange Format (.gif)

Format ini dapat digunakan pada citra warna dengan palet 8 bit. Pada umumnya digunakan pada aplikasi web. Kualitas yang rendah menyebabkan format ini tidak terlalu populer di kalangan peneliti pengolahan citra digital.

- Tagged Image Format (.tif, .tiff)

Format ini merupakan format citra yang dapat digunakan untuk menyimpan citra *bitmap* hingga citra dengan warna palet terkompresi. Format ini dapat digunakan untuk menyimpan citra tidak terkompresi dan citra terkompresi.

- Portable Network Graphics (*.png)

Format .png adalah format penyimpanan citra terkompresi. Format ini dapat digunakan pada citra *grayscale*, citra dengan palet warna dan juga citra *full color*. Format .png juga mampu menyimpan informasi hingga kanal *alpha* dengan penyimpanan sebesar 1 hingga 16 bit per kanal.

- MPEG (.mpg)

Format ini digunakan di dunia *internet* dan diperuntukkan sebagai format penyimpanan citra bergerak (*video*).

2.6 Kriptografi

Kriptografi adalah ilmu yang mempelajari bagaimana suatu pesan atau dokumen kita aman, tidak bisa dibaca oleh pihak yang tidak berhak. Dalam perkembangannya, kriptografi juga digunakan untuk identifikasi pengirim pesan dengan tanda tangan digital dan keaslian pesan dengan sidik jari digital (*fingerprint*).

3. METODE PENELITIAN

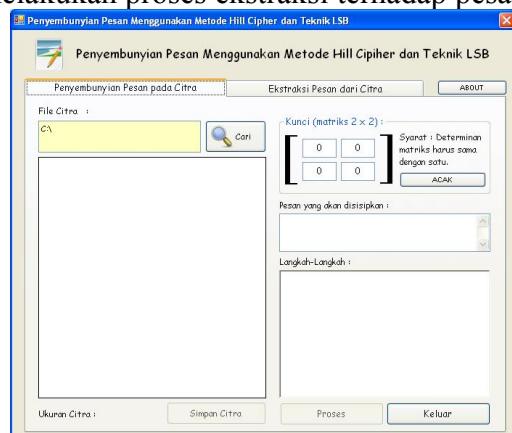
3.1 Metode Hill Cipher

Hill cipher termasuk dalam salah satu kriptosistem polialfabetik, artinya setiap karakter alfabet bisa dipetakan ke lebih dari satu macam karakter alfabet. Cipher ini ditemukan pada tahun 1929 oleh Lester S. Hill. Misalkan m adalah bilangan bulat positif, dan $P = C = (Z26)^m$. Ide dari Hill cipher adalah dengan mengambil m kombinasi linier dari m karakter alfabet dalam satu elemen plaintext, sehingga menghasilkan m alfabet karakter dalam satu elemen plaintext.

Hill Cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci berukuran $m \times m$ sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam *Hill Cipher* antara lain adalah perkalian antar matriks dan melakukan invers pada matriks.

4. HASIL DAN PEMBAHASAN

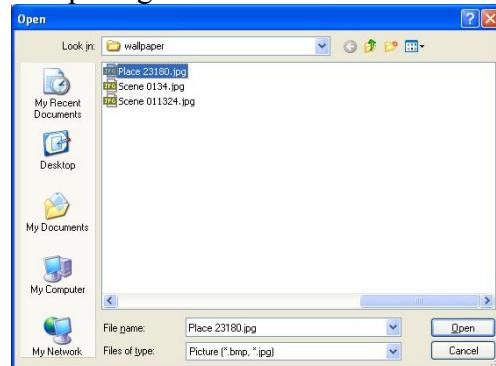
Pada saat aplikasi dijalankan, *form Utama* akan tampil seperti terlihat pada gambar dibawah berikut. Form ini berisi *tab* untuk menyembunyikan pesan dan tab untuk melakukan proses ekstraksi terhadap pesan.



Gambar 3. 1 Form Utama (Tab Penyembunyian Pesan)

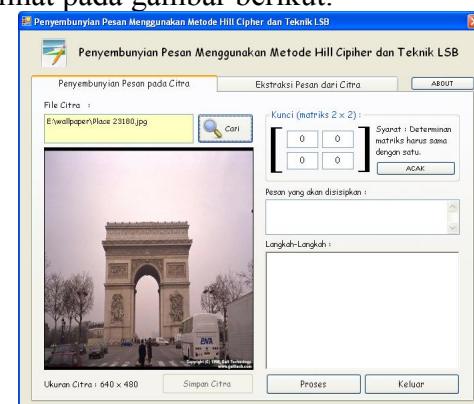
Tekan tombol ‘Cari’ untuk membuka *file* citra sebagai media penyembunyian pesan.

Kotak dialog Open akan muncul seperti terlihat pada gambar berikut.



