BAB II
KAJIAN PUSTAKA DAN DASAR TEORI

2.1 Konsep Dasar Kriptografi

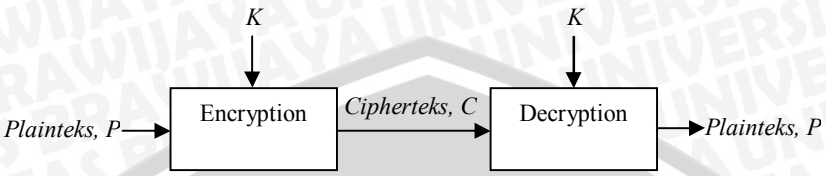
Kriptografi berasal dari bahasa Yunani, yaitu *kripto* dan *graphia*. *Kripto* berarti rahasia (*secret*) dan *graphia* berarti tulisan (*writing*). Menurut teminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Ariyus, 2008).

Tujuan mendasar dalam kriptografi adalah untuk keamanan informasi, mencegah dan mendeteksi kecurangan dan kegiatan yang terlarang. Menurut Menezes, pengamanan pesan yang dilakukan mencakup beberapa aspek yang termasuk dalam aspek keamanan informasi, yaitu:

1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki wewenang atau kunci rahasia untuk membuka atau mengupas informasi yang telah disandi.
2. Integritas data, adalah berhubungan dengan penjagaan dari perubahan. data 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. Autentikasi, adalah berhubungan dengan identifikasi atau pengenalan baik secara kesatuan sistem maupun informasi itu sendiri. Dengan kata lain, informasi itu benar-benar datang dari orang yang dikehendaki.
4. *Non-repudiation*, adalah usaha untuk mencegah suatu pihak untuk menyangkal aksi yang sudah dilakukan sebelumnya.

Teknik kriptografi pada dasarnya terdiri dari dua proses, yaitu proses enkripsi dan proses dekripsi. Proses enkripsi adalah proses penyandian pesan terbuka menjadi pesan rahasia (*ciphertext*). *Ciphertext* inilah yang nantinya akan dikirimkan melalui saluran komunikasi terbuka. Pada saat *ciphertext* diterima oleh penerima pesan, maka pesan rahasia tersebut diubah lagi menjadi pesan terbuka

melalui proses dekripsi sehingga pesan tadi dapat dibaca kembali oleh penerima pesan. Secara umum, proses enkripsi dan dekripsi dapat digambarkan sebagai berikut (Wahana, 2003) :



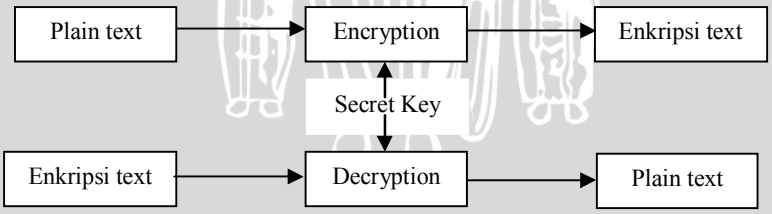
Gambar 2.1 Proses Enkripsi dan Dekripsi

2.2 Algoritma Kriptografi

Terdapat dua jenis algoritma kriptografi berdasar jenis kuncinya, yaitu:

2.2.1 Algoritma Simetris

Algoritma simetris disebut juga sebagai algoritma konvensional, yaitu algoritma yang menggunakan kunci yang sama pada proses enkripsi dan dekripsi. Pada Gambar 2.2 memperlihatkan skema algoritma simetri yang hanya membutuhkan satu buah kunci yang sama. Keamanan algoritma simetris tergantung pada kuncinya. Algoritma simetris sering juga disebut algoritma kunci rahasia, algoritma kunci tunggal atau algoritma satu kunci. Dua kategori yang termasuk pada algoritma simetris ini adalah algoritma *block cipher* dan *stream cipher* (Kurniawan, 2004).



Gambar 2.2 Algoritma Kriptografi Simetris

(sumber : Nugraha Ilham, 2008)

Kelebihan algoritma kriptografi simetris adalah:

1. Algoritma ini dirancang sehingga proses enkripsi/dekripsi membutuhkan waktu yang singkat.
2. Ukuran kunci relatif lebih pendek.

