BAB II
TINJAUAN PUSTAKA DAN DASAR TEORI

2.1. Tinjauan Pustaka

Setelah melakukan penelusuran terhadap beberapa penelitian terdahulu, ada beberapa yang penelitian yang memiliki keterkaitan dengan penelitian yang dilakukan. Penelitian yang dilakukan oleh (Ariska dkk., 2018). Tujuan dari penelitian ini adalah penelitian tersebut berfokus pada racangan atau uraian proses pembentukan kunci, proses enkripsi dan proses dskripsi dalam pengamatan pesan menggunakan dua metode kriptografi. Metode yang duganakan dalam penelitian tersebut terdiri dari mengindetidfikasi masalah kemudian dialkukannya studi literature lalu menganalisa masalah yang terjadi. Jika sudah mendapatkan solusi, peneliti menerapkan kriptografi hybrid lalu di proses yang menggunakan kombinasi dari dua metode. Setelah dikombinasi, peneliti melakukan proses enkripsi menggunakan kunci publik lalu dari proses tersebut didapatkan ciperteks hasil enkripsi dari dua metode setelah proses kunci publik, peneliti menggunakan proses deskripsi menggunakan kunci rahasia. Dari proses deskripsi kunci rahasia, didapatkan plainteks hasil deskripsi dua metode yang mana merupakan sebuah pesan asli.

Penelitian yang dilakukan oleh (Ikhsan dkk., 2018) dengan judul. Tujuan dari penelitian ini adalah untuk meningkatkan keamanan dan kerahasiaan kominkasi media sosial dengan menggabungkan berbagai teknik kriptografi dan metode penyembunyian pesan. Dari penelitian ini, peneliti memodifikasi Vigenere Cipher dan Caesar Cipher dengan diagram Cartesius kemudian hasil enkripsi disisipkan pada dokumen/gambar menghasilkan data enkripsi yang susah untuk dipecahkan dan memerlukan waktu untuk melakukan dekripsi sehingga data/informasi yang penting aman setelah dilakukan enkripsi.

Penelitian yang dilakukan oleh (Cadullah, 2023) dengan judul. Tujuan dari penelitian tersebut untuk menerapkan enkripsi dan deskripsi menggunakan metode ECC (Elliptic Curve Cryptography) dan Vigenere Cipher serta untuk menyembunyikan dan mengekstrak pesan pada citra dengan menerapkan metode

Ind of File (EoF). Pengujian menggunakan aplikasi matlab dan berhasil membuat sebuah aplikasi enkrpsi dan deskripsi sehingga aplikasi tersebut dapat untuk membuktikan jawaban yang dihasilkan konverter sesuai dengan jawaban menggunakan rumus atau algoritma yang digunakan. Dari pengujian fungsionalitas dan akurasi perhitungan diketahui bahwa penggunaan algortima Vigenere serta algoritma ECC dapat dengan baik melakukan proses enskripsi dan dekripsi dari pesan yang diinputkan dan pada proses steganografi diketahui bahwa pesan text berhasil disisipkan (disembunyikan) pada bagian akhir dari file sebuah citra. Tetapi tidak berhasil kembali diekstrak dari file citra, sehingga pesan tidak dapat dibaca kembali.

Penelitian yang dilakukan oleh (Boukerrou dkk., 2024) yang melakukan pendekatan desain cipher sinkronisasi-diri (*Self-Synchronizing Stream Cipher* - SSSC) menggunakan sistem dinamis hibrida berbasis *Linear Parameter Varying* (LPV) untuk meningkatkan keamanan pada sistem siber-fisik (*Cyber-Physical Systems* - CPS). Dengan memanfaatkan properti *flatness* dan analisis struktural, desain cipher ini diformulasikan ulang sebagai masalah kontrol-teoretik untuk memastikan sinkronisasi otomatis antara enkripsi dan dekripsi. Sistem LPV dipilih karena fleksibilitasnya dalam mengintegrasikan non-linearitas melalui parameterisasi, yang relevan untuk keamanan kunci rahasia. Pendekatan ini menjawab tantangan sinkronisasi, kompleksitas komputasi, dan keamanan, dengan memanfaatkan graf berarah (digraph) untuk menjamin *flatness* struktural. Hasil penelitian menunjukkan bahwa metode ini menghasilkan SSSC yang efisien, tahan terhadap serangan, dan mampu memenuhi kebutuhan enkripsi data dengan throughput tinggi, menjadikannya solusi yang relevan untuk aplikasi komunikasi modern.

