

IMPLEMENTASI ALGORITMA HILL CIPHER UNTUK PROSES ENKRIPSI DATA MENGGUNAKAN MEDIA CITRA DIGITAL

Alun Sujjada ^{a,1,*}, Erlinda Juniar ^{b,2}

^{a, b} Program Studi Teknik Informatika Universitas Nusaputra, Jl. Raya Cibatu Cisaat No.21, Cibolang Kaler, Kec. Cisaat, Kabupaten Sukabumi, Jawa Barat 43152

¹ alun.sujjada@nusaputra.ac.id; ² erlinda.juniar_ti18@nusaputra.ac.id

* Alun Sujjada

ABSTRAK

Melihat kondisi saat ini dimana semakin marak kejahatan pada media digital terutama pada data citra atau media gambar, semakin mengganggu hak dan privasi setiap orang. Banyak sekali bentuk penyalahgunaan yang terjadi pada media digital ini melalui sarana internet seperti penjiplakan karya fotografer, pengakuan hak milik gambar, sampai dengan mengupload foto-foto privasi seseorang ke media internet. Salah satu cara untuk pengamanan data digital dalam bentuk gambar adalah dengan mengacak (enkripsi) gambar-gambar yang dirasa sangat penting sehingga gambar tersebut tidak dapat lagi dimaknai oleh orang lain. Jika kita memerlukan data-data tersebut maka tinggal mengembalikannya (dekripsi) sehingga gambar enkripsi tersebut dapat kembali ke bentuk semula. Algoritma Hill Cipher merupakan salah satu metode untuk mengacak sebuah data dengan cara penyandian dan perkalian matriks. Untuk penerapannya kedalam bentuk data citra diperlukan ujicoba dengan membuat sebuah perangkat lunak yang kemudian akan dianalisa hasilnya kedalam beberapa model warna seperti RGB, Grayscale (Keabuan) dan Thresholding (Hitam Putih). Berdasarkan hasil pengujian maka dapat disimpulkan bahwa semakin besar nilai input matriks dari Algoritma Hill Cipher, maka hasil enkripsi citra yang didapatkan akan semakin maksimal atau dengan kata lain semakin tidak dapat dimengerti bentuk visualnya oleh manusia. Algoritma Hill Cipher tidak dapat diterapkan pada model warna threshold (hitam putih) dikarenakan perkalian matriks yang didapatkan tidak mempunyai nilai kisaran yang beragam.



KATA KUNCI

Keamanan Data
Enkripsi Citra
Algoritma Hill Cipher
Citra Digital

ABSTRACT

With a lot of misuse of digital media especially in form of many image or vision, disturbing people's right and privacy. Digital media misuse are from internet like copying a photographer's creation, claiming an image's copy right until uploading private photos to the internet. Therefore one of the methods to secure digital data by randomizing (encrypting) the images that we feel very important so those images can't be fathomed by others anymore. If we need those data we can taking it back (describing) so the encrypted images can be turned to their former form. Hill cipher algorithm is one of the methods to randomize or encrypt data by passwording and matrix multiplication for its application into vision data form a test is required by making a software that the result latter will be analyzed into several color models like RGB, Grayscale and thresholding (Black and White). From the test result can be concluded that the bigger the matrix input value from the hill cipher algorithm, the more maximal the image encryption obtained or in other words the harder it's visual form to be understood by human. But then Hill Cipher Algorithm can't be used to a threshold color model (Black and White) because the matrix multiplications obtained can't have varied range value.



KEYWORD

Data Security
Image Encryption
Hill Cipher Algorithm
Digital Image



This is an open-access article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license

1. Pendahuluan

Kriptografi adalah sebuah bidang ilmu yang membahas keamanan data. dengan metode untuk menjaga kerahasiaan pesan dari pihak yang tidak berkepentingan dan tidak bertanggung jawab. Pesan dirahasiakan dengan cara mengacak nilai-nilai yang ada didalamnya sehingga dapat menghasilkan pesan yang tidak lagi memiliki arti dan tidak dapat mengambil informasi dari pesan tersebut. Adapun pesan adalah informasi yang dapat berbentuk teks, gambar (citra), audio dan video. Citra digital bisa diartikan menjadi sebuah pesan karena didalamnya terdapat sejumlah informasi yang dapat digunakan sebagai

penunjang aktifitas manusia dalam berinteraksi satu sama lain. Kerahasiaan pesan yang ada pada citra gambar juga dapat dijaga menggunakan metode kriptografi.[1]

Kriptografi di gambaran digital dapat dilakukan dengan cara merubah informasi warna pada setiap pixel yang terdapat pada data citra tersebut. Dengan merubah informasi warna pada setiap pixel maka pesan yang terkandung didalamnya tidak lagi dapat terbaca. Ada beberapa jenis metode kriptografi, salah satunya kriptografi klasik, dimana kriptografi ini merupakan kriptografi yang terdiri dari macam-macam prosedur pemecahan. maka dari itu penulis disini ingin menguji salah satu dari algoritma tersebut. Metode yang akan dibahas disini adalah metode Hill Cipher, yaitu sebuah teknik penyandian dengan menggunakan inspirasi perkalian matriks.[2]

2. Tinjauan Pustaka

A. Sistem Bilangan Biner

Number system atau sering juga disebut system bilangan merupakan satu cara untuk mewakili besaran dari suatu item fisik. Sistem bilangan yang sering digunakan oleh manusia yaitu sistem bilangan desimal, yakni sistem bilangan yang menggunakan 10 simbol untuk mewakili suatu besaran. Manusia lebih banyak dan sering mempergunakan system ini, hal ini dikarenakan manusia hanya memiliki 10 buah jari yang dapat membantu perhitungan bilangan desimal. Beda dengan komputer, logika di komputer terbentuk dalam dua keadaan (*two-state elements*), yaitu keadaan off (tidak ada arus) dan keadaan on (ada arus). Konsep itulah yang saat ini dipakai dalam sistem bilangan biner, yang memakai 2 macam nilai untuk mewakili suatu besaran nilai. Komputer tidak hanya menggunakan bilangan biner (*binary number system*) saja, komputer juga memakai sistem bilangan yang lain, yaitu sistem bilangan oktal (*octal number system*) dan sistem bilangan hexadesimal (*hexadecimal number system*). Sistem bilangan memakai bilangan dasar atau basis (*base* atau disebut juga *radix*) yang tertentu. Basis yang digunakan pada masing-masing sistem bilangan tergantung dari berapa jumlah nilai bilangan yang dipergunakan.

