IMPLEMENTASI ALGORITMA KRIPTOGRAFI *ADVANCE HILL CIPHER* DENGAN KUNCI TERENKRIPSI *ELGAMAL* UNTUK ENKRIPSI CITRA DIGITAL BERWARNA

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Meraih Gelar Sarjana Matematika (S.Mat) Jurusan Matematika Fakultas Sains Dan Teknologi Universitas Islam Negeri Alauddin Makassar

Oleh:

MUH. AFRIZAL NUR
NIM. 60600122061

JURUSAN MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI ALAUDDIN MAKASSAR

2026

DAFTAR ISI

DAFTAR ISI i
DAFTAR GAMBAR ii
DAFTAR TABEL iii
DAFTAR SIMBOL iv
BAB I PENDAHULUAN 1
A. Latar Belakang 1
B. Rumusan Masalah 6
C. Tujuan Penelitian 6
D. Manfaat Penelitian 6
E. Batasan Masalah 7
F. Sistematika Penulisan 7
BAB II TINJAUAN PUSTAKA 9
A. Aritmatika Modulo 9
B. Matriks 10
C. Kriptografi 19
D. Hill Cipher 21
E. Advance Hill Cipher 23
F. ElGamal 24
G. Representasi Matematis Citra Digital 26
H. Peak Signal-to-Noise Ratio (PSNR) 29
I. Structural Similarity Index Measure (SSIM) 30
J. Mean Square Error (MSE) 32
BAB III METODOLOGI PENELITIAN 34
A. Jenis Penelitian 34
B. Jenis dan Sumber Data 34
C. Waktu dan Tempat Pengambilan Data 34
D. Prosedur Penelitian 34
E. Flowchart Penelitian 36
BAB IV HASIL DAN PEMBAHASAN 36
A. Data Citra Digital 37
B. Proses Enkripsi dan Dekripsi Citra Digital 38
C. Pembahasan Hasil Enkripsi dan Dekripsi Citra Digital 58
BAB V PENUTUP 61
DAFTAR PUSTAKA 62

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SIMBOL

K : Matriks kunci involutori

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi yang begitu cepat, khususnya di era digital saat ini, telah membuat internet digunakan secara luas di hampir semua aspek kehidupan. Berdasarkan laporan dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia pada tahun 2024 diperkirakan mencapai sekitar 221.563.479 orang. Angka pengguna internet yang begitu tinggi ini telah mendorong pertumbuhan pesat berbagai layanan berbasis internet, seperti media sosial, *e-commerce*, dan layanan penyimpanan data (APJII, 2024).

Dengan begitu tingginya penggunaan layanan berbasis internet, tantangan terhadap keamanan data juga semakin serius. Data digital yang dikirim melalui internet, terutama yang bersifat sensitif seperti foto pribadi atau dokumen penting, sangat rentan terhadap ancaman seperti peretasan dan penyalahgunaan. Oleh karena itu, penting untuk menjaga data pribadi agar tidak jatuh ke tangan pihak yang tidak berwenang.

Al-Qur'an juga menganjurkan untuk menjaga rahasia yang seharusnya dijaga, anjuran ini terdapat dalam QS An-Nisā' /4:58.

اِنَّ اللّٰهَ يَأْمُرُكُمْ اَنْ تُؤَدُّوا الْاَمٰنٰتِ اِلٰٓى اَهْلِهَاۙ وَاِذَا حَكَمْتُمْ بَيْنَ النَّاسِ اَنْ تَحْكُمُوْا بِالْعَدْلِۗ اِنَّ اللّٰهَ نِعِمَّا يَعِظُكُمْ بِهٖۗ اِنَّ اللّٰهَ كَانَ سَمِيْعًاۢ بَصِيْرًا

Terjemahnya:

> "Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha Mendengar lagi Maha Melihat".

Dalam tafsir Al-Wasith, Syekh Muhammad Sayyid Tantawi menjelaskan bahwa ayat ini menekankan bahwa amanat diharuskan dalam segala hal, baik dalam hal yang berkaitan dengan harta milik orang lain, barang titipan, tidak menyebarkan rahasia dan aib orang lain, maupun amanat dalam agama seperti mengerjakan hal yang diperintahkan Allah SWT dan menjauhi larangannya. Tafsir Al-Wasith surat An-Nisa ayat 58 ini menjelaskan bahwa kita diperintahkan untuk menyampaikan amanat yang benar yang sudah diselidiki asal muasalnya dan nantinya akan disampaikan kepada yang berhak menerimanya, termasuk data atau informasi digital.

Salah satu bentuk informasi digital yang paling umum digunakan adalah citra digital. Namun, penggunaan citra digital juga menghadirkan tantangan tersendiri dalam hal keamanan, terutama saat citra tersebut mengandung informasi sensitif dan dipertukarkan melalui jaringan yang tidak aman (Azam, 2020).

Keamanan citra digital menjadi isu yang sangat krusial, mengingat banyaknya ancaman yang muncul, seperti penyalahgunaan citra yang berisi informasi pribadi. Ancaman tersebut berpotensi membuat gambar atau citra yang bersifat rahasia dapat dibuka oleh pihak yang tidak memiliki izin. Oleh karena itu, dibutuhkan metode pengamanan data yang kuat agar kerahasiaan

serta keaslian citra digital yang dikirim tetap terjaga. Salah satu cara untuk melindungi keamanan citra digital adalah dengan menerapkan kriptografi. Bidang ini membahas berbagai metode matematis yang berkaitan dengan pengamanan informasi, meliputi kerahasiaan data, keutuhan isi, dan proses autentikasi. Dalam penerapannya, kriptografi mengubah informasi rahasia menjadi bentuk sandi tertentu sehingga apabila data tersebut jatuh ke tangan pihak yang tidak berhak, isi aslinya tetap tidak dapat diketahui karena telah melalui proses penyandian (Jamaludin, 2018).

Pada dasarnya, terdapat tiga tipe algoritma kriptografi, yaitu algoritma simetri, asimetri, dan *hybrid*. Algoritma simetri menggunakan satu kunci tunggal yang sama untuk proses enkripsi dan dekripsi pesan. Sebaliknya, algoritma asimetri menggunakan sepasang kunci, yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Kunci publik bersifat terbuka dan dapat diketahui oleh banyak pihak, sedangkan kunci privat bersifat rahasia dan hanya diketahui oleh pihak yang berwenang. Sementara itu, algoritma *hybrid* menggabungkan keunggulan dari algoritma simetri dan asimetri untuk meningkatkan keamanan dan efisiensi dalam proses kriptografi.

Salah satu contoh algoritma kriptografi simetris adalah *Hill Cipher*, yang merupakan sandi polialfabetik berbasis metode substitusi dengan memanfaatkan perkalian matriks sebagai kunci untuk proses enkripsi dan dekripsi. Kunci dalam *Hill Cipher* berbentuk matriks bujur sangkar yang harus memiliki invers modulo terhadap jumlah alfabet yang digunakan. Invers ini diperlukan dalam proses dekripsi agar pesan dapat dikembalikan ke bentuk

semula. Namun, pencarian matriks kunci yang memiliki invers dapat menjadi kompleks secara komputasi. Untuk mengatasi hal ini, digunakan matriks involutori, yaitu matriks yang merupakan invers dari dirinya sendiri, sebagai kunci dalam algoritma yang disebut *Advance Hill Cipher* (Acharya et al., 2009).

Berdasarkan hasil penelitian yang dilakukan oleh Khazaei dan Ahmadi (2017), algoritma Hill Cipher terbukti cukup tangguh dalam menghadapi jenis serangan *Ciphertext-Only Attack* (COA). Meskipun demikian, serangan COA ternyata dapat diuraikan menggunakan *Chinese Remainder Theorem* (Khazaei & Ahmadi, 2017). Temuan ini mengindikasikan bahwa Hill Cipher masih memiliki kelemahan dalam aspek keamanan kuncinya. Oleh karena itu, diperlukan upaya untuk meningkatkan tingkat keamanan algoritma ini tanpa mengabaikan efisiensi dan kecepatan dalam proses enkripsinya.

Dalam penelitiannya, (Fadlilah et al., 2022) mengusulkan kombinasi *Hill Cipher* dan *ElGamal* untuk mengamankan pesan teks, didapatkan hasil bahwa penggabungan algoritma *Hill Cipher* dan *ElGamal* untuk mengamankan pesan teks dapat dilakukan dengan baik. Namun, penelitian tersebut masih terbatas pada pengamanan pesan berbasis teks dan belum menyentuh aspek keamanan data berbentuk citra digital yang memiliki kompleksitas yang lebih tinggi. Penelitian (Hakim, 2021) menyatakan bahwa gabungan algoritma *Hill Cipher* dan *Arnold Cat Map* berhasil menghasilkan suatu citra digital yang lebih acak dengan rata-rata nilai *Structural Similarity Index Metrics* (SSIM) yang diperoleh dalam proses pengujian dengan menerapkan algoritma *Hill Cipher*

dan *Arnold Cat Map* adalah 0,027. Namun, penelitian tersebut belum menerapkan algoritma asimetris seperti *ElGamal* dalam pengamanan kunci.

Berdasarkan kajian penelitian sebelumnya yang sebagian besar masih terbatas pada pengamanan pesan teks maupun citra dengan kombinasi algoritma lain, penelitian ini difokuskan pada implementasi algoritma kriptografi *Advance Hill Cipher* dengan kunci terenkripsi *ElGamal* untuk enkripsi citra digital berwarna. Pemilihan citra digital berwarna didasarkan pada tingkat kompleksitas data yang lebih tinggi dibandingkan teks, sehingga diperlukan metode enkripsi yang tidak hanya efisien, tetapi juga memiliki tingkat keamanan yang memadai. *Advance Hill Cipher* sebagai algoritma simetris dipilih karena keunggulannya dalam melakukan proses enkripsi secara cepat pada data berukuran besar, meskipun masih memiliki kelemahan dalam hal distribusi kunci. Untuk mengatasi permasalahan tersebut, digunakan algoritma asimetris *ElGamal* yang memiliki kekuatan keamanan berbasis permasalahan logaritma diskret, sehingga mampu meningkatkan perlindungan distribusi kunci. Dengan mengombinasikan keunggulan algoritma simetris yang efisien dan algoritma asimetris yang aman. Penelitian ini diharapkan dapat memberikan kontribusi berupa analisis komprehensif mengenai potensi penggabungan algoritma simetris dan asimetris tersebut dalam enkripsi citra digital berwarna.

B. Rumusan Masalah

Berdasarkan uraian pada latar belakang, penelitian ini merumuskan permasalahan sebagai berikut:

1. Bagaimana hasil enkripsi dan dekripsi citra digital berwarna dengan metode kriptografi *Advance Hill Cipher* dengan kunci terenkripsi *ElGamal*?
2. Bagaimana lama waktu enkripsi dan dekripsi *Advance Hill Cipher* dengan kunci terenkripsi *ElGamal*?

C. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan, penelitian ini bertujuan untuk:

1. Untuk mengetahui hasil enkripsi dan dekripsi citra digital berwarna menggunakan algoritma *Advance Hill Cipher* dengan kunci terenkripsi *ElGamal*.
2. Untuk mengetahui lama waktu enkripsi dan dekripsi *Advance Hill Cipher* dengan kunci terenkripsi *ElGamal*.

D. Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah:

1. Bagi Penulis, penelitian ini dapat menjadi sarana untuk memperdalam pemahaman tentang kriptografi algoritma *Advance Hill Cipher* dan *ElGamal*.

2. Bagi Pembaca, penelitian ini dapat memberikan wawasan tentang bagaimana implementasi algoritma *Advance* Hill Hipher dan *ElGamal* dalam mengenkripsi citra digital berwarna.

E. Batasan Masalah

Agar pembahasan pada penelitian ini tidak meluas, maka diperlukan batasan – batasan masalah sebagai berikut.

1. Matriks kunci *Advance Hill Cipher* menggunakan matriks ordo $n \times n$ dengan n genap.
2. Data yang dienkripsi berupa citra digital berwarna dengan format *.jpg* dengan ukuran $n \times n$ piksel dengan n genap.

F. Sistematika Penulisan

I. PENDAHULUAN

Bagian ini terdiri dari latar belakang, rumusan masalah, tujuan penelitian manfaat penelitian, batasan masalah dan sistematika penulisan.