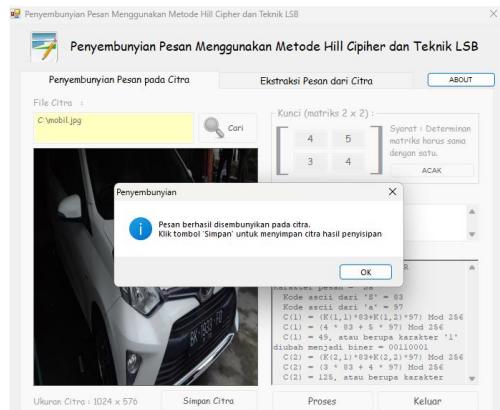
Gambar 3. 2 Kotak Dialog Open File

Tekan tombol ‘Open’ dan gambar akan ditampilkan pada form Utama seperti terlihat pada gambar berikut.

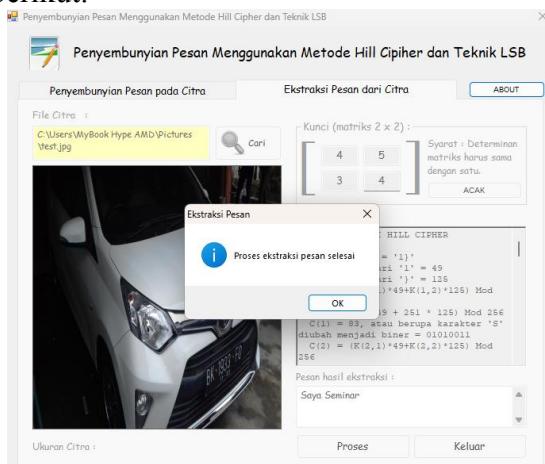


Gambar 3. 3 Tampilan Gambar Form Utama (Tab Penyembunyian Pesan)

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 matriks invers yang dapat digunakan untuk proses dekripsi. Proses penyembunyian pesan dapat dilihat pada gambar berikut.

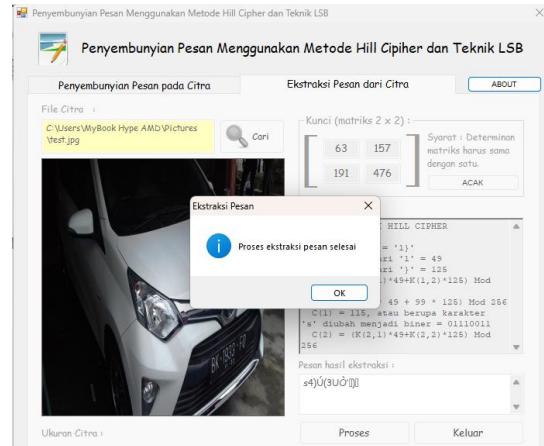


Gambar 3. 4 Proses Penyembunyian Pesan
Selanjutnya, klik tombol “Simpan Citra” untuk menyimpan citra hasil steganografi yang telah disisipkan pesan rahasia.
Untuk melakukan proses ekstraksi citra, klik pada tab “Ekstraksi Pesan”, lalu pilih citra yang telah disisipkan pesan, masukkan kunci yang sama dengan kunci pada saat penyembunyian pesan, dan pesan rahasia akan terekstrak seperti terlihat pada gambar berikut.



Gambar 3. 5 Proses Ekstraksi Pesan

Proses ekstraksi pesan rahasia dengan menggunakan kunci yang salah dapat dilihat pada gambar berikut.



Gambar 3. 6 Proses Ekstraksi Pesan dengan Kunci yang Salah

5. KESIMPULAN

5.1 Kesimpulan

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

1. Aplikasi hasil rancangan dapat digunakan untuk menyembunyikan pesan pada citra digital dengan menggunakan teknik LSB dan pengamanan pesan menggunakan metode kriptografi *Hill Cipher*.
2. Citra yang telah disisipkan pesan tidak dapat dibedakan secara kasat mata dengan citra sebelum penyisipan, sehingga tidak menimbulkan kecurigaan akan keberadaan pesan rahasia.
3. Proses ekstraksi pesan rahasia harus menggunakan kunci yang sama dengan kunci pada saat proses penyisipan pesan.

5.2 Saran

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

1. Aplikasi dapat dikembangkan sehingga dapat menyembunyikan file pada citra, seperti: file dokumen dan file office.
2. Aplikasi dapat ditambahkan algoritma kompresi untuk memperkecil ukuran

pesan / file yang akan disisipkan pada citra.

6. DAFTAR PUSTAKA

- Apriansyah, Mitra Unik, & Mukhtar, H. (2020). Implementasi Sistem Keamanan Pesan Text Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB). *Jurnal Computer Science and Information Technology*, 1(1), 8-15
- Doo, S. Y., Tena, S., & Ndolu, V. M. (2019). Implementasi Pengamanan Data Menggunakan Metode Kriptografi Hill Cipher Dan Steganografi Least Significant Bit (LSB) Pada Media Citra Digital. *Jurnal Media Elektro*, 8(2), 90-99.
- Hamrul, H., Awaldi, Suhardi, & Heri, A. (2022). Steganografi Berbasis Citra Digital untuk Menyembunyikan Data Menggunakan Kombinasi Multi Bit LSB dengan Hill Cipher. *Jurnal Ilmiah Information Technology d'Computare*, 12(Juli), 10-20.
- Laoli, D., & Sinaga, B. (2018). Penerapan Algoritma Hill Cipher Dan Least Significant Bit (LSB) Untuk Pengamanan Pesan Pada Citra Digital. *JIKOMSI [Jurnal Ilmu Komputer dan Sistem Informasi]*, 1(2), 30-40