Penelitian yang dilakukan oleh (Junling, 2024) yang pengembangan korpus besar untuk pengajaran bahasa Inggris dan sistem pembelajaran elektronik berbasis algoritma Apache Hadoop. Dengan menggabungkan model komputasi MapReduce, sistem ini meningkatkan kemampuan pengolahan data secara paralel, mendukung efisiensi tinggi, skalabilitas, dan toleransi kesalahan. Dalam pengajaran bahasa Inggris, penggunaan korpus membantu meningkatkan metode pembelajaran,

memperkaya materi, dan meningkatkan interaksi antara siswa dan guru. Studi ini menunjukkan bahwa pendekatan ini tidak hanya meningkatkan hasil belajar siswa, tetapi juga memberikan pengalaman belajar yang lebih mandiri dan efektif. Algoritma yang digunakan juga mengoptimalkan keamanan data dan efisiensi sistem. Secara keseluruhan, penelitian ini menawarkan solusi inovatif untuk reformasi pengajaran bahasa Inggris melalui teknologi modern berbasis big data.

Penelitian yang dilakukan (Babiano dkk., 2023) oleh metode baru untuk mitigasi ransomware kriptografi berbasis algoritma Salsa20 dengan teknik forensik memori langsung. Ransomware modern menggunakan skema enkripsi hybrid yang rumit, sering kali melibatkan kunci unik per file yang disimpan sementara di memori selama proses enkripsi. Penelitian ini mengembangkan metode untuk mengekstraksi pasangan kunci dan nonce Salsa20 dari memori volatil perangkat yang terinfeksi, memungkinkan dekripsi file korban tanpa memerlukan kunci master yang biasanya hanya tersedia setelah membayar tebusan. Dengan eksperimen pada ransomware nyata seperti Sodinokibi, metode ini berhasil mengidentifikasi lebih dari 90% kunci dari memori dan mendekripsi file korban. Temuan ini memberikan dasar untuk sistem mitigasi ransomware yang lebih efektif dengan memanfaatkan analisis memori untuk pemulihan data tanpa pembayaran tebusan.

Penelitian dari jurnal (Naif dkk., 2023) ini membahas algoritma enkripsi EAMSA 512-bit yang berbasis pada SALSA20 yang dimodifikasi, menggunakan sistem chaos 11-dimensi untuk menghasilkan kunci yang aman. Algoritma ini memecah data 512bit menjadi dua bagian 256bit dan mengenkripsi menggunakan kunci chaos serta S-box, menunjukkan hasil yang baik dalam pengujian keamanan dan kekuatan, termasuk lulus berbagai pengujian NIST. EAMSA 512-bit cocok untuk berbagai aplikasi dan lingkungan seperti IoT, WoT, dan cloud computing, serta dapat meningkatkan kecepatan dan keamanan transfer atau penyimpanan data dengan penambahan algoritma enkripsi cerdas.

Jurnal oleh (P & Mira, 2022) membahas tentang analisis algoritma kriptografi klasik, seperti Caesar Cipher, Vigenere Cipher, dan Hill Cipher, dalam proses enkripsi dan deskripsi data, termasuk pesan teks, file, dan citra. Penelitian

menunjukkan bahwa penggunaan satu algoritma saja dianggap rentan terhadap serangan, sehingga diperlukan modifikasi atau kombinasi beberapa algoritma untuk meningkatkan keamanan data. Selain itu, pentingnya studi literatur dan analisis mendalam terhadap proses enkripsi dan deskripsi juga ditekankan untuk mendukung pengembangan sistem yang lebih aman.

Jurnal yang dibuat oleh (Eko dkk., 2015) ini membahas tentang peningkatan keamanan data teks melalui modifikasi algoritma Vigenere Cipher untuk mencegah pencurian data yang sering terjadi pada aplikasi dan jaringan komunikasi. Penelitian ini menunjukkan bahwa modifikasi Vigenere Cipher tidak memiliki pola perulangan, sehingga membuat kunci enkripsi lebih sulit diprediksi, berbeda dengan Vigenere Cipher tradisional yang memiliki peluang prediksi informasi hingga 74,07%. Dengan menggunakan kombinasi teknik enkripsi, penelitian ini berhasil menciptakan prosedur pengamanan yang lebih efektif untuk melindungi data teks, yang diimplementasikan menggunakan bahasa pemrograman Java.