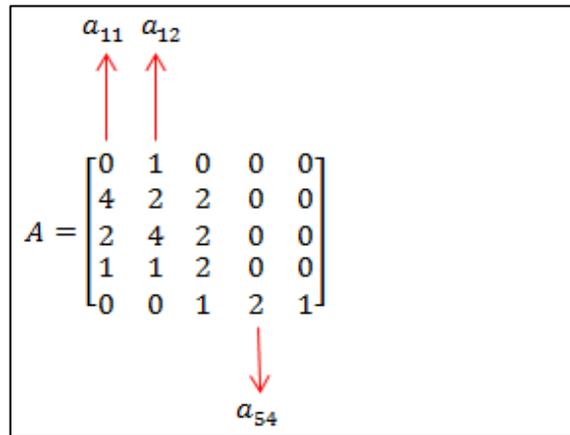
1. Sistem bilangan desimal dengan basis 10 (*deca* berarti 10), memakai 10 macam simbol bilangan; 0,1,2,3,4,5,6,7,8,9
2. Sistem bilangan binari dengan basis 2 (*binary* berarti 2), memakai 2 macam simbol bilangan, yaitu : 0, 1
3. Sistem bilangan oktal dengan basis 8 (*octal* berarti 8), menggunakan 8 macam simbol bilangan, yaitu : 0,1,2,3,4,5,6,7
4. Sistem bilangan hexadesimal dengan basis 16 (*hexa* berarti 6 dan *deca* berarti 10), menggunakan 16 macam simbol bilangan, yaitu : 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F . [3]

B. Matriks

Matriks adalah sekumpulan bilangan yang disusun berdasarkan baris dan kolom, serta ditempatkan di dalam tanda kurung, baik itu kurung biasa () maupun kurung siku []. Matriks mempunyai sebuah ukuran yang disebut dengan *ordo*. *Ordo* matriks ini berdasarkan dari banyak baris dan banyak kolom pada matriks. Jadi jika sebuah matriks A memiliki m baris dan n kolom, maka matriks A tersebut berukuran (*berordo*) $m \times n$.

Masing-masing bilangan yang terdapat di dalam matriks disebut elemen matriks. Elemen-elemen matriks juga memiliki notasi. Jika matriks dinotasikan dengan huruf kapital, maka elemen-elemen matriks dinotasikan dengan huruf kecil dan diberi indeks yang menyatakan letak baris dan kolomnya. Sebagai contoh terdapat matriks A dengan jumlah barisnya 5 (lima) dan jumlah kolomnya juga ada 5 (lima), maka ordonya adalah 5×5 , atau bisa ditulis dengan $A_{5 \times 5}$. Elemen-elemen matriks A dapat dinotasikan dengan A_{ij} , yang menyatakan elemen matriks A pada baris ke-*i* dan kolom ke-*j*. Gambar 2.1 berikut ini adalah contoh dari sebuah matriks.

Sama dengan konsep bilangan, maka setiap matriks dapat dilakukan operasi aritmatika baik dengan vector maupun matriks lainnya. Operasi matematika tersebut meliputi penjumlahan, pengurangan, perkalian dan pembagian dimana setiap operasi tersebut memiliki syarat-syarat yang harus dipenuhi. Matriks dalam konsep pemrograman dituangkan dalam konsep struktur data Array, yaitu penyimpanan data dalam ruang memori dimana setiap ruang tersebut memiliki indeks pengenalan masing-masing.

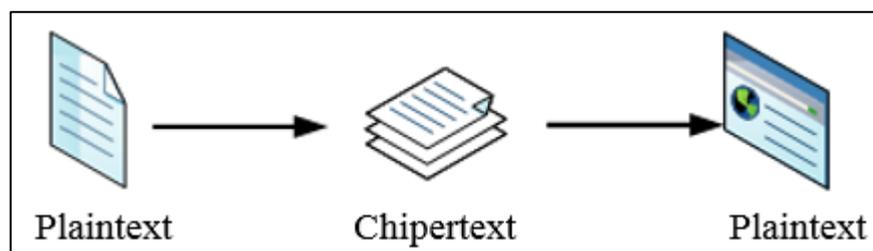


Gambar 2.1 Matriks A

Matriks pada gambar tersebut disebut dengan Matriks A yang mempunyai i(5) baris dan j(5) kolom. Nilai-nilai yang terdapat dalam kurung siku adalah elemen matriks. Sebagai contoh elemen matriks a_{11} maka dapat diartikan Matriks A baris ke 1 kolom ke 1 mempunyai nilai sama dengan 0, matriks a_{12} dapat diartikan Matriks A baris ke 1 kolom ke 2 mempunyai nilai sama dengan 1 dan Matriks a_{54} dapat diartikan Matriks A baris ke 5 kolom ke 4 mempunyai nilai sama dengan 2.

C. Enkripsi dan Dekripsi

Enkripsi yaitu salah satu bagian dari kriptografi, hal ini amat sangat penting agar data yang dikirimkan terjaga kerahasiaannya. Enkripsi juga dapat diartikan dengan chiper atau sering disebut kode, dimana pesan asli (plaintext) diubah menjadi kode-kode tersendiri sesuai metode yang disepakati oleh kedua belah pihak, baik pihak pengirim pesan maupun penerima pesan. Proses enkripsi terlihat seperti pada gambar 2.2 berikut ini:



Gambar 2.2 Proses enkripsi secara umum

Informasi asal yang dapat dimengerti disebut sebagai *plaintext*, kemudian oleh algoritma enkripsi diartikan menjadi informasi acak yang tidak lagi dapat dimengerti dan disebut dengan chipertext. Proses enkripsi terdiri dari algoritma dan kunci. Kunci biasanya merupakan suatu string bit pendek yang mengontrol algoritma. Jika kunci yang digunakan berbeda maka algoritma enkripsi akan memberikan hasil yang berbeda. Perubahan kunci enkripsi ini sendiri dapat merubah output (keluaran) dari algoritma enkripsi. Setelah itu ciphertext ditransmisikan oleh pengirim. Lalu akan dilakukan sebuah proses untuk mengembalikan teks yang telah acak menjadi ke bentuk semula dengan algoritma dan kunci yang sama, dalam hal ini dilakukan oleh penerima, sehingga akan kembali menjadi sebuah informasi yang dapat dipahami oleh penerima atau sering disebut dekripsi.[4]

D. Algoritma Hill Cipher

Kripto sistem polialfabetik yang salah satunya yaitu Hill Cipher, artinya setiap karakter alfabet bisa dipetakan ke lebih dari satu macam karakter alfabet. Cipher tersebut ditemukan pada tahun 1929 oleh Lester S. Hill. Ide dari Hill Cipher adalah misalkan m adalah bilangan bulat positif, Dengan cara mengambil m kombinasi linier dari m karakter alfabet dalam satu elemen plaintext. Misalkan $m=2$, maka kita dapat menuliskan suatu elemen plaintext sebagai $x = (x_1, x_2)$ dan suatu elemen ciphertext sebagai $y = (y_1, y_2)$. Disini (y_1, y_2) adalah kombinasi linier dari x_1 dan x_2 . Sehingga dapat ditulis dalam bentuk persamaan 1 sebagai berikut:

$$y_1 = 11x_1 + 3x_2 \quad (1)$$

$$y_2 = 8x_1 + 7x_2 \quad (2)$$

Sehingga dapat dituliskan kedalam bentuk matrik sebagai berikut:

$$(y_1, y_2) = (x_1, x_2) = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} \quad (3)$$

E. Pengolahan Citra

Pengolahan citra adalah kegiatan memperbaiki kualitas citra agar mudah diinterpretasi oleh manusia/mesin(komputer), kegiatan tersebut sering disebut dengan pengolahan citra. Sebagai media input adalah citra dan outputnya juga citra yang berbeda dengan citra aslinya. Contoh operasi pengolahan citra yaitu misal citra "A" warnanya kurang tajam, kabur (blurring), mengandung noise (misal bintik-bintik putih), sehingga perlu ada proses untuk bisa memperbaiki citra karena citra tersebut menjadi sulit diinterpretasikan karena informasi yang disampaikan tidak lengkap.

