



Pengamanan Pada Citra Digital dengan Menggunakan Modifikasi Blok Data Algoritma AES - Rijndael

Muhammad Haris, Maya Silvi Lydia, Sutarman*

Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Medan, Indonesia

Email: ¹harismuhammad199@gmail.com, ²maya.silvi@usu.ac.id, ^{3,*}sutarman@usu.ac.id

Email Penulis Korespondensi: sutarman@usu.ac.id

Abstrak—Pengamanan Citra Digital merupakan salah satu topik keamanan informasi yang cukup penting saat ini. Seiring dengan meningkatnya penggunaan citra digital baik itu untuk keperluan komunikasi maupun dokumentasi, keamanan terhadap informasi yang terdapat pada citra digital perlu mendapat perhatian yang serius. Rijndael merupakan metode kriptografi yang tidak hanya digunakan untuk enkripsi teks namun juga digunakan untuk enkripsi citra digital. Sama seperti metode kriptografi berbasis blok pada umumnya, penyandian byte data hanya memiliki pengaruh pada lingkungan internal blok, dikarenakan proses transformasi pada Rijndael dilakukan secara terpisah pada setiap blok input. Pada citra digital, hal ini dapat mengakibatkan terlihatnya pola atau bentuk dari objek yang terdapat pada citra terutama jika menggunakan ukuran blok standard Rijndael yaitu 4x4. Untuk meningkatkan kualitas enkripsi citra digital pada Rijndael, beberapa penelitian melakukan modifikasi terutama pada tahapan putaran transformasi. Secara data nilai statistik yang diperoleh dari hasil enkripsi seperti koefisien korelasi memang menunjukkan peningkatan, namun secara visual pola objek masih terlihat dan kompleksitas modifikasi cenderung tinggi. Penelitian ini mengajukan modifikasi Rijndael yang berfokus kepada peningkatan ukuran blok input dari 4x4 menjadi 8x8 dengan perubahan minimal pada fungsi transformasi. Hasil penelitian menunjukkan nilai koefisien korelasi yang lebih baik dan hasil enkripsi yang secara visual lebih menyamarkan bentuk dari objek daripada Rijndael biasa khususnya pada citra teks, logo dan karikatur. Dari proses yang dilakukan terdapat peningkatan akurasi keamanan terhadap proses enkripsi sebesar 13,22% sampai dengan 91,48%.

Kata Kunci: Modifikasi; Rijndael; Input; Citra; Enkripsi;

Abstract—Digital Image Security is one of the most important information security topics today. Along with the increasing use of digital images both for communication and documentation purposes, the security of information contained in digital images needs serious attention. Rijndael is a cryptographic method that is not only used for text encryption but also for digital image encryption. Just like block-based cryptographic methods in general, encoding data bytes only has an effect on the internal environment of the block, because the transformation process in Rijndael is done separately for each input block. In digital images, this can result in visible patterns or shapes of objects contained in the image, especially when using the Rijndael standard block size of 4x4. To improve the quality of digital image encryption on Rijndael, several studies have made modifications, especially at the transformation stage. In terms of data, the statistical values obtained from the encryption results such as the correlation coefficient do show an increase, but visually the pattern of objects is still visible and modifications tend to be high. This research proposes a modification of Rijndael which focuses on increasing the input block size from 4x4 to 8x8 with minimal changes to the transformation function. The results showed that the value of the correlation coefficient was better and the results of the encryption visually disguised the shape of the object more than the usual Rijndael, especially in text images, logos and caricatures. From the process carried out there is an increase in the quality of security for the encryption process by 13.22% to 91.48%.

Keywords: Modification; Rijndael; Input; Image; Encryption

1. PENDAHULUAN

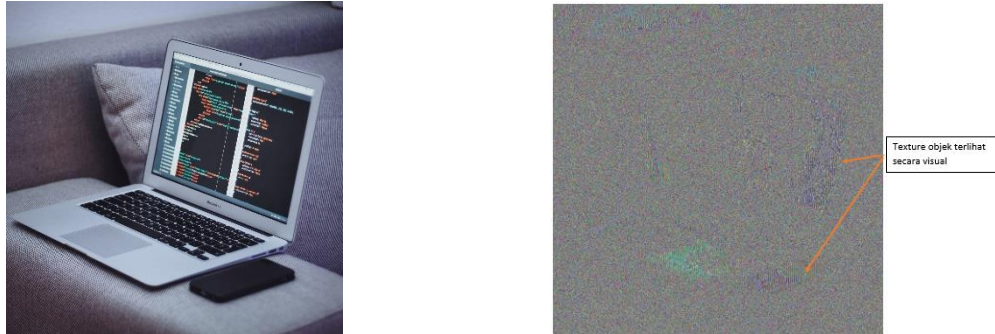
Pengamanan Citra Digital merupakan salah satu topik keamanan informasi yang cukup penting saat ini. Sekitar 70% dari data yang ditransmisikan melalui internet adalah citra digital [1]. Jumlah ini bisa saja bertambah mengingat seiring dengan berkembangnya teknologi, layanan dan teknologi informasi berbasis multimedia semakin meningkat popularitasnya [2]. Seiring dengan meningkatnya penggunaan citra digital baik itu untuk keperluan komunikasi maupun dokumentasi, keamanan terhadap informasi yang terdapat pada citra digital perlu mendapat perhatian yang serius.

Implementasi kriptografi dapat menjadi salah satu bentuk pengamanan informasi seperti citra digital. Berbagai metode kriptografi dapat diterapkan pada citra digital dikarenakan pada dasarnya citra digital merupakan rangkaian byte data sama seperti data digital lainnya. AES Rijndael merupakan salah satu metode kriptografi yang sangat populer sampai saat ini. AES Rijndael merupakan metode kriptografi simetris yang diajukan oleh Joan Daemen dan Vincent Rijmen pada tahun 1999 [3] sebelum akhirnya menjadi rekomendasi oleh NIST pada tahun 2001. Sampai saat ini AES Rijndael masih tetap digunakan melihat tersedianya pustaka enkripsi dan dekripsi AES Rijndael pada hampir semua programming development tools. Nur Rachmat dan Samsuryadi menunjukkan bahwa aplikasi AES Rijndael memberikan konsumsi CPU yang lebih efisien dibandingkan dengan metode kriptografi simetris lainnya seperti Serpent dan Blowfish [4]. Samar dan Abdelrahim melakukan percobaan terhadap aplikasi AES Rijndael pada cloud computing yang menunjukkan bahwa AES Rijndael membutuhkan memory yang lebih sedikit, keamanan yang lebih baik, dan performa yang fleksibel dibandingkan dengan algoritma kriptografi simetris lainnya [5].