3. Algoritmanya bisa menghasilkan *cipher* yang lebih kuat.
4. Autentikasi pengiriman pesan langsung diketahui dari *ciphertext* yang diterima, karena kuncihanya diketahui oleh pengirim dan penerima pesan saja.

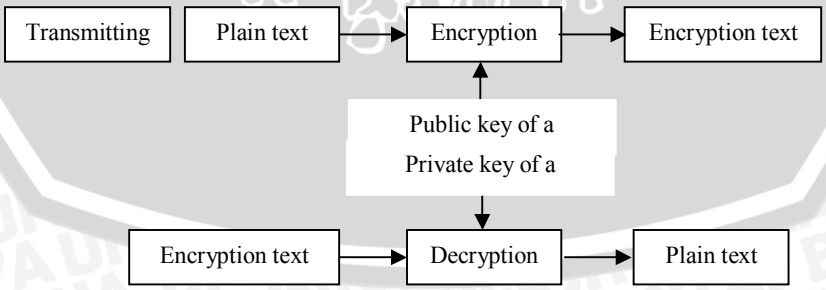
Kelemahan algoritma kriptografi simetris adalah:

1. Kunci harus dikirim melalui saluran yang aman. Kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci ini.
2. Kunci harus sering diubah, mungkin pada setiap sesi komunikasi (Munir, 2004).

2.2.2 Algoritma Asimetri

Algoritma asimetrik atau biasa disebut algoritma kunci publik dirancang sedemikian sehingga kunci yang digunakan dalam proses enkripsi dan dekripsi berbeda. Pada Gambar 2.3 memperlihatkan skema algoritma asimetri yang menggunakan dua buah kunci. Sehingga kunci dekripsi tidak dapat dihitung dari kunci enkripsi. Algoritma tersebut disebut *public-key* karena kunci enkripsi dapat dibuat secara *public*.

Orang asing dapat menggunakan kunci enkripsi tersebut untuk mengenkripsi sebuah pesan, tetapi hanya orang tertentu dengan kunci dekripsi sepadan dapat mendekripsi pesan tersebut. Dalam sistem ini kunci enkripsi sering disebut *public key* sedangkan key dekripsi sering disebut *private key* (Kurniawan, 2004).



Gambar 2.3 Algoritma Kriptografi Asimetris

(sumber : Wibowo Ivan, 2009)

Kelebihan algoritma kriptografi asimetri adalah:

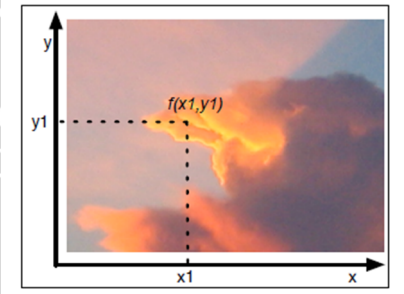
1. Hanya *Private key* yang harus benar-benar rahasia/aman.
2. Sangat jarang untuk perlu merubah *public key* dan *private key*.

Kelemahan algoritma kriptografi asimetri adalah:

a. Ukuran kunci lebih besar dari pada algoritma kunci simetri.
b. Tidak adanya jaminan bahwa *public key* benar-benar aman (Munir, 2004).

2.3 Konsep Dasar Citra Digital

Citra digital dapat didefinisikan sebagai fungsi dua variable *f(x,y)*, dimana *x* dan *y* adalah koordinat spasial dan nilai *f (x,y)* adalah intensitas citra pada koordinat tersebut, hal tersebut diilustrasikan pada Gambar 2.4. Teknologi dasar untuk menciptakan dan menampilkan warna pada citra digital berdasarkan pada penelitian bahwa sebuah warna merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau, dan biru (*Red, Green, Blue* – RGB) (Gonzalez Rafael C. , 2002)



Gambar 2.4. Citra Digital
(Gonzalez Rafael C., 2002)

Sebuah citra diubah ke bentuk digital agar dapat disimpan dalam memori komputer atau media lain. Proses mengubah citra ke bentuk digital bisa dilakukan dengan beberapa perangkat, misalnya *scanner*, kamera digital, dan *handycam*. Ketika sebuah citra sudah diubah ke dalam bentuk digital (selanjutnya disebut citra digital), bermacam – macam proses pengolahan citra dapat diperlakukan terhadap citra tersebut.