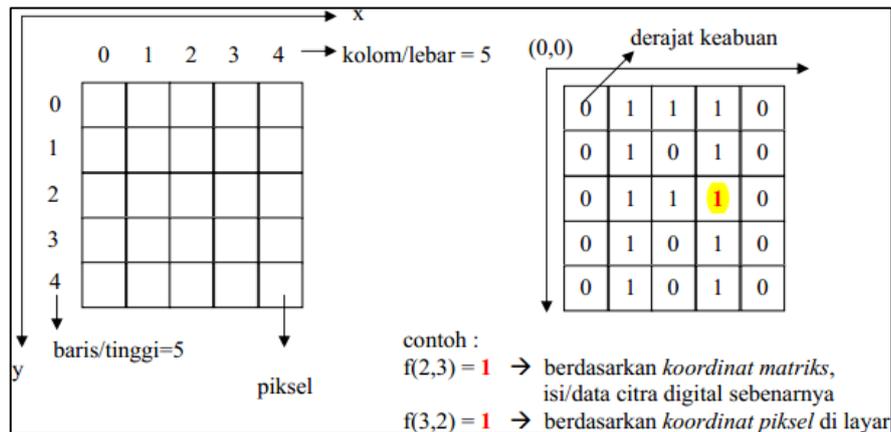
F. Gambar (Citra)

Citra merupakan gambar dua dimensi yang didapat dari gambar analog dua dimensi yang kontinu menjadi gambar diskrit melalui proses sampling. Gambar analog dibagi menjadi N baris dan M kolom sehingga menjadi gambar diskrit. Persilangan antara baris dan kolom tertentu disebut dengan piksel. Contohnya adalah gambar atau titik diskrit pada baris n dan kolom m disebut dengan piksel $[n,m]$. Sedangkan proses untuk menentukan warna pada piksel tertentu pada citra dari sebuah gambar yang kontinu disebut dengan sampling. Proses sampling ini dilakukan dengan mencari rata-rata warna dari gambar analog yang kemudian dibulatkan kedalam angka bulat. Atau sering juga disebut dengan proses digitasi. [5].

G. Format Citra

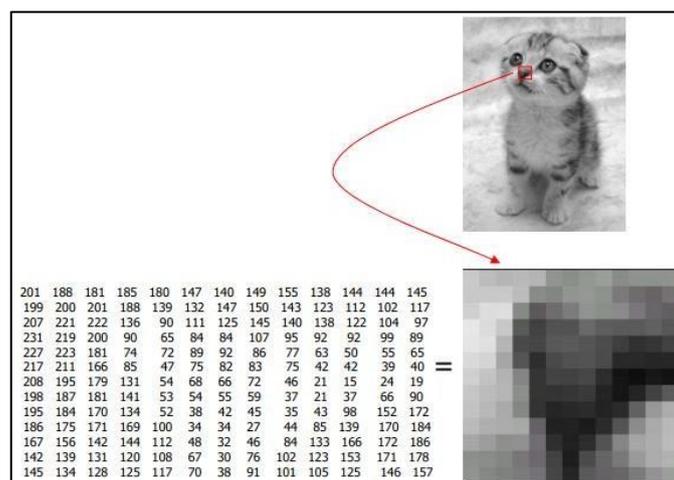
Citra digital biasanya berbentuk persegi panjang, secara visualisasi dimensi ukurannya dinyatakan sebagai (lebar * tinggi) serta dinyatakan dalam titik atau piksel (pixel=picture element). Ukurannya dapat pula dinyatakan dalam satuan panjang (mm atau inci = inch). Satuan panjang tersebut mempengaruhi resolusi yang dimiliki oleh masing-masing citra. Sedangkan banyaknya titik untuk setiap satuan panjang (dot per inch) disebut dengan resolusi. Makin besar resolusi maka makin banyak titik yang terkandung dalam citra, sehingga visualisasinya lebih halus. Resolusi spasial dan resolusi kecermerlangan, berpengaruh pada besarnya informasi citra yang hilang. Resolusi spasial yaitu halus / kasarnya pembagian kisi-kisi baris dan kolom.

Digitalisasi (sampling) merupakan transformasi citra kontinue ke citra digital disebut, misal hasil digitalisasi dengan jumlah baris 256 dan jumlah kolom 256 maka resolusi spasial adalah 256×256 . Sedangkan untuk resolusi kecermerlangan (intensity/brightness) adalah halus/kasarnya pembagian tingkat kecermerlangan. Transformasi data analog yang bersifat kontinue ke daerah intensitas diskrit disebut kuantisasi. Bila intensitas piksel berkisar antara 0 dan 255 maka resolusi kecermerlangan citra adalah 256. Adapun jenis format citra tersusun dari konsep warna hasil tangkapan cahaya oleh mata manusia. Format citra BMP (Bitmap) adalah citra *true color* dengan 24 bit nilai komponen pembentuk warna citra dimana 8 bit untuk representasi warna merah (red), 8 bit warna hijau (green), 8 bit warna biru (blue) sehingga dikenal dengan istilah warna RGB (Red, Green dan Blue). Gambar 2.3 berikut ini adalah ilustrasi dari sebuah citra.



Gambar 2.3 Ilustrasi Citra

Pada ilustrasi tersebut terdapat citra dengan ukuran 5 baris dan 5 kolom dengan penomoran indeks dimulai dari 0, dimana baris disimbolkan dengan sumbu X, dan kolom disimbolkan dengan sumbu Y. Konsep koordinat disesuaikan dengan koordinat monitor yaitu x positif ke arah kanan dan y positif ke arah bawah. Citra tersebut pada struktur data direpresentasikan dalam bentuk array sama dengan nilai pada matriks, dikarenakan memang secara bentuk sama antara representasi citra dengan matriks. Sebagai contoh $f(2,3)$ yaitu fungsi yang menyusun proses sampling pada baris ke 2 kolom ke 3 mempunyai derajat keabuan yaitu 1 (satu).



