STEGANOGRAFI CITRA MENGGUNAKAN METODE PIXEL VALUE DIFFERENCING (PVD) UNTUK DATA TERENKRIPSI DARI METODE HILL CIPHER

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer pada Program Studi Sistem Informasi Departemen Matematika Fakultas Matematika danIlmu Pengetahuan Alam Universitas Hasanuddin Makassar

ARVINA SULVIYANI

H131 16 013

PROGRAM STUDI SISTEM INFORMASI
DEPARTEMEN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS HASANUDDIN
MAKASSAR

MARET 2022

STEGANOGRAFI CITRA MENGGUNAKAN METODE PIXEL VALUE DIFFERENCING (PVD) UNTUK DATA TERENKRIPSI DARI METODE HILL CIPHER

Disusun dan diajukan oleh

ARVINA SULVIYANI
H131 16 013

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana pada Program Studi Sistem Informasi Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Hasanuddin dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama	Pembimbing Pertama
Dr. Hendra, S.Si., M.Kom.	Andi Muhammad Anwar, S.Si., M.Si
NIP. 19760102 200212 1 001	NIP. 19901228 201803 1 001

Ketua Program Studi

Dr. Muhammad Hasbi, M.Sc
NIP. 19630720 198903 1 003

HALAMAN PERNYATAAN KEOTENTIKAN

Yang bertanda tangan di bawah ini:

Nama	:	ARVINA SULVIYANI
NIM	:	H131 16 013
Program Studi	:	Sistem Informasi
Jenjang	:	S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

STEGANOGRAFI CITRA MENGGUNAKAN METODE PIXEL VALUE DIFFERENCING (PVD) UNTUK DATA TERENKRIPSI DARI METODE HILL CIPHER

Adalah benar hasil karya saya sendiri bukan merupakan pengambilan alihan tulisan orang lain dan belum pernah dipublikasikan dalam bentuk apapun.

Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan skripsi ini merupakan hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Makassar, 29 Maret 2022

ARVINA SULVIYANI

NIM. H131 16 013

KATA PENGANTAR

Alhamdulillahi Rabbil'alamin, segala puji dan syukur penulis panjatkan kehadirat Allah SWT, yang senantiasa melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan tugas akhir ini. Shalawat dan salam senantiasa tercurahkan kepada baginda Rasulullah Muhammad SAW yang telah membawa kita ke luar dari zaman kegelapan menuju zaman yang terang benderang saat ini.

Dalam penyelesaian skripsi dengan judul "*STEGANOGRAFI CITRA MENGGUNAKAN METODE PIXEL VALUE DIFFERENCING (PVD) UNTUK DATA TERENKRIPSI DARI METODE HILL CIPHER*" ini tidak sedikit hambatan dan kesulitan yang dialami penulis, seperti adanya wabah Covid-19. Namun berkat bantuan serta bimbingan dari berbagai pihak skripsi ini terselesaikan meski dengan segala kekurangan.

Penulis menghanturkan ungkapan hormat dan terima kasih yang tulus kepada keluarga besar penulis terkhusus bagi Ayahanda **Muhtar** dan Ibunda **Nurjannah** atas segala doa, nasihat, motivasi, cinta, serta kasih sayang yang tulus untuk kesukseksan anak-anaknya. Ucapan terima kasih juga kepada saudara tercinta **Wawan Ardiansyah, S.E** dan **Sherli Apriani** yang senantiasa memberikan dukungan dan doa bagi penulis dalam menyelesaikan skripsi ini. Semoga Allah Yang Maha Pengasih senantiasa memberikan rahmat-Nya atas kalian, orang-orang yang paling kucintai.

Penulis menyadari bahwa penelitian ini dapat terselesaikan dengan adanya bantuan, bimbingan, dukungan dan motivasi dari berbagai pihak. Oleh karena itu, penulis mengungkapkan ucapan terima kasih dengan tulus kepada :

1. Rektor Universitas Hasanuddin, Ibu **Prof. Dr. Dwia Aries Tina Pulubuhu** beserta jajarannya, dan Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam **Dr. Eng. Amiruddin** beserta jajarannya, serta seluruh pihak birokrasi atas pengetahuan dan kemudahan-kemudahan yang diberikan baik, dalam bidang akademik maupun bidang kemahasiswaan.
2. Ketua Departemen Matematika FMIPA, **Dr. Nurdin, S.Si., M.Si** dan juga

Dr. Muhammad Hasbi, M.Sc. sebagai ketua Program Studi Sistem Informasi Universitas Hasanuddin.

3. Bapak **Dr. Hendra, S.Si., M.Kom.** selaku pembimbing utama atas segala ilmu, ide, motivasi, nasehat, dan kesabaran dalam membimbing penulis serta meluangkan waktu disela-sela rutinitas yang begitu padat sehingga skripsi ini dirampungkan.
4. Bapak **Andi Muhammad Anwar, S.Si., M.Si** sebagai pembimbing pertama yang berkenan dan rela mengorbankan waktu, tenaga dan pikiran guna memberikan petunjuk dan bimbingannya dalam penulisan skripsi ini.
5. Bapak **Dr. Muhammad Hasbi, M.Sc** dan bapak **Supri Bin Hj Amir, S.Si., M.Eng.** sebagai dosen penguji atas saran dan kritik yang membangun pada penelitian yang telah dilakukan oleh penulis.
6. Bapak **Dr. Hendra, S.Si., M.Kom.** sebagai dosen pembimbing akademik yang senantiasa memberikan motivasi, dorongan, dan masukan dalam hal akademik.
7. Bapak/Ibu dosen FMIPA Universitas Hasanuddin yang telah mendidik dan memberikan ilmunya sehingga penulis mampu menyelesaikan program sarjana. Serta para staff yang telah membantu dalam pengurusan berkas administrasi.
8. Keluarga besar **Ilmu Komputer Unhas 2016** yang mambantu dan memberi support kepada penulis selama menjalani pendidikan.
9. Sahabat penulis, **Alvionita Tini Kadola** yang telah menemani penulis selama menjalani masa perkuliahan, berbagi suka-duka serta kebersamaan. Selalu menjadi partner terbaik dalam banyak hal. Terima kasih karena selalu menjadi pendengar yang baik, pengertian, sabar mendengarkan keluhan, dan selalu memahami penulis. Serta senantiasa membantu dan memeberi dukungan kepada penulis.
10. Saudari **Hajrah, Nirwana Sari Hamka, Susilawati, Nurfadillah** yang telah menemani penulis selama perkuliahan, saling memberi motivasi dan bantuan, serta kebersamaan selama menuntut ilmu.
11. Teman-teman **MOA** dan **TXT** yang senantiasa memberikan semangat, dukungan, dan memotivasi penulis untuk selalu melalukan yang terbaik. Terima kasih telah menjadi *support system* terbaik bagi penulis.