Penelitian yang dilakukan oleh (Afdhila Diyana dkk., 2016) ini membahas implementasi algoritma stream cipher Salsa20 untuk mengamankan data suara pada aplikasi Push to Talk (PTT) berbasis Android. Aplikasi ini dirancang menggunakan Android KitKat 4.4.2 ke atas dan menggunakan UDP untuk komunikasi suara seperti walkie-talkie. Salsa20 dipilih karena kecepatan dan performanya yang unggul dalam proses enkripsi dan dekripsi dibandingkan algoritma lain seperti AES. Pengujian menunjukkan bahwa waktu enkripsi dan dekripsi per paket hanya membutuhkan 0-2 ms, dengan nilai Avalanche Effect sebesar 52%, yang menunjukkan perubahan bit yang signifikan dan keamanan data yang baik. Selain itu, pengujian aplikasi menunjukkan bahwa suara terenkripsi hanya dapat didengar melalui perangkat yang memiliki dekripsi Salsa20, menghindari penyadapan. Delay rata-rata 1,9 detik tidak memengaruhi performa aplikasi secara signifikan, sehingga algoritma ini cocok untuk mengamankan data suara dalam PTT.

2.2. Dasar Teori

2.2.1. Kriptografi

Kriptografi (*cryptography)* berasal dari Bahasa Yunani: "*kryptós"* artinya "*secret"* (rahasia), sedangkan "*graphein"* artinya *"writing"* (tulisan). Jadi,

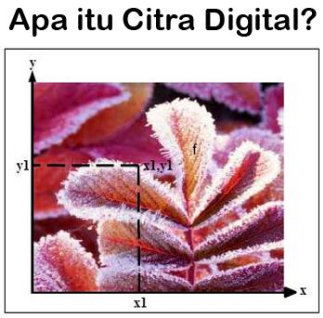
kriptografi secara harafiah berarti *"secret writing"* (tulisan rahasia). Ada beberapa definisi kriptografi yang telah ditemukan di dalam berbagai pustaka. Definisi lama yang dipakai salah satunya yang menyatakan yaitu Meyer di tahun 1982 yang menyatakan bahwa: Kriptografi adalah ilmu dan seni untuk menjaga kerhasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dipahami lagi maknanya (Munir, 2019).

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (SIlaban & Limbong, 2017) Kata "seni" di dalam semua definisi di atas berasal dari fakta sejarah bahwa pada masa - masa awal sejarah kriptografi setiap orang mempunyai cara yang unik untuk merahasiakan pesan. Cara – cara unik tersebut mungkin berbeda – berbeda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia memiliki nilai estetika sendiri (Munir, 2019).

Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai plaintext (teks biasa). Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah plaintext melibatkan penggunaan suatu bentuk kunci. Pesan plaintext yang telah dienkripsi (atau dikodekan) dikenal sebagai ciphertext (teks sandi).

2.2.2. Citra Digital

Citra atau gambar dalam bahasa latin imago adalah suatu representasi, kemiripan, atau imitasi dari suatu obyek atau benda. Citra dapat dikelompokkan menjadi citra tampak dan citra tidak tampak. Contoh citra tampak dalam kehidupan sehari-hari: foto, gambar, dan lukisan, sedangkan citra tidak tampak misalnya: data gambar dalam file (citra digital), dan citra yang direpresentasikan menjadi fungsi matematis (Gazali dkk., 2012).



Gambar 2.1 Citra Digital

Citra digital dapat didefinisikan sebagai fungsi dua variable, f(x,y), di mana x dan y adalah koordinat spasial dan nilai f(x,y) adalah intensitas citra pada koordinat tersebut, hal tersebut diilustrasikan pada Gambar 2.1 diatas. 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) (Gazali dkk., 2012).

2.2.3. Chaos

Pembangkit bilangan atau angka acak imajiner yang sulit untuk diprediksi oleh pihak lain atau Cryptographyically Secure Pseudorandom Generator (CSPRNG) biasa dikenal sebagai Chaos. Chaos diperkenalkan oleh Edward Lorentz seorang ahli meteorologi ketika sedang membuat model perkiraan cuaca pada tahun 1960. Model tersebut di iterasi agar menghasilkan perkiraan cuaca di kurun waktu mendatang. Semakin lama waktu perkiraan cuaca yang dihitung, semakin panjang iterasi yang harus dilakukan. Dengan mengubah sedikit awal iterasi yang hanya sebesar 0.000127, ia menemukan bahwa perkiraan cuaca yang dihasilkan mengalami divergensi yang besar (Irawan & Rachmawanto, 2022). Beragam metode yang ada pada teori ini antara lain: Tent Map, Tinkerbell map, Modified Henon Map, Duffing Map, Arnold Map, Logistic Map, Gaus-iterated map, dll (Sneha dkk., 2020).