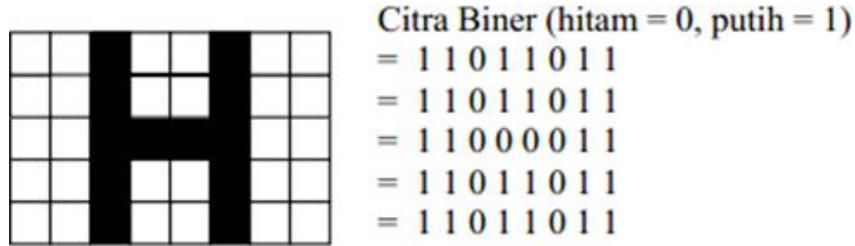
Gambar 2.4 Representasi Citra

Apabila menyimpan gambar kucing ke dalam sebuah file (kucing.bmp) maka yang tersimpan dalam file tersebut yaitu angka-angka yang diperoleh dari matriks kanvas. Sehingga representasi dari citra gambar adalah sebuah nilai angka yang tergantung dari format penyimpanan nilainya.

H. Tipe Citra berdasarkan Format Penyimpanan Nilai Warna

1. Citra Biner

Format citra biner merupakan salah satu citra yang terdiri dari 2 warna yang mempunyai nilai angka 0 dan 1, dimana warna hitam itu 0 dan angka 1 untuk warna putih, sehingga citra tersebut terdiri dari warna hitam dan putih atau bisa juga disebut dengan citra monokrom. Gambar 2.5 berikut ini adalah contoh dari citra dengan format biner.[6]



Gambar 2.5 Format Citra Biner

2. Citra Keabuan

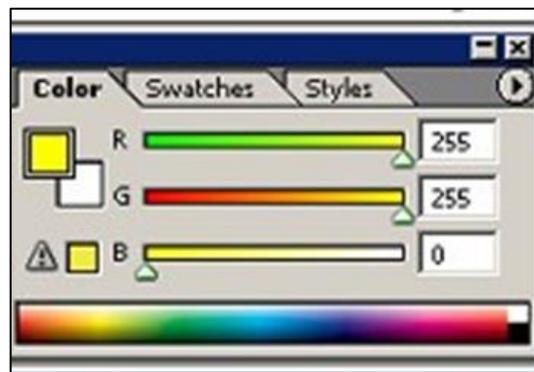
Format (grayscale) kemungkinan memiliki warna antara hitam (minimal) dan putih (maksimal) dimana nilai maksimum warna sesuai dengan bit penyimpanan yang digunakan. Contohnya skala keabuan 4 bit, jumlah kemungkinan $2^4 = 16$ warna, kemungkinan warna 0 (min) sampai 15 (max). Sedangkan untuk skala keabuan 8 bit, jumlah kemungkinan $2^8 = 256$ warna, kemungkinan warna 0 (min) sampai 255 (max). Gambar 2.6 berikut ini adalah ilustrasi citra skala keabuan.



Gambar 2.6 Citra Skala Keabuan

3. Citra Warna (True Color)

Warna dasar yaitu merah hijau biru atau yang dikenal dengan citra RGB (Red Green Blue) dikombinasikan sehingga mewakili setiap titik atau (*pixel*) pada citra warna. Warna dasar ini mempunyai intensitas sendiri dengan nilai maksimum 255 (8 bit). Dalam warna dasar RGB tiap-tiap warna memiliki warna minimum putih dan maksimum warna masing-masing. Misal warna kuning adalah kombinasi warna merah dan hijau sehingga mempunyai nilai RGB = (255, 255, 0), contoh lain kombinasi warna merah dan biru sehingga menghasilkan warna ungu muda mempunyai nilai RGB = (150, 0, 150). Gambar 2.7 ini adalah contoh representasi warna pada perangkat lunak Adobe Photoshop yang menggambarkan kombinasi warna red, green dan blue.

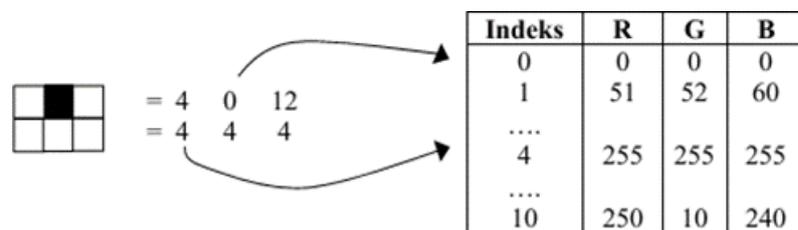


Gambar 2.7 Kombinasi warna RGB di photoshop

Maka setiap titik pada citra warna membutuhkan data 3 byte maka jumlah kemungkinan kombinasi warna adalah 224 yaitu lebih dari 16 juta warna yang terdiri dari 24 bit atau disebut juga dengan citra true color karena dianggap sudah mencakup semua warna yang ada. Ada perbedaan warna dasar untuk cahaya (misal display di monitor komputer) dan untuk cat/tinta (misal cetakan di atas kertas). Citra cahaya menggunakan warna dasar RGB (Red Green Blue) sedangkan Citra cat menggunakan warna dasar CMY (Cyan Magenta Yellow).

4. Citra Warna Berindeks

Palet warna adalah Setiap titik (pixel) pada citra warna berindeks mewakili indeks dari suatu tabel warna, adapun manfaat dari penggunaan palet warna adalah kita dapat dengan cepat memanipulasi warna tanpa harus mengubah informasi pada setiap titik dalam citra. Keuntungan yang lain adalah dalam hal kapasitas penyimpanan pada storage akan memerlukan ruang alokasi memori yang lebih kecil. Contoh penggunaan warna berindeks ini dapat kita jumpai pada pengaturan warna tampilan pada MS Window biasanya format 16 colors, 256 colors, high color, true color, yang merupakan citra warna berindeks dengan ukuran palet masing- masing 4 bit, 8 bit, 16 bit dan 24 bit.

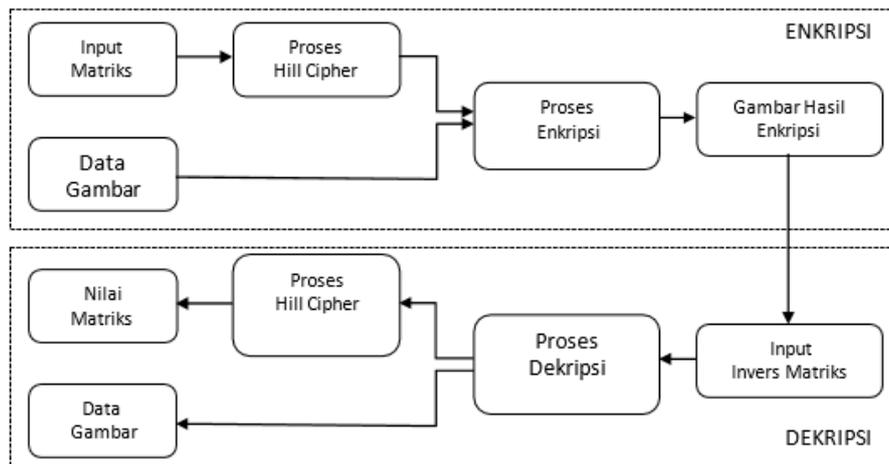


Gambar 2.8 Citra warna berindeks

3. Metodologi Penelitian

A. Analisis Rencana Penelitian

Penelitian ini terdapat 2 proses yang dapat dilakukan yaitu enkripsi dan dekripsi, seperti dilihat pada gambar 3.1 berikut ini:



Gambar 3.1 Blok Diagram Penelitian

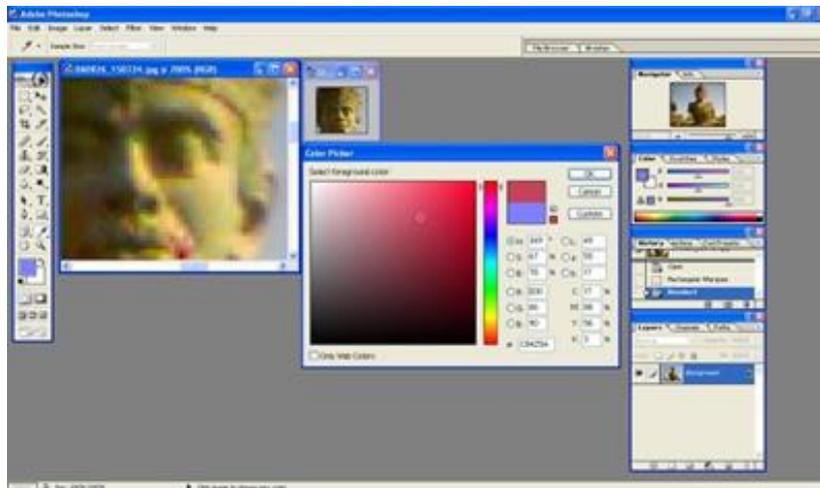
Tahap penelitian pada proses enkripsi yaitu mengambil inputan data berupa nilai matriks dan data gambar, setelah itu akan dilakukan proses hill cipher untuk pengacakan nilai data pada gambar, sehingga menghasilkan Hasil data gambar yang terenkripsi. Sedangkan tahap dekripsi, hasil gambar yang telah terenkripsi akan melalui proses dekripsi yaitu dengan cara mengambil data gambar yang terenkripsi dengan nilai input dari invers matrik awal. lalu dilakukan proses Hill Cipher balik sehingga data gambar yang telah diacak dapat kembali pada data gambar semula.

B. Format Matriks

Matriks yang digunakan dalam enkripsi data ini menggunakan matriks berordo 2*2 dimana nantinya matriks tersebut akan diproses menggunakan algoritma Hill Cipher. Nilai matriks tersebut akan dikalikan dengan nilai-nilai warna pada setiap pixel. Nilai elemen matriks yang digunakan harus mempunyai nilai determinan sama dengan 1. Hal ini diperlukan agar data dapat dilakukan proses dekripsi atau mengembalikan data yang sudah teracak ke data semula, karena proses dekripsi membutuhkan nilai matriks inverse.

C. Pengolahan Warna RGB

Terdapat sebuah komponen atau kontrol yang digunakan untuk menampilkan sebuah citra gambar pada Visual Basic 6. Komponen tersebut merupakan Image yang terdapat dalam kontrol standard. Visual Basic mempunyai format bitmap 24 bit, dimana tiap pixel yang mewakili representasi dari sebuah citra terdiri dari 8 bit warna R (Red), 8 bit warna G (Green) dan 8 bit warna B (Blue) dalam menampilkan citra gambar, dengan menggunakan metode Little Endian yaitu sebuah metode pengambilan warna RGB dimana nilai 8 bit bawah adalah nilai R dan nilai 8 bit atas adalah nilai B[1][2]. Sebelum melakukan operasi Little Endian kita perlu mengimplementasikannya dengan mengambil nilai tiap-tiap pixel dengan sintak point yang dimiliki Visual Basic. Gambar 3.2 berikut ini merupakan salah satu ilustrasi tentang pengolahan warna.

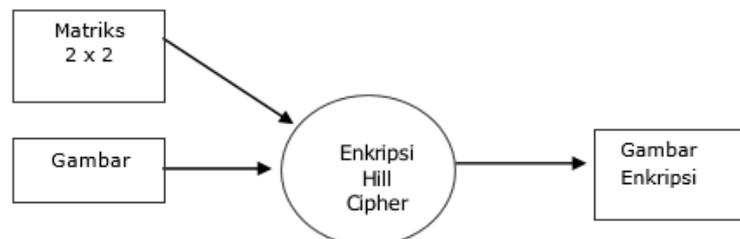


Gambar 3.2 Ilustrasi pengolahan warna

D. Desain Alur dan Struktur Program

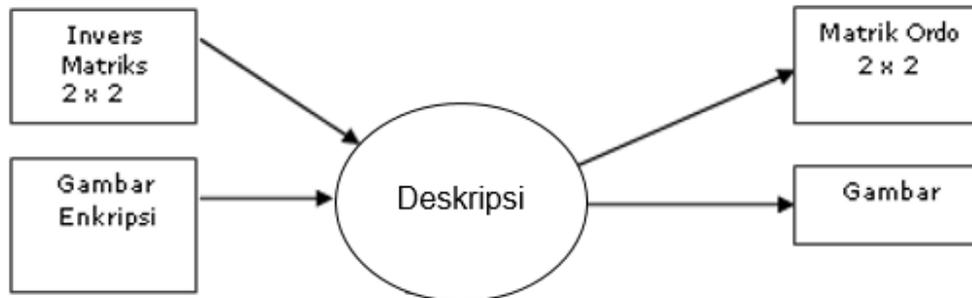
Langkah – langkah proses mulai penentuan nilai matriks, perkalian matriks sampai pada proses pengkodean karakter untuk proses enkripsi dan dekripsi dijabarkan melalui *Data Flow Diagram* (Diagram Alur Data) berikut ini:

1. DFD Level 0



Gambar 3.3 DFD Level 0 untuk proses enkripsi

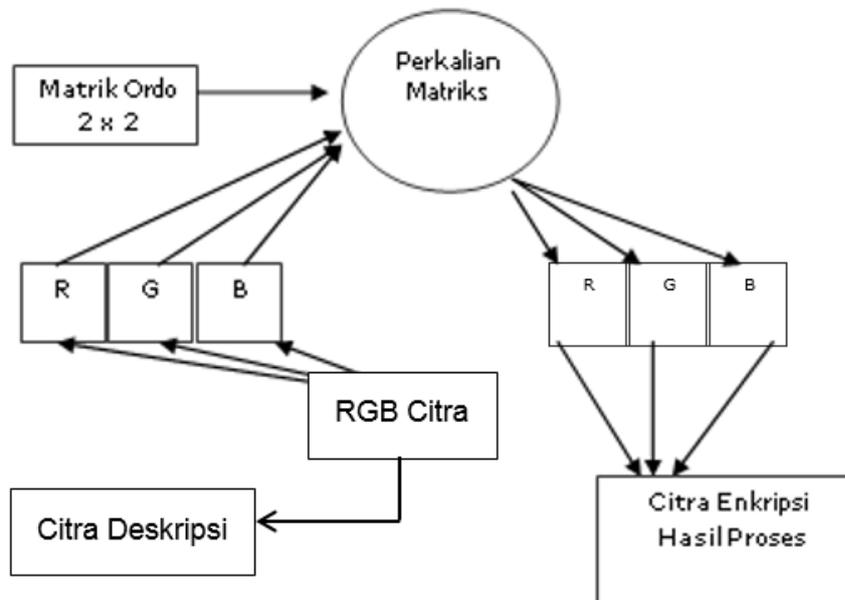
Proses membutuhkan input matriks dengan ordo 2×2 yang mempunyai nilai determinan sama dengan 1, artinya jika secara berurutan terdapat elemen matriks dengan simbol a, b, c, d maka nilai determinan didapat dengan rumus $(a * d) - (b * c)$. Selain itu dibutuhkan juga input citra gambar yang akan dilakukan proses enkripsi.



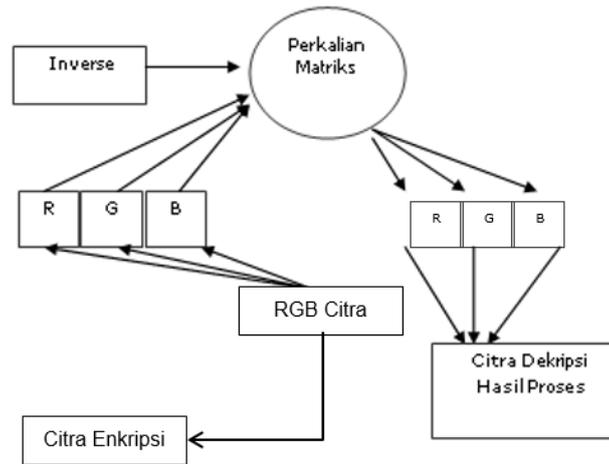
Gambar 3.4 DFD level 0 untuk proses dekripsi sistem

Pada proses dekripsi membutuhkan nilai inverse matriks dari matriks yang digunakan untuk proses enkripsi. Selain itu juga membutuhkan gambar yang sudah dilakukan enkripsi pada proses sebelumnya.

2. DFD Level 1



Gambar 3.5 DFD level 1 untuk proses enkripsi

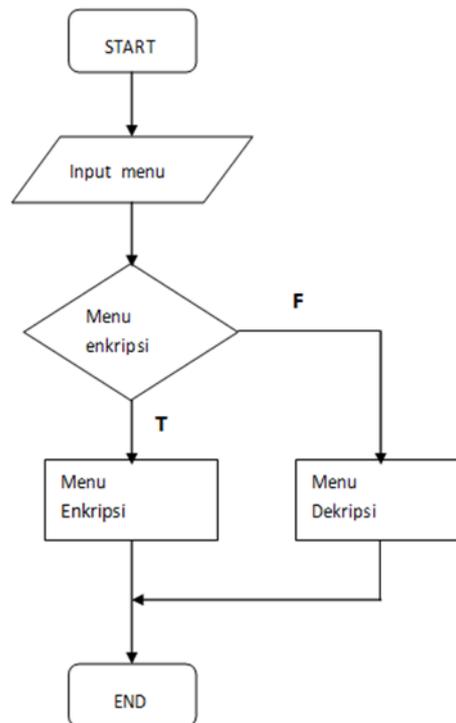


Gambar 3.6 DFD level 1 untuk proses dekripsi

F. Flowchart Program

1. Flowchart Menu

Alur program awal yaitu dimulai dari pemilihan proses yang mempunyai 2 (dua) yaitu enkripsi dan dekripsi, seperti pada gambar 3.7 berikut ini:

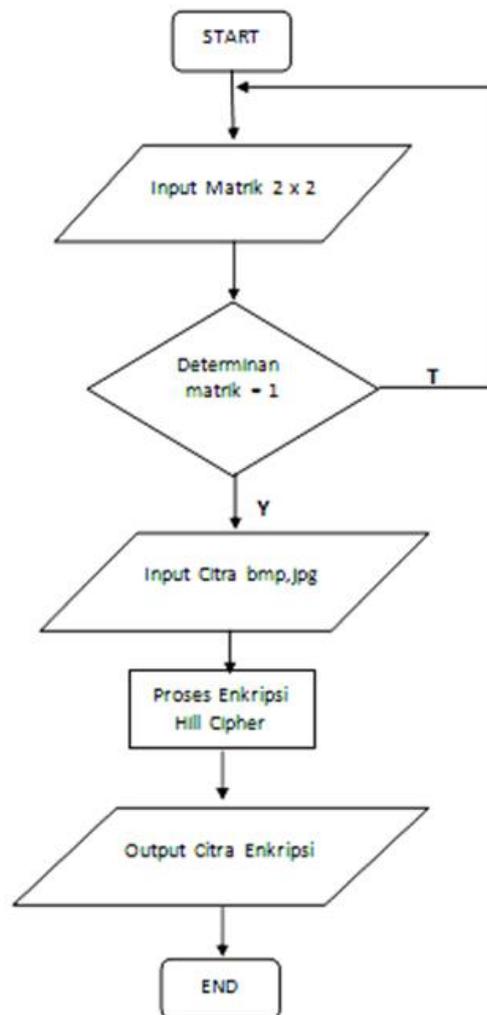


Gambar 3.7 Flowchart Menu

Program berjalan akan memberikan 2 pilihan proses yaitu proses enkripsi atau dekripsi. Jika user memilih enkripsi, maka alur proses akan menuju ke proses enkripsi, jika tidak maka akan melakukan proses dekripsi.

2. Flowchart Enkripsi Citra

Gambar 3.8 berikut ini adalah flowchart untuk proses enkripsi.