12. Kakak-kakak dan adik-adik **Sistem Informasi 2014, 2015, 2017, 2018** yang telah banyak membantu, semoga tetap semangat dalam mengejar impian.
13. Rekan-rekan **KKN E-Commerce Luwu Utara Gelombang 102** yang tel;ah menjadi keluarga baru selama KKN dan menjadikannya sebagai momen yang membahagiakan.
14. Seluruh Keluarga yang telah membesarkan dan mendidik penulis serta Sahabat yang telah memberikan motivasi dan doa yang tiada henti-hentinya.
15. Semua pihak yang telah banyak berpartisipasi, baik secara lanngsung maupun tidak langsung dalam penyusunan skripsi ini yang tidak sempat penulis sebutkan satu per satu.

Penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna dikarenakan terbatasnya pengalaman dan pengetahuan yang dimiliki penulis. Oleh karena itu, penulis mengharapkan segala bentuk saran serta masukan bahkan kritik yang membangun dari berbagai pihak demi kesempurnaan skripsi ini.

Makassar, 29 Maret 2022

ARVINA SULVIYANI
NIM. H13116013

ABSTRAK

Sistem teknologi yang berkembang dengan sangat pesat mengakibatkan cepatnya laju pertukaran informasi. Semua informasi dapat didapatkan dengan mudah, khususnya melalui pengiriman pesan. Namun seringkali pesan yang ingin dikirimkan tidak sampai kepada penerima, melainkan terkirim kepada penerima yang tidak seharusnya. Untuk menjaga keamanan pesan dapat dilakukan dengan menerapkan teknik kriptografi dan steganografi. Pesan asli yang ingin dikirimkan akan dienkripsi dengan menggunakan metode kriprografi Hill Cipher. Kemudian pesan yang telah dienkripksi akan disisipkan dalam media berupa citra. Untuk penyisipan pesan itu sendiri dilakukan dengan menerapkan metode *Pixel Value Differencing* (PVD) yang merupakan salah satu metode steganorafi. Sehingga pesan asli hanya dapat diketahui oleh pengirim dan penerima pesan. Sedangkan jika pesan diterima oleh penerima yang tidak diinginkan, maka pesan asli tidak dapat diketahui dengan mudah.

Kata kunci: Kriptografi, Hill Cipher, Steganografi, PVD

ABSTRACT

Rapidly expanding technological systems gave rise to the rapid pace of information exchange. All information can be obtained easily, especially through messenger. But often the message that wants to be sent doesn't reach the receiver, it is sent to the one who shouldn't. To keep the message safe can be done by applying cryptography techniques and steganography. The original message wanted to be sent will be encrypted using hill cipher's cryptography method. Then encrypted messages are inserted into a medium of image. For the insertion of the message itself was done by applying the Pixel Value Differencing (PVD) one of the steganography methods. So that the original message can only be known by the sender and the recipient of the message. When a message is received by an unwanted recipient, the original message cannot be known easily.

Keyword: *Cryptographic, Hill cipher, Steganography, PVD*

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PENGESAHAN ii
HALAMAN PERNYATAAN KEOTENTIKAN iii
KATA PENGANTAR iv
ABSTRAK vii
ABSTRACT viii
DAFTAR ISI ix
DAFTAR GAMBAR xi
DAFTAR TABEL xii
DAFTAR LAMPIRAN xiii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Tujuan Penelitian 3
1.4 Manfaat Penelitian 3
1.5 Batasan Masalah 3
BAB II TINJAUAN PUSTAKA 4
2.1 Citra Digital 4
2.2 Steganografi 6
2.3 Pixel Value Differrencing (PVD) 8
2.4 Kriptografi 11
2.4.1 Notasi Matematis pada Kriptografi 13
2.4.2 Algoritma Kriptografi 14

2.5 Hill Cipher 15
2.6 Matriks 17
2.7 *Peak Signal to Noise Ratio* (PSNR) 18
2.8 Kompresi File 18
BAB III METODOLOGI PENELITIAN 22
3.1 Waktu dan Lokasi Penelitian 22
3.2 Prosedur Penelitian 22
3.3 Sumber Data 23
3.4 Instrumen Penelitian 23
BAB IV HASIL DAN PEMBAHASAN 24
4.1 Enkripsi dan Dekripsi Menggunakan *Hill Cipher* 24
4.1.1 Enkripsi *Hill Cipher* 25
4.1.2 Dekripsi *Hill Cipher* 29
4.2 Implementasi Enkripsi-Dekripsi dengan *Hill Cipher* 34
4.3 Penyisipan dan Ekstraksi Menggunakan PVD (*Pixel Value Differencing)*. 36
4.4 Implementasi Metode PVD pada Citra 42
4.5 Pengujian Kualitas Citra 44
4.5.1 *Mean Square Error* (MSE) 44
4.5.2 *Peak Signal to Noise Ratio* (PSNR) 45
4.6 Kompresi 48
BAB V PENUTUP 51
5.1 Kesimpulan 51
5.2 Saran 51
DAFTAR PUSTAKA 52
LAMPIRAN 55

DAFTAR GAMBAR

Gambar 2.1 Proses *encoding* dan *decoding* 7
Gambar 2.2 Proses penyisipan file cover secara zigzag 9
Gambar 2.3 Proses enkripsi dan dekripsi 13
Gambar 3.1 Skema penelitian 23
Gambar 4.1 Flowchart proses enkripsi *Hill Cipher* 25
Gambar 4.2 Flowchart proses dekripsi *Hill Cipher* 29
Gambar 4.3 Potongan kode untuk enkripsi 35
Gambar 4.4 Potongan kode untuk dekripsi 36
Gambar 4.5 Flowchart *embedding* dengan metode PVD 37
Gambar 4.6 Flowchart ekstraksi dengan metode PVD 37
Gambar 4.7 Potongan kode untuk penyisipan pesan pada citra 42
Gambar 4.8 Potongan kode untuk ekstraksi pada citra 43
Gambar 4.9 Potongan kode untuk kompresi DCT 48

DAFTAR TABEL

Tabel 4.1 Kode ASCII 24
Tabel 4.2 Plainteks dikonversi ke angka 26
Tabel 4.3 Plainteks dikonversi ke angka 28
Tabel 4.4 Cipherteks dikonversi ke angka 30
Tabel 4.5 Cipherteks dikonversi ke angka 33
Tabel 4.6 Embedding dengan metode PVD 39
Tabel 4.7 Ekstraksi dengan metode PVD 41
Tabel 4.8 Nilai PSNR pada citra 46
Tabel 4.9 Hasil kompresi 49

DAFTAR LAMPIRAN

Lampiran 1. Source Code Enkripsi Hill Cipher 55
Lampiran 2. Source Code Dekripsi Hill Cipher 55
Lampiran 3. Source Code Embedding PVD 56
Lampiran 4. Source Code Ekstraksi PVD 58
Lampiran 5. Source Code MSE dan PSNR 59
Lampiran 6. Source Code Kompresi DCT 59

BAB I
PENDAHULUAN

1.1 Latar Belakang

Sistem teknologi informasi sekarang ini sudah berkembang dengan sangat pesat, tak terkecuali pada aspek komunikasi seperti pengiriman pesan. Keamanan dalam proses pengiriman pesan sangatlah penting. Dikarenakan seringkali pesan yang ingin disampaikan tidak sampai kepada penerima, melainkan jatuh ke pihak yang tidak diinginkan. Untuk melindungi keamanan pesan dapat dilakukan dengan menerapkan teknik kriptografi dan steganografi.

Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *cryptology*, bertujuan menjaga kerahasiaan informasi yang terkandung dalam data agar informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Oleh karena itu kriptografi dikatakan sebagai metode yang tangguh menjaga kerahasiaan informasi karena dalam kriptografi data yang dikirimkan melalui jaringan akan disamarkan sedemikianrupa menggunakan algoritma sandi. Data tetap aman kendati setiap orang dapat mengaksesnya secara bebas. Sehingga kalaupun data tersebut dapat dibaca, maka tidak dapat dipahami oleh pihak yang tidak berhak (Mu'mi, 2017).

Metode *Hill Cipher* merupakan salah satu metode yang dapat digunakan pada kriptografi. Metode ini memiliki keuntungan yaitu ketahanan terhadap analisis frekuensi dan *implicity* karena metode ini menggunakan perkalian matriks dan inversi untuk enkripsi dan dekripsi (Puspita & Wayahdi, 2015). Selain itu dimana kelebihan metode *Hill Cipher* dibandingkan dengan metode lain adalah *key* yang diambil bisa merupakan matriks persegi ukuran berapapun, dengan demikian pemecahan kode akan sulit menentukan "pemotongan" dari kata terenkripsi tersebut. Semakin besar ukuran matriks kunci, maka akan semakin sulit *Hill* Cipher dipecahkan (Suryani & Martini, 2008). Namun pengamanan data menggunakan teknik kriptografi ternyata dianggap belum baik dalam mengamankan data, karena *ciphertext* mengandung banyak karakter-karakter yang

tidak wajar sehingga dapat menimbulkan kecurigaan. Untuk mengatasi hal tersebut dapat digunakan teknik lain yaitu steganografi.

Steganografi berbeda dengan kriptografi atau metode keamanan informasi lainnya, metode ini yaitu menyembunyikan informasi atau pesan ke dalam media lain seperti citra digital, teks, suara, atau video sehingga tidak menimbulkan kecurigaan orang lain. Steganografi membutuhkan dua properti, yaitu informasi dan media penampung (cover) (Setiawan, 2013).

Metode pixel value differencing (PVD) merupakan salah satu metode yang dapat digunakan untuk steganografi. Metode ini menawarkan kapasitas penyimpanan yang lebih besar, dengan kualitas citra yang lebih baik dibandingkan dengan metode lain (Tseng & Leng, 2013). Namun metode PVD termasuk *fragile steganography* yang berarti informasi yang disisipkan pada media cover akan hancur jika dilakukan modifikasi terhadap *stego-object*.

Berdasarkan uraian diatas penulis ingin mengkaji lebih dalam tentang pengamanan informasi menggunakan steganografi dan kriptografi. Untuk itu penulis akan melalukan penyembunyian pesan yang berupa teks menggunakan kriptografi dengan metode *Hill Cipher* yang akan disisipkan pada citra digital menggunakan steganografi dengan metode *Pixel Value Differencing* (PVD). Citra yang dihasilkan akan diuji untuk melihat pesan yang disisipkan tetap aman dan hanya dapat diketahui oleh penerima pesan. Penulis akan menuangkannya dalam bentuk skripsi dengan judul "Steganografi Citra Menggunakan Metode Pixel Value Differencing (PVD) Untuk Data Terenkripsi Dari Metode Hill Cipher".

1.2 Rumusan Masalah

Adapun rumusan masalah dari penelitian ini adalah :

1. Apakah metode PVD dapat menyisipkan dan mengekstraksi pesan yang sudah dienkripsi dengan *Hill Cipher* dengan baik
2. Bagaimana kualitas citra setelah disisipkan pesan menggunakan metode PVD
3. Bagaimana efek kompresi citra terhadap pesan yang disembunyikan

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Untuk mengimplementasikan penyembunyian pesan yang sudah dienkripsi dengan *Hill Cipher* pada citra menggunakan metode PVD
2. Untuk mengetahui kualitas citra yang telah disisipkan pesan menggunakan metode PVD
3. Untuk mengetahui efek dari kompresi citra terhadap pesan yang disembunyikan.

1.4 Manfaat Penelitian

Hasil dari penelitian ini dapat memberikan manfaat sebagai berikut :

1. Dapat merahasiakan pesan tanpa diketahui keberadaan dari pesan tersebut.
2. Dapat menjaga pesan agar lebih aman.
3. Dapat digunakan sebagai referensi bacaan untuk mahasiswa yang akan melalukan penelitian serupa.

1.5 Batasan Masalah

Adapun batasan masalah pada penilitian ini adalah :

a. Pesan rahasia berupa pesan teks
b. Panjang matriks kunci untuk metode kriptografi adalah 3x3
c. Metode steganografi yang digunakan adalah *Pixel Value Differencing* (PVD)
d. Metode kriptografi yang digunakan yaitu metode *Hill Cipher*.
e. Citra yang dihasilkan bersifat *fragile.*

BAB II
TINJAUAN PUSTAKA

2.1 Citra Digital

Citra (*image*) secara harfiah, adalah gambar pada bidang dua dimensi (dwimatra). Ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (*continue*) dari intensitas cahaya pada bidang dwimatra. Sedangkan citra digital adalah citra yang dapat diolah oleh komputer (Mu'mi, 2017). Sebuah citra digital dapat diwakili oleh sebuah matriks yang terdiri dari M kolom dan N baris, dimana perpotongan antara kolom dan baris disebut *pixel*, yaitu elemen terkecil dari sebuah citra. Sebuah citra digital dapat ditulis dalam bentuk fungsi seperti berikut:

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

Berdasarkan warna-warna penyusunnya, citra digital dapat dibagi menjadi tiga jenis (Hidayat, 2018) yaitu:

a. Citra biner, yaitu citra yang terdiri dari dua warna, yaitu hitam dan putih. Oleh karena itu, setiap *pixel* pada cita biner cukup direpresentasikan dengan 1 bit.
b. Citra *grayscale*, yaitu citra yang nilai *pixel*-nya merepresentaikan derajat keabuan atau intensitas warna putih. Nilai intensitas paling rendah merepresentasikan warna hitam dan nilai intensitas paling tinggi merepresentasikan warna putih. Pada umumnya citra *grayscale* yang kedalaman *pixel* 8 bit (256 derajat keabuan), tetapi ada juga citra *grayscale* yang kedalaman *pixel*-nya bukan 8 bit, misalnya 16 bit untuk penggunaan yang memerlukan ketelitian tinggi.
c. Citra berwarna, yaitu citra yang nilai *pixel*-nya merepresentasikan warna tertentu. Banyaknya warna yang mungkin digunakan bergantung pada kedalaman *pixel* citra yang bersangkutan. Setiap *pixel* pada citra warna

memiliki warna yang merupakan kombinasi tiga warna dasar yaitu merah, hijau, dan biru (RGB = Red, Green, Blue).