II. TINJAUAN PUSTAKA

Bagian ini terdiri tentang landasan teori, yang berisikan teori-teori serta Pustaka yang digunakan pada saat penelitian. Teori – teori tersebut terkait dengan Algoritma kriptografi *Advance Hill Cipher*, *ElGamal*, dan metrics pengukuran *Structural Similarity Index Metrics* (SSIM), *Mean Square Error* (MSE) dan *Peak Signal Noise Ratio* (PSNR) ini didapatkan dari buku literatur, jurnal, dan internet.

III. METODOLOGI PENELITIAN

Bagian ini dikemukakan metode penelitian yang mencangkup ruang lingkup kegiatan, waktu penelitiaan, jenis dan sumber data dan prosedur penelitiian.

DAFTAR PUSTAKA

BAB II

TINJAUAN PUSTAKA

A. Aritmatika Modulo

Aritmatika modulo merupakan bagian dari teori bilangan yang mempelajari operasi – operasi bilangan bulat berdasarkan pembagian terhadap suatu bilangan bulat positif tertentu, yang disebut modulus (Rosen, 2019).

Aritmetika modular melibatkan penggunaan operator modulo, di mana terdapat sebuah bilangan bulat $a$dan bilangan bulat $n$yang disebut sebagai modulus. Operasi ini dinyatakan dengan simbol berikut:

$$a \ mod \ n = r \tag{2.1}$$

Contoh:

Hasil dari 58 mod 7 adalah 2.

Hasil dari operasi modular adalah 58 mod 7 = 2, karena tujuan operasi modular adalah mengembalikan nilai r, sisa dari operasi a, dibagi n.

Definisi 2.2.1 (Kekongruenan)

Jika sebuah bilangan m yang tidak nol membagi selisih a-b, dikatakan a kongruen dengan b modulo m, dan ditulis:

$$a \equiv b \ (mod \ m) \tag{2.2}$$

Jika $a - b$ tidak habis dibagi m, maka dikatakan a tidak kongruen dengan $b \ mod \ m$, dan ditulis:

$$a \not\equiv b \ (mod\ m) \qquad (2.3)$$

Teorema 2.2.1 Jika m merupakan bilangan bulat positif, maka dua bilangan bulat $a$dan $b$bersifat kongruen modulo $m$apabila terdapat bilangan bulat k sedemikian sehingga a dapat dinyatakan sebagai $a = b + km$.

Bukti:

Jika $a \equiv b \ (mod\ m)$, maka berdasarkan definisi kongruensi (Definisi 2.2.1), diketahui bahwa $m \mid (a - b)$. Ini berarti terdapat suatu bilangan bulat k sedemikian sehingga $a - b = km$, sehingga $a = b + km$. Sebaliknya, jika terdapat suatu bilangan bulat k sehingga $a = b + km$, maka $km = a - b$. Dengan demikian, m membagi $a - b$, sehingga $a \equiv b \ (mod\ m)$ (Rosen, 2019).

Contoh:

Periksa apakah $23 \equiv 5 \ (mod\ 6)$!

$$a - b = 23 - 5 = 18$$

Karena $6 \mid 18$, maka benar bahwa $23 \equiv 5 \ (mod\ 6)$, dapat ditulis sebagai.

$$23 = 5 + 3 \times 6$$

B. Matriks

Matriks merupakan suatu susunan bilangan berbentuk persegi panjang yang disusun secara teratur dalam baris dan kolom. Setiap bilangan dalam susunan tersebut disebut sebagai entri matriks (Anton & Rorres, 2013). Dalam konteks sistem persamaan linear, matriks digunakan untuk

merepresentasikan koefisien-koefisien dari persamaan tersebut dalam bentuk entri-entri matriks.

Definisi 2.1.1 (Matriks)

Matriks A berordo $m \times n$ merupakan susunan elemen-elemen bilangan yang tersusun dalam bentuk persegi panjang berukuran m baris dan n kolom sebagai berikut:

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \quad (2.4)$$

Matriks tersebut berukuran (ordo) $m \times n$ atau $A = (a_{ij})$.

Matriks berukuran $n \times n$ disebut matriks persegi. Sementara itu, matriks yang memiliki satu baris dan n kolom, yaitu berordo $1 \times n$, disebut matriks baris atau vektor baris. Adapun matriks yang terdiri atas n baris dan satu kolom, yakni berordo $n \times 1$, disebut matriks kolom atau vektor kolom (Anton & Rorres, 2013).

1. Operasi Matriks

   Definisi 2.1.2 (Perkalian Matriks)

   Jika A merupakan matriks berukuran $m \times r$ dan B merupakan matriks berukuran $r \times n$, maka hasil kali AB adalah sebuah matriks berukuran $m \times n$. Setiap entri pada posisi baris ke-i dan kolom ke-j dari matriks AB diperoleh dengan mengalikan elemen-elemen yang bersesuaian antara

baris ke-i dari matriks A dan kolom ke-j dari matriks B, kemudian menjumlahkan seluruh hasil perkalian tersebut.

Contoh 1:

Misalkan diberikan dua buah matriks A dan B, masing – masing berukuran 3×3, sebagai berikut:

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}, B = \begin{bmatrix} 9 & 8 & 7 \\ 6 & 5 & 4 \\ 3 & 2 & 1 \end{bmatrix}$$

Hasil perkalian dua matriks tersebut adalah matriks C berukuran 3×3 seperti berikut.

$$C = \begin{bmatrix} 30 & 24 & 18 \\ 84 & 69 & 54 \\ 138 & 114 & 90 \end{bmatrix}$$

2. Determinan Matriks

Definisi 2.1.3 (Hasil Kali Elementer)

Hasil kali elementer dari suatu matriks persegi $A_{n \times n}$ didefinisikan sebagai hasil perkalian dari $n$entri matriks A, dengan ketentuan bahwa tidak ada dua entri yang berasal dari baris atau kolom yang sama.

Definisi 2.1.4 (Minor - Kofaktor)

Jika A merupakan matriks persegi, maka minor dari entri a_{ij} dilambangkan dengan M_{ij}, yaitu determinan dari submatriks yang diperoleh dengan menghapus baris ke-i dan kolom ke-j dari matriks A. Nilai $(-1)^{i+j} M_{ij}$ disebut sebagai kofaktor dari entri a_{ij} dan dilambangkan dengan C_{ij}.

Contoh 2:

Hitung minor dan kofaktor entri a_{11} matriks $A = \begin{bmatrix} 2 & 4 & 1 \\ 3 & 1 & 5 \\ 1 & 2 & 2 \end{bmatrix}$

Minor dari entri a_{11} adalah.

$$M_{11} = \begin{bmatrix} 1 & 5 \\ 2 & 2 \end{bmatrix} = 1(2) - 5(2) = -8$$

Kofaktor dari entri a_{11} adalah.

$$C_{11} = (-1)^{1+1} M_{11} = 1(-8) = -8$$

Definisi 2.1.5 (Determinan)

Misalkan A merupakan suatu matriks persegi. Fungsi determinan dinotasikan dengan det, dan didefinisikan bahwa det(A) xmerupakan jumlah dari seluruh hasil kali elementer bertanda dari matriks A. Nilai det(A)disebut sebagai determinan dari matriks A.

Teorema 2.1.1. Jika A adalah suatu matriks persegi yang memiliki satu baris yang seluruh elemennya bernilai nol, maka berlaku $\det(A) = 0$.

Bukti:

Karena setiap hasil kali elementer bertanda dari matriks A memuat satu elemen dari setiap baris matriks tersebut, maka masing-masing hasil kali elementer bertanda akan mengandung elemen dari

baris yang seluruhnya bernilai nol. Akibatnya, setiap hasil kali elementer bertanda bernilai nol.

Contoh 3:

Hitunglah determinan dari matriks: $A = \begin{bmatrix} 2 & 4 & 1 \\ 3 & 1 & 5 \\ 1 & 2 & 2 \end{bmatrix}$

$$\det(A) = \begin{bmatrix} 2 & 4 & 1 \\ 3 & 1 & 5 \\ 1 & 2 & 2 \end{bmatrix}$$

$$= (-1)^{1+1}2\begin{vmatrix} 1 & 5 \\ 2 & 2 \end{vmatrix} + (-1)^{1+2}4\begin{vmatrix} 3 & 5 \\ 1 & 2 \end{vmatrix} + (-1)^{1+3}1\begin{vmatrix} 3 & 1 \\ 1 & 2 \end{vmatrix}$$

$$= 2(2-10) - 4(6-5) + 1(6-1)$$

$$= -15$$

3. Invers Matriks

Definisi 2.1.6 (Invers)

Jika A merupakan suatu matriks persegi dan terdapat matriks B berukuran sama sehingga memenuhi $AB = BA = I$, maka matriks A disebut dapat dibalik (*invertible*), sedangkan matriks B disebut sebagai invers dari A (Anton & Rorres, 2013).

Definisi 2.1.7 (Kofaktor-Adjoin)

Jika A merupakan suatu matriks persegi dan C_{ij} menyatakan kofaktor dari elemen a_{ij}, maka matriks .

$$C = \begin{bmatrix} C_{11} & C_{12} & \dots & C_{1n} \\ C_{21} & C_{22} & \dots & C_{2n} \\ \vdots & \vdots & & \vdots \\ C_{n1} & C_{n2} & \dots & C_{nn} \end{bmatrix}$$

Disebut matriks kofaktor dari A. Transpos dari matriks ini disebut adjoin dari A dan dinyatakan sebagan $adj(A)$.

Teorema 2.1.2. Jika A suatu matriks yang dapat dibalik, maka

$$A^{-1} = \frac{1}{\det(A)} adj(A) \tag{2.5}$$

Bukti:

Akan ditunjukkan bahwa.

$$A \cdot adj(A) = \det(A) \cdot I$$

Perhatikan hasil kali.

$$A \cdot adj(A) = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} C_{11} & C_{21} & \dots & C_{j1} & \dots & C_{n1} \\ C_{12} & C_{22} & \dots & C_{j2} & \dots & C_{n2} \\ \vdots & \vdots & & \vdots & & \vdots \\ C_{1n} & C_{2n} & \dots & C_{jn} & \dots & C_{nn} \end{bmatrix}$$

Entri pada baris ke-i dan kolom ke-j dari hasil kali $A \cdot adj(A)$ adalah.

$$a_{i1}C_{j1} + a_{i2}C_{j2} + \cdots + a_{in}C_{jn} \tag{2.6}$$

Jika $i = j$, maka persamaan (2.6) merepresentasikan ekspansi kofaktor dari det(A)sepanjang baris ke-i pada matriks A. Namun, apabila $i \neq j$, maka seluruh elemen a dan kofaktornya berasal dari baris yang berbeda dalam A, sehingga hasil dari persamaan (2.6) bernilai nol. Oleh karena itu.

$$A \cdot adj(A) = \begin{bmatrix} \det(A) & 0 & \dots & 0 \\ 0 & \det(A) & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \det(A) \end{bmatrix} = \det(A) \cdot I \qquad (2.7)$$

Karena A dapat dibalik, $\det(A) \neq 0$. Karena itu, persamaan (2.7) dapat ditulis kembali sebagai.

$$\frac{1}{\det(A)}[A \cdot adj(A)] = I \qquad (2.8)$$

Atau

$$A \cdot \left[\frac{1}{\det(A)} \cdot adj(A)\right] = I \qquad (2.9)$$

Dengan mengalikan kedua sisi dengan A^{-1} menghasilkan.

$$A^{-1} = \frac{1}{\det(A)} adj(A) \qquad (2.10)$$

Suatu matriks A memiliki invers apabila A merupakan matriks persegi dan determinannya tidak sama dengan nol ($\det(A) \neq 0$). Apabila nilai determinan A sama dengan nol ($\det(A) = 0$), maka matriks tersebut disebut matriks singular. Invers dari matriks A dinotasikan dengan A^{-1}.

Contoh 4:

Carilah invers dari matriks

$$A = \begin{bmatrix} 2 & 4 & 1 \\ 3 & 1 & 5 \\ 1 & 2 & 2 \end{bmatrix}$$

$$\det(A) = \begin{bmatrix} 2 & 4 & 1 \\ 3 & 1 & 5 \\ 1 & 2 & 2 \end{bmatrix}$$

$$= (-1)^{1+1}2\begin{vmatrix}1 & 5\\ 2 & 2\end{vmatrix} + (-1)^{1+2}4\begin{vmatrix}3 & 5\\ 1 & 2\end{vmatrix} + (-1)^{1+3}1\begin{vmatrix}3 & 1\\ 1 & 2\end{vmatrix}$$

$$= 2(2-10) - 4(6-5) + 1(6-1)$$

$$= -15$$

Cari kofaktor matriks A.