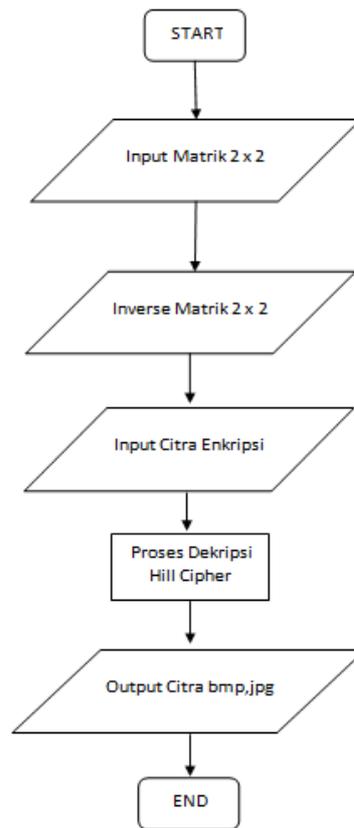


Gambar 3.8 Flowchart Enkripsi

Proses enkripsi dimulai dengan memasukkan matriks dengan ordo 2 x 2, kemudian proses akan melakukan pengecekan nilai determinan matriks tersebut. Jika nilai determinan tidak sama dengan 1 maka proses akan kembali untuk memasukkan matriks kembali dengan nilai yang lain. Jika nilai determinan matriks sama dengan 1, maka proses selanjutnya yaitu memberikan input citra atau gambar dalam format bmp ataupun jpg, kemudian dilanjutkan dengan proses enkripsi sehingga muncul berupa citra atau gambar yang terenkripsi.

3. Flowchart Dekripsi Citra

Proses dekripsi citra adalah sebuah proses kebalikan dari enkripsi. Jika enkripsi adalah mengacak data, maka dekripsi adalah proses mengembalikan data kedalam bentuk semula sehingga dapat dimaknai atau mempunyai informasi bagi pengguna yang berhak mengaksesnya. Gambar 3.9 berikut ini adalah alur untuk proses dekripsi.



Gambar 3.9 Flowchart proses dekripsi

G. Metode Pengujian

Uji coba pada penelitian ini bertujuan untuk mengetahui sejauh mana algoritma Hill Cipher dapat melakukan enkripsi dan dekripsi pada data berbentuk gambar (citra) maka dibuat sebuah tahapan-tahapan dalam pengujiannya. Pengujian ini dilakukan dengan format seperti pada tabel 3.1 berikut ini:

Tabel 3.1 Skenario pengujian

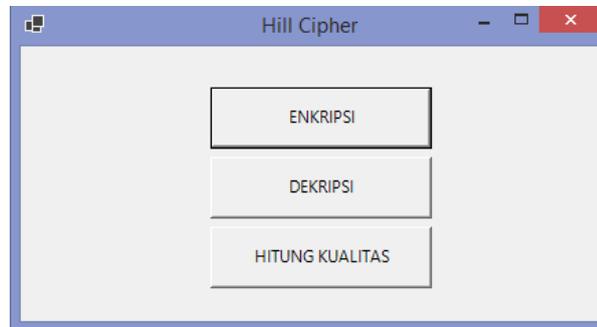
Pengujian ke	Matriks Enkripsi	Matriks Dekripsi	Format Citra
1.	a=11, b=12, c=10, d=11	sesuai	Format True color berekstensi bmp
2.	a=3, b=4, c=2, d=3	sesuai	Format True color berekstensi bmp
3.	a=11, b=12, c=10, d=11	sesuai	Format Citra biner (threshold) dengan level =100
4.	a=11, b=12, c=10, d=11	sesuai	Format Citra keabuan (Grayscale)
5.	a=11, b=12, c=10, d=11	Tidak sesuai	Format True color berekstensi bmp
6.	a=5, b=2, c=8, d=4	sesuai	Format True color berekstensi bmp

4. Hasil dan Pembahasan

4.1. Implementasi Program

A. Menu Utama

Program menyediakan 2 (dua) pilihan menu yaitu enkripsi dan dekripsi, serta menu tambahan untuk menghitung kualitas dari hasil enkripsi seperti pada gambar 4.1 berikut ini:

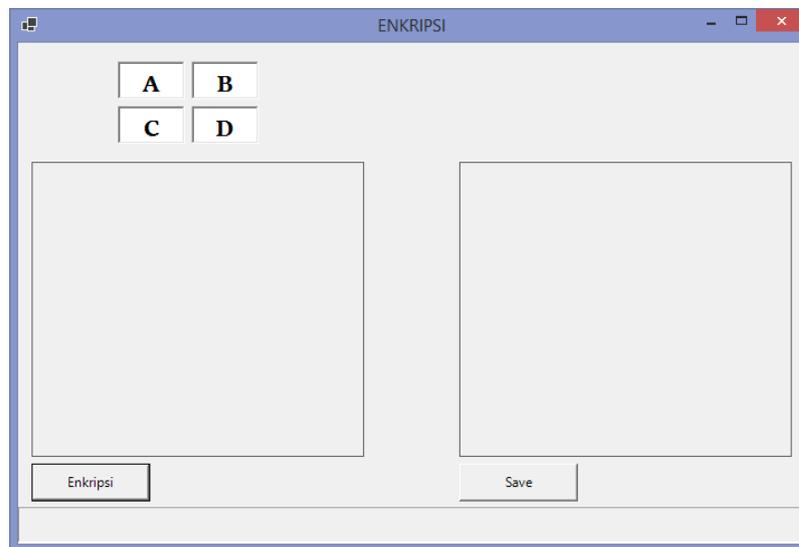


Gambar 4.1 Menu Implementasi Program

Menu enkripsi yaitu untuk mengacak / enkripsi dari gambar awal menjadi gambar baru yang telah terenkripsi bit-bit warna yang terkandung didalamnya dengan melakukan perkalian matriks Hill Cipher. Sedangkan untuk menu dekripsi adalah proses kebalikan dari enkripsi yaitu mengembalikan gambar yang telah diubah bit-bit warnanya kembali ke bentuk bit gambar semula.

B. Form Enkripsi

Gambar 4.2 berikut ini adalah form untuk proses enkripsi:

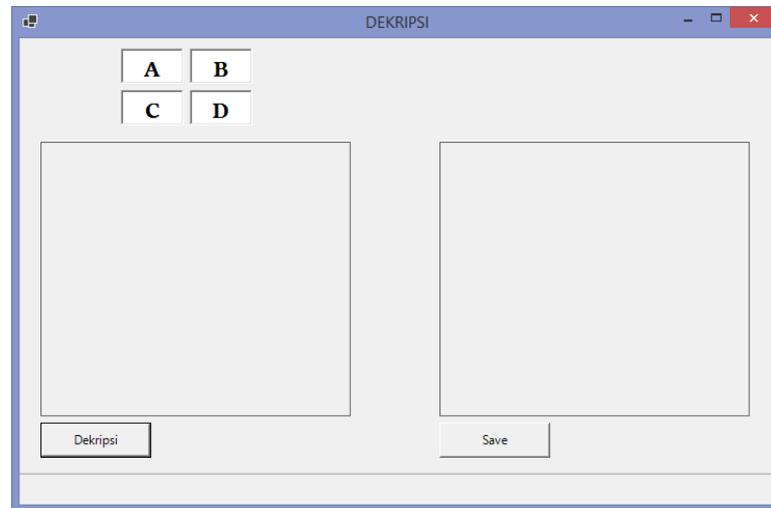


Gambar 4.2 Form Enkripsi

Form tersebut mempunyai 4 buah input berupa textbox yang digunakan untuk input nilai-nilai matriks dengan ordo 2 x 2, kemudian user dapat melakukan klik pada area bingkai gambar untuk mencari file citra yang akan dienkripsi dengan filter ekstensi file jpg atau bmp, dan juga tombol untuk menyimpan file hasil dari proses enkripsi