Citra digital memiliki banyak format file yang setiap jenisnya memiliki karakteristik masing-masing. Format file ini umumnya didasarkan pada tipe dan cara kompresi yang digunakan pada citra digital tersebut (Setiawan, 2013). Berikut ini beberapa contoh format file pada citra digital :

a. *Bitmap* (BMP), merupakan format baku citra pada sistem operasi *windows* dan IBMOS/2. Citra berformat BMP merupakan citra yang tidak terkompresi, sehingga pada umumnya citra berformat BMP mempunyai ukuran yang relatif lebih besar dibandingkan dengan citra format lainnya. Intensitas *pixel* dari citra berformat BMP dipetakan ke sejumlah bit tertentu. Panjang setiap *pixel* pada *bitmap* yaitu 4 bit, 8 bit, sampai 24 bit yang merepresentasikan nilai intensitas *pixel*. Dengan demikian ada sebanyak $2^8 = 256$ derajat keabuan, mulai dari 0 sampai 255.
b. *Joint Photographic Group Experts* (JPEG), merupakan citra terkompresi yang bersifat *lossy*, artinya citra tidak bisa dikembalikan ke bentuk aslinya. Citra ini memiliki ukuran yang relatif lebih kecil dibandingkan dengan citra berformat BMP karena telah terkompresi. JPEG sebenarnya hanyalah algoritma kompresi, bukan merupakan nama format file. File yang biasa disebut JPEG pada jaringan sebenarnya adalah JFIF (*JPEG File Interchange Format*).
c. *Portable Network Graphics* (PNG), merupakan salah satu format penyimpanan citra yang menggunakan metode kompresi yang tidak menghilangkan bagian dari citra tersebut (*lossless compression*). Citra berformat PNG merupakan salah satu format yang baik untuk digunakan pengolahan citra, karena format ini tidak menghilangkan bagian dari citra yang sedang diolah. Format PNG ini diperkenalkan untuk menggantikan format penyimpanan citra GIF.

2.2 Steganografi

Steganografi (*steganography*) berasal dari Bahasa Yunani, yaitu "*steganos*" yang artinya menyembunyikan dan "*graphein*" yang artinya tulisan. Jadi steganografi berarti juga tulisan yang disembunyikan. Steganografi adalah seni dan ilmu menulis pesan tersembunyi yang sedemikian rupa sehingga tidak ada satu orang pun selain pengirim dan penerima yang dapat menyadari isi pesan tersebut (Pavan, dkk., 2013). Steganografi citra adalah metode komunikasi rahasia yang menggunakan citra sebagai media penampung (cover) untuk menyembunyikan kebenaran dari penyerang bahwa terdapat pesan rahasia pada citra tersebut (Wu & Hwang, 2007).

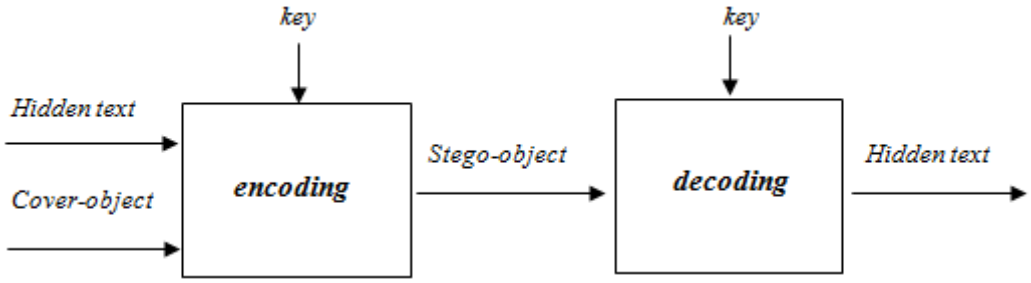
Secara teori, semua file umum yang terdapat di dalam komputer dapat digunakan sebagai media seperti file gambar berformat JPEG, GIF, BMP, atau file musik MP3, atau bahkan didalam sebuah video dengan format WAV atau AVI. Semua dapat dijadikan sebagai media cover, asalkan file tersebut memiliki bit-bit data redundan yang dapat dimodifikasi. Setelah dimodifikasi file media cover tersebut tidak akan banyak terganggu fungsinya dan kualitasnya tidak akan jauh berbeda dengan aslinya (Cahyadi, 2012). Namun file hasil modifikasi dapat berupa file *fragile* atau *robust*. *Fragile steganography* berarti penyisipan informasi ke dalam media cover dengan cara memodifikasi berkas *host* akan menghancurkan semua informasi yang tertanam. Karena hal tersebut dapat dengan mudah dihilangkan dari *carrier file*. Berbeda dengan teknik *fragile*, manipulasi bit dengan metode *robust* tidak akan mudah dihilangkan dari berkas *host*. Meskipun tidak ada metode yang menjamin bahwa data yang tertanam tidak dapat diubah tetapi jika upaya yang digunakan untuk menghancurkan informasi cukup banyak maka akan dikatakan sebagai metode *robust* (Altaay, dkk.,).

Menurut (Rachmawati, 2016), steganografi mempunyai dua komponen utama, komponen pertama adalah media penampung (cover) dan komponen kedua adalah data atau pesan yang akan disembunyikan. Terdapat beberapa istilah yang berkaitan dengan steganografi, yaitu:

a. *Hidden text* atau *embedded message*, merupakan pesan rahasia yang ingin disisipkan dalam suatu media.

b. *Cover-object* atau *stego-medium* atau media cover, yaitu tempat dari penyisipan pesan dan sebagai pembawa pesan.
c. *Carrier file* atau *stego-object*, adalah media cover yang sudah terdapat pesan rahasia didalam media tersebut.
d. *Steganalysis*, merupakan proses untuk mengidentifikasi keberadaan sebuah pesan dalam media cover.

Didalam steganografi digital, baik *embedded message* maupun *cover-object* dapat berupa citra, audio, maupun video, penyisipan pesan ke dalam media *cover-object* dinamakan *encoding*. Sedangkan ekstraksi pesan dari *stego-objec*t dinamakan *decoding*. Kedua proses ini mungkin memerlukan kunci rahasia (*stegokey*) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan pesan dan ekstraksi pesan sehingga menambah tingkat keamanan data. Gambaran untuk proses *encoding* dan *decoding* diberikan dalam Gambar 2.1 berikut:



Gambar 2.1 Proses *encoding* dan *decoding*

Ada beberapa kriteria-kriteria yang harus dipenuhi dalam pembuatan steganografi. Kriteria – kriteria tersebut yaitu (Setiawan, 2013):

a. *Impercepbility*, yaitu keberadaan pesan tidak dapat dipersepsi oleh indrawi. Jika pesan disisipkan ke dalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli oleh mata. Begitu pula dengan suara, telinga harus mendapati perbedaan antara suara asli dan suara yang telah disisipi pesan.
b. *Fidelity*, yaitu mutu media cover tidak berubah banyak akibat penyisipan. Perubahan yang terjadi harus tidak dapat dipersepsi oleh indrawi.

c. *Recovery,* yaitu pesan yang disembunyikan harus dapat diungkap kembali. Tujuan steganografi adalah menyembunyikan informasi, maka sewaktu-waktu informasi yang disembunyikan harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai keperluan.