Baris 1.

$$C_{11} = (+1)\cdot\begin{vmatrix}1 & 5\\ 2 & 2\end{vmatrix} = 1(2) - 5(2) = -8$$

$$C_{12} = (-1)\cdot\begin{vmatrix}3 & 5\\ 1 & 2\end{vmatrix} = -(3(2) - 5(1)) = -1$$

$$C_{13} = (+1)\cdot\begin{vmatrix}3 & 1\\ 1 & 2\end{vmatrix} = 3(2) - 1(1) = 5$$

Baris 2.

$$C_{21} = (-1)\cdot\begin{vmatrix}4 & 1\\ 2 & 2\end{vmatrix} = -(4(2) - 1(2)) = -6$$

$$C_{22} = (+1)\cdot\begin{vmatrix}2 & 1\\ 1 & 2\end{vmatrix} = 2(2) - 1(1) = 3$$

$$C_{23} = (-1)\cdot\begin{vmatrix}2 & 4\\ 1 & 2\end{vmatrix} = -(2(2) - 4(1)) = 0$$

Baris 3.

$$C_{31} = (+1)\cdot\begin{vmatrix}4 & 1\\ 1 & 5\end{vmatrix} = 4(5) - 1(1) = 19$$

$$C_{32} = (-1)\cdot\begin{vmatrix}2 & 1\\ 3 & 5\end{vmatrix} = -\big(2(5) - 1(3)\big) = -7$$

$$C_{33} = (+1)\cdot\begin{vmatrix}2 & 4\\ 3 & 1\end{vmatrix} = 2(1) - 4(3) = -10$$

$$kof(A) = \begin{bmatrix} -8 & -1 & 5 \\ -6 & 3 & 0 \\ 19 & -7 & -10 \end{bmatrix}$$

Transpos matriks kofaktor

$$adj(A) = \begin{bmatrix} -8 & -6 & 19 \\ -1 & 3 & -7 \\ 5 & 0 & -10 \end{bmatrix}$$

$$A^{-1} = \frac{1}{-15} \cdot \begin{bmatrix} -8 & -6 & 19 \\ -1 & 3 & -7 \\ 5 & 0 & -10 \end{bmatrix} = \begin{bmatrix} \frac{8}{15} & \frac{2}{5} & -\frac{19}{15} \\ \frac{1}{15} & -\frac{1}{5} & \frac{7}{15} \\ -\frac{1}{3} & 0 & \frac{2}{3} \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} \frac{8}{15} & \frac{2}{5} & -\frac{19}{15} \\ \frac{1}{15} & -\frac{1}{5} & \frac{7}{15} \\ -\frac{1}{3} & 0 & \frac{2}{3} \end{bmatrix}$$

4. Kongruensi Matriks

Misalkan A dan B merupakan matriks berukuran $r \times n$ yang memiliki elemen-elemen berupa bilangan bulat, dengan elemen ke-(i, j) masing-masing dinyatakan sebagai a_{ij} dan b_{ij}. Matriks A dikatakan kongruen terhadap matriks B modulo m, apabila $a_{ij} \equiv b_{ij} (\text{mod } m)$untuk setiap pasangan indeks (i, j) dengan $1 \leq i \leq r$ dan $1 \leq j \leq n$. Hubungan ini dinotasikan dengan $A \equiv B (\text{mod } m)$.

Contoh 5:

$$\begin{bmatrix} 15 & 14 \\ 16 & 30 \end{bmatrix} \equiv \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} (mod\ 13)$$

C. Kriptografi

Kriptografi merupakan ilmu yang mempelajari teknik–teknik matematika untuk menjaga kerahasiaan dan keamanan informasi dari pihak yang tidak berwenang (Stinson, 2005). Menurut (Stallings, 1995) kriptografi tidak hanya menyediakan kerahasiaan, tetapi juga aspek penting lainnya seperti autentikasi, integritas data, dan non-repudiation.

1. Terminologi dalam Kriptografi

   a. Pesan

      Pesan (*message*) merupakan data atau informasi yang dapat dibaca serta dipahami maknanya. Pesan dapat berbentuk teks, citra (*image*), suara atau bunyi (*audio*), video, maupun bentuk biner lainnya, baik dalam format digital maupun analog.

   b. *Plaintext*

      Plaintext merupakan pesan asli berupa kumpul karakter yang dapat berupa abjad, angka atau simbol yang dapat dibaca dan memiliki makna.

   c. *Ciphertext*

      Ciphertext adalah pesan yang telah mengalami proses penyandian sehingga bentuknya tidak lagi dapat dibaca atau dipahami maknanya, sehingga tidak dapat dimengerti oleh pihak yang tidak berwenang.

d. Enkripsi

Enkripsi merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiannya menggunakan proses penyandian plainteks menjadi cipherteks. Proses enkripsi menerima masukan berupa plainteks dan kunci kemudian menghasilkan sebuah cipherteks.

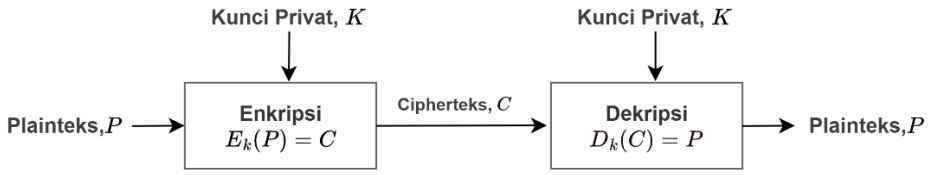
e. Dekripsi

Dekripsi merupakan proses untuk mengubah *ciphertext* kembali menjadi *plaintext*. Proses ini menggunakan *ciphertext* dan kunci sebagai masukan, kemudian menghasilkan *plaintext* sebagai keluarannya.

2. Algoritma Kriptografi

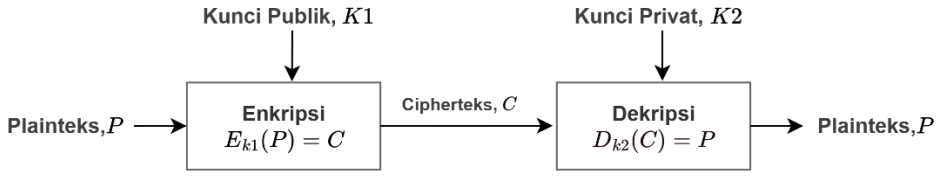
a. Algoritma Simetri

Algoritma simetri adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Untuk menggunakan algoritma ini, penerima pesan harus tahu kunci. Contoh algoritma yang memakai kunci simetri adalah *Hill Cipher, Advance Encryption Standard (AES), One Time Pad*, dan lain sebagainya.



Gambar 2. 1. Proses enkripsi dan dekripsi algoritma simetri

Algoritma asimetri adalah algoritma yang menggunakan kunci berbeda untuk proses enkripsi dan dekripsinya. Algoritma asimetri memiliki kelebihan yaitu kunci untuk enkripsi dibuat umum (public key) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsinya hanya diketahui oleh orang yang berwenang atau sering disebut kunci pribadi (private key).



Gambar 2. 2. Proses Enkripsi dan Dekripsi Algoritma Asimetri

D. *Hill Cipher*

Hill Cipher dikembangkan oleh seorang matematikawan yaitu Lester S. Hill pada tahun 1929. *Hill Cipher* termasuk kriptosistem polygrafik. Sebuah poly grafik adalah sebuah cipher dimana plaintext dibagi dalam sebuah group yang berdekatan dari panjang n, dan kemudian setiap group ditransformasikan ke dalam sebuah group yang berbeda dari n (Jamaludin, 2018).

Metode *Hill Cipher* menggunakan matriks kunci sebagai kunci enkripsi. eks yang akan dienkripsi dibagi menjadi blok-blok yang memiliki ukuran yang sama dengan matriks kunci. Setiap blok teks diubah menjadi vektor kolom dan dikalikan dengan matriks kunci. Hasil perkalian tersebut menghasilkan teks terenkripsi. Salah satu syarat penting dalam metode Hill

Cipher adalah determinan matriks kunci harus relatif prima dengan ukuran alfabet yang digunakan. Misalkan untuk karakter ASCII 256 atau PBB(d, 256) = 1, dimana Jika determinan matriks kunci tidak memenuhi syarat ini, matriks invers dari matriks kunci tidak akan ada, dan metode Hill Cipher tidak dapat diterapkan.

Proses enkripsi pada algoritma Hill Cipher diterapkan pada setiap blok teks asli (plaintext). Ukuran setiap blok disesuaikan dengan ukuran matriks kunci yang digunakan. Sebelum teks dibagi menjadi beberapa blok, plaintext terlebih dahulu dikonversi ke dalam bentuk bilangan berdasarkan tabel ASCII 256. Secara matematis, tahapan enkripsi pada Hill Cipher dapat dinyatakan sebagai berikut.

$$C = K \cdot P \; mod \; N \tag{2.11}$$

Keterangan:

C : *Ciphertext*

P : *Plaintext*

K : Matriks Kunci

N : Nilai modulo

Proses dekripsi pada Hill Cipher pada dasarnya memiliki tahapan yang serupa dengan proses enkripsinya. Perbedaannya terletak pada penggunaan invers dari matriks kunci, yang harus terlebih dahulu dihitung sebelum proses dekripsi dilakukan.

$$K^{-1} = \frac{1}{\det(K)} adj(K) \tag{2.12}$$

Keterangan:

$\det(K)$: Determinan matriks kunci

$adj(K)$: Adjoin matriks kunci

K^{-1} : Invers matriks kunci

Jika invers matriks kunci berupa bilangan pecahan, konversikan matriks kunci menjadi bilangan bulat. Kemudian untuk mendapatkan *plaintext* kembali menggunakan rumus.

$$P = K^{-1}C \ mod \ N \tag{2.13}$$

Keterangan:

P : *plaintext*

C : *ciphertext*

K^{-1} : invers matriks kunci

N : nilai modulo

(Pangaribuan, 2018)

E. *Advance Hill Cipher*

Algoritma *Advance Hill Cipher* diusulkan Acharya, mereka mengklain bahwa algoritma *Advance Hill Cipher* lebih aman dibandingkan dengan *Hill Cipher* asli (Acharya et al., 2009). Pada kasus enkripsi, algoritma *Advance Hill Cipher* menggunakan matriks kunci involutori. Suatu matriks A dikatakan suatu matrix involutori, jika matriks tersebut merupakan inversnya. Perkalian terhadap matriks A dikatakan involusi, jika $A^2 = I$. (Azam, 2020)

Berikut ini merupakan sifat – sifat dari matriks involutori.

1. $A = A^{-1}/A^2 = I$.
2. $\det(A) = \pm 1$.
3. A dikatakan involutori jika $\frac{1}{2}(A + I)$ idempoten.
4. A involutori, B involutori maka AB juga involutori.
5. Untuk n = genap $A^n = I$ dan untuk n = ganjil $A^n = A$.
6. Matriks dengan periode 2 adalah involutori.
7. A involutori jika $a_{11} + a_{22} \equiv 0$.
8. $|A| = -1$ jika $a_{11} + a_{22} \equiv 0$.
9. $\det(I) = 1 \Longrightarrow \det(A)$ harus berupa angka yang kuadratnya harus 1.

F. *ElGamal*

Algoritma *ElGamal* termasuk dalam jenis algoritma kriptografi asimetris yang pertama kali diperkenalkan oleh Taher ElGamal pada tahun 1985. Dasar keamanan algoritma ini bertumpu pada permasalahan logaritma diskrit. *ElGamal* terdiri atas tiga tahapan utama, yaitu pembentukan kunci, enkripsi, dan dekripsi. Dalam proses enkripsi dan dekripsi, algoritma ini melibatkan beberapa parameter yang bersifat rahasia maupun publik.

Besaran yang bersifat tidak rahasia atau yang dapat diketahui pengirim dan penerima yaitu:

1. Bilangan prima p.
2. Akar primitif g dengan $g < p$.
3. y yang diperoleh dari perhitungan $y = g^d mod\ p$.
4. Kunci publik yang terdiri dari (y, g, p).

5. Ciphertext a dan b.

Kemudian besaran yang bersifat rahasia hanya diketahui oleh penerima saja atau pengirim saja seperti.

1. Plaintext P.
2. Sembarang bilangan bulat d dengan $1 \leq d \leq p-2$.
3. Pilih acak elemen matriks r dengan $r \in \{0, 1, 2, \dots, p-2\}$.
4. Kunci privat d.