Pengolahan citra digital dapat dilakukan dengan cara – cara sebagai berikut :

1. Representasi dan pemodelan citra
2. Peningkatan kualitas citra

3. Restorasi citra
4. Analisis citra
5. Rekonstruksi citra
6. Kompresi citra

2.4 Warna dan Ruang Warna

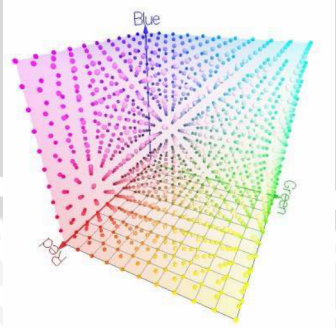
Warna merupakan hasil persepsi dari warna cahaya dalam spektrum wilayah yang terlihat oleh retina mata, dengan panjang gelombang antara 400/nm sampai dengan 700/nm.

Ruang warna atau yang sering juga disebut sebagai model warna merupakan sebuah cara atau metode untuk menentukan, membuat dan memvisualisasikan warna. Dalam skripsi ini, penulis hanya akan membahas beberapa ruang warna yang biasa digunakan untuk aplikasi *watermarking*. Beberapa ruang warna tersebut antara lain adalah sebagai berikut (Gonzalez Rafael C, 2002):

1. RGB (*Red, Green, Blue*)
2. HSI (*Hue Saturation Intensity*)
3. YCbCr (*Luminance – Chrominance*)

2.4.1 RGB (*Red Green Blue*)

Citra berwarna umumnya memiliki ruang warna RGB. Ruang warna RGB dapat divisualisasikan sebagai sebuah kubus, dengan tiga sumbunya yang mewakili komponen warna merah(*red*)R, hijau (*green*)G, dan biru (*blue*)B.



Gambar 2.5. Ruang warna RGB
(sumber : http://www.couleur.org/, 2013)

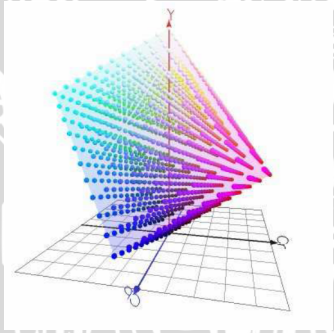
RGB sering digunakan didalam sebagian besar aplikasi komputer karena dengan ruang warna ini, tidak diperlukan transformasi untuk menampilkan informasi di layar monitor. Hal tersebut juga menyebabkan RGB banyak dimanfaatkan sebagai ruang warna dasar bagi sebagian besar aplikasi.

2.4.2 HSI (*Hue Saturation Intensity*)

Untuk menyediakan repersentasi warna bagi antar – muka pengguna (*user interface)* , biasa digunakan ruang warna HIS. HIS sendiri merupakan kependekan dari *Hue*, *Saturation, Intensity*).

2.4.3 YCbCr (*Luminance – Chrominance*)

YCbCr merupakan standart internasional bagi pengkodean digital gambar televise yang didefinisikan di CCIR *Recommended* 601. Y merupakan komponen luminance, C_b dan C_r adalah komponen *chrominance*.

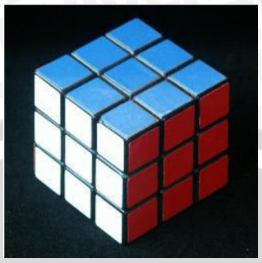


Gambar 2.6 Ruang Warna Y C_bC_r
(sumber : http://www.couleur.org/, 2009)

2.5 Rubic's Cube

Rubik's Cube adalah sebuah *twisty puzzle*, yaitu permainan puzzle mekanik tiga dimensi yang ditemukan pada tahun 1974 oleh seorang pemahat dan professor arsitektur dari Hungaria bernama Erno Rubik . Rubik member nama hasil temuanny yaitu *Magic Cube* , yang kemudian dipatenkan di Hungaria dan dijual pertama kali melalui perusahaan Ideal Toy Corporation. Pada tahun 1980, perusahaan Ideal Toy mengubah nama *magic cube* tersebut menjadi "*Rubik's*

Cube". Dan hingga saat ini, lebih dari 350 juta *Rubik's Cube* telah dijual di seluruh dunia (Michaelale, 2013).