Citra digital merupakan media cover yang banyak digunakan dalam steganografi. Hal ini karena adanya keterbatasan pada indra penglihatan manusia dalam mengenali warna, sehingga manusia sulit untuk membedakan citra digital yang asli dengan citra digital yang telah disisipkan pesan rahasia yang hanya memiliki sedikit perbedaan warna. Terdapat dua macam metode yang digunakan untuk penerapan steganografi pada citra digital yakni penyisipan pada *spatial domain (imager domain)* dan pada *transform domain* (Setiawan, 2013).

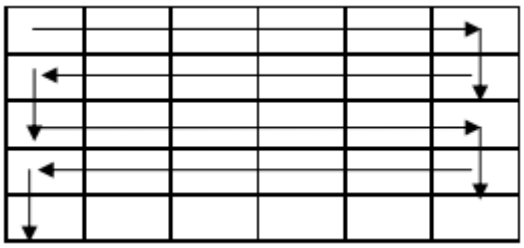
a. *Spatial domain*, yaitu penyisipan data dilakukan dengan mengubah nilai *pixel* citra aslinya. *Spatial domain* juga dikenal sebagai teknik subtitusi. Teknik subtitusi ini dilakukan sedemikian rupa sehingga media cover yang disisipkan pesan tidak dapat dipersepsi oleh indrawi perubahannya,. Metode steganografi yang beroperasi pada *spatial domain* diantaranya yaitu *Least Bit Significant* (LSB), *Dynamic Cell Spreadig* (DCS), *Pixel Value Differrencing* (PVD).
b. *Transform domain*, ranah ini memfokuskan penyisipan pesan ke dalam frekuensi dari media cover. *Transform domain* memanfaatkan area media cover yang cenderung tidak akan mengalami pemrosesan digital. Metode steganografi yang termasuk *transform domain* diantaranya *Discrete Cosine Transform* (DCT), *Fourier Transform*, *Wavelet Transform*, dan *Discrete Cosine Transform* (DWT).

2.3 Pixel Value Differrencing (PVD)

Pixel Value Differencing (PVD) merupakan salah satu metode yang dapat digunakan dalam steganografi. Metode ini beropersi pada ranah *spatial domain* dari citra digital. Penelitian awal algoritma PVD dilakukan oleh Wu *et al.*, 2001, dengan mencari selisih nilai dua piksel terdekat. Selisih digunakan untuk menentukan jumlah data yang dapat disisipkan berdasarkan jangkauan tabel yang

dipilih. Berdasarkan analisis terhadap sistem penglihatan manusia yang menyatakan bahwa, mata manusia tidak sensitif terhadap perubahan pada *pixel* yang memiliki kekontrasan tinggi melainkan sensitif terhadap perubahan pada *pixel* yang memiliki kekontrasan rendah. Melalui sifat tersebut maka lebih banyak *bit* data rahasia yang dapat disisipkan pada *pixel* yang memiliki nilai kekontrasan tinggi, dan sedikit *bit* yang dapat disisipkan pada *pixel* dengan kekontrasan rendah. Hal tersebut yang menjadi dasar pemikiran metode *Pixel value differencing* (PVD) pada steganografi (Wu & Tsai, 2003).

Proses penyisipan pesan dengan PVD dilakukan secara *zigzag*, dimulai dari kiri ke kanan kemudian turun ke bawah lalu ke kanan dan turun ke bawah kembali lagi dari kiri ke kanan dan seterusnya (Wu *et al.*, 2001) seperti pada Gambar 2.2 berikut:



Gambar 2.2 Proses penyisipan file cover secara zigzag

Pixel Value Differencing (PVD) menggunakan nilai perbedaan antara dua *pixel* yang bertetangga (P_i dan P_{i+1}) untuk menentukan berapa banyak bit rahasia harus tertanam. Persamaan yang digunakan yaitu :

$$d = |P_i - P_{i+1}| \tag{2.1}$$

Metode ini menggunakan pada skema Wu dan Tsai untuk mengetahui *range* dari perbandingan *pixel* sebelumnya. Skema Wu dan Tsai yang digunakan yaitu *continuous ranges* (R) = {[0,7],[8,15],[16,31],[32,63],[64,127],[128,255]}. Skema ini digunakan untuk mengetahui terdapat di *range* mana selisih dari dua *pixel* tersebut, jika telah diketahui dimana letak *range* nya, maka dapat diketahui batas bawah (l_i) dan batas atas (u_i). Setelah itu, untuk menghitung lebar (*width*) dari *optimum range* (w_i) digunakan persamaan berikut :

$$w_i = u_i - l_i + 1 \tag{2.2}$$

Selanjutnya yaitu mencari jumlah *bit* pesan yang dapat disisipkan (t_i) pada media cover, dapat diketahui dengan persamaan berikut :

$$t_i = \lfloor Log_2 w_i \rfloor \quad (2.3)$$

Penyisipan pesan dapat dilakukan dengan mengambil sebanyak t_i bit dari pesan yang akan disisipkan. Setelah itu, ubahlah bit-bit pesan yang akan disisipkan tersebut ke dalam nilai *decimal* (*b*). Kemudian dihitung nilai *difference value* yang baru untuk penyisipan ke dalam citra menggunakan persamaan berikut :

$$d_i' = l_i + b \quad (2.4)$$

Untuk menentukkan nilai *pixel* baru yang telah disisipkan pesan, ada beberapa aturan yang harus dipenuhi yaitu :

1. Jika $P_i \geq P_{i+1}$ dan $d_i' > d_i$, maka $(P_i + \lceil m/2 \rceil, P_{i+1} - \lfloor m/2 \rfloor)$
2. Jika $P_i < P_{i+1}$ dan $d_i' > d_i$, maka $(P_i - \lfloor m/2 \rfloor, P_{i+1} + \lceil m/2 \rceil)$
3. Jika $P_i \geq P_{i+1}$ dan $d_i' \leq d_i$, maka $(P_i - \lceil m/2 \rceil, P_{i+1} + \lfloor m/2 \rfloor)$
4. Jika $P_i < P_{i+1}$ dan $d_i' \leq d_i$, maka $(P_i + \lceil m/2 \rceil, P_{i+1} - \lfloor m/2 \rfloor)$

Dimana m merupakan selisih dari d_i' dengan d_i, m didapatkan dengan menggunakan persamaaan berikut :

$$m = |d' - d| \quad (2.5)$$

Proses-proses tersebut dilakukan hingga semua bit pesan tersisipkan kedalam media cover.

Proses ekstraksi pesan dari citra stego menggunakan metode PVD dimulai dengan mengurutkan semua piksel pada *stego-object*, sesuai cara pengambilan pesannya. Kemudian dihitung selisih nilai *difference value* baru (d_i). Nilai tersebut digunakan untuk mengetahui nilai *continuous ranges* (R) yang sudah didefinisikan menggunakan skema Wu dan Tsai. Dengan demikian didapatkan pesan yang telah disisipkan (b').