1. Proses Pembentukan Kunci

Algoritma *ElGamal* memerlukan sepasang kunci yang dibentuk melalui penentuan sebuah bilangan prima p dan dua bilangan acak g dan x. Kedua bilangan acak tersebut harus memenuhi ketentuan $g < p$ dan $1 \leq x \leq p-2$, serta digunakan dalam pembentukan persamaan tertentu yang menjadi dasar proses kriptografi *ElGamal*.

$$y = g^x mod\ p \tag{2.14}$$

Keterangan:

y : kunci publik

g : generator (akar primitif dari bilangan prima)

p : bilangan prima

2. Proses Enkripsi

Proses enkripsi pada algoritma *ElGamal* menggunakan kunci publik (y, g, p) serta sebuah bilangan acak k yang memenuhi syarat $1 \leq k \leq p-2$.

Setiap karakter pada pesan dienkripsi menggunakan nilai k yang berbeda, sehingga tingkat keamanan *ciphertext* yang dihasilkan menjadi lebih tinggi.

$$a = g^k mod\ p \qquad (2.15a)$$

$$b = m\ y^k mod\ p \qquad (2.15b)$$

Keterangan:

g : *generator* (akar primitif dari bilangan prima).

m : *Plaintext*.

p : Bilangan prima.

Proses enkripsi pada algoritma *ElGamal* akan menghasilkan kode dalam bentuk blok yang terdiri atas dua nilai (a, b).

3. Proses Dekripsi

Pada proses dekripsi digunakan sepasang kunci pribadi (x, p) untuk mendekripsi (a, b) menjadi plaintext dengan persamaan:

$$m = b \cdot c\ mod\ p \qquad (2.16a)$$

Nilai dari variabel c didapat dengan menggunakan persamaan:

$$c = a^{p-1-x}\ mod\ p \qquad (2.16b)$$

Keterangan:

m : *Plaintext.*

b : Ciphertext.

p : Bilangan prima.

(Stallings, 1995)

G. Representasi Matematis Citra Digital

Citra Digital merupakan gambaran atau representasi dari suatu objek pada bidang dua dimensi. Dalam bentuk matematisnya citra digital didefiniskan pada fungsi dua dimensi $f(x, y)$, dimana x dan y merupakan koordinat spasial, dan amplitudo f di titik koordinat (x, y) dinamakan intensitas atau level keabuan pada citra di titik tersebut (Gonzalez, 2009).

1. **Pencuplikan (*Sampling*)**

Pencuplikan atau *sampling* adalah proses mendiskritisasi koordinat spasial citra. Sebuah citra analog dapat dinotasikan sebagai fungsi $f(x, y)$ yang bersifat kontinu, artinya fungsi tersebut memiliki nilai pada setiap titik koordinat x dan y. Untuk melakukan citra diskrit, dilakukan proses pendefinisian nilai fungsi pada interval spasial spesifik. Secara matematis dapat direpresentasikan sebagai.

$$f(m, n) = f(m\Delta x, n\Delta y) \tag{2.17}$$

dimana Δx dan Δy adalah bilangan ril konstan yang disebut sebagai interval pencuplikan (*sampling intervals*). Persamaan ini menunjukkan bahwa koordinat diskrit (m, n) merupakan hasil pemetaan dari koordinat kontinu berdasarkan interval tersebut (Jayaraman, 2009). Dalam konteks citra berwarna, fungsi $f(m, n)$ pada persamaan (2.7) tidak bernilai tunggal, melainkan merupakan representasi vektor yang memuat intensitas dari tiga kanal warna (*red, green blue*).

$$f(m, n) = \begin{bmatrix} f_R(m, n) \\ f_G(m, n) \\ f_B(m, n) \end{bmatrix}$$

Hal ini menunjukkan bahwa setiap elemen matriks citra hasil pencuplikan menyimpan informasi warna yang lengkap dalam struktur tiga dimensi.

2. **Kuantisasi**

Setelah koordinat spasial didiskritisasi melalui *sampling*, nilai intensitas dari fungsi $f(x, y)$ pada tiap piksel masih berada dalam bentuk bilangan ril kontinu. Oleh karena itu, diperlukan tahap kuantisasi, yaitu proses mengubah nilai intensitas kontinu tersebut menjadi nilai bilangan bulat (*integer*) yang terbatas (Jayaraman, 2009).

Kuantisasi memetakan rentang intensitas kontinu ke dalam himpunan nilai diskrit. Jumlah tingkatan nilai yang tersedia ditentuijkan oleh kedalaman bit atau B, dengan hubungan:

$$L = 2^B$$

Dalam konteks citra digital berwarna, misalnya untuk kedalaman 8-bit ($B = 8$). Hal ini menghasilkan $2^8 = 256$ tingkatan intensitas diskrit untuk masing – masing kanal *Red*, *Green* dan *Blue* (Jain, 1989).

3. **Matriks Hasil Digitalisasi**

Citra digital diperoleh melalui dua proses utama yaitu *sampling spasial* dan kuantisasi intensitas. *Sampling spasial* mengubah citra kontinu menjadi kumpulan titik diskret (piksel), sedangkan kuantisasi mengubah nilai intensitas kontinu menjadi bilangan bulat dalam rentang terbatas (misalnya 0–255 untuk citra 8-bit). Hasil akhirnya adalah representasi diskret berupa matriks, yang menjadi dasar bagi seluruh operasi pengolahan citra digital.

Sebuah citra digital dapat dibentuk dalam sebuah matriks $M \times N$ berupa.

$$A = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,N-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,N-1} \\ \cdots & \cdots & \cdots & \\ f(M-1,0) & f(M-1,1) & \cdots & f(M-1,N-1) \end{bmatrix}$$

Setiap elemen pada matriks citra disebut sebagai piksel. Dalam citra digital, terdapat hubungan antara koordinat dan tingkat keabuan (gray-level). Koordinat menunjukkan posisi suatu entri dalam matriks citra, sedangkan tingkat keabuan merepresentasikan nilai dari setiap piksel yang menentukan warna pada citra tersebut. Nilai tingkat keabuan ini berkaitan dengan digit biner (bit) yang tersusun dari angka 0 dan 1. Seluruh variasi warna pada piksel berasal dari kombinasi tiga warna utama, yaitu merah, hijau, dan biru.

H. *Peak Signal-to-Noise Ratio* (PSNR)

PSNR (Peak Signal-to-Noise Ratio) merupakan metrik yang digunakan untuk menilai kualitas suatu citra dengan membandingkan kekuatan sinyal (citra asli) terhadap kekuatan derau atau noise (gangguan yang menurunkan kualitas citra). Nilai PSNR dinyatakan dalam satuan desibel (dB), yang menggunakan skala logaritmik karena rentang nilai pada data citra umumnya sangat luas.

Metode ini banyak digunakan untuk menilai hasil kompresi *lossy*, yaitu jenis kompresi yang menghilangkan sebagian data guna mengurangi ukuran file. Dalam konteks ini, sinyal merujuk pada citra asli, sedangkan derau merupakan kesalahan atau distorsi yang muncul akibat proses kompresi.

Walaupun PSNR bukan merupakan ukuran yang sepenuhnya akurat, metrik ini memberikan gambaran umum tentang seberapa baik kualitas citra hasil kompresi menurut persepsi visual manusia.

Secara umum, untuk citra 8-bit, nilai PSNR yang dianggap baik berada pada kisaran 30 hingga 50 dB. Sedangkan pada citra 16-bit yang memiliki kualitas lebih tinggi, nilai PSNR biasanya berada dalam rentang 60 hingga 80 dB (Sara et al., 2019).

PSNR dinyatakan sebagai:

$$PSNR = 10 \log_{10} \left(\frac{peakval^2}{MSE} \right) \tag{2.17}$$

Keterangan:

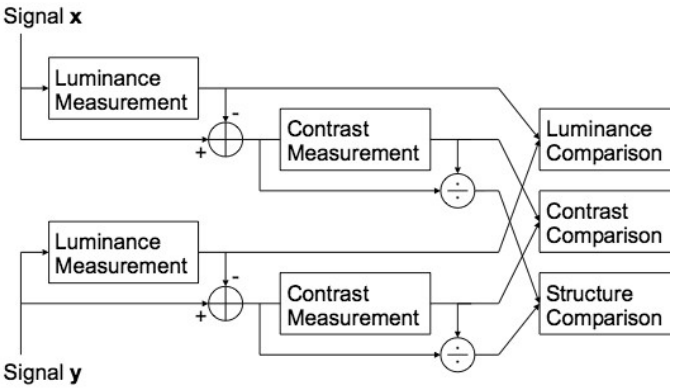
$peakval$: nilai piksel maksimum

MSE : mean squared error

I. *Structural Similarity Index Measure* (SSIM)

SSIM merupakan kualitas metric yang digunakan untuk mengukur kemiripan diantara 2 citra dan dipercaya berkorelasi dengan kualitas persepsi *Human Visual System* (HVS) . Model SSIM dibuat dengan memperhatikan 3 faktor yaitu *loss of correlation*, *luminanced distortion* dan *contrast distortion*. Persamaan SSIM dapat dilihat pada.

$$SSIM(f, g) = l(f, g)c(f, g)s(f, g) \tag{2.18}$$



Gambar 2. 3. Diagram Sistem Pengukuran SSIM

Dengan faktor – faktornya yaitu:

$$\begin{cases} l(f,g) = \dfrac{2\mu_f\mu_g + C_1}{\mu_f^2 + \mu_g^2 + C_1} \\ c(f,g) = \dfrac{2\sigma_f\sigma_g + C_2}{\sigma_f^2 + \sigma_g^2 + C_2} \\ s(f,g) = \dfrac{2\sigma_{fg} + C_3}{\sigma_f\sigma_g + C_3} \end{cases}$$

Fungsi $l(f,g)$ merepresentasikan perbandingan luminansi yang digunakan untuk menilai tingkat kesamaan nilai rata-rata luminansi dari dua citra, yaitu μ_f dan μ_g. Nilai maksimum dari $l(f,g)$ adalah 1, yang dicapai ketika $\mu_f = \mu_g$.

Selanjutnya, $c(f,g)$ menunjukkan perbandingan kontras yang mengukur kesamaan nilai simpangan baku dari dua citra, yakni σ_f dan σ_g. Nilai tertinggi dari $c(f,g)$ juga bernilai 1, dan hal ini terjadi apabila $\sigma_f = \sigma_g$.

Adapun $s(f,g)$ merupakan perbandingan struktur yang menggambarkan tingkat korelasi antara dua citra f dan g, dengan σ_{fg} sebagai nilai kovarian di antara keduanya.

Nilai *Structural Similarity Index Measure* (SSIM) berada dalam rentang 0 hingga 1. Nilai 0 menunjukkan bahwa kedua citra tidak memiliki kesamaan struktur, sedangkan nilai 1 menandakan bahwa kedua citra identik atau $f = g$. Konstanta C_1, C_2, dan C_3digunakan untuk mencegah penyebut bernilai nol dalam perhitungan (Wulandari, 2017).

J. *Mean Square Error* (MSE)

Mean Squared Error (MSE) merupakan salah satu metode evaluasi kuantitatif yang umum digunakan dalam bidang pengolahan citra digital untuk mengukur tingkat distorsi antara dua citra, yakni citra asli dan citra hasil transformasi, baik berupa enkripsi maupun dekripsi. Metrik ini memberikan gambaran numerik mengenai seberapa besar perbedaan piksel antara dua citra dengan menghitung rata-rata kuadrat dari selisih intensitas piksel pada posisi yang bersesuaian.

Secara matematis, MSE dapat dinyatakan sebagai berikut:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j}^{N}[I(i,j) - K(i,j)]^2 \qquad (2.19)$$

dengan:

$I(i,j)$: nilai intensitas piksel pada koordinat (i,j) dari citra asli.

$K(i,j)$: nilai intensitas piksel pada koordinat (i,j) dari citra hasil dekripsi atau enkripsi.

M : jumlah baris dari citra.

N : jumlah kolom dari citra.

Nilai MSE yang rendah menunjukkan bahwa perbedaan antara citra yang dibandingkan relatif kecil, sedangkan nilai yang tinggi mengindikasikan adanya perbedaan yang signifikan.

BAB III

METODOLOGI PENELITIAN

A. Jenis Penelitian

Penelitian ini menggunakan metode penelitian kepustakaan atau studi pustaka. Kutipan informasi diperoleh dari buku, artikel atau skripsi-skripsi terdahulu dan dikumpulkan sesuai dengan judul.

B. Jenis dan Sumber Data

Data yang digunakan dalam penelitian ini berupa data citra digital yang berukuran $n \times n$ piksel dimana n genap dan format citra **.jpg* yang diperoleh dari *standard image test.*

C. Waktu dan Tempat Pengambilan Data

Data penelitian tersebut diambil dari *standard image test*, pada bulan Oktober 2025.