2.2.4. Modified Henon Map

Pada tahun 1978, Modified Henon Map dua dimensi diusulkan oleh H'enon sebagai pendekatan kecil untul mempelajari dinamika sistem lorenz (Sabah dkk., 2020). Ini adalah peta dinamis diskrit yang menunjukkan perilaku acak, karena

sensitif terhadap kondisi awalnya (Kanwal dkk., 2024). Hal ini didefinisikan seperti pada persamaan.

$$x_{n+1} = 1 - ax_n^2 + by_n \quad (2.1)$$

$$y_{n+1} = x_n \quad (2.2)$$

Perilaku suatu *chaos system* bergantung pada nilai parameter a dan b yang disebut parameter kontrol. Parameter dan kondisi Modified Henon Map adalah sebagai berikut:

1. **(x_0, y_0)** adalah kondisi awal dari Modified Henon Map, yaitu nilai iterasi awal $X_0 = 0{,}1$ dan $Y_0 = 0{,}1$.
2. a dan b adalah parameter kontrol yang mengatur perilaku Modified Henon Map dimana nilai a = 1,4 dan b = 0,3. Nilai a dan b harus berada dalam rentang tertentu untuk menghasilkan perilaku chaos yang stabil

Modified Henon Map dikenal sebagai sistem dinamis diskrit yang paling umum dipelajari, Ini adalah model yang disederhanakan dari bagian coincare dari model lorenz. Ini adalah salah satu contoh yang paling banyak dipelajari dari sistem dinamis yang menunjukkan perilaku *chaos* yang mengambil (x0, y0) di bidang dan memetakannya ke titik baru (Irawan & Rachmawanto, 2022).

Seiring berjalannya waktu, metode Modified Henon Map telah berkembang dan memliki modifikasinya sendiri (*Modified* Modified Henon Map) seperti dikutip oleh (Sheela dkk., 2018) bahwa penulisan untuk *Modified* bisa ditulis seperti pada persamaan 2.3.

$$H\,(x_n, y_n) = \begin{pmatrix} x_n+1 \\ y_n+1 \end{pmatrix} = \begin{pmatrix} 1-b_1\cos(x_n) - b_2 y_n \\ -x_n \end{pmatrix} \quad (2.3)$$

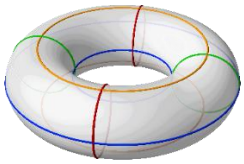
dimana:

H (x_n, y_n) = adalah peta yang dapat dibalik pada R2 kecuali jika b=0

2.2.5. Modified Arnold's Cat Map

Modified Arnold's Cat Map ini pertama kali di kemukakan oleh Vladimir Arnold's pada tahun 1960, kata "cat" digunakan karena gambar kucing digunakan dalam eksperimennya (Arham & Lestari, 2023). Modified Arnold's Cat Map (ACM) adalah peta acak dua dimensi yang banyak digunakan dalam proses pembiasan pada enkripsi citra modern. Salah satu cara umum untuk memahami sifat

acaknya adalah melalui representasi geometrisnya pada permukaan torus seperti pada Gambar 2.2.



Gambar 2.2 Skema Continuous Automorphism of the Torus

Pada peta ini, koordinat piksel diregangkan, diputar, dan kemudian dilipat kembali melalui operasi modulo, menghasilkan perubahan posisi yang kompleks namun terprediksi dan dapat dibalik. Visualisasi torus menunjukkan bagaimana ACM meregangkan dan melipat bidang koordinat, karakteristik inti dari sistem *chaos* yang membuat distribusi posisi piksel tidak dapat diprediksi dan efektif dalam meningkatkan tingkat keacakan citra. Studi terbaru juga mengkonfirmasi bahwa pemetaan modular linier seperti ACM bersifat mempertahankan luas, dapat dibalik, dan memberikan efek pencampuran acak yang signifikan, sehingga cocok untuk tahap permutasi enkripsi citra (Fan dkk., 2021), (Wang dkk., 2021).

Modified Arnold's Cat Map 2D adalah algoritma pengacakan piksel yang terus menerus mengubah lokasi piksel dalam sebuah citra selama banyak iterasi. Seiring bertambahnya jumlah iterasi, koordinat piksel dalam matriks persegi menjadi berulang, membentuk transformasi periodik. Dalam proses ini, setiap posisi piksel (X_i, Y_i) dipetakan ke posisi baru ($X_i + 1$, $Y_i + 1$). Perumusan enkripsi Modified Arnold's Cat Map dapat ditulis seperti pada persamaan 2.4 (Adi Putra dkk., 2022).