Berdasarkan informasi tersebut dapat diketahui seberapa panjang data rahasia yang disisipkan pada kedua *pixel*, sehingga pesan rahasia yang telah disisipkan didapatkan kembali. Proses algoritma PVD untuk ekstraksi pesan dapat dijelaskan secara singkat sebagai berikut:

1. Hitung nilai d_i dengan persamaan berikut :

$$d_i = \mathrm{P_i'} - \mathrm{P_{i+1}'} \tag{2.6}$$

   Dimana $\mathrm{P_i'}$ dan $\mathrm{P_{i+1}'}$ adalah *pixel* dari *stego-object*.

2. Cari nilai u_i dan l_i yang merupakan nilai batas atas dan nilai batas bawah pada *range table* dengan menggunakan nilai d_i yang sudah didapatkan sebelumnya.
3. Hitunglah lebar (*width*) dari *optimum range* (w_i) dengan persamaan berikut :

$$w_i = u_i - l_i + 1 \tag{2.7}$$

4. Untuk mengetahui pesan yang telah disisipkan gunakan persamaan berikut :

$$b' = d_i - l_i \tag{2.8}$$

   Jika *stego-object* tidak berubah maka $b' = b$. Setelah mendapatkan nilai b' ubalah ke biner.
5. Gunakan perhitungan t_i pada persamaan (2.9) untuk mengetahui seberapa panjang bit pesan yang diekstraksi.

$$t_i = |log_2(w_i)| \tag{2.9}$$

6. Lakukan hingga semua *pixel* telah berhasil diekstraksi.

2.4 Kriptografi

Kriptografi berasal dari bahasa yunani yang terdiri dari kata *kryptos* yang berarti "*hidden, secret*" dan *graphin* yang berarti "*writing, study*". Jadi kriptografi

dapat diartikan sebagai sebuah ilmu yang mempelajari tentang bagaimana menyembunyikan informasi. Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Pradipta, 2016). Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan keamanan informasi, seperti kerahasiaan data dan autentifikasi data (Menezes, dkk., 1996).

Secara umum, kriptografi terdiri dari dua buah bagian utama yaitu enkripsi (*encryption*) dan dekripsi (*decryption*). Enkripsi adalah proses transformasi data menjadi bentuk lain sehingga isi pesan yang sebenarnya tidak dapat dipahami, hal ini dimaksudkan agar informasi tetap terlindung dari pihak yang tidak berhak menerimanya. Sedangkan dekripsi adalah proses kebalikan enkripsi, yaitu transformasi data terenkripsi ke data bentuk semula. Proses transformasi dari pesan asli (*plaintext*) menjadi pesan yang disamarkan (*ciphertext*) akan dikontrol oleh kunci. Kunci bersama-sama dengan algoritma matematisnya akan memproses *plaintext* menjadi *ciphertext* dan sebaliknya.

Tujuan utama kriptografi adalah menjaga kerahasiaan informasi dalam data agar informasi tersebut tidak dapat diketahui oleh pihak yang tidak diinginkan. Oleh karena itu dapat dikatakan bahwa kriptografi merupakan metode yang tangguh dalam menjaga kerahasiaan informasi karena data yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa menggunakan algoritma sandi. Sehingga kalaupun data tersebut dapat dibaca, maka tidak dapat dipahami oleh pihak yang tidak berhak. Berdasarkan tujuannya, kriptografi hanya memenuhi empat aspek dari keamanan informasi, yaitu :

1. Kerahasiaan (*confidentiality*), adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah disandi.
2. Integritas data (*integrity*), adalah layanan yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

3. Otentikasi (*authentication*), adalah layanan yang berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui jaringan harus diotentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. Non-repudiasi (*Non-repudiation*), adalah layanan yang mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

2.4.1 Notasi Matematis pada Kriptografi

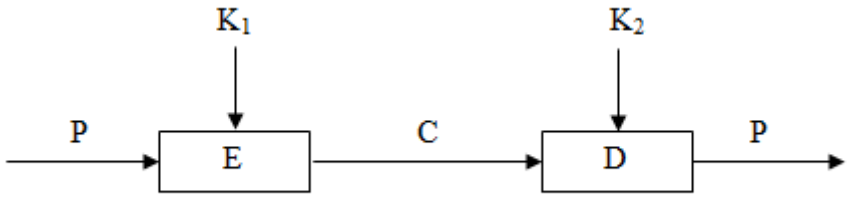
Jika *ciphertext* dilambangkan dengan *C* dan *plaintext* dilambangkan dengan *P*, maka fungsi enkripsi *E* memetakan *P* ke *C*, sebagaimana pada persamaan berikut :

$$E\ (P) = C \tag{2.10}$$

Proses kebalikannya, fungsi dekripsi *D* memetakan *C* ke *P*, sebagaimana pada persamaan berikut :

$$D\ (C) = P \tag{2.11}$$

Atau dengan kata lain, *D* adalah fungsi inversi dari *E*, atau $D = E^{-1}$



Gambar 2.3 Proses enkripsi dan dekripsi

Berdasarkan Gambar 2.3, maka dapat diperoleh model matematika berikut ini :

$$E\ (P, K_1) = C \tag{2.12}$$

$$D(E\ (P, K_1)) = P \text{ atau } D\ (C, K_2) = P \quad (2.13)$$

Dimana K_1 dan K_2 adalah kunci 1 dan kunci 2. Enkripsi pesan menggunakan kunci 1 sedangkan dekripsi menggunakan kunci 2.

2.4.2 Algoritma Kriptografi

Berdasarkan kunci yang digunakan dalam proses enkripsi dan dekripsi, algoritma kunci kriptografi dapat dibedakan menjadi 2 bagian, yaitu algoritma kriptografi kunci simetri dan algoritma kriptografi kunci asimetri (Toni, 2015).

a. Algoritma Simetris *(symmetric algorithm)*

Algoritma simetris disebut dengan algoritma kriptografi klasik, algoritma kriptografi kunci privat atau algoritma kriptografi konvensional. Hal tersebut dikarenakan kunci yang digunakan sama pada proses enkripsi dan dekripsi pesan. Keamanan menggunakan sistem ini terletak pada kerahasiaan kunci yang digunakan. Kekurangannya yaitu jika kunci dapat diketahui maka informasi pun dapat diketahui.

b. Algoritma Asimetris *(asymmetric algorithm)*

Algoritma asimetris disebut algoritma kunci publik, sebab kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun. Sementara kunci untuk dekripsi hanya diketahui oleh yang berwenang. Pada kriptografi jenis ini, setiap orang berkomunikasi mempunyai sepasang kunci, yaitu kunci privat (*private key*) dan kunci publik (*public key*). Algoritma asimetris mempunyai keamanan yang lebih baik, karena jika *public key* diketahui, informasi belum tentu diketahui karena *private key* kemungkinan berbeda. Namun pembuatan kunci untuk proses enkripsi memerlukan komputasi yang lebih intensif karena menggunakan bilangan-bilangan yang besar.