Gambar 2.7 Rubik's Cube

(sumber : http://www.rubiks.com/, 2013)

2.5.1 Dasar Algoritma *Rubic's Cube*

Algoritma *Rubic'c cube* berkerja dengan menggunakan prisip dari kubus rubic, Gambar 2.7. proses enkripsi dan dekripsi dilakukan dengan melakukan proses pergeseran pada masing-masing baris dan kolom piksel citra digital. Dimisalkan I adalah citra digital dengan α-bit dan ukuran panjang x lebar adalah M x N. Nilai matrik piksel dari I diwakili dengan notasi Io, K untuk kunci (Loukhaoukha K, 2012). Berikut ini detail variable yang digunakan dalam proses enkripsi dan dekripsi citra menggunakan algoritma *Rubic's Cube*:

1. *I*, merupakan simbol variable untuk matrik piksel dari citra digital baik untuk citra hasil dekripsi ataupun citra asli yang digunakan
2. *K*, merupakan simbol variable untuk kunci. Dimana kunci ini digunakan untuk melakukan operasi pergeseran pada baris dan kolom matrik piksel serta untuk operasi biner pada piksel.
3. *ITER*, merupakan simbol variable untuk proses iterasi atau perulangan.
4. α , merupakan simbol variable untuk perhitungan baris pada matrik piksel.
5. β, merupakan simbol variable untuk perhitungan kolom padaa matrik piksel.
6. M, merupakan simbol variable hasil modulo dari nilai α atau nilai β

2.5.2 Proses Enkripsi Algoritma *Rubic's Cube*

Proses enkripsi merupakan proses untuk melakukan pengacakan matrik Io dengan menggunakan metode *Rubic's cube*. Berikut ini detail variable yang digunakan dalam proses enkripsi citra menggunakan algoritma *Rubic's Cube*:

1. *Ienc, Io, I1, Ii, Iscr* : merupakan simbol variable untuk matrik piksel dari citra, baik yang digunakan pada proses enkripsi maupun hasil enkripsi .
2. K_C, K_R : merupakan simbol variable untuk kunci untuk proses jumlah pergeseran baris , kolom dan proses operasi xor.
3. *ITER, ITERmax, i, j* : merupakan simbol variable untuk proses iterasi atau perulangan.
4. $\alpha(i)$, merupakan simbol variable untuk perhitungan masing-masing baris pada matrik piksel.
5. $\beta(i)$, merupakan simbol variable untuk perhitungan masing-masing kolom pada matrik piksel.
6. $M_\alpha(i)$, $M_\beta(j)$:merupakan simbol variable hasil modulo dari nilai α atau nilai β

Berikut ini tahapan dari proses enkripsi pada algoritma *Rubic's cube:*

1. Inisialisasi bilangan kunci pada dua vektor K_R dan K_C dengan panjang masing-masing M dan N. Pada masing elemen K_R dan K_C diisi dengan nilai $\{0, 1, 2, \ldots, 2^{\alpha} - 1\}$.
2. Inisialisasi jumlah dari iterasi, *ITERmax* dan memberikan nilai *ITER* = 0.
3. Menambahkan nilai *ITER* = *ITER* +1.
4. Melakukan proses perulangan pada tiap-tiap baris *i* pada matrik Io, proses tersebut antara lain :

   a. Menghitung jumlah semua elemen pada baris *i*, dimana jumlah tersebut diwakili dengan notasi $\alpha(i)$, dengan persamaan 2.1.

$$\alpha(i) = \sum_{j=1}^{N} Io(i,j), \qquad i = 1,2 \ldots M \tag{2.1}$$

   b. Menghitung nilai $M_\alpha(i)$ dimana $M_\alpha(i)$ adalah modulo 2 dari $\alpha(i)$,

$$M\alpha(i) = \alpha(i) \bmod 2$$

(2.2)

c. Pada baris *i* dirotasi dengan posisi K_R(i) dimana piksel pada citra diganti dengan posisi K_R(i) pada arah kanan atau kiri, dan piksel pertama dipindah pada akhir piksel, dapat diperlihatkan dengan persamaan 2.3.