D. Prosedur Penelitian

Adapun langkah – langkah yang dilakukan untuk mendapatkan tujuan penelitian dengan menggunakan metode kriptografi *Advance Hill Cipher* dengan kunci terenkripsi *ElGamal* yaitu:

1. Persiapan Data
   a. Mengumpulkan beberapa citra digital berwarna yang akan digunakan sebagai data uji coba.
2. Penerapan Algoritma

a. Pembentukan Kunci

1) Membentuk matriks kunci untuk algoritma *Advance Hill Cipher* yang invertibel modulo 256.

2) Menghasilkan pasangan kunci publik dan privat untuk algoritma *ElGamal*.

b. Proses Enkripsi

1) Mengenkripsi citra digital menggunakan *Advance Hill Cipher* dengan matriks kunci.

2) Mengenkripsi matriks kunci menggunakan *ElGamal*.

c. Proses Dekripsi

1) Mendekripsi matriks kunci menggunakan *ElGamal*.

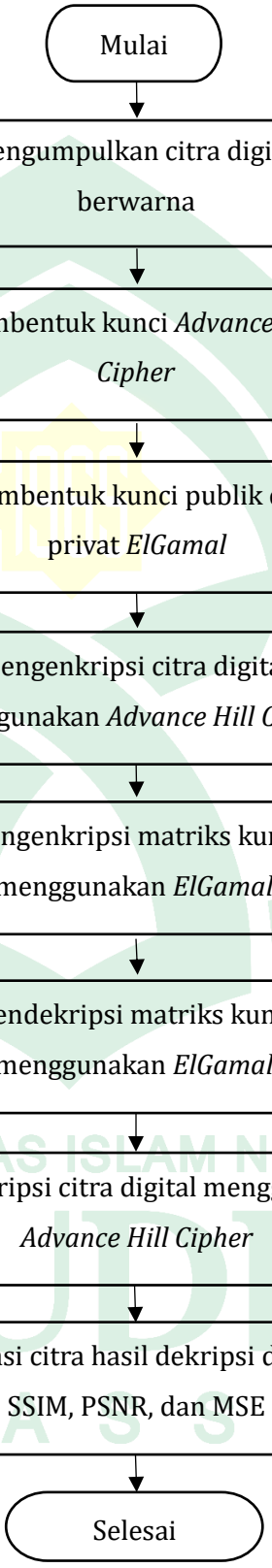
2) Mendekripsi citra menggunakan *Advance Hill Cipher* dengan matriks kunci dekripsi.

3. Evaluasi Hasil

a. Menilai kualitas citra hasil enkripsi dan dekripsi menggunakan SSIM, PSNR dan MSE.

b. Mengamati hasil visual untuk memastikan citra dapat dikenali.

E. Flowchart Penelitian



BAB IV

HASIL DAN PEMBAHASAN

A. Data Citra Digital

Citra digital yang digunakan dalam penelitian ini merupakan citra digital berwarna hasil proses *sampling* dan kuantisasi 8-bit. Sesuai dengan batasan masalah yang telah ditetapkan, data yang digunakan adalah citra berformat *.jpg* dengan ukuran $n \times n$, untuk keperluan ilustrasi digunakan citra yang digunakan 256×256 piksel. Data citra yang digunakan.

Gambar 4. 1 Citra Asli

Sebagai ilustrasi penyederhanaan proses, pembahasan ini hanya menyajikan operasional algoritma pada blok pertama kanal *Red*. Meskipun demikian, langkah-langkah matematis yang didemonstrasikan tersebut berlaku secara konstan dan menyeluruh untuk setiap blok hasil partisi pada matriks kanal *Red*, *Green* maupun *Blue*, hingga seluruh dimensi citra digital tersebut terenkripsi secara sempurna.

Adapun nilai intensitas piksel pada blok pertama kanal *Red* tersebut adalah sebagai berikut.

$$P_R = \begin{bmatrix} 117 & 120 & 122 & 122 \\ 112 & 113 & 116 & 118 \\ 118 & 118 & 119 & 122 \\ 123 & 123 & 125 & 127 \end{bmatrix}$$

B. Proses Enkripsi dan Dekripsi Citra Digital

1. Pembentukan Matriks Kunci Involutori (*Advance Hill Cipher*)

Sesuai dengan batasan masalah yang ditetapkan, matriks kunci K yang digunakan adalah matriks yang berordo $n \times n$ dimana n adalah genap. Untuk keperluan ilustrasi perhitungan, dipilih $n = 4$ (matriks 4×4). Proses pembentukan kunci simetris untuk algoritma *Advance Hill Cipher* akan merujuk pada algoritma yang diuraikan oleh Acharya et. al. (2009). Algoritma ini mengkonstruksi matriks kunci K berordo $n \times n$, dimana n harus genap dan matriks kunci tersebut akan bersifat involutori ($K^2 = I$).

$$K = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$$

Proses pembentukan kunci diawali dengan memilih matriks A_{22} berordo 2×2 secara acak. Pada penelitian ini, dipilih.

$$A_{22} = \begin{bmatrix} 102 & 179 \\ 92 & 14 \end{bmatrix} (mod\ 256)$$

Selanjutnya, perhitungan matriks A_{11} ditentukan berdasarkan $A_{11} = -A_{22}\ (mod\ 256)$. Perhitungan ini menghasilka n.

$$A_{11} = -\begin{bmatrix} 102 & 179 \\ 92 & 14 \end{bmatrix} = \begin{bmatrix} -102 & -179 \\ -92 & -14 \end{bmatrix} (mod\ 256) = \begin{bmatrix} 154 & 77 \\ 164 & 242 \end{bmatrix}$$

Kemudian, dipilih sebuah skalar k yang koprima dengan 256 (harus ganjil). Dipilih $k = 7$. Invers dari k, yaitu $k^{-1} = 7^{-1}\ (mod\ 256)$, dihitung menggunakan algoritma *Extended Euclidean* dan diperoleh $k^{-1} = 183$.

Matriks A_{12} dihitung menggunakan formula $A_{12} = k(I - A_{11})\ mod\ 256$, di mana I adalah matriks identitas 2×2. Perhitungan ini dilakukan sebagai berikut.

$$A_{12} = 7\left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} - \begin{bmatrix}154 & 77\\ 164 & 242\end{bmatrix}\right)\ mod\ 256$$

$$A_{12} = 7\begin{bmatrix}103 & 179\\ 92 & 15\end{bmatrix}\ mod\ 256$$

$$A_{12} = \begin{bmatrix}721 & 1253\\ 644 & 105\end{bmatrix}\ mod\ 256$$

$$A_{12} = \begin{bmatrix}209 & 229\\ 132 & 105\end{bmatrix}$$

Setelah itu, A_{21} dihitung menggunakan formula komplementer $A_{21} = k^{-1}(I + A_{11})\ mod\ 256$.

$$A_{21} = 183\left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + \begin{bmatrix}154 & 77\\ 164 & 242\end{bmatrix}\right)\ mod\ 256$$

$$A_{21} = 183\left(\begin{bmatrix}155 & 77\\ 164 & 243\end{bmatrix}\right)\ mod\ 256$$

$$A_{21} = \begin{bmatrix}28365 & 14091\\ 30012 & 44469\end{bmatrix}\ mod\ 256$$

$$A_{21} = \begin{bmatrix}205 & 11\\ 60 & 181\end{bmatrix}$$

Dengan menyusun kembali keempat sub-matriks tersebut, diperoleh matriks kunci K berordo 4×4 yaitu:

$$K = \begin{bmatrix}A_{11} & A_{12}\\ A_{21} & A_{22}\end{bmatrix} = \begin{bmatrix}154 & 77 & 209 & 229\\ 164 & 242 & 132 & 105\\ 205 & 11 & 102 & 179\\ 60 & 181 & 92 & 14\end{bmatrix}$$

Validasi matematis terhadap K menunjukkan bahwa $\det(K) \equiv 1 \ (mod\ 256)$ (memenuhi syarat *invertible*) dan $K^2 \equiv I \ (mod\ 256)$ (memenuhi involutori). Dengan demikian, matriks ini valid untuk digunakan dalam penelitian ini.

2. Penentuan Parameter dan Pembangkitan Kunci *ElGamal*

Proses pembangkitan kunci (*Key Generation*) *ElGamal* terdiri dari beberapa langkah matematis. Pertama, dipilih sebuah bilangan prima p berukuran besar dan sebuah generator g (atau akar primitif) dari p. Kedua parameter ini bersifat publik. Selanjutnya, dipilih sebuah bilangan bulat acak d yang akan berfungsi sebagai kunci privat (rahasia), dengan batasan $1 \leq x \leq p-2$. Terakhir, komponen kunci publik y dihitung melalui proses eksponensiasi modular dengan persamaan $y = g^x \ mod\ p$.

Berikut proses pembentukan kunci *ElGamal*.

a. Menentukan sebuah bilangan prima $p = 65537$ yang akan mendefinisikan grup $(\mathbb{Z}^*_{65537}, \times)$.
b. Memilih akar primitif pada grup $(\mathbb{Z}^*_{65537}, \times)$ maka $\phi(65537) = 65536$, karena 65537 merupakan bilangan prima. Dari himpunan generator yang valid untuk grup ini, dipilih $g = 3$.
c. Memilih sembarang bilangan bulat $x = 1640$ sebagai kunci privat yang memenuhi $1 \leq x \leq 65535$.
d. Menghitung komponen kunci publik y melalui eksponensiasi modular menggunakan persamaan $y = g^x \ mod\ p$ sebagai berikut.

$$y = g^x \ mod\ p = 3^{1640} \ mod\ 65537 = 30969$$

e. Sehingga diperoleh kunci publik $(y, g, p) = (30969, 3, 65537)$ dan kunci privat $x = 1640$.

Berikut alur pembentukan kunci algoritma ElGamal.

Flowcharttt

3. **Proses Enkripsi Citra Menggunakan Algoritma *Advance Hill Cipher***

Setelah matriks kunci involutori K berhasil dibentuk dan diamankan, langkah selanjutnya adalah menerapkan proses enkripsi terhadap citra digital berwarna menggunakan algoritma *Advance Hill Cipher*. Citra berformat *.jpg* diproses per kanal warna (*Red, Green*, dan *Blue*), masing – masing direpresentasikan sebagai matriks intensitas piksel berukuran $n \times n$ dimana n genap dengan nilai piksel dalam rentang 0-255 (*8-bit*)

Proses enkripsi dilakukan secara terpisah namun identik untuk setiap kanal warna (*Red, Green*, dan *Blue*). Berdasarkan ordo matriks kunci K yang digunakan, yaitu 4×4, maka matriks piksel dari setiap kanal dipartisi menjadi blok – blok P yang juga berordo 4×4.