2.5 Hill Cipher

Metode *Hill Cipher* diciptakan oleh Leaster Hill pada tahun 1929 dalam jurnal *The American Mathematical Montly*. *Hill Cipher* merupakan salah satu algoritma kriptografi paling populer yang termasuk kedalam algoritma kunci simetri, yang menggunakan metode subtitusi dengan perhitungan perkalian matriks (Abood, 2017). *Hill Cipher* dikategorikan sebagai blok cipher karena pesan yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Selain itu *Hill Cipher* juga merupakan algoritma kriptografi *polyalphabetic*.

Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas *ciphertext* saja. Karena *Hill Cipher* tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya (Farid, dkk., 2016). Metode ini juga memiliki beberapa keuntungan termasuk ketahanan terhadap analisis frekuensi dan *implicity* (Puspita & Wayahdi, 2015). Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas ciphertext dan potongan berkas plaintext. Teknik kriptanalisis ini disebut *known- plaintext attack* (Megantara & Rafrastara, 2019).

Algoritma Hill Cipher merupakan salah satu algoritma ktiprografi yang memanfaatkan aritmatika modulo dan matriks. Setiap karakter pada plainteks dan cipherteks dikonversikan kedalam angka. Proses enkripsi dilakukan dengan memecahkan plainteks menjadi blok-blok ukuran *m* kemudian mengalikan setiap blok dengan matriks kunci *m* x *m*, sedangkan proses dekripsi mengalikan invers matriks kunci dengan blok matriks cipherteksnya. *Hill Cipher* hanya dapat menggunakan matriks persegi. Fungsi enkripsi dan dekripsi dapat didefinisikan sebagai berikut :

$$E(P) = P(K) \; mod \; m \tag{2.14}$$

$$D(C) = C(K^{-1}) \; mod \; m \tag{2.15}$$

P adalah blok *plaintext*, *C* adalah blok *ciphertext*, *K* adalah kunci (key). Kunci *K* berbentuk matriks. K^{-1} merupakan invers dari kunci. *M* adalah banyaknya karakter ataupun nilai yang akan dimodulokan.

Matriks kunci (K) merupakan matriks kunci yang berupa matriks persegi dan determinannya tidak sama dengan nol atau disebut juga sebagai matriks *invertible* dalam modulus *m*, dengan kata lain matriks kunci memiliki *multiplicative inverse* K^{-1} sehingga $K \cdot K^{-1} = K^{-1} \cdot K = I$. Kunci harus mempunyai invers karena kunci invers akan digunakan pada proses dekripsi.

Pada operasi perkalian di $\mathbb{Z}_m$ nilai identitas adalah 1 karena semua $a \in \mathbb{Z}_m$ berlaku $a \times 1 \equiv a(mod\ m)$. Jika a dan b di $\mathbb{Z}_m$ berlaku $a \times b \equiv 1\ (mod\ m)$ maka b merupakan invers perkalian terhadap a begitupun sebaliknya. Tidak semua elemen pada $\mathbb{Z}_m$ memiliki invers perkalian. Elemen yang memiliki invers perkalian hanya elemen yang merupakan bilangan relatif prima terhadap *m*, yaitu $a \in \mathbb{Z}_m$ berlaku $\gcd(m, a) = 1$.

Salah satu contoh kunci yang dapat digunakan pada $\mathbb{Z}_{95}$, yaitu :

$$K = \begin{bmatrix} 5 & 14 & 7 \\ 20 & 2 & 19 \\ 17 & 9 & 24 \end{bmatrix}$$

Catatan :

$\frac{1}{\det K} mod\ 95 = x$

$(\det K * x) mod\ 95 = 1$

Hitung nilai determinan kunci K dalam mod 95 dan cari nilai invers determinannya. Jika determinan kunci K memiliki nilai invers maka kunci K tersebut dapat digunakan pada operasi *Hill Cipher*.

$$K^{-1} = \frac{\text{adj}\ (K)}{|K|}$$

$$K^{-1} = \frac{1}{\det\ K} \begin{bmatrix} 67 & 12 & 62 \\ 33 & 1 & 45 \\ 51 & 3 & 15 \end{bmatrix} mod\ 95$$

$$K^{-1} = \frac{1}{14}\begin{bmatrix} 67 & 12 & 62 \\ 33 & 1 & 45 \\ 51 & 3 & 15 \end{bmatrix} mod\ 95$$

$$K^{-1} = 34\begin{bmatrix} 67 & 12 & 62 \\ 33 & 1 & 45 \\ 51 & 3 & 15 \end{bmatrix} mod\ 95$$

$$K^{-1} = \begin{bmatrix} 2278 & 408 & 2108 \\ 1122 & 34 & 1530 \\ 1734 & 102 & 510 \end{bmatrix} mod\ 95$$

$$K^{-1} = \begin{bmatrix} 93 & 28 & 18 \\ 77 & 34 & 10 \\ 24 & 7 & 35 \end{bmatrix} mod\ 95$$

2.6 Matriks

Matriks adalah susunan skalar elemen-elemen dalam bentuk baris dan kolom. Matriks A yang berukuran dari *m* baris dan *n* kolom ($m \times n$) adalah :

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \quad (2.16)$$

Entri a_{ij} disebut elemen matriks pada baris ke-*i* dan kolom ke-*j*. Jika *m* = *n*, maka matriks tersebut dinamakan juga matriks bujur sangkar (Munir, 2010). Matriks dengan elemen a_{ij} dimana $i = j$ = I dan elemen lainnya adalah 0 disebut matriks identitas (I).

$$I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (2.17)$$

Perkalian dua matriks A dan B dapat dilakukan jika jumlah kolom pada matriks A sama dengan jumlah baris pada matriks B. Sebuah matriks B disebut invers matriks dari matriks A jika $AB = I$, ditulis $B = A^{-1}$.

$$A^{-1} = \frac{1}{\det A}\ adj\ (A) \tag{2.18}$$

2.7 *Peak Signal to Noise Ratio* (PSNR)

Salah satu cara untuk mengetahui bahwa *stego-object* memiliki kualitas yang baik adalah dengan cara mengukur tingkat kesamaan antara cita asli dengan *stego-object*. Pengukuran dapat dilakukan dengan mengghitung *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) dari citra.

MSE adalah nilai error kuadrat rata-rata antara citra asli dengan citra manipulasi (dalam kasus steganografi, MSE adalah nilai error kuadrat rata-rata antara citra asli (media cover) dengan citra hasil penyisipan (*stego-ojbect*)). *Peak Signal to Noise Ratio* (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan desibel (dB). Untuk menentukan PSNR terlebih dahulu harus ditentukan nilai *Mean Square Error* (MSE).

$$MSE = \frac{1}{MN}\sum_{x=1}^{m}\sum_{y=1}^{n}[P(x,y) - P'(x,y)]^2 \tag{2.19}$$

Dimana : M dan N adalah dimensi citra.

$P(x,y)$ adalah nilai *pixel* citra asli.

