

# Perbandingan Kriptografi Klasik Hill Cipher dengan Affine Cipher dalam Pengamanan Data Citra

I Nyoman Dwi Pradnyana Putra<sup>a1</sup>, I Gede Santi Astawa<sup>a2</sup>

<sup>a</sup>Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,  
Universitas Udayana  
Badung, Indonesia

<sup>1</sup>dwipradnyana68@gmail.com

<sup>2</sup>santi.astawa@unud.ac.id

## Abstract

*The development of technology affects several aspects of life, especially in securing confidential data and information. Because of this, there is a way to secure data, namely cryptography, many cryptography techniques have been implemented to hide data information, one of which image data, the purpose of securing image data is to prevent unwanted things. In this research, two classical cryptography algorithms will be tested, namely hill cipher and affine cipher by comparing the MSE and PSNR Image values when encryption is carried out. The encryption process is done 6 times with different image in each algorithm, the results of the encryption are compared between the results of the hill cipher encryption image with the affine cipher. After test that two of algorithms can change the encrypted image into a random pattern, but seen from the MSE and PSNR image values, the hill cipher algorithm has a value that matcher the requirements, with the best value being MSE 7073.40 and PSNR image 9.63 dB.*

**Keywords:** Cryptography, Encryption, Hill Cipher, Affine Cipher, MSE, PSNR Image

## 1. Pendahuluan

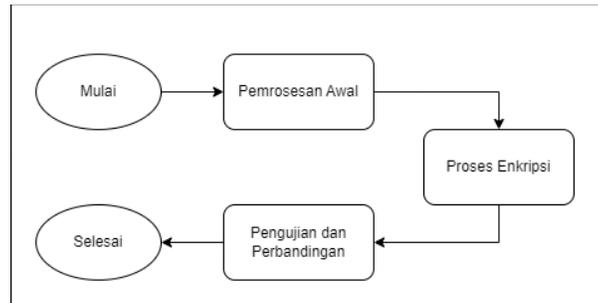
Perkembangan teknologi informasi saat ini sangat berpengaruh dalam segala aspek kehidupan, terutama dalam pengamanan data dan informasi yang bersifat rahasia. Informasi yang bersifat rahasia seharusnya perlu disembunyikan agar tidak diketahui oleh orang-orang yang tidak berhak agar tidak disalahgunakan. Karena hal tersebut diperlukan sebuah cara yang dilakukan untuk mengamankan data, salah satunya dengan menerapkan kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta autentikasi dimana proses penggunaannya memiliki berbagai teknik dan atau ilmu dan seni untuk menjaga keamanan data[1].

Banyak teknik kriptografi yang telah diimplementasikan untuk menyembunyikan informasi data, salah satunya data citra, tujuan dari pengamanan data citra yaitu agar tidak terjadi hal yang tidak diinginkan seperti penipuan dengan menggunakan identitas orang lain yang didukung dengan foto pribadi. Masih ada yang harus dipertimbangkan ketika menggunakan suatu algoritma baik itu dari tingkat kecepatan enkripsi sampai dengan seberapa baik algoritma dalam menyembunyikan informasi.

Dalam penelitian ini, peneliti ingin membandingkan dua buah algoritma yaitu hill cipher dan affine cipher. Algoritma hill cipher merupakan algoritma yang menggunakan matriks  $m \times m$  yang menggunakan operasi perkalian matriks untuk proses enkripsi maupun dekripsi, sedangkan algoritma affine cipher merupakan perluasan dari algoritma caesar cipher dengan perkalian dan pergeseran nilai sebagai kunci. Kedua algoritma ini merupakan algoritma kriptografi klasik simetris dimana menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, peneliti menggunakan kriptografi klasik untuk mengetahui seberapa baik kedua algoritma ini dalam menyembunyikan informasi.