Seperti halnya algoritma block chipper lainnya, penyandian informasi byte – byte dari data hanya dipengaruhi oleh blok dimana byte itu berada. Pada data seperti citra digital, hal ini dapat memberikan dampak

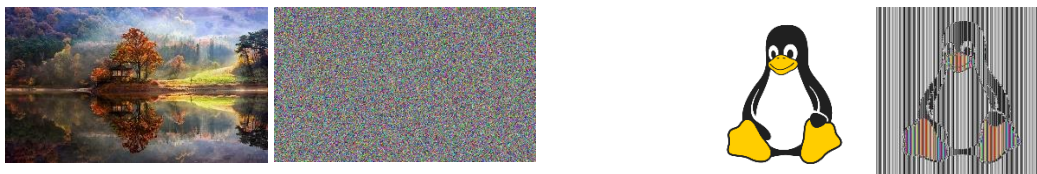


negatif yang cukup signifikan. Enkripsi pada citra digital menggunakan metode kriptografi block chipper seperti AES Rijndael akan membagi area citra kedalam blok berukuran 4 x 4 yang kemudian akan melakukan enkripsi pada blok – blok tersebut secara terpisah. Dikarenakan tidak ada kaitan antara blok yang satu dengan blok yang lain dalam proses enkripsi, maka hasil enkripsi akan menghasilkan pola yang terlihat jelas secara visual. Hal ini dapat dilihat pada beberapa penelitian [6] [7] dimana texture atau pola dari objek yang terdapat pada citra dapat terlihat secara visual. Kelemahan enkripsi pada citra digital dapat ditemukan pada beberapa citra dengan dimensi tinggi dan memiliki sebaran distribusi warna yang rendah seperti yang dapat dilihat pada gambar 1, dimana semakin tinggi dimensi sebuah citra maka akan semakin terlihat pola dari blok hasil enkripsi yang terpisah.



Gambar 1. Texture objek terlihat secara visual pada citra hasil enkripsi.

Pada gambar 1. merupakan gambar yang akan dilakukan pengamanan gambarnya. Kelemahan enkripsi citra digital pada Rijndael juga dapat ditemukan pada citra yang memiliki fitur sederhana, dimana texture dan bentuk objek terlihat dengan jelas secara visual. Pada dasarnya fitur dari citra asal yang terlihat pada citra hasil enkripsi dapat dianalisa menggunakan beberapa cara seperti perbandingan histogram dan perbandingan statistik lainnya. Namun, pendekatan perbandingan berdasarkan distribusi warna saja tidak dapat menjamin hasil enkripsi yang baik dikarenakan fitur citra seperti tekstur objek dapat saja memiliki warna yang berbeda namun masih memiliki susunan posisi yang sama sehingga pola dan bentuk dari objek masih dapat terlihat secara visual.



Gambar 2. Perbandingan Rijndael pada dua citra dengan fitur yang berbeda.

Pada gambar 2 dapat dilihat perbedaan dari hasil proses Rijndael. Beberapa parameter dapat digunakan untuk mengukur efisiensi dan tingkat keamanan dari sebuah model enkripsi citra digital seperti Correlation Coefficient, Information Entropy, Histogram Analysis dan PSNR [8] [9] [10] [11]. Parameter – parameter tersebut merupakan pengukuran yang menggunakan pendekatan statistik, pendekatan berbeda dapat menggunakan parameter lainnya seperti NPCR dan UACI [12]. Pendekatan statistik paling banyak digunakan pada enkripsi citra digital untuk mengukur perubahan yang terjadi pada citra hasil enkripsi dimana semakin besar nilai perubahan byte piksel dari citra hasil enkripsi maka semakin baik model enkripsi yang digunakan.

Secara teori, ukuran blok yang lebih kecil sehingga menghasilkan jumlah blok yang lebih banyak dapat meningkatkan keamanan dari citra hasil enkripsi khususnya pada kriptografi block chipper. Pada AES Rijndael, pengurangan ukuran blok akan merubah keseluruhan proses enkripsi dan dekripsi dari Rijndael itu sendiri. Sehingga penggunaan ukuran blok input yang lebih kecil bukanlah sebuah alternatif yang baik. Pada penelitian ini, ukuran blok input dari proses enkripsi pada AES Rijndael akan diperbesar yang semula berukuran 4x4 menjadi 8x8. Selain implementasi dan modifikasi terhadap metode AES Rijndael yang lebih sederhana, penambahan ukuran blok bertujuan untuk meminimalisir texture objek yang terlihat dari hasil enkripsi yang dapat diukur menggunakan parameter statistik.

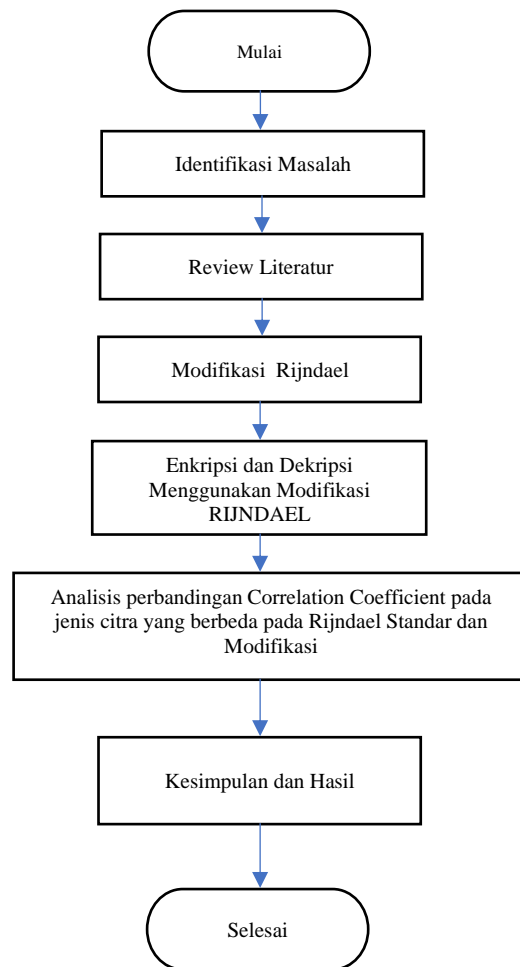
Tujuan yang akan dilakukan pada penelitian ini yaitu melakukan modifikasi blok data pengamanan citra digital pada Algoritma Rijndael dengan menggunakan algoritma AES. Dengan proses modifikasi tersebut kiranya tingkat keamanan yang dihasilkan akan menjadi lebih baik