$P'(x,y)$ adalah nilai *pixel stego-object*

$$PSNR = 10\ log_{10}\ \left(\frac{255^2}{MSE}\right) \text{ dB} \tag{2.20}$$

Semakin besar nilai PSNR, maka *stego-object* semakin mendekati citra aslinya, dengan kata lain kualitas dari *stego-object* semakin baik. Sebaliknya semakin kecil nilai PSNR semakin berkurang kualitas dari *stego-object* (Setiawan, 2013). Nilai PSNR yang baik yaitu lebih dari 30-50 dB (Mu'mi, 2017).

2.8 Kompresi File

Citra digital berdasarkan teknik kompresinya dapat dibedakan menjadi 2 (dua) macam teknik kompresi, yaitu *lossless* dan *lossy compression*. Kompresi

lossless adalah kompresi yang memungkinkan data yang asli dapat disusun kembali dari data kompresi. *Lossless* data kompresi digunakan dalam berbagai aplikasi seperti format Rar, ZIP dan GZIP. Sedangkan kompresi *lossy* menyebabkan adanya perubahan data dibandingkan sebelum dilakukan proses kompresi. Sebagai gantinya kompresi *lossy* memberikan derajat kompresi lebih tinggi. Tipe ini cocok untuk kompresi file suara digital dan gambar digital. File suara dan gambar secara alamiah masih bisa digunakan walaupun tidak berada pada kondisi yang sama sebelum dilakukan kompresi (Laia & Turnip, 2016). Teknik kompresi *lossy* juga dapat menghasilkan ukuran yang lebih kecil, namun ada kemungkinan informasi yang tersebunyi di dalamnya hilang karena banyak informasi dari citra yang akan dihapus (Wiryawan, dkk., 2019).

Discrete Cosine Transform (DCT) merupakan salah satu metode transformasi yang dapat digunakan untuk kompresi data citra yang mempunyai sifat *lossy*. Pada dasarnya DCT akan mengubah detil warna dari gambar asli, namun karena keterbatasan indera manusia, maka perubahan yang terjadi tidak begitu terlihat (Noviardhi, 2008). Terdapat dua persamaan yang dapat pada DCT yaitu DCT 1-dimensi yang digunakan untuk menghitung dua vektor dan DCT 2-dimensi yang digunakan untuk menghitung data matriks. Pada citra yang merupakan sinyal 2 dimensi, diperlukan persamaan DCT 2-dimensi. Untuk matriks $N \times M$, 2-D DCT dapat dihitung dengan cara 1-D DCT diterapkan pada setiap baris dari C dan kemudian hasilnya dihitung DCT untuk setiap kolomnya.

$$C(u,v) = \alpha(u)\,\alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} f(x,y) \cos\left(\frac{\pi(2x+1)u}{2N}\right) \cos\left(\frac{\pi(2x+1)v}{2M}\right) \quad (2.21)$$

dengan u = 0, 1, 2, ..., $N-1$, dan v = 0, 1, 2, ..., $M-1$

$$\alpha(u) = \begin{cases} \frac{1}{\sqrt{N}} & \text{untuk } u = 0 \\ \sqrt{\frac{2}{N}} & \text{untuk } u \neq 0 \end{cases} \quad (2.22)$$

$$\alpha(v) = \begin{cases} \frac{1}{\sqrt{M}} & \text{untuk } u = 0 \\ \sqrt{\frac{2}{M}} & \text{untuk } u \neq 0 \end{cases} \quad (2.23)$$

Ket :

M, N = Banyaknya kolom dan baris.

$C(u,v)$ = Titik koordinat dari matriks yang telah mengalami transformasi 2-D DCT.

$f(x,y)$ = Nilai piksel dari matriks pada titik (x,y).

$\alpha(u)\ \alpha(v)$ = Himpunan hasil yang nilainya ditentukan dari koefisien u dan v.

Pada matriks $N \times N, C * A$ merupakan matriks yang kolomnya berisi 1-D DCT dari kolom A. Oleh karena itu 2-D DCT dapat dihitung dengan $B = C * A * C^T$ (MathWorks, 2021).

Contoh penerapan DCT pada sebuah matriks 2 dimensi :

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

$u = 0, 1, 2$ dan $v = 0, 1, 2$

Untuk u = 0

v = 0, $C(0,0) = \frac{1}{\sqrt{M}} = \frac{1}{\sqrt{3}}$

v = 1, $C(0,1) = \frac{1}{\sqrt{M}} = \frac{1}{\sqrt{3}}$

v = 2, $C(0,2) = \frac{1}{\sqrt{M}} = \frac{1}{\sqrt{3}}$

Untuk u = 1

v = 0, $C(1,0) = \sqrt{\frac{2}{M}} \cos\left(\frac{\pi(2v+1)u}{2M}\right) = \sqrt{\frac{2}{3}} \cos\left(\frac{\pi(2*0+1)1}{2*3}\right) = \frac{1}{\sqrt{2}}$

v = 1, $C(1,1) = \sqrt{\frac{2}{M}} \cos\left(\frac{\pi(2v+1)u}{2M}\right) = \sqrt{\frac{2}{3}} \cos\left(\frac{\pi(2*1+1)1}{2*3}\right) = 0$

v = 2, $C(1,2) = \sqrt{\frac{2}{M}} \cos\left(\frac{\pi(2v+1)u}{2M}\right) = \sqrt{\frac{2}{3}} \cos\left(\frac{\pi(2*2+1)1}{2*3}\right) = -\frac{1}{\sqrt{2}}$

Untuk u = 2

v = 0, $C(2,0) = \sqrt{\frac{2}{M}} \cos\left(\frac{\pi(2v+1)u}{2M}\right) = \sqrt{\frac{2}{3}} \cos\left(\frac{\pi(2*0+1)2}{2*3}\right) = \frac{1}{6}$

$v = 1, C(2,1) = \sqrt{\frac{2}{M}} \cos\left(\frac{\pi(2v+1)u}{2M}\right) = \sqrt{\frac{2}{3}} \cos\left(\frac{\pi(2*1+1)2}{2*3}\right) = -\sqrt{\frac{2}{3}}$

$v = 2, C(2,2) = \sqrt{\frac{2}{M}} \cos\left(\frac{\pi(2v+1)u}{2M}\right) = \sqrt{\frac{2}{3}} \cos\left(\frac{\pi(2*2+1)2}{2*3}\right) = \frac{1}{\sqrt{6}}$

Sehingga diperoleh,

$$C(u,v) = \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{6}} & -\sqrt{\frac{2}{3}} & \frac{1}{\sqrt{6}} \end{bmatrix}$$

Matriks hasil transformasi dapat diketahui dengan menggunakan persamaan berikut :

$$B = C * A * C^T$$

$$B = \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{6}} & -\sqrt{\frac{2}{3}} & \frac{1}{\sqrt{6}} \end{bmatrix} \begin{bmatrix} 9 & 8 & 7 \\ 6 & 5 & 4 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{6}} & -\sqrt{\frac{2}{3}} & \frac{1}{\sqrt{6}} \end{bmatrix}^T$$

$$= \begin{bmatrix} 15 & \sqrt{6} & 0 \\ 3\sqrt{6} & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$