$$if\ M\alpha(i) = 0 \rightarrow Rotasi\ Kekanan$$
$$else\ \rightarrow Rotasi\ Kekiri$$

(2.3)

5. Melakukan proses perulangan pada tiap-tiap kolom *j* pada matrik *Io*, proses tersebut antara lain :

a. Menghitung semua elemen pada kolom *j*, yang dinotasikan dengan $\beta(j)$, dengan menggunakan persamaan 2.4:

$$\beta(j) = \sum_{i=1}^{M} Io(i,j), \qquad j = 1,2 \ldots N$$

(2.4)

b. Menghitung $M_\beta(j)$ dimana $M_\beta(j)$ adalah modulo 2 dari $\beta(j)$.

$$M\beta(i) = \beta(i) \bmod 2$$

(2.5)

c. Menggeser naik atau turun pada kolom *j* dengan posisi *Kc*(i), dapat diperlihatkan dengan persamaan 2.6.

$$if\ M\beta(i) = 0 \rightarrow Rotasi\ Keatas$$
$$else\ \rightarrow Rotasi\ Kebawah$$

(2.6)

6. Pada langkah 4 dan 5 dihasilkan citra inisialisasi acak dengan simbol I_{SCR}. Kemudian pada masing-masing baris I_{SCR}, dilakukan operasi biner XOR dengan vector K_C, dengan menggunakan persamaan 2.7 :

$$I1(2i-1,j) = Iscr(2i-1,j) \oplus Kc(j)$$
$$Ii(2i,j) = Iscr(2i,j) \oplus rot180(Kc(j))$$

(2.7)

Dimana $\oplus$ dan rot180 (K_C) adalah proses operasi bit XOR dan pergeseran vector K_C dari atas ke bawah atau sebaliknya.

7. Pada masing-masing kolong dari I_1 dilakukan operasi biner XOR dengan K_R dengan menggunakan persamaan 2.8 :

$$Ienc(i, 2j-1) = Iscr(i, 2j-1) \oplus Kr(j)$$
$$Ienc(i, 2j) = Iscr(i, 2j) \oplus rot180(Kr(j)) \quad (2.8)$$

Dimana rot180(K_R) adalah proses pergeseran dari kiri ke kanan pada vector K_R.

8. Jika *ITER* = *ITERmax* maka proses selesai dan gambar terenkripsi disimpan pada I_{enc}, dan jika tidak maka menuju langkah ke 3.
9. Pembentukan citra baru yang sudah terenkripsi dari matrik I_{enc}.

2.5.3 Proses Dekripsi Algoritma *Rubic's Cube*

Proses dekripsi adalah proses mengembalikan citra yang telah terenkripsi kedalam bentuk citra asli, dimana vector K_R , K_C *ITERmax* dan merupakan kunci dari algoritma ini. Selain itu untuk mendapatkan proses yang lebih cepat maka digunakan *ITERmax* = 1. Sebaliknya jika *ITERmax* lebih dari 1 maka akan dihasilkan citra enkripsi yang lebih aman karena proses pergeseran key lebih besar jika dibandingkan jika dengan *ITERmax* =1 (Loukhaoukha. K, 2013).. Gambar yang telah terenkirpsi dinotasikan dengan I_{enc} dan *Io* merupakan citra hasil dekripsi dari parameter K_R, *Kc* dan *ITERmax*. Berikut detail variable yang digunakan dalam proses dekripsi citra menggunakan algoritma *Rubic's Cube*:

1. *Ienc, Io, I1, Ii, Iscr* : merupakan simbol variable untuk matrik piksel dari citra , baik yang digunakan pada proses dekripsi maupun hasil dekripsi .
2. K_C, K_R : merupakan simbol variable untuk kunci untuk proses jumlah pergeseran baris , kolom dan proses operasi xor.
3. *ITER, ITERmax, i, j* : merupakan simbol variable untuk proses iterasi atau perulangan.