2. METODOLOGI PENELITIAN

Penelitian ini dimulai dengan mengidentifikasi masalah yang ditemukan pada enkripsi citra digital menggunakan Rijndael. Dimana terdapat kelemahan khususnya pada citra dengan dimensi tinggi dan citra dengan fitur yang rendah. Berdasarkan masalah tersebut, penelitian dilanjutkan dengan menganalisa literatur – literatur yang berkaitan dengan Rijndael dan implementasinya terhadap pengamanan citra digital. Penelitian dilanjutkan dengan




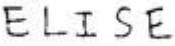

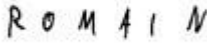


melakukan modifikasi metode Rijndael dengan menggunakan blok input berukuran 8x8. Uji coba dilakukan pada model enkripsi dan dekripsi citra digital hasil modifikasi Rijndael menggunakan beberapa citra dengan fitur yang berbeda. Analisis hasil enkripsi kemudian dilakukan menggunakan parameter correlation coefficient.



Gambar 3. Tahapan Penelitian

Gambar 3 merupakan tahapan yang dilalui pada penelitian, pada gambar tersebut dapat dilihat tahapan awal penelitian hingga tahapan akhir dari penelitian. Penelitian ini menggunakan citra uji yang diperoleh dari beberapa citra digital dari berbagai sumber dataset seperti Kaggle, VisualQA dan ImageNet. Adapaun citra dibagi menjadi beberapa jenis yaitu citra natural, citra karakter tulisan tangan dan citra teks atau karikatur. Dapat dilihat pada tabel 1

Tabel 1. Citra Natural dan Citra Karikatur

Nama Citra	Citra	Nama Citra	Citra
Car		Teks 1	
Flower		Teks 2	
Person		Karikatur	

Selanjutnya akan di enkripsi citra tersebut kedalam algoritma Rijndael dan Rijndael Modifikasi. Setelah mendapatkan hasil enkripsi atau cipherdata kemudian akan dilakukan analisis berdasarkan korelasi dari nilai kemiripan yang dimiliki oleh masing-masing enkripsi yang dihasilkan dengan menggunakan algoritma Rijndael original dengan algoritma Rijndael yang telah di modifikasi dengan ukuran matriks blok enkripsi 8x8. Hasil korelasi akan digunakan sebagai nilai penutup seberapa acak peletakan dan posisi piksel pada citra hasil enkripsi dari kedua



algoritma tersebut. Berikut ini adalah contoh enkripsi citra digital menggunakan algoritma Rijndael matriks 4x4 dan algoritma Rijndael matriks 8x8.

2.1 AES - Rijndael

AES Rijndael merupakan algoritma simetris yang termasuk kedalam kategori block chipper, dimana input plaintext akan dibagi kedalam beberapa blok dengan ukuran 128, 192 atau 256 bit. Kunci enkripsi juga akan dibagi menjadi beberapa blok dengan ukuran 128, 192 atau 256 bit. Setiap blok input terdiri dari empat baris dan **Nb** kolom dimana **Nb** adalah panjang blok dibagi 32. Sama seperti blok input, blok kunci terdiri dari empat baris dan **Nk** kolom dimana **Nk** adalah panjang blok dibagi 32. **Nb** tidak harus sama dengan **Nk**. Menggunakan ukuran blok yang sama (**Nb** = **Nk**) memberikan tingkat keamanan dan performa yang lebih baik [13]. Pada implementasi secara umum, ukuran blok pada AES Rijndael adalah 128 bit (4 byte x 4 byte) [14].

Proses AES – Rijndael secara garis besar dibagi menjadi dua proses utama yaitu Key Expansion dan Round Transformation. Key Expansion merupakan proses dimana kunci enkripsi dibentuk kedalam blok – blok kunci putaran yang akan digunakan pada proses enkripsi dan dekripsi menggunakan Round Transformation. Round Transformation merupakan proses transformasi yang terdiri dari n-putaran. Jumlah putaran proses untuk blok input AES Rijndael adalah 9 putaran untuk blok kunci berukuran 128 bit, 11 putaran untuk 192 bit dan 13 putaran untuk 256 bit [15]. Jika ditambah dengan putaran akhir maka jumlah putaran secara keseluruhan adalah 10 putaran untuk blok berukuran 128 bit, 12 putaran untuk 192 bit dan 14 putaran untuk 256 bit [16]. Tahapan putaran transformasi pada AES-Rijndael adalah [3] :

```
Round(State, RoundKey)
    ByteSub(State);
    ShiftRow(State);
    MixColumn(State);
    AddRoundKey(State, RoundKey);
FinalRound(State, RoundKey)
    ByteSub(State);
    ShiftRow(State);
    AddRoundKey(State, RoundKey);
```

2.2 Modifikasi Rijndael

Pada penelitian ini, modifikasi AES-Rijndael dilakukan dengan melakukan perubahan pada ukuran blok matriks dari AES – Rijndael biasa. Pada rancangan AES-Rijndael standar [3], dapat dilihat ukuran blok dapat dirubah hanya pada panjang blok (kolom) sedangkan jumlah baris adalah tetap (4 baris). Perubahan yang dilakukan pada penelitian ini adalah menggunakan ukuran blok simetris dimana penambahan panjang blok tidak hanya secara kolom, tapi juga dilakukan penambahan blok secara baris dimana pada penelitian ini dilakukan modifikasi blok dengan ukuran 8x8.