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod\ (N) \quad (2.4)$$

dimana ($X_i + 1$, $Y_i + 1$) adalah posisi piksel baru setelah transformasi, (X_i , Y_i) adalah posisi piksel pada gambar saat ini, b dan c adalah kunci dengan nilai bilangan bulat positif sembarang, dan N adalah ukuran gambar M x M. Hasil dari Arnold Cat Map bersifat reversibel, artinya dapat dikembalikan ke bentuk aslinya. Untuk mengembalikan hasil Arnold Cat Map yang terenkripsi atau Arnold Cat Map invers, berikut ini dapat ditulis seperti pada persamaan 2.5 (Adi Putra dkk., 2022).

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} mod\ (N) \quad (2.5)$$

Berbagai penelitian sebelumnya telah menunjukkan bahwa penggunaan ACM sebagai tahap awal permutasi dapat meningkatkan ketahanan terhadap serangan statistik dan memperluas ruang kunci karena parameter iterasi bertindak sebagai kunci kriptografi. Penelitian dari (Gupta dkk., 2023) ini menunjukkan bahwa penerapan ACM sebelum proses difusi meningkatkan pengacakan pola piksel, sehingga menghasilkan histogram gambar terenkripsi yang lebih seragam. Studi yang lain oleh (Ratna dkk., 2021) dan (Siti Nurul Hatikah Mohammad & Arif Mandangan, 2025), Studi-studi ini juga mendukung bahwa ACM efektif sebagai mekanisme pengacauan dan dapat memberikan peningkatan keamanan bila dikombinasikan dengan *chaos map* lainnya seperti Henon, Logistik, atau Tent Map. Studi-studi ini menyimpulkan bahwa ACM bukanlah generator angka acak, tetapi struktur acak dan sifat periodiknya dapat meningkatkan kualitas enkripsi dalam sistem multi-level.

2.2.6. *Avalanche Effect* (AE)

Avalanche Effect adalah sebuah metode untuk mencari dan mengetahui berapa persen pengubahan pesan pada saat proses enkripsi dilakukan dengan melihat rasio antara jumlah bit dari cipherteks yang berubah dan jumlah bit dari plainteks sebelum dirubah dalam proses enkripsi (Muslih & Handoko, 2022). Persamaan untuk menghitung nilai Avalanche Effect bisa dilihat pada persamaan 2.6.

$$\mathrm{AE} = \frac{\text{Jumlah bit berbeda}}{\text{total bit}} \text{ x } 100\% \qquad (2.6)$$

Sebagian besar nilai yang dihasilkan oleh Avalanche Effect merupakan hasil dari *Butterfly Effect* dan blok data yang berukuran besar, perubahan kecil pada nilai input dapat menyebabkan perubahan yang signifikan pada *Output* Bit (Al-Kuwari dkk., 2011). Dengan adanya sifat dari Avalanche Effect ini, setidaknya 50% bit dari nilai hash dibalik oleh perubahan kecil pada saat input objek. Biasanya, selisih yang dihasilkan seperti aslinya akan lebih dari 50% bit dari output asli dan perlu dibalik untuk mendapatkan nilai hash yang baru (Upadhyay dkk., 2022).

2.2.7. *Unified Average Changing Intensity* (UACI)

UACI merupakan tolok ukur standar rata-rata perbedaan intensitas diantara dua citra yang terenkripsi (Irawan & Rachmawanto, 2022). Menurut Mehdi Sadiq (Mehdi & Ali, 2020) nilai ideal untuk UACI masing-masing bernilai antara 33,25% dan 33,48%, dan perhitungannya bisa dilakukan dengan rumus (Kareem & Rahma, 2020).

$$\text{UACI} = \frac{1}{\text{W x H}} \sum_{ij} \frac{[C_1(i,j) - C_2(i,j)]}{255} \text{ x } 100\% \quad (2.7)$$

dimana:

W = lebar citra

H = panjang citra

C1(i, j) = citra hasil1 (cipher-image1)

C2(i, j) = citra hasil2 (cipher-image2)

2.2.8. *Number of Pixels Change Rate* (NPCR)