4. $\alpha scr(i)$, merupakan simbol variable untuk perhitungan masing-masing baris pada matrik piksel.
5. $\beta scr(i)$, merupakan simbol variable untuk perhitungan masing-masing kolom pada matrik piksel.
6. $M_{\alpha scr}(i)$, $M_{\beta scr}(j)$:merupakan simbol variable hasil modulo dari nilai α atau nilai β

Langkah-langkat dari proses dekripsi yakni:

1. Inisialisasi *ITER* = 0
3. Menambahkan dengan 1 nilai *ITER*, *ITER* = *ITER* +1.
4. Melakukan proses operasi bit XOR pada vector K_R dan tiap-tiap kolom dari citra yang terenkripsi I_{enc} dengan persamaan 2.9.

$$I1(i, 2j-1) = Ienc(i, 2j-1) \oplus Kr(j)$$
$$I1(i, 2j) = Ienc(i, 2j) \oplus rot180(Kr(j)) \quad (2.9)$$

4. Kemudian dengan menggunakan vector K_C, dilakukan operasi bit XOR dengan tiap-tiap baris pada citra I_1 dengan persamaan 2.10 :

$$Iscr(2i-1, j) = I1(2i-1, j) \oplus Kc(j)$$
$$Iscr(2i, j) = I1(2i, j) \oplus rot180(Kc(j)) \quad (2.10)$$

5. Pada tiap-tiap kolom I_{enc} yang merupakan citra teracak, dilakukan proses :
   a. Menghitung jumlah semua elemen pada colom *j*, yang disimbolkan dengan $\beta_{SCR}(j)$ dengan persamaan 2.11

$$\beta scr(j) = \sum_{i=1}^{M} Iscr(i, j), \qquad j = 1,2 \ldots N \quad (2.11)$$

   b. $M_{\beta SCR}(i)$ adalah modulo 2 dari βSCR(*i*),

$$M\beta scr(i) = \beta scr(i) \bmod 2 \quad (2.12)$$

   c. Menggeser naik atau turun pada kolom *j* dengan posisi *Kc*(i), dapat diperlihatkan dengan.

$$if M\beta scr(i) = 0 \rightarrow Rotasi\ Kekeatas$$
$$else \rightarrow Rotasi\ Kebawah$$

(2.13)

6. Pada tiap-tiap kolom pada citra I_{scr}, dilakukan proses:
   a. Menghitung jumlah semua elemen pada baris i yang dinotasi dengan $\alpha_{SCR}(i)$, dengan menggunakan persamaan 2.14 :

$$\alpha scr(i) = \sum_{j=1}^{N} Iscr(i,j), \quad i = 1,2 \ldots M$$

(2.14)

   b. $M_{\alpha SCR}(i)$ adalah modulo 2 dari $\alpha_{SCR}(j)$,

$$Mascr(i) = \alpha scr(i) \bmod 2$$

(2.15)

7. Pada baris i digeser dengan posisi $K_R(i)$, dapat diperlihatkan dengan:

$$if\ Mascr(i) = 0 \rightarrow Rotasi\ Kekanan$$
$$else \rightarrow Rotasi\ Kekiri$$

(2.16)

8. Jika *ITER* = *ITERmax* maka proses selesai dan gambar hasil disimpan pada *Iscr*, dan jika tidak maka menuju langkah ke 2.
9. Pembentukan citra baru yang sudah terdekripsi dari matrik *Iscr*.

2.5.4 Operator XOR

Operator biner yang sering digunakan dalam *cipher* yang beroperasi dalam mode bit adalah *XOR* atau *exclusive-or* dan notasi matematis untuk operator *XOR* adalah "⊕" (Kur2003, 2003).

Operator *XOR* dioperasikan pada dua bit dengan aturan sebagai berikut:

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

Perhatikan bahwa operator *XOR* identik dengan penjumlahan modul 2:

$$0 + 0 \pmod 2 = 0$$

$$0 + 1 \pmod 2 = 1$$

$$1 + 0 \pmod 2 = 1$$

$$1 + 1 \pmod 2 = 0$$

Jika dua rangkaian dioperasikan dengan *XOR*, maka operasinya dilakukan dengan meng-*XOR*-kan setiap bit yang berkoresponden dari kedua rangkaian bit tersebut.