C. Form Dekripsi

Gambar 4.3 berikut ini adalah form untuk proses dekripsi

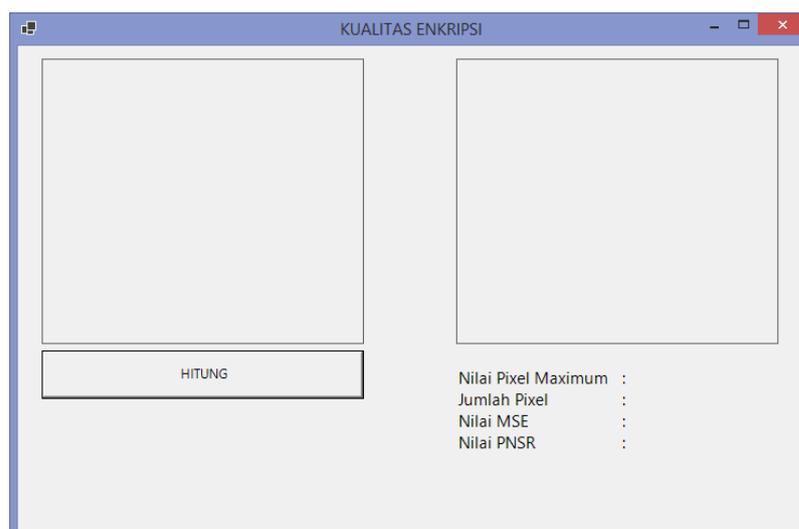


Gambar 4.3 Form Dekripsi

Begitu juga dengan form dekripsi mempunyai 4 buah input berupa textbox yang akan digunakan sebagai input nilai-nilai matriks dengan ordo 2 x 2, kemudian user dapat melakukan klik pada area bingkai gambar untuk mencari file citra yang akan didekripsi dengan filter ekstensi file jpg atau bmp, dan juga tombol untuk menyimpan file hasil dari proses dekripsi.

D. Form Hitung Kualitas

Form hitung kualitas berfungsi untuk mencari nilai Nilai MSE dan Nilai PNSR yaitu perbedaan nilai awal citra dan nilai hasil enkripsi. Semakin besar nilai hasil perhitungan, maka semakin baik hasilnya dalam artian gambar semakin susah untuk dikenali. Gambar 4.4 berikut ini adalah form untuk melakukan perhitungan kualitas.



Gambar 4.4 Form Hitung Kualitas

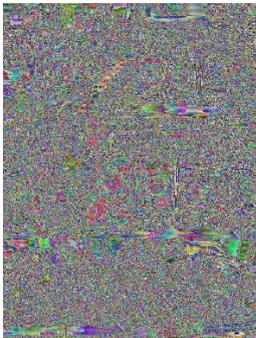
E. Pengujian Program

1. Pengujian Pertama

Parameter yang digunakan dalam pengujian pertama yaitu:

Matriks : $\begin{pmatrix} 3 & 4 \\ 5 & 7 \end{pmatrix}$

Gambar : 

Hasil Enkripsi : 

Hasil Kualitas : Nilai Maximum Pixel : 16581375
Jumlah Pixel : 1595415
Nilai MSE : 12819613767353.23
Nilai PNSR : 13.313

2. Pengujian kedua

Parameter yang digunakan dalam pengujian kedua yaitu:

Matriks : $\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$

Gambar : 

Hasil Enkripsi :



Hasil Kualitas : Nilai Maximum Pixel : 16581375
Jumlah Pixel : 12000000
Nilai MSE : 1882065412502.0989
Nilai PNSR : 21.64

5. Penutup

5.1. Kesimpulan

Berdasarkan analisa, implementasi, serta pembahasan yang telah dilakukan maka dapat diambil beberapa kesimpulan yaitu:

1. Enkripsi serta dekripsi data dapat digunakan pada data berupa citra atau gambar dengan cara mengambil bit-bit nilai RGB dari tiap-tiap pixel yang berupa bilangan numeric, dimana nilainya minimal 0 dan maksimal 255. Nilai-nilai pixel tersebutlah yang kemudian diproses dengan cara dikalikan dengan matriks dari algoritma Hill Cipher.
2. Data berupa citra atau gambar yang dapat di enkripsi menggunakan algoritma Hill Cipher merupakan citra yang true color dan grayscale, namun untuk citra threshold (black and white) tidak dapat di enkripsi dikarenakan keragaman warna yang hanya sedikit, yaitu nilai yang hanya 0 dan 255. Untuk input data matrik algoritma Hill Cipher yaitu semakin besar nilai matrik yang dimasukkan, maka proses enkripsi akan semakin baik dan tidak mudah dikenali bentuk asalnya.

5.2. Saran

1. Enkripsi serta dekripsi data citra dengan menggunakan algoritma Hill Cipher dengan ordo yang bebas dan tidak ditentukan, sehingga dapat dilihat perbedaan hasil acaknya.
2. Format citra gambar dalam uji coba diperbanyak lagi, seperti format citra HSV, CMYK, YUV, YcBcR dan format-format lainnya, sehingga dapat diketahui karakteristik dari algoritma Hill Cipher.
3. Algoritma yang digunakan untuk enkripsi dan dekripsi data menggunakan metode konvensional yang lain seperti substitusi, veginere chipper dan lain-lain. Bagian saran dalam hal ini merupakan temuan-temuan yang nantinya dijadikan masukkan kedepan agar lebih baik dari pembahasan yang dituliskan pada bab 4.

Daftar Pustaka

- [1] S. A. Fadhil, A. K. Farhan, and A. H. Radie, "Visual Cryptography Techniques: Short Survey," in 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), 2021, pp. 276–282.
- [2] R. Mahendran and K. Mani, "Generation of Key Matrix for Hill Cipher Encryption Using Classical Cipher," in 2017 World Congress on Computing and Communication Technologies (WCCCT), 2017, pp. 51–54. doi: 10.1109/WCCCT.2016.22.
- [3] J. Hutahaean, Konsep sistem informasi. Deepublish, 2015.
- [4] D. Ariyus, "Computer Security," 2006.
- [5] R. D. Kusumanto and A. N. Tomponu, "pengolahan citra digital untuk mendeteksi obyek menggunakan pengolahan warna model normalisasi RGB," Semantik, vol. 1, no. 1, 2011.
- [6] I. Fawwaz and N. P. Dharshinni, "Perbandingan Deteksi Tepi Citra Menggunakan Operator Robert, Canny, dan Frei Chen Pada Citra Bitmap dan JPEG," Jurnal Sistem Informasi dan Teknologi Jaringan (SISFOTEKJAR), vol. 2, no. 2, pp. 41–45, 2021.