Persamaan matematis untuk proses enkripsi pada satu blok P adalah sebagai berikut :

$$C = K \cdot (K \cdot P)^T \ (mod\ 256)$$

Dimana:

K : matriks kunci involutori 4×4

P : blok plaintext (piksel) 4×4

C : blok *ciphertext* (piksel terenkripsi) 4×4

Misalnya, dilakukan ilustrasi pada blok pertama 16 piksel pertama kanal *Red* (P_R) berordo 4×4 piksel, dengan matriks intensitas dan matriks kunci K sebagai berikut:

$$P_R = \begin{bmatrix} 117 & 120 & 122 & 122 \\ 112 & 113 & 116 & 118 \\ 118 & 118 & 119 & 122 \\ 123 & 123 & 125 & 127 \end{bmatrix}, K = \begin{bmatrix} 154 & 77 & 209 & 229 \\ 164 & 242 & 132 & 105 \\ 205 & 11 & 102 & 179 \\ 60 & 181 & 92 & 14 \end{bmatrix}$$

$$P_{temp} = K \cdot P_R \ (mod\ 256)$$

$$P_{temp} = \begin{bmatrix} 154 & 77 & 209 & 229 \\ 164 & 242 & 132 & 105 \\ 205 & 11 & 102 & 179 \\ 60 & 181 & 92 & 14 \end{bmatrix} \begin{bmatrix} 117 & 120 & 122 & 122 \\ 112 & 113 & 116 & 118 \\ 118 & 118 & 119 & 122 \\ 123 & 123 & 125 & 127 \end{bmatrix} (mod\ 256)$$

Berikut adalah penjabaran perhitungan untuk setiap elemen $P_{temp}(i, j)$ (baris i dari K dikalikan kolom j dari P_R).

$$P_{temp}(1,1) = (154 \cdot 117) + (77 \cdot 112) + (209 \cdot 118) + (229 \cdot 123)$$
$$= 18018 + 8624 + 24662 + 28167 = 79471$$
$$\equiv 111\ (mod\ 256)$$

$$P_{temp}(1,2) = (154 \cdot 120) + (77 \cdot 113) + (209 \cdot 118) + (229 \cdot 123)$$
$$= 18480 + 8701 + 24662 + 28167 = 80010$$
$$\equiv 138\ (mod\ 256)$$

$$P_{temp}(1,3) = (154 \cdot 122) + (77 \cdot 116) + (209 \cdot 119) + (229 \cdot 125)$$
$$= 18788 + 8932 + 24871 + 28625 = 81216 \equiv 64\ (mod\ 256)$$

$$P_{temp}(1,4) = (154 \cdot 122) + (77 \cdot 118) + (209 \cdot 122) + (229 \cdot 127)$$
$$= 18788 + 9086 + 25498 + 29083 = 82455 \equiv 23\ (mod\ 256)$$

$$P_{temp}(2,1) = (164 \cdot 117) + (242 \cdot 112) + (132 \cdot 118) + (105 \cdot 123)$$
$$= 19188 + 27104 + 15576 + 12915 = 74783$$
$$\equiv 31 \ (mod\ 256)$$
$$P_{temp}(2,2) = (164 \cdot 120) + (242 \cdot 113) + (132 \cdot 118) + (105 \cdot 123)$$
$$= 19680 + 27{,}346 + 15576 + 12915 = 75517$$
$$\equiv 253 (mod\ 256)$$
$$P_{temp}(2,3) = (164 \cdot 122) + (242 \cdot 116) + (132 \cdot 119) + (105 \cdot 125)$$
$$= 20008 + 28072 + 15708 + 13125 = 76913$$
$$\equiv 113 \ (mod\ 256)$$
$$P_{temp}(2,4) = (164 \cdot 122) + (242 \cdot 118) + (132 \cdot 122) + (105 \cdot 127)$$
$$= 20008 + 28556 + 16104 + 13335 = 78003$$
$$\equiv 179 \ (mod\ 256)$$
$$P_{temp}(3,1) = (205 \cdot 117) + (11 \cdot 112) + (102 \cdot 118) + (179 \cdot 123)$$
$$= 23985 + 1232 + 12036 + 22017 = 59270$$
$$\equiv 134 \ (mod\ 256)$$
$$P_{temp}(3,2) = (205 \cdot 120) + (11 \cdot 113) + (102 \cdot 118) + (179 \cdot 123)$$
$$= 24600 + 1243 + 12036 + 22017 = 59896$$
$$\equiv 127 \ (mod\ 256)$$
$$P_{temp}(3,3) = (205 \cdot 122) + (11 \cdot 116) + (102 \cdot 119) + (179 \cdot 125)$$
$$= 25010 + 1276 + 12138 + 22375 = 60799$$
$$\equiv 248 \ (mod\ 256)$$

$$P_{temp}(3,4) = (205 \cdot 122) + (11 \cdot 118) + (102 \cdot 122) + (179 \cdot 127)$$

$$= 25010 + 1298 + 12444 + 22733 = 61485 \equiv 45 \ (mod\ 256)$$

$$P_{temp}(4,1) = (60 \cdot 117) + (181 \cdot 112) + (92 \cdot 118) + (14 \cdot 123)$$

$$= 7020 + 20272 + 10856 + 1{,}722 = 39870 \equiv 190 \ (mod\ 256)$$

$$P_{temp}(4,2) = (60 \cdot 120) + (181 \cdot 113) + (92 \cdot 118) + (14 \cdot 123)$$

$$= 7200 + 20453 + 10856 + 1722 = 40231 \equiv 39 \ (mod\ 256)$$

$$P_{temp}(4,3) = (60 \cdot 122) + (181 \cdot 116) + (92 \cdot 119) + (14 \cdot 125)$$

$$= 7320 + 20996 + 10948 + 1750 = 41014 \equiv 54 \ (mod\ 256)$$

$$P_{temp}(4,4) = (60 \cdot 122) + (181 \cdot 118) + (92 \cdot 122) + (14 \cdot 127)$$

$$= 7320 + 21358 + 11224 + 1778 = 41680 \equiv 208 \ (mod\ 256)$$

Setelah semua elemen dihitung, hasil matriks temporer P_{temp} adalah:

$$P_{temp} = \begin{bmatrix} 111 & 138 & 64 & 23 \\ 31 & 253 & 113 & 179 \\ 134 & 248 & 127 & 45 \\ 190 & 39 & 54 & 208 \end{bmatrix}$$

Hasil dari enkripsi level pertama ini kemudian dilakukan operasi transpose $P_{trans} = \left(P_{temp}\right)^T$ untuk mengacak posisi elemen-elemen matriks, menghasilkan:

$$P_{trans} = \begin{bmatrix} 111 & 31 & 134 & 190 \\ 138 & 253 & 248 & 39 \\ 64 & 113 & 127 & 54 \\ 23 & 179 & 45 & 208 \end{bmatrix}$$

Selanjutnya, dilakukan enkripsi level kedua dengan mengalikan kembali matriks kunci K dengan matriks P_{trans} untuk mendapatkan blok *ciphertext* final.

$$C_R = K \cdot P_{trans} \ (mod\ 256)$$

$$C_R = \begin{bmatrix} 154 & 77 & 209 & 229 \\ 164 & 242 & 132 & 105 \\ 205 & 11 & 102 & 179 \\ 60 & 181 & 92 & 14 \end{bmatrix} \begin{bmatrix} 111 & 31 & 134 & 190 \\ 138 & 253 & 248 & 39 \\ 64 & 113 & 127 & 54 \\ 23 & 179 & 45 & 208 \end{bmatrix} (mod\ 256)$$

Berikut adalah penjabaran perhitungan untuk setiap elemen $P_R(i,j)$ (baris i dari K dikalikan kolom j dari P_{trans}).

$$C_R(1,1) = (154 \cdot 111) + (77 \cdot 138) + (209 \cdot 64) + (229 \cdot 23)$$
$$= 17094 + 10626 + 13376 + 5267 = 46363 \equiv 27\ (mod\ 256)$$

$$C_R(1,2) = (154 \cdot 31) + (77 \cdot 253) + (209 \cdot 113) + (229 \cdot 179)$$
$$= 4774 + 19481 + 23617 + 40991 = 88863 \equiv 31\ (mod\ 256)$$

$$C_R(1,3) = (154 \cdot 134) + (77 \cdot 248) + (209 \cdot 127) + (229 \cdot 45)$$
$$= 20636 + 19096 + 26543 + 10305 = 76580$$
$$\equiv 36\ (mod\ 256)$$

$$C_R(1,4) = (154 \cdot 190) + (77 \cdot 39) + (209 \cdot 54) + (229 \cdot 208)$$
$$= 29260 + 3003 + 11286 + 47632 = 91181 \equiv 45\ (mod\ 256)$$

$$C_R(2,1) = (164 \cdot 111) + (242 \cdot 138) + (132 \cdot 64) + (105 \cdot 23)$$
$$= 18204 + 33396 + 8448 + 2415 = 62463 \equiv 255\ (mod\ 256)$$

$$C_R(2,2) = (164 \cdot 31) + (242 \cdot 253) + (132 \cdot 113) + (105 \cdot 179)$$
$$= 5084 + 61226 + 14916 + 18795 = 100021$$
$$\equiv 181\ (mod\ 256)$$

$$C_R(2,3) = (164 \cdot 134) + (242 \cdot 248) + (132 \cdot 127) + (105 \cdot 45)$$
$$= 21976 + 60016 + 16764 + 4725 = 103481$$
$$\equiv 57\ (mod\ 256)$$

$$C_R(2,4) = (164 \cdot 190) + (242 \cdot 39) + (132 \cdot 54) + (105 \cdot 208)$$

$$= 31160 + 9438 + 7128 + 21840 = 69566 \equiv 190 \ (mod\ 256)$$

$$C_R(3,1) = (205 \cdot 111) + (11 \cdot 138) + (102 \cdot 64) + (179 \cdot 23)$$

$$= 22755 + 1518 + 6528 + 4117 = 34918 \equiv 102 \ (mod\ 256)$$

$$C_R(3,2) = (205 \cdot 31) + (11 \cdot 253) + (102 \cdot 113) + (179 \cdot 179)$$

$$= 6355 + 2{,}783 + 11526 + 32041 = 52705 \equiv 225 \ (mod\ 256)$$

$$C_R(3,3) = (205 \cdot 36) + (11 \cdot 57) + (102 \cdot 7) + (179 \cdot 218)$$

$$= 7380 + 627 + 714 + 39022 = 47743 \equiv 127 \ (mod\ 256)$$

$$C_R(3,4) = (205 \cdot 45) + (11 \cdot 190) + (102 \cdot 199) + (179 \cdot 227)$$

$$= 9225 + 2090 + 20298 + 40633 = 72246 \equiv 54 \ (mod\ 256)$$

$$C_R(4,1) = (60 \cdot 27) + (181 \cdot 255) + (92 \cdot 102) + (14 \cdot 216)$$

$$= 1620 + 46155 + 9384 + 3024 = 60183 \equiv 23 \ (mod\ 256)$$

$$C_R(4,2) = (60 \cdot 31) + (181 \cdot 181) + (92 \cdot 225) + (14 \cdot 139)$$

$$= 1860 + 32761 + 20700 + 1946 = 57267 \equiv 179 \ (mod\ 256)$$

$$C_R(4,3) = (60 \cdot 36) + (181 \cdot 57) + (92 \cdot 7) + (14 \cdot 218)$$

$$= 2160 + 10317 + 644 + 3052 = 16173 \equiv 45 \ (mod\ 256)$$

$$C_R(4,4) = (60 \cdot 45) + (181 \cdot 190) + (92 \cdot 199) + (14 \cdot 227)$$

$$= 2700 + 34390 + 18308 + 3178 = 58576 \equiv 208 \ (mod\ 256)$$

Setelah semua elemen dihitung, hasil matriks untuk blok pertama kanal *Red* adalah:

$$C_R = \begin{bmatrix} 111 & 31 & 134 & 190 \\ 138 & 253 & 248 & 39 \\ 64 & 113 & 127 & 54 \\ 23 & 179 & 45 & 208 \end{bmatrix}$$

Blok C_R ini merepresentasikan 16 piksel terenkripsi untuk kanal *Red*. Proses iteratif yang sama kemudian diterapkan pada blok P_G (*Green*) dan P_B (*Blue*), serta diulangi untuk seluruh blok piksel hingga keseluruhan citra selesai dienkripsi

4. **Proses Enkripsi Matriks Kunci Menggunakan *ElGamal***

Setelah matriks kunci involutori $K_{4\times4}$ dibentuk, langkah berikutnya mengamankan distribusi kunci tersebut dengan mengenkripsi matriks menggunakan algoritma *ElGamal*, yang merupa5kan kriptosistem asimetris berbasis *discrete logarithm problem*.

Parameter dan kunci *ElGamal* yang telah dibangkitkan sebelumnya dan digunakan dalam simulasi ini adalah:

a. Kunci publik $(y, g, p) = (30969, 3, 65537)$

b. Kunci privat $x = 1640$

Matriks kunci K berordo 4×4 yang akan dienkripsi adalah.

$$\begin{bmatrix} 154 & 77 & 209 & 229 \\ 164 & 242 & 132 & 105 \\ 205 & 11 & 102 & 179 \\ 60 & 181 & 92 & 14 \end{bmatrix}$$

Proses enkripsi ElGamal diaplikasikan pada setiap elemen (entri) matriks K secara individual. Matriks K berordo 4×4 ini dipetakan menjadi 16 nilai pesan $m_1, m_2, \ldots, m_{16}$ dimana $m_1 = 154, m_2 = 77$, dan seterusnya.

Untuk setiap pesan m_i, sebuah bilangan bulat acak k_i harus dipilih (dengan$1 \leq k_i \leq p - 2$). *Ciphertext* yang dihasilkan untuk setiap elemen adalah pasangan $(a_i, b_{i)}$, yang dihitung menggunakan persamaan:

a. $a_i = g^{k_i} \ (mod\ p)$

b. $b = m_i \cdot y^{k_i} \ (mod\ p)$

Untuk mendemonstrasikan proses ini, berikut adalah simulasi perhitungan untuk matriks kunci K.