Contoh: 10011 ⊕ 11001 = 01010, yang dalam hal ini, hasilnya diperoleh sebagai berikut:

$$\begin{array}{ccccccc} 1 & & 0 & & 0 & 1 & 1 \\ 1 & & 1 & & 0 & 0 & 1 \quad \oplus \\ \hline 1 \oplus 1 & & 0 \oplus 1 & & 0 \oplus 0 & 1 \oplus 0 & 1 \oplus 1 \\ 0 & & 1 & & 0 & 1 & 0 \end{array}$$

Algoritma enkripsi sederhana yang menggunakan *XOR* adalah dengan meng-*XOR*-kan *plainteks* (*P*) dengan kunci (*K*) menghasilkan cipherteks seperti yang ditunjukan pada Persamaan 2.17:

$$C = P \oplus K \qquad (2.17)$$

Karena meng-*XOR*-kan nilai yang sama dua kali berturut-turut menghasilkan nilai semula, maka dekripsi menggunakan Persamaan 2.18:

$$P = C \oplus K \qquad (2.18)$$

2.6 *Mean Square Error* (MSE)

MSE merupakan salah satu cara untuk mengukur jumlah perbedaan antara nilai perkiraan dengan nilai yang sebenarnya. MSE mengukur rata – rata wilayah kesalahan (*error*). MSE (*Mean Square Error*) merupakan sigma dari jumlah kesalahan (*error*) antara citra hasil kompresi dan citra asli. Perhitungan nilai MSE

dari citra digital berukuran NxM, dilakukan sesuai dengan persamaan 2.19, dimana nilai MSE yang rendah akan lebih baik (S. Linda, 2005).:

$$MSE = \frac{1}{MN}\sum_{Y=1}^{M}\sum_{X=1}^{N}[I(x,y) - I'(x,y)]^2 \quad (2.19)$$

Dimana I(x,y) adalah nilai piksel di citra asli,
I'(x,y) adalah nilai piksel pada citra hasil kompresi,
M,N adalah dimensi citra.

2.7 Peak Signal Noise to Ratio (PSNR)

PSNR merupakan salah satu cara untuk mengukur tingkat kesalahan akibat hilangnya informasi atau perubahan piksel pada citra. PSNR memiliki satuan decibel (dB), semakin besar nilai PSNR semakin bagus kualitas hasil. Perhitungan nilai PSNR dari citra digital berukuran N x M, dilakukan sesuai dengan persamaan 2.20, dimana nlai PSNR yang tinggi menunjukkan nilai yang lebih baik (S. Linda, 2005).

$$PSNR = 20xLog10\left(\frac{255}{\sqrt{\frac{1}{MN}\sum_{Y=1}^{M}\sum_{X=1}^{N}[I(x,y) - I'(x,y)]^2}}\right) \quad (2.20)$$

Dimana I(x,y) adalah nilai piksel di citra asli,
I'(x,y) adalah nilai piksel pada citra hasil,
M,N adalah dimensi citra.

2.8 Analisis Korelasi

Analisis korelasi adalah metode statistika yang digunakan untuk menentukan kuatnya atau derajat hubungan linier antara dua variable atau lebih. Semakin nyata hubungan linier (garis lurus), maka semakin kuat atau tinggi derajat hubungan

garis lurus antara kedua variable. Ukuran untuk derajat hubungan garis lurus ini dinamakan koefisien korelasi. Persamaan koefisien korelasi diperlihatkan pada persamaan 2.21. Dimana nilai hasil dari proses analisis korelasi digunakan untuk mengetahui hubungan korelasi antara citra asli dan citra hasil dari proses dekripsi.

$$r_x = \frac{n(\sum xy) - (\sum x - \sum y)}{\sqrt{\{n\sum x^2 - (\sum x)^2\}\{n\sum y^2 - (\sum y)^2\}}} \quad (2.21)$$

Dimana r adalah nilai koefisien korelasi
n adalah jumlah responden,
x adalah nilai image asli,
y adalah nilai image uji,

Nilai r tidak lebih dari harga (-1≤r≤ 1). Apabila nilai r =-1 artinya korelasi negatif sempurna; r = 0 artinya tidak adakorelasi; dan r = 1 artinya korelasinya sangat kuat (Usu , 2013). Interpretasi koefisien korelasi nilai r diperlihatkan pada Tabel 2.1.

Tabel 2.1 Interpretasi koefisien korelasi

Interval	Koefisien Tingkat Hubungan
0,800–1,000	Sangat Kuat
0,600–0,799	Kuat
0,400–0,599	Cukup Kuat
0,200–0,399	Lemah
0,000–0,199	Sangat Lemah

.