Kedua algoritma tersebut dibandingkan dari nilai pengujian MSE dan PSNR. Mean Square Error (MSE) adalah nilai error kuadrat rata-rata antara citra asli dengan citra enkripsi, MSE didapatkan dengan membandingkan nilai selisih *pixel* citra asli dengan citra enkripsi. Peak Signal to Noise Ratio *Image* adalah perbandingan antara nilai maksimum dari sinyal yang diukur berdasarkan derau yang dinyatakan dalam desibel (dB).

## 2. Metode Penelitian

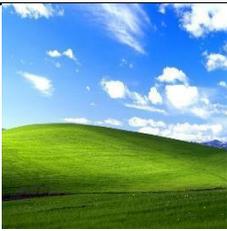


**Gambar 1.** Desain Metode

### 2.1. Pemrosesan Awal

Algoritma kriptografi yang digunakan dalam pengujian yaitu algoritma hill cipher dan affine cipher, dimana kedua algoritma ini merupakan algoritma simetris yang berarti menggunakan kunci yang sama dalam proses enkripsi dan dekripsi. Citra yang akan digunakan untuk pengujian dalam penelitian ini yaitu citra digital RGB yang berjumlah 5 citra dengan dengan ukuran yang dapat dilihat pada **Tabel 1**. Citra yang digunakan. Ukuran citra sengaja dibedakan agar dapat terlihat berapa rata-rata *pixel* yang mampu ditampung oleh citra tersebut[2].

**Tabel 1.** Citra yang digunakan

Nama Citra Uji	Gambar	Ukuran Citra ( <i>pixel</i> )
windows.png		720 x 720
lenna.png		512 x 512

bunga.png		500 x 500
buah.png		480 x 480
hewan.png		400 x 400

## 2.2. Enkripsi Citra

### a. Algoritma Hill Cipher

Pada tahap ini citra di enkripsi menggunakan algoritma Hill Cipher. Pada tahap ini dibutuhkan sebuah kunci dimana kunci tersebut terdiri dari 42 karakter yaitu 23 yang akan diubah menjadi nilai ASCII. Lalu ubah kunci menjadi matriks  $2 \times 2$ [3]. Berikut adalah langkah detail dari proses enkripsi citra dengan algoritma Hill Cipher.

1. Baca citra yang akan dienkripsi.
2. Ubah citra menjadi nilai double.
3. Inputkan kunci berupa 2 karakter.
4. Ubah kunci menjadi matriks  $2 \times 2$ .
5. Lakukan proses enkripsi dengan persamaan 1.
6. Dapatkan citra terenkripsi.

$$C = (K \times P) \text{ mod } 256 \quad (1)$$

### b. Algoritma Affine Cipher

Affine cipher pada metode affine adalah perluasan dari metode Caesar Cipher, yang mengalihkan plaintext dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran  $P$  menghasilkan ciphertext  $C$  dinyatakan dengan fungsi kongruen[4]:

$$C \equiv m P + b \pmod{n} \quad (2)$$

Yang mana  $n$  adalah ukuran alphabet,  $m$  adalah bilangan bulat yang harus relatif prima dengan  $n$  (jika tidak relatif prima, maka dekripsi tidak bisa dilakukan) dan  $b$  adalah jumlah pergeseran (Caesar cipher adalah khusus dari affine cipher dengan  $m=1$ ). Untuk melakukan dekripsi, persamaan tersebut harus dipecahkan untuk memperoleh  $P$ . Solusi kekongruenan tersebut hanya ada jika inver  $m \pmod{n}$ , dinyatakan dengan  $m^{-1}$ . Jika  $m^{-1}$  ada maka dekripsi dilakukan dengan persamaan sebagai berikut:

$$P \equiv m^{-1}(C - b) \pmod{n} \quad (3)$$

### 2.3. Parameter Pengujian

#### a. Mean Square Error (MSE)

MSE merupakan tolak ukur analisis kuantitatif yang digunakan untuk menilai kualitas sebuah citra keluaran dan keunggulan sebuah metode yang