Enkripsi Elemen $K(1,1) = 154$:

a. Pesan $m_1 = 154$

b. Dipilih bilangan acak $k_1 = 48599$.

c. Komponen a_1 dihitung sebagai

$$a_1 = g^{k_1} \ (mod\ p) = 3^{48599} \ (mod\ 65537) = 44784.$$

d. Komponen b_1 dihitung sebagai

$$b_1 = m_1 \cdot g^{k_1} \ (mod\ p) = 154 \cdot 30969^{48599} \ (mod\ 65537) = 37910$$

e. Hasil *ciphertext* C_1 untuk elemen $K(1,1)$ adalah $(44784, 37910)$

Enkripsi Elemen $K(1,2) = 77$:

a. Pesan $m_2 = 77$

b. Dipilih bilangan acak $k_2 = 18025$.

c. Komponen a_2 dihitung sebagai

$$a_2 = g^{k_2} \ (mod\ p) = 3^{18025} \ (mod\ 65537) = 5739.$$

d. Komponen b_2 dihitung sebagai

$$b_2 = m_2 \cdot g^{k_2} \ (mod\ p) = 77 \cdot 30969^{18025} \ (mod\ 65537) = 9159$$

e. Hasil *ciphertext* C_2 untuk elemen $K(1,2)$ adalah $(5739, 9159)$

Enkripsi Elemen $K(1,3) = 209$:

a. Pesan $m_3 = 209$

b. Dipilih bilangan acak $k_3 = 16050$.

c. Komponen a_3 dihitung sebagai

$$a_3 = g^{k_3} \ (mod\ p) = 3^{16050} \ (mod\ 65537) = 22376.$$

d. Komponen b_3 dihitung sebagai

$$b_3 = m_3 \cdot g^{k_3} \ (mod\ p) = 209 \cdot 30969^{16050} \ (mod\ 65537) = 3459$$

e. Hasil *ciphertext* C_3 untuk elemen $K(1,3)$ adalah $(22376, 3459)$

Enkripsi Elemen $K(1,4) = 229$:

a. Pesan $m_4 = 229$

b. Dipilih bilangan acak $k_4 = 14629$.

c. Komponen a_4 dihitung sebagai

$$a_4 = g^{k_4} \ (mod\ p) = 3^{14629} \ (mod\ 65537) = 48234.$$

d. Komponen b_4 dihitung sebagai

$$b_4 = m_4 \cdot g^{k_4} \ (mod\ p) = 229 \cdot 30969^{14629} \ (mod\ 65537) = 5638$$

e. Hasil *ciphertext* C_4 untuk elemen $K(1,4)$ adalah $(48234, 5638)$

Enkripsi Elemen $K(2,1) = 164$:

a. Pesan $m_5 = 164$

b. Dipilih bilangan acak $k_5 = 9145$.

c. Komponen a_5 dihitung sebagai

$$a_5 = g^{k_5} \ (mod\ p) = 3^{9145} \ (mod\ 65537) = 4270.$$

d. Komponen b_5 dihitung sebagai

$$b_5 = m_5 \cdot g^{k_5} \ (mod\ p) = 164 \cdot 30969^{9145} \ (mod\ 65537) = 11980$$

e. Hasil *ciphertext* C_5 untuk elemen $K(2,1)$ adalah $(4270, 11980)$

Enkripsi Elemen $K(2,2) = 242$:

a. Pesan $m_6 = 242$

b. Dipilih bilangan acak $k_6 = 48266$.

c. Komponen a_6 dihitung sebagai

$$a_6 = g^{k_6} \ (mod\ p) = 3^{48266} \ (mod\ 65537) = 20687.$$

d. Komponen b_6 dihitung sebagai

$$b_6 = m_6 \cdot g^{k_6} \ (mod\ p) = 242 \cdot 30969^{48266} \ (mod\ 65537) = 17453$$

e. Hasil *ciphertext* C_6 untuk elemen $K(2,2)$ adalah $(20687, 17453)$

Enkripsi Elemen $K(2,3) = 132$:

a. Pesan $m_7 = 132$

b. Dipilih bilangan acak $k_7 = 6718$.

c. Komponen a_7 dihitung sebagai

$$a_7 = g^{k_7} \ (mod\ p) = 3^{6718} \ (mod\ 65537) = 4305.$$

d. Komponen b_7 dihitung sebagai

$$b_7 = m_7 \cdot g^{k_7} \ (mod\ p) = 132 \cdot 30969^{6718} \ (mod\ 65537) = 15831$$

e. Hasil *ciphertext* C_7 untuk elemen $K(2,3)$ adalah $(4305, 15831)$

Enkripsi Elemen $K(2,4) = 105$:

a. Pesan $m_8 = 105$

b. Dipilih bilangan acak $k_8 = 44349$.

c. Komponen a_8 dihitung sebagai

$$a_8 = g^{k_8} \ (mod\ p) = 3^{44349} \ (mod\ 65537) = 6352.$$

d. Komponen b_8 dihitung sebagai

$$b_8 = m_8 \cdot g^{k_8} \ (mod\ p) = 105 \cdot 30969^{44349} \ (mod\ 65537) = 29593$$

e. Hasil *ciphertext* C_8 untuk elemen $K(2,4)$ adalah $(6352, 29593)$

Enkripsi Elemen $K(3,1) = 205$:

a. Pesan $m_9 = 205$

b. Dipilih bilangan acak $k_9 = 48541$.

c. Komponen a_9 dihitung sebagai

$$a_9 = g^{k_9} \ (mod\ p) = 3^{48541} \ (mod\ 65537) = 30747.$$

d. Komponen b_9 dihitung sebagai

$$b_9 = m_9 \cdot g^{k_9} \ (mod\ p) = 205 \cdot 30969^{48541} \ (mod\ 65537) = 25738$$

e. Hasil *ciphertext* C_9 untuk elemen $K(3,1)$ adalah $(30747, 25738)$

Enkripsi Elemen $K(3,2) = 11$:

a. Pesan $m_{10} = 11$

b. Dipilih bilangan acak $k_{10} = 58470$.

c. Komponen a_{10} dihitung sebagai

$$a_{10} = g^{k_{10}} \ (mod\ p) = 3^{58470} \ (mod\ 65537) = 44195.$$

d. Komponen b_{10} dihitung sebagai

$$b_{10} = m_{10} \cdot g^{k_{10}} \ (mod\ p) = 11 \cdot 30969^{58470} \ (mod\ 65537) = 63776$$

e. Hasil *ciphertext* C_{10} untuk elemen $K(3,2)$ adalah $(44195, 63776)$

Enkripsi Elemen $K(3,3) = 102$:

a. Pesan $m_{11} = 102$

b. Dipilih bilangan acak $k_{11} = 35742$.

c. Komponen a_{11} dihitung sebagai

$$a_{11} = g^{k_{11}} \ (mod\ p) = 3^{35742} \ (mod\ 65537) = 57721.$$

d. Komponen b_{11} dihitung sebagai

$$b_{11} = m_{11} \cdot g^{k_{11}} \ (mod\ p) = 102 \cdot 30969^{35742} \ (mod\ 65537) = 37430$$

e. Hasil *ciphertext* C_{11} untuk elemen $K(3,3)$ adalah $(57721, 37430)$

Enkripsi Elemen $K(3,4) = 179$:

a. Pesan $m_{12} = 179$

b. Dipilih bilangan acak $k_{12} = 5698$.

c. Komponen a_{12} dihitung sebagai

$$a_{12} = g^{k_{12}} \ (mod\ p) = 3^{5698} \ (mod\ 65537) = 18650.$$

d. Komponen b_{12} dihitung sebagai

$$b_{12} = m_{12} \cdot g^{k_{12}} \ (mod\ p) = 179 \cdot 30969^{5698} \ (mod\ 65537) = 27575$$

e. Hasil *ciphertext* C_{12} untuk elemen $K(3,4)$ adalah $(18650, 27575)$

Enkripsi Elemen $K(4,1) = 60$:

a. Pesan $m_{13} = 60$

b. Dipilih bilangan acak $k_{13} = 38699$.

c. Komponen a_{13} dihitung sebagai

$$a_{13} = g^{k_{13}} \ (mod\ p) = 3^{38699} \ (mod\ 65537) = 60596.$$

d. Komponen b_{13} dihitung sebagai

$$b_{13} = m_{13} \cdot g^{k_{13}} \ (mod\ p) = 60 \cdot 30969^{38699} \ (mod\ 65537) = 46117$$

e. Hasil *ciphertext* C_{13} untuk elemen $K(4,1)$ adalah $(60596, 46117)$

Enkripsi Elemen $K(4,2) = 181$:

a. Pesan $m_{14} = 181$

b. Dipilih bilangan acak $k_{14} = 27652$.

c. Komponen a_{14} dihitung sebagai

$$a_{14} = g^{k_{14}} \ (mod\ p) = 3^{27652} \ (mod\ 65537) = 62742.$$

d. Komponen b_{14} dihitung sebagai

$$b_{14} = m_{14} \cdot g^{k_{14}} \ (mod\ p) = 181 \cdot 30969^{27652} \ (mod\ 65537) = 55062$$

e. Hasil *ciphertext* C_{14} untuk elemen $K(4,2)$ adalah $(62742, 55062)$

Enkripsi Elemen $K(4,3) = 92$:

a. Pesan $m_{15} = 92$

b. Dipilih bilangan acak $k_{15} = 2083$.

c. Komponen a_{15} dihitung sebagai

$$a_{15} = g^{k_{15}} \ (mod\ p) = 3^{2083} \ (mod\ 65537) = 5844.$$

d. Komponen b_{15} dihitung sebagai

$$b_{15} = m_{15} \cdot g^{k_{15}} \ (mod\ p) = 92 \cdot 30969^{2083} \ (mod\ 65537) = 30262$$

e. Hasil *ciphertext* C_{15} untuk elemen $K(4,3)$ adalah $(5844, 30262)$

Enkripsi Elemen $K(4,4) = 14$:

a. Pesan $m_{16} = 14$

b. Dipilih bilangan acak $k_{16} = 1953$.

c. Komponen a_{16} dihitung sebagai

$$a_{16} = g^{k_{16}} \ (mod\ p) = 3^{1953} \ (mod\ 65537) = 52111.$$

d. Komponen b_{16} dihitung sebagai

$$b_{16} = m_{16} \cdot g^{k_{16}} \ (mod\ p) = 14 \cdot 30969^{1953} \ (mod\ 65537) = 12677$$

e. Hasil *ciphertext* C_{16} untuk elemen $K(4,4)$ adalah $(52111, 12677)$

Berdasarkan proses enkripsi ElGamal yang dilakukan untuk tiap elemen dari matriks kunci (berjumlah 16 elemen) menggunakan pasangan kunci publik $(y, g, p) = (30969, 65537, 3)$ dan nilai acak *k* yang berbeda untuk setiap elemen. Hasil enkripsi berupa 16 pasangan bilangan, yang secara keseluruhan membentuk ciphertext kunci. Tabel berikut menampilkan hasil lengkap enkripsi matriks kunci tersebut.

Tabel 4. 1 Hasil Enkripsi Elemen Kunci K

Posisi Elemen Kunci	Nilai Elemen (m_i)	Hasil Ciphertext (a_i, b_i)
$K(1,1)$	154	(44784, 37910)
$K(1,2)$	77	(5739, 9159)
$K(1,3)$	209	(22376, 3459)
$K(1,4)$	229	(48234, 5638)
$K(2,1)$	164	(4270, 11980)
$K(2,2)$	242	(20687, 17453)
$K(2,3)$	132	(4305, 15831)
$K(2,4)$	105	(6352, 29593)
$K(3,1)$	205	(30747, 25738)
$K(3,2)$	11	(44195, 63776)
$K(3,3)$	102	(57721, 37430)
$K(3,4)$	179	(18650, 27575)
$K(4,1)$	60	(60596, 46117)
$K(4,2)$	181	(62742, 55062)
$K(4,3)$	92	(5844, 30262)
$K(4,4)$	14	(52111, 12677)

5. **Proses Dekripsi Matriks Kunci Menggunakan *ElGamal***

Setelah matriks kunci $K_{4\times4}$ berhasil dienkripsi menggunakan algoritma *ElGamal* dan dikirim bersama citra *ciphertext* penerima (yang memiliki kunci privat). Selanjutnya, dilakukan proses dekripsi matriks kunci K bertujuan untuk memulihkan matriks kunci simetris K dari himpunan *ciphertext* (a_i, b_i) yang diterima (disajikan pada Tabel 1).