Selain UACI, perhitungan yang paling umum digunakan untuk mengukur sensitivitas sistem kriptografi terhadap modifikasi kecil pada gambar biasa yaitu NPCR. NPCR menghitung perbandingan pada masing-masing piksel diantara dua citra yang terenkripsi dari citra asli yang sesuai jika terdapat perubahan pada kunci nilai sebesar 1 bit (Irawan & Rachmawanto, 2022). Menurut (Mehdi & Ali, 2020) nilai ideal untuk NPCR lebih besar dari 99.6%, dan perhitungannya bisa dilakukan dengan rumus (Kareem & Rahma, 2020)

$$NPCR(C_1C_2) = \frac{\sum_{ij} D(i,j)}{\text{W x H}} \text{ x } 100\% \quad (2.8)$$

$$D(i,j) = \begin{cases} 0, C_1(i,j) \neq C_2(i,j) \\ 1, C_1(i,j) = C_2(i,j) \end{cases} \quad (2.9)$$

dimana:

W = lebar citra

H = panjang citra

D (i, j) = nilai dari kedua citra yang dibandingkan (0 atau 1)

C1(i, j) = citra hasil1 (cipher-image1)

C2(i, j) = citra hasil2 (cipher-image2)

2.2.9. *Mean Square Error* (MSE)

Mean Square Error (MSE) merupakan salah satu metode alternatif untuk melakukan evaluasi teknik prediksi untuk masing-masing masalah (perbedaan data yang nyata terhadap data yang terprediksi) kemudian dikuadradkan lalu dijumlahkan dan dibagi dengan jumlah data (Bima dkk., 2022). Rumus untuk menghitung MSE bisa dilihat pada persamaan 2.10

$$MSE = \sum(\frac{y_t - x_t}{n})^2 \quad (2.10)$$

dimana:

y_t = permintaan pada periode t

x_t = ramalan untuk periode t

n = total jumlah periode.

2.2.10. *Peak Signal to Noise Ratio* (PSNR)

Peak Signal to Noise Ratio merupakan rasio antara daya maksimum yang mungkin diterima oleh suatu sinyal dan dari *noise* yang memengaruhi tingkat keakuratan representasinya. Biasanya PSNR dinyatakan dalam skala desibel (dB) dan merupakan sebuah perkiraan kasar terhadap sudut pandang manusia tentang kualitas rekonstruksi (Poobathy & Chezian, 2014).

Nilai PSNR yang lebih tinggi terbilang bagus karena perbandingan sinyal yang lebih unggul daripada noise itu sendiri. Semakin besar nilai dari PSNR, maka semakin baik juga hasil pemisahan citranya. Perhitungan nilai PSNR dapat dilihat pada persamaan 2.11 (Abbas, 2016).

$$PSNR = 10 \log_{10} \left(\frac{255}{\sqrt{MSE}}\right) (dB) \quad (2.11)$$

Nilai Mean Square Error (MSE) yang lebih rendah berarti memiliki kesalahan yang lebih kecil, dan seperti yang terlihat dari hubungan terbalik antara MSE dan PSNR, ini menujukkan bahwa nilai PSNR yang tinggi (Abbas, 2016).

2.2.11. Koefisien Corelasi (*Correlation Coeffisient*)

Secara teoritis, koefisien korelasi antara dua piksel yang berdekatan berkisar dari -1 hingga +1, dengan nilai ±1 menunjukkan hubungan linier yang kuat dan nilai mendekati 0 menunjukkan tidak ada korelasi sama sekali. Dalam enkripsi gambar yang baik, nilai koefisien korelasi dalam gambar terenkripsi diharapkan mendekati

nol dalam arah horizontal, vertikal, dan diagonal, yang menunjukkan bahwa hubungan statistik antara piksel telah dihilangkan. Nilai nol ini digunakan sebagai tolak ukur untuk keamanan statistik gambar terenkripsi (Ibrahim & Venkatesan, 2025).

Kesamaan antara dua variabel ditunjukkan oleh metode korelasi. Koefisien ini sangat berguna untuk menghitung kualitas suatu sistem kriptografi (Djamel dkk., 2023). Koefisien ini sangat berguna untuk menghitung kualitas sistem kriptografi.

$$F_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}} \quad (2.12)$$

$$\mathrm{cov}(x,y) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)][y_i - E(y)] \quad (2.13)$$

dan

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)]^2 \quad (2.14)$$

$$E(x) = \frac{1}{n}\sum_{i=1}^{n} x_i \quad (2.15)$$

dimana X dan Y adalah himpunan yang terdiri dari N nilai abu-abu piksel, $X_i \in X$ dan $Y_i \in Y$, adalah dua piksel yang berdekatan