2.2.1 Inisialisasi Blok

Input yang digunakan pada penelitian ini adalah piksel dari citra input. Piksel dari citra akan dibagi menjadi blok area 8x8 (64 byte). Padding pada piksel atau pengurangan jumlah blok dilakukan jika ternyata terdapat kelebihan piksel citra yang tidak cukup untuk membentuk blok berukuran 8x8. Pada citra warna, blok input untuk R, G, B dapat dibentuk secara terpisah dan di enkripsi secara terpisah yang kemudian pada citra hasil enkripsi blok hasil enkripsi dari masing – masing kanal digabungkan kembali menjadi sebuah piksel. Ukuran blok kunci yang digunakan juga akan sama dengan ukuran blok input yaitu 8x8 (64 byte).

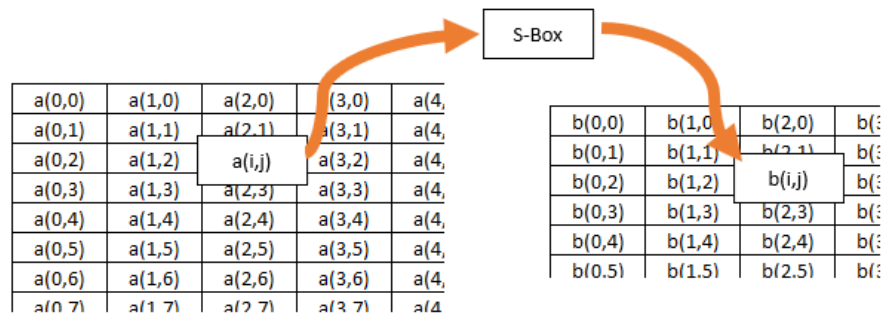
a(0,0)	a(1,0)	a(2,0)	a(3,0)	a(4,0)	a(5,0)	a(6,0)	a(7,0)
a(0,1)	a(1,1)	a(2,1)	a(3,1)	a(4,1)	a(5,1)	a(6,1)	a(7,1)
a(0,2)	a(1,2)	a(2,2)	a(3,2)	a(4,2)	a(5,2)	a(6,2)	a(7,2)
a(0,3)	a(1,3)	a(2,3)	a(3,3)	a(4,3)	a(5,3)	a(6,3)	a(7,3)
a(0,4)	a(1,4)	a(2,4)	a(3,4)	a(4,4)	a(5,4)	a(6,4)	a(7,4)
a(0,5)	a(1,5)	a(2,5)	a(3,5)	a(4,5)	a(5,5)	a(6,5)	a(7,5)
a(0,6)	a(1,6)	a(2,6)	a(3,6)	a(4,6)	a(5,6)	a(6,6)	a(7,6)
a(0,7)	a(1,7)	a(2,7)	a(3,7)	a(4,7)	a(5,7)	a(6,7)	a(7,7)
a(0,8)	a(1,8)	a(2,8)	a(3,8)	a(4,8)	a(5,8)	a(6,8)	a(7,8)

k(0,0)	k(1,0)	k(2,0)	k(3,0)	k(4,0)	k(5,0)	k(6,0)	k(7,0)
k(0,1)	k(1,1)	k(2,1)	k(3,1)	k(4,1)	k(5,1)	k(6,1)	k(7,1)
k(0,2)	k(1,2)	k(2,2)	k(3,2)	k(4,2)	k(5,2)	k(6,2)	k(7,2)
k(0,3)	k(1,3)	k(2,3)	k(3,3)	k(4,3)	k(5,3)	k(6,3)	k(7,3)
k(0,4)	k(1,4)	k(2,4)	k(3,4)	k(4,4)	k(5,4)	k(6,4)	k(7,4)
k(0,5)	k(1,5)	k(2,5)	k(3,5)	k(4,5)	k(5,5)	k(6,5)	k(7,5)
k(0,6)	k(1,6)	k(2,6)	k(3,6)	k(4,6)	k(5,6)	k(6,6)	k(7,6)
k(0,7)	k(1,7)	k(2,7)	k(3,7)	k(4,7)	k(5,7)	k(6,7)	k(7,7)
k(0,8)	k(1,8)	k(2,8)	k(3,8)	k(4,8)	k(5,8)	k(6,8)	k(7,8)

Gambar 4. Blok input dan blok kunci (8x8)

2.2.2 ByteSubstitution

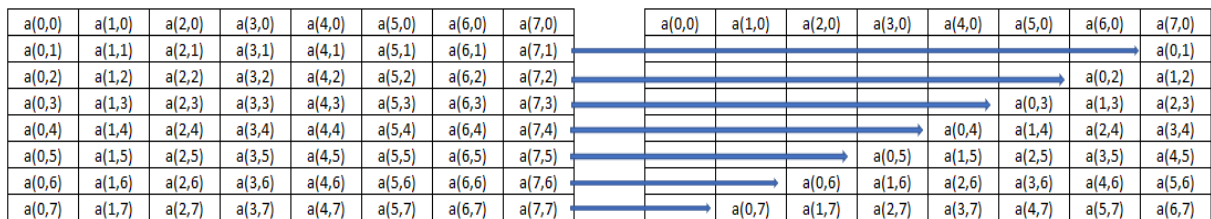
Substitusi byte dilakukan dengan melakukan substitusi nilai byte dari blok input dengan nilai byte pada S-Box sesuai dengan nilai substitusinya. Proses substitusi byte pada modifikasi Rijndael 8x8 tidak memiliki perbedaan dengan substitusi byte pada Rijndael biasa (4x4). Dimana proses substitusi byte hanya merubah nilai byte dari tiap blok dengan nilai yang ada pada S-Box berukuran 16x16 sesuai dengan nilai dari blok tersebut.



Gambar 5. ByteSubstitution

2.2.3 ShiftRow

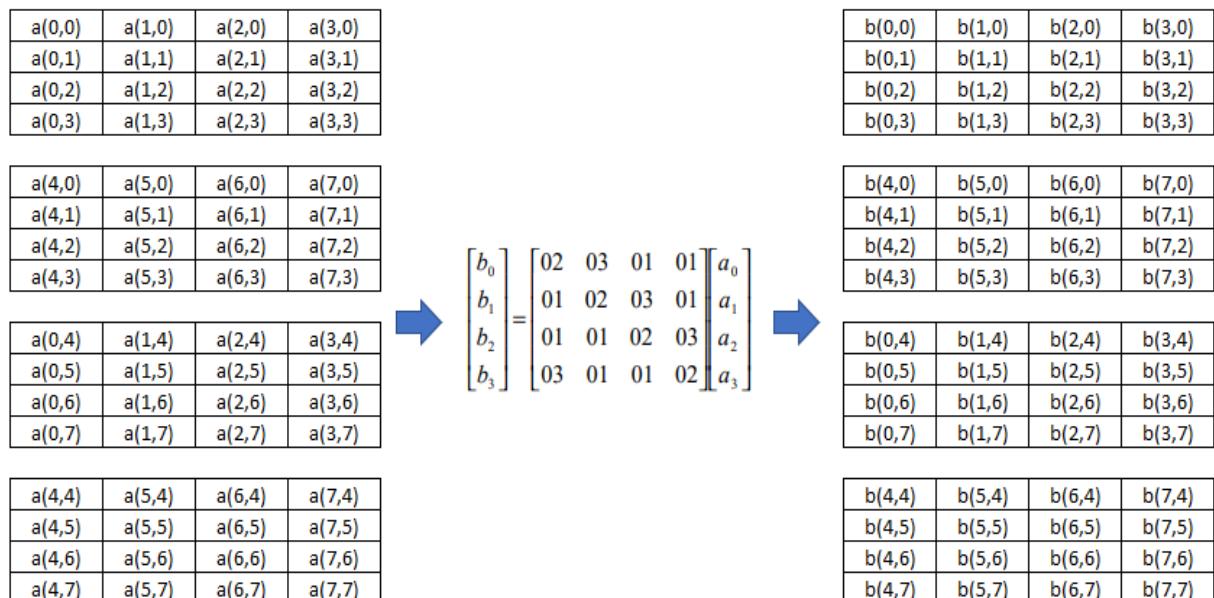
Operasi shiftrow pada modifikasi Rijndael 8x8 memiliki perbedaan dengan Rijndael biasa (4x4) dikarenakan jumlah baris dari blok yang digunakan. Pergeseran baris pada baris ke – 1 sampai baris ke – 4 memiliki proses yang sama dengan Rijndael biasa dimana untuk $N_b = 8$ pada rijndael biasa maka pergeseran adalah sebanyak 0 pada baris pertama, 1 untuk baris kedua, 3 untuk baris ketiga dan 4 untuk baris ke-empat. Sedangkan pada modifikasi Rijndael yang dilakukan pada penelitian ini adalah dengan menggunakan penambahan satu siklus pergeseran untuk setiap baris blok selain baris pertama.



Gambar 6. Skema Operasi Shitrow

2.2.4 MixColumn

Operasi MixColumn pada modifikasi AES yang dilakukan pada penelitian ini adalah mengikuti operasi MixColumn pada AES biasa namun dengan membagi blok 8x8 menjadi empat buah blok 4x4 lalu kemudian melakukan operasi MixColumn seperti pada AES biasa pada setiap blok tersebut.



Gambar 7. Skema Operasi MixColumn

2.2.5 AddRoundKey

Operasi addroundkey pada modifikasi Rijndael sama dengan operasi addroundkey pada Rijndael biasa, yaitu dengan melakukan operasi XOR pada setiap nilai dari blok input dengan nilai dari blok kunci pada posisi yang sama.



a(0,0)	a(1,0)	a(2,0)	a(3,0)	a(4,0)	a(5,0)	a(6,0)	a(7,0)
a(0,1)	a(1,1)	a(2,1)	a(3,1)	a(4,1)	a(5,1)	a(6,1)	a(7,1)
a(0,2)	a(1,2)	a(2,2)	a(3,2)	a(4,2)	a(5,2)	a(6,2)	a(7,2)
a(0,3)	a(1,3)	a(2,3)	a(3,3)	a(4,3)	a(5,3)	a(6,3)	a(7,3)
a(0,4)	a(1,4)	a(2,4)	a(3,4)	a(4,4)	a(5,4)	a(6,4)	a(7,4)
a(0,5)	a(1,5)	a(2,5)	a(3,5)	a(4,5)	a(5,5)	a(6,5)	a(7,5)
a(0,6)	a(1,6)	a(2,6)	a(3,6)	a(4,6)	a(5,6)	a(6,6)	a(7,6)
a(0,7)	a(1,7)	a(2,7)	a(3,7)	a(4,7)	a(5,7)	a(6,7)	a(7,7)

⊕

k(0,0)	k(1,0)	k(2,0)	k(3,0)	k(4,0)	k(5,0)	k(6,0)	k(7,0)
k(0,1)	k(1,1)	k(2,1)	k(3,1)	k(4,1)	k(5,1)	k(6,1)	k(7,1)
k(0,2)	k(1,2)	k(2,2)	k(3,2)	k(4,2)	k(5,2)	k(6,2)	k(7,2)
k(0,3)	k(1,3)	k(2,3)	k(3,3)	k(4,3)	k(5,3)	k(6,3)	k(7,3)
k(0,4)	k(1,4)	k(2,4)	k(3,4)	k(4,4)	k(5,4)	k(6,4)	k(7,4)
k(0,5)	k(1,5)	k(2,5)	k(3,5)	k(4,5)	k(5,5)	k(6,5)	k(7,5)
k(0,6)	k(1,6)	k(2,6)	k(3,6)	k(4,6)	k(5,6)	k(6,6)	k(7,6)
k(0,7)	k(1,7)	k(2,7)	k(3,7)	k(4,7)	k(5,7)	k(6,7)	k(7,7)

=

b(0,0)	b(1,0)	b(2,0)	b(3,0)	b(4,0)	b(5,0)	b(6,0)	b(7,0)
b(0,1)	b(1,1)	b(2,1)	b(3,1)	b(4,1)	b(5,1)	b(6,1)	b(7,1)
b(0,2)	b(1,2)	b(2,2)	b(3,2)	b(4,2)	b(5,2)	b(6,2)	b(7,2)
b(0,3)	b(1,3)	b(2,3)	b(3,3)	b(4,3)	b(5,3)	b(6,3)	b(7,3)
b(0,4)	b(1,4)	b(2,4)	b(3,4)	b(4,4)	b(5,4)	b(6,4)	b(7,4)
b(0,5)	b(1,5)	b(2,5)	b(3,5)	b(4,5)	b(5,5)	b(6,5)	b(7,5)
b(0,6)	b(1,6)	b(2,6)	b(3,6)	b(4,6)	b(5,6)	b(6,6)	b(7,6)
b(0,7)	b(1,7)	b(2,7)	b(3,7)	b(4,7)	b(5,7)	b(6,7)	b(7,7)

Gambar 8. Skema Operasi AddRoundKey

2.3 Correlation Coefficient

Koefisien korelasi antara citra asal dan citra hasil merupakan formula pengukuran yang sangat banyak diterapkan untuk mengukur perubahan yang terjadi antara citra sebelum dan setelah enkripsi. Nilai koefisien korelasi menunjukkan relasi yang di-indikasikan sejumlah piksel yang sama pada citra hasil enkripsi dan citra asal adalah sebagai berikut [17] :

$$NC = \frac{\sum m \cdot \sum n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{(\sum m - \bar{A})^2 (\sum n - \bar{B})^2}} \quad (1)$$

Dimana A dan B merupakan citra asal dan citra hasil enkripsi berukuran m x n piksel. Sebuah enkripsi dikatakan baik jika koefisien korelasi antara citra asal dengan citra hasil semakin mendekati 0. Selain perbandingan antara citra hasil dan citra asal. Koefisien korelasi juga dapat digunakan untuk menghitung korelasi antar piksel yang saling berdekatan [18]. Dimana nilai dari koefisien korelasi dapat dihitung menggunakan persamaan berikut [19] :

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \quad (2)$$

Dimana r_{xy} ada nilai koefisien korelasi dari dua kumpulan piksel dari citra.

$$cov(x,y) = E\{[x - E(x)][y - E(y)]\} \quad (3)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)]^2 \quad (5)$$

$cov(x,y)$ merupakan kovarian dari dua himpunan piksel x dan y, $E(x)$ adalah rata – rata nilai piksel x dan $D(x)$ adalah variance dari piksel x. Di dalam natural image, pixel – pixel yang bertetangga memiliki hubungan linier yang kuat. Ini ditandai oleh koefisien korelasinya yang tinggi (mendekati +1 atau -1). Di dalam citra acak, korelasi antar pixel bertetangga tidak ada atau koefisien korelasinya nol. Enkripsi citra bertujuan membuat korelasi pixel – pixel yang bertetangga didalam cipher image menjadi lemah atau dengan kata lain membuat koefisien korelasinya mendekati nol. Untuk mengetahui korelasi pixel – pixel didalam plain image maupun cipher image, maka dihitung koefisien korelasi antara dua pixel bertetangga secara horizontal dan dua pixel bertetangga secara vertical.

3. HASIL DAN PEMBAHASAN





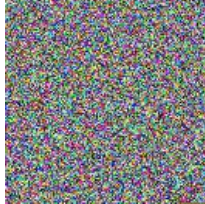


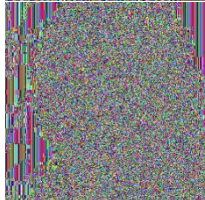
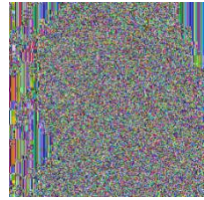
3.1 Hasil Pengujian

Proses pengujian dilakukan dengan melakukan enkripsi terhadap citra dataset yang kemudian akan dibandingkan koefisien korelasinya antara hasil enkripsi Rijndael biasa dengan Rijndael modifikasi menggunakan blok input 8x8. Koefisien korelasi akan dihitung secara vertical dan horizontal pada citra asli, citra hasil enkripsi Rijndael standar dan citra hasil enkripsi Rijndael modifikasi.

3.1.1 Penerapan Algoritma Rijndael dan Modifikasi AES

Pengujian enkripsi citra natural dilakukan dengan melakukan enkripsi pada dataset citra natural sebanyak tiga buah citra yang diperoleh dari dataset Kaggle [20]. Adapun hasil pengujian citra natural dapat dilihat pada tabel 2.

Tabel 2. Pengujian enkripsi citra natural

Citra	AES Standard	AES Modifikasi
		
		
		

Pada hasil enkripsi citra natural dapat dilihat untuk citra yang memiliki contrast yang tinggi dan kaya fitur seperti yang terlihat pada citra mobil dan citra bunga, maka hasil enkripsi akan menghasilkan keacakan piksel yang baik. Sedangkan pada citra dengan kontras rendah dan fitur objek yang rendah seperti pada citra person (citra ketiga), maka pola atau bentuk dari objek yang terdapat pada citra masih tercetak jelas pada citra hasil enkripsi. Selanjutnya adalah menghitung correlation coefficient pada citra hasil enkripsi. Pertama sekali akan diambil sample sebanyak total piksel citra dibagi dengan dua untuk menghitung correlation coefficient. Pada citra hasil enkripsi terdapat 64 piksel sehingga akan diambil 32 piksel secara diagonal dan kemudian mentransformasikannya ke warna grayscale. Pada perhitungan correlation coefficient, terdiri dari dua nilai yaitu Horizontal dan Vertical.

Pada perhitungan correlation coefficient horizontal, dibutuhkan dua nilai input, yaitu nilai piksel yang akan dibandingkan dengan nilai piksel tetangga nya untuk dapat melihat nilai korelasi antara sebuah piksel dengan tetangganya secara horizontal. Nilai tetangga yang diambil adalah nilai tetangga pada posisi (X+1) sehingga nilai piksel yang akan digunakan pada perhitungan correlation coefficient horizontal. Tahap selanjutnya adalah menghitung nilai standard deviasi dari piksel Grayscale(x,y) dan Grayscale (x+1,y) dengan rumus sebagai berikut:

$$Std(Gray(x,y)) = \sqrt{\frac{\sum (Gray(x,y)_i - \overline{Gray(x,y)})^2}{n}} \quad (6)$$

$$Std(Gray(x+1,y)) = \sqrt{\frac{\sum (Gray(x+1,y)_i - \overline{Gray(x+1,y)})^2}{n}} \quad (7)$$

Berikutnya dapat dihitung korelasi horizontal yang terjadi pada piksel pada citra hasil enkripsi adalah sebagai berikut :

$$CorrH = \frac{\sum (Gray(x,y)_i - \overline{Gray(x,y)}) * (Gray(x+1,y)_i - \overline{Gray(x+1,y)})}{n} * \frac{1}{Std(Gray(x,y)) * Std(Gray(x+1,y))} \quad (8)$$

Pada perhitungan correlation coefficient vertical, dibutuhkan dua nilai input, yaitu nilai piksel yang akan dibandingkan dengan nilai piksel tetangga nya untuk dapat melihat nilai korelasi antara sebuah piksel dengan tetangganya secara vertikal. Nilai tetangga yang diambil adalah nilai tetangga pada posisi (Y+1) sehingga nilai piksel yang akan digunakan pada perhitungan correlation coefficient vertical. Tahap selanjutnya adalah menghitung nilai standard deviasi dari piksel Grayscale(x,y) dan Grayscale (x,y+1) dengan rumus sebagai berikut:

$$Std(Gray(x,y)) = \sqrt{\frac{\sum (Gray(x,y)_i - \overline{Gray(x,y)})^2}{n}} \quad (9)$$

$$Std(Gray(x,y+1)) = \sqrt{\frac{\sum (Gray(x,y+1)_i - \overline{Gray(x,y+1)})^2}{n}} \quad (10)$$

Berikutnya dapat dihitung korelasi vertical yang terjadi pada piksel pada citra hasil enkripsi adalah sebagai berikut :

$$CorrV = \frac{\sum (Gray(x,y)_i - \overline{Gray(x,y)}) * (Gray(x,y+1)_i - \overline{Gray(x,y+1)})}{n} * \frac{1}{Std(Gray(x,y)) * Std(Gray(x,y+1))} \quad (11)$$



Adapun hasil perhitungan koefien korelasi antara citra asli, citra enkripsi Rijndael standard dan citra enkripsi Rijndael modifikasi dengan rumus diatas, dapat dilihat pada tabel 3.





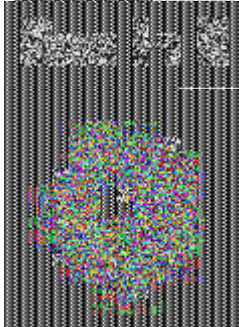
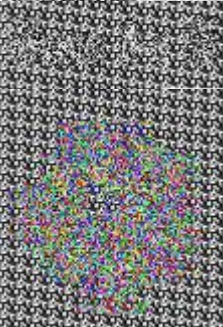
Tabel 3. Koefiesien Korelasi Citra Natural

	Original Image		Rijndael Standard		To Original	Rijndael Modifikasi		To Original
	Horizontal	Vertikal	Horizontal	Vertikal		Horizontal	Vertikal	
Car	0.9161	0.9146	-0.0401	-0.0177	-0.0401	-0.0348	-0.0158	-0.0348
Flower	0.634	0.6375	-0.0157	0.064	-0.0157	0.0198	-0.0334	0.0198
Person	0.9954	0.9963	-0.0182	-0.0013	-0.0182	0.0375	0.04	0.0375

3.1.2 Pengujian Enkripsi Citra Teks dan Karikatur

Selanjutnya setelah melakukan pengujian dengan menggunakan citra natural sebagai input, akan dilakukan pengujian terhadap citra teks dan karikatur. Pengujian ini dilakukan untuk melihat performa Rijndael standard dan Rijndael modifikasi dalam melakukan enkripsi terhadap citra sederhana yang diperoleh dari opendataset [21] [22].

Tabel 4. Pengujian enkripsi citra teks dan karikatur

Citra	Rijndael Standard	Rijndael Modifikasi
		
		

Pada hasil enkripsi citra teks dan karikatur dapat dilihat hampir semua hasil enkripsi menggunakan Rijndael standard memperlihatkan bentuk dari objek berupa karakter atau objek karikatur dengan sangat jelas, sehingga secara visual bentuk objek asli dapat di prediksi dengan Teknik pencocokan atau Teknik lainnya. Adapun nilai koefisien korelasi pada pengujian citra teks dan karakter dapat dilihat pada tabel 5.

Tabel 5. Koefiesien Korelasi Citra Natural

	Original Image		Rijndael Standard		To Original	Rijndael Modifikasi		To Original
	Horizontal	Vertical	Horizontal	Vertical		Horizontal	Vertical	
Teks1	0.7238	0.6756	-0.1089	-0.0818	-0.1089	-0.0254	-0.0419	-0.0254
Teks2	0.6006	0.5887	-0.1226	-0.0807	-0.1226	0.0254	-0.0682	0.0254
Karikatur	0.8972	0.8918	-0.1842	-0.2161	-0.1842	-0.0157	-0.0497	-0.0157

3.2 Pembahasan

Pada proses pengujian yang telah dilakukan dengan menggunakan metode enkripsi Rijndael standard dan Rijndael modifikasi pada dataset citra natural, teks dan karikatur, maka kinerja metode dapat diukur dengan nilai koefisin korelasi seperti yang terlihat pada tabel 6.

Tabel 6. Hasil Pengukuran Koefisien Korelasi

No	Pengujian	Rijndael	Rijndael Modifikasi
1	Car	-0.0401	-0.0348
2	Flower	-0.0157	0.0198
3	Person	-0.0182	0.0375
4	Teks1	-0.1089	-0.0254
5	Teks2	-0.1226	0.0254
6	Karikatur	-0.1842	-0.0157



Berdasarkan beberapa penelitian yang menggunakan parameter koefisien korelasi dalam mengukur kinerja enkripsi pada citra digital, diperoleh pernyataan bahwa semakin mendekati 0 nilai koefisien korelasi baik secara negative maupun positive maka semakin baik model enkripsi yang digunakan. Berdasarkan pernyataan tersebut maka dapat diperoleh peningkatan dari modifikasi Rijndael seperti yang terlihat pada tabel 7.

Tabel 7. Besarnya peningkatan koefisien korelasi

No	Pengujian	Rijndael	Rijndael Modifikasi	Peningkatan
1	Car	-0.0401	-0.0348	13.22 %
2	Flower	-0.0157	0.0198	-26.11 %
3	Person	-0.0182	0.0375	-106.04 %
4	Teks1	-0.1089	-0.0254	76.68 %
5	Teks2	-0.1226	0.0254	79.28 %
6	Karikatur	-0.1842	-0.0157	91.48

4. KESIMPULAN

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan maka dapat ditarik kesimpulan bahwasannya metode Rijndael modifikasi secara umum dapat memberikan peningkatan nilai koefisien korelasi yang cukup baik khususnya pada citra sederhana seperti citra teks, logo dan karikatur. Sedangkan pada citra natural, peningkatan sangat bergantung pada kontras, kekayaan fitur, sebaran warna dan faktor – faktor lainnya yang perlu untuk diteliti lebih lanjut. Pada proses yang telah dilakukan dapat dilihat peningkatan terbesar yaitu 91,48%

REFERENCES

- [1] A. Arab, M. J. Rostami dan B. Ghavami, "An image encryption method based on chaos system and AES algorithm," *The Journal of Supercomputing*, vol. 75, no. 10, pp. 6663-6682, 2019.
- [2] N. Nguyen-Thanh, D. Marinca, K. Khawam, S. Martin dan L. Boukhatem, "Multimedia content popularity: Learning and recommending a prediction method," dalam *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018.
- [3] J. Daemen dan V. Rijmen, *AES proposal: Rijndael*, 1999.
- [4] N. Rachmat dan Samsuryadi, "Performance Analysis of 256-bit AES Encryption Algorithm on Android Smartphone," *Journal of Physics: Conference Series*, vol. 1196, p. 012049, 2019.
- [5] S. Zaineldeen dan A. Ate, "Review of cryptography in cloud computing," *Int. J. Comput. Sci. Mobile Comput.*, vol. 9, no. 3, pp. 211-220, 2020.
- [6] R. J. Rasras, M. Abuzalata, Z. Alqadi, J. Al-Azzeh dan Q. Jaber, "Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 3, pp. 14-26, 2019.
- [7] M. Zeghid, M. Machhout, L. Khriji, A. Baganne dan R. Tourki, "A modified AES based algorithm for image encryption," *International Journal of Computer Science and Engineering*, vol. 1, no. 1, pp. 70-75, 2007.
- [8] O. F. Mohammad, M. S. M. Rahim, S. R. M. Zeebaree dan F. Y. Ahmed, "A survey and analysis of the image encryption methods," *International Journal of Applied Engineering Research*, vol. 12, no. 23, pp. 13265-13280, 2017.
- [9] H. V. Gamido, A. M. Sison dan R. P. Medina, "Implementation of modified AES as image encryption scheme," *Indonesian Journal of Electrical Engineering and Informatics (IJEI)*, vol. 6, no. 3, pp. 301-308, 2018.
- [10] P. Sharma dan H. Sabharwal, "A New Image Encryption using Modified AES Algorithm and its Comparison with AES," *International Journal Of Engineering Research & Technology (IJERT)*, vol. 9, no. 8, pp. 194-197, 2020.
- [11] I. N. Ibraheem, S. M. Hassan dan A. Abead, "Comparative Analysis & Implementation of Image Encryption & Decryption for Mobile Cloud Security," *International Journal of Advanced Science and Technology*, vol. 29, no. 3s, pp. 109-121, 2020.
- [12] A. Alabaichi, "True Color Image Encryption Based On Dna Sequence, 3d Chaotic Map, And Key-Dependent Dna S-Box Of Aes," *Journal of Theoretical & Applied Information Technology*, vol. 96, no. 2, pp. 304-321, 2018.
- [13] R. Hongal, H. Jyoti dan S. Rajashekar, "An Approach towards Design of N-Bit AES to Enhance Security using Reversible Logic," *Communications on Applied Electronics*, vol. 7, no. 22, pp. 7-13, 2018.
- [14] R. Debnath, P. Agrawal dan G. Vaishnav, "DES, AES And Triple DES: Symmetric Key Cryptography Algorithm," *International Journal of Science, Engineering and Technology Research*, vol. 3, no. 3, p. 652-654, 2014.
- [15] H. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, M. Shabbir dan Y. Al-Nabhani, "New comparative study between DES, 3DES and AES within nine factors," *arXiv preprint arXiv:1003.4085*.
- [16] S. S. Gaur, H. S. Kalsi dan S. Gautam, "A Comparative Study and Analysis of Cryptographic Algorithms: RSA, DES, AES, BLOWFISH, 3-DES, and TWOFISH," *International Journal Of Research In Electronics And Computer Engineering (IJRECE)*, vol. 7, no. 1, pp. 996-999, 2019.
- [17] Y. Pourasad, R. Ranjbarzadeh dan A. Mardani, "A New Algorithm for Digital Image Encryption Based on Chaos Theory," *Entropy*, vol. 23, no. 3, p. 341, 2021.
- [18] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish dan M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855-37865, 2021.
- [19] J. Hao, H. Li, H. Yan dan J. Mou, "A New Fractional Chaotic System and Its Application in Image Encryption With DNA Mutation," *IEEE Access*, vol. 9, pp. 52364-52377, 2021.
- [20] P. Roy, S. Bhattacharya, S. Ghosh dan U. Pal, "Effects of Degradations on Deep Neural Network Architectures," *arXiv preprint arXiv:1807.10108*, 3 12 2018.



- [21] Arpanio, "OCR - Handwriting Recognition," kaggle, 2020.
- [22] V. Subbiah, "Pokemon Image Dataset," kaggle, 2019
- [23] Zebua, T & Ndruru, E. (2017). Pengamana Citra Digital Berdasarkan Modifikasi Algoritma RC4. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIK). Vol. 4, No. 4, Desember 2017, hlm. 275-282