Proses ini memanfaatkan komponen rahasia dari algoritma *ElGamal*, yaitu kunci privat x, yang hanya diketahui oleh penerima. Parameter dan kunci *ElGamal* yang digunakan dalam simulasi dekripsi ini adalah:

a. Kunci publik $(y, g, p) = (30969, 3, 65537)$

b. Kunci privat $x = 1640$

Pada tahap dekripsi kunci menggunakan algoritma *ElGamal*, proses untuk memperoleh kembali pesan asli m_i yang merupakan elemen kunci K dari pasangan ciphertext (a_i, b_i) dinyatakan melalui persamaan matematis berikut:

$$m_i = b_i \cdot a_i^{p-1-x} mod\ p \qquad (\ )$$

Pada kasus ini digunakan $p = 3$ dan $x = 1640$, nilai eksponen (pangkat) yang digunakan untuk dekripsi adalah $p - 1 - x = 65537 - 1 - 1640 = 63896$

Sehingga formula dekripsi yang digunakan adalah.

$$m_i = b_i \cdot a_i^{63896}\ mod\ 65537 \qquad (\ )$$

Berikut adalah simulasi dekripsi untuk memulihkan elemen matriks K dari *ciphertext* yang disajikan pada Tabel 4.1.

Dekripsi $K(1,1)$ dari $C_1 = (44784, 37910)$.

a. Pesan *ciphertext* $(a_1, b_1) = (44784, 37910)$

b. Perhitungan komponen dekripsi.

$$m_1 = b_1 \cdot a_1^{63896}\ mod\ 65537$$
$$= 37910 \cdot 44784^{63896}\ mod\ 65537$$
$$= 154$$

c. Pesan yang dipulihkan adalah 154.

Dekripsi $K(1,2)$ dari $C_2 = (5739, 9159)$.

a. Pesan *ciphertext* $(a_2, b_2) = (5739, 9159)$

b. Perhitungan komponen dekripsi.

$$m_2 = b_2 \cdot a_2^{63896} \; mod \; 65537$$

$$= 9159 \cdot 5739^{63896} \; mod \; 65537$$

$$= 77$$

c. Pesan yang dipulihkan adalah 154.

Posisi Elemen Kunci	**Nilai *Ciphertext* (a_i, b_i)**	**Hasil *Plaintext* (m_i)**
$K(1,1)$	30969, 3, 65537)	154
$K(1,2)$	(44784, 37910)	77
$K(1,3)$	(5739, 9159)	209
$K(1,4)$	(22376, 3459)	229
$K(2,1)$	(48234, 5638)	164
$K(2,2)$	(4270, 11980)	242
$K(2,3)$	(20687, 17453)	132
$K(2,4)$	(4305, 15831)	105
$K(3,1)$	(6352, 29593)	205

$K(3,2)$	(30747, 25738)	11
$K(3,3)$	(44195, 63776)	102
$K(3,4)$	(57721, 37430)	179
$K(4,1)$	(18650, 27575)	60
$K(4,2)$	(60596, 46117)	181
$K(4,3)$	(62742, 55062)	92
$K(4,4)$	(5844, 30262)	14

6. **Proses Dekripsi Citra Menggunakan Algoritma *Advance Hill Cipher***

Proses dekripsi citra bertujuan untuk memulihkan blok *plaintext* P (piksel asli) dari blok *ciphertext* C (piksel terenkripsi), dengan menggunakan matriks kunci K yang telah dipulihkan. Persamaan dekripsi untuk memulihkan P dapat diturunkan sebagai berikut:

$$P = K \cdot (K \cdot C)^T \ (mod\ 256)$$

Misalnya, dilakukan simulasi pada satu blok 16 piksel pertama kanal *Red* (P_R) berordo 4×4 piksel, dengan matriks intensitas dan matriks kunci K sebagai berikut:

$$K = \begin{bmatrix} 154 & 77 & 209 & 229 \\ 164 & 242 & 132 & 105 \\ 205 & 11 & 102 & 179 \\ 60 & 181 & 92 & 14 \end{bmatrix}, C_R = \begin{bmatrix} 111 & 31 & 134 & 190 \\ 138 & 253 & 248 & 39 \\ 64 & 113 & 127 & 54 \\ 23 & 179 & 45 & 208 \end{bmatrix}$$

$$C_{temp} = K \cdot C_R \ (mod\ 256)$$

$$C_{temp} = \begin{bmatrix} 154 & 77 & 209 & 229 \\ 164 & 242 & 132 & 105 \\ 205 & 11 & 102 & 179 \\ 60 & 181 & 92 & 14 \end{bmatrix} \begin{bmatrix} 111 & 31 & 134 & 190 \\ 138 & 253 & 248 & 39 \\ 64 & 113 & 127 & 54 \\ 23 & 179 & 45 & 208 \end{bmatrix} (mod\ 256)$$

Berikut adalah penjabaran perhitungan untuk setiap elemen $C_{temp}(i,j)$ (baris i dari K dikalikan kolom j dari P_R).

$$C_{temp}(1,1) = (154 \cdot 111) + (77 \cdot 138) + (209 \cdot 64) + (229 \cdot 23)$$
$$= 17094 + 10626 + 13376 + 5267 = 46363 \equiv 27 \ (mod\ 256)$$

$$P_{temp}(1,2) = (154 \cdot 31) + (77 \cdot 253) + (209 \cdot 118) + (229 \cdot 123)$$
$$= 18480 + 8701 + 24662 + 28167 = 80010$$
$$\equiv 138 \ (mod\ 256)$$

$$P_{temp}(1,3) = (154 \cdot 122) + (77 \cdot 116) + (209 \cdot 119) + (229 \cdot 125)$$
$$= 18788 + 8932 + 24871 + 28625 = 81216 \equiv 64 \ (mod\ 256)$$

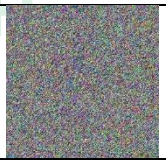
$$P_{temp}(1,4) = (154 \cdot 122) + (77 \cdot 118) + (209 \cdot 122) + (229 \cdot 127)$$
$$= 18788 + 9086 + 25498 + 29083 = 82455 \equiv 23 \ (mod\ 256)$$

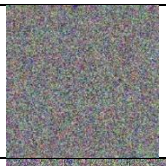
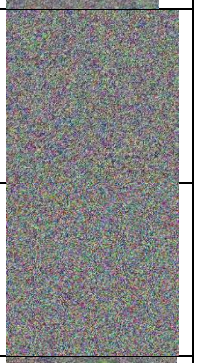
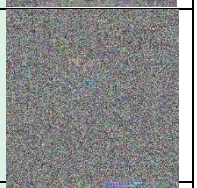
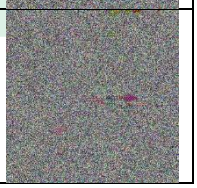
C. Pembahasan Hasil Enkripsi dan Dekripsi Citra Digital

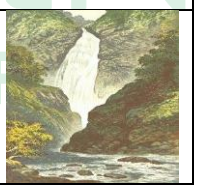
1. Pembahasan Hasil Enkripsi Citra Digital Dengan *Advance Hill Cipher* dan *ElGamal*

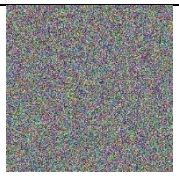
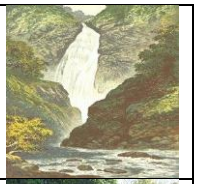
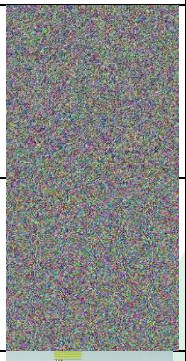
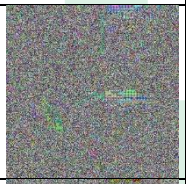
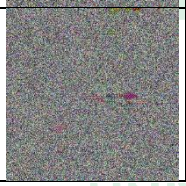
Berikut pengujian menggunakan algoritma *Advance Hill Cipher* dan *ElGamal* terhadap 5 citra digital dengan ukuran yang berbeda dan menggunakan variasi 2 kunci yang berbeda

Tabel 4. 2.

No.	Citra Awal	Ukuran (piksel)	Ukuran Kunci	Lama Proses Enkripsi	Metriks Evaluasi (Citra Asli dan Enkripsi)			Hasil Enkripsi
					MSE	PSNR	SSIM	
1.		256 x 256	2 x 2	0.29	5864.844264	10.45 dB	0.0171	

2.		256 x 256	4x4	0.17	5785.383270	10.51 dB	0.0194	
3.		256 x 256	2x2	0.27	8584.852737	8.79 dB	0.0167	
4.		256 x 256	4x4	0.14	8495.163549	8.84 dB	0.0153	
3.		512 x 512	2 x 2	1.17	8418.921195	8.88 dB	0.0189	
4.		512 x 512	4 x 4	0.36	8223.470736	8.98 dB	0.0171	
5		512 x 512	2x2	1.12	6732.253624	9.85 dB	0.0180	
		512 x 512	4x4	0.33	6901.366336	9.74 dB	0.0175	

No.	Citra eNKRIPSI	Ukuran (piksel)	Ukuran Kunci	Lama Proses Dekripsi	Metriks Evaluasi (Citra Asli dan Dekripsi)			Hasil Enkripsi
					MSE	PSNR	SSIM	
1.		256 x 256	2 x 2	0.31	38.898188	32.23 dB	0.9511	

2.		256 x 256	4x4	0.12 detik	38.898188	32.23 dB	0.9511	
		256 x 256	2x2	0.23 detik	84.666789	28.85 dB	0.9263	
		256 x 256	4x4	0.089 detik	84.666789	28.85 dB	0.9263	
3.		512 x 512	2 x 2	1.17	8418.921195	8.88 dB	0.0189	
4.		512 x 512	4 x 4	0.36	8223.470736	8.98 dB	0.0171	
5		512x512	2x2	1.05	9.314021	38.44 dB	0.9657	
6.		512x512	4x4	0.24	9.314021	38.44 dB	0.9657	

BAB V

PENUTUP

DAFTAR PUSTAKA

Acharya, B., Panigrahy, S. K., Patra, S. K., Kumar Panigrahy, S., & Panda, G. (2009). Image Encryption Using Advanced Hill Cipher Algorithm. In *International Journal of Recent Trends in Engineering* (Vol. 1, Issue 1). https://www.researchgate.net/publication/229012891

Anton, H., & Rorres, C. (2013). *Elementary linear algebra: applications version*. John Wiley & Sons.

APJII. (2024). *Laporan Survei Pengguna Internet APJII 2024*.

Azam, T. (2020). *Cryptanalysis of the Encryption Scheme based on Advanced Hill Cipher Algorithm*.

Fadlilah, S. N., Turmudi, T., & Khudzaifah, M. (2022). Penggabungan Algoritma Hill Cipher dan ElGamal untuk Mengamankan Pesan teks. *Jurnal Riset Mahasiswa Matematika*, *1*(5), 230–235. https://doi.org/10.18860/jrmm.v1i5.14496

Gonzalez, R. C. (2009). *Digital image processing*. Pearson education india.

Hakim, M. L. (2021). *Implementasi algoritma Hill Cipher dan Arnold cat map dalam pemanfaatan enkripsi dan dekripsi citra digital berbasis website*.

Jain, A. K. (1989). *Fundamentals of digital image processing*.

Jamaludin, J. (2018). Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem. *Sinkron: Jurnal Dan Penelitian Teknik Informatika*, *2*(2), 86–93.

Jayaraman, S. (2009). S. Esakkirajan dan T. Veerakumar. In *Digital Image Processing, New Delhi: Tata McGraw-Hill Education Private Limited*.

Khazaei, S., & Ahmadi, S. (2017). Ciphertext-only attack on d × d Hill in O(d13d). *Information Processing Letters*, *118*, 25–29. https://doi.org/10.1016/j.ipl.2016.09.006

Pangaribuan, L. J. (2018). Kriptografi Hybrida Algoritma Hill Cipher Dan RSA Sebagai Pengembangan Kriptografi Kunci Simetris (Studi Kasus: Nilai Mahasiswa Amik Mbp). *Jurnal Teknologi Informasi Dan Komunikasi*, *7*(1), 11–26.

Rosen, K. H. (2019). *Discrete Mathematics and Its Applications*. New York, NY, USA: McGraw-Hill.

Sara, U., Akter, M., & Uddin, M. S. (2019). Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study. *Journal of Computer and Communications*, *07*(03), 8–18. https://doi.org/10.4236/jcc.2019.73002

Stallings, W. (1995). *Network and internetwork security: principles and practice*. Prentice-Hall, Inc.

Stinson, D. R. (2005). *Cryptography: theory and practice*. Chapman and Hall/CRC.

Wulandari, M. (2017). Index Quality Assesment Citra Terinterpolasi (SSIM dan FSIM). *Jurnal Terapan Teknologi Informasi*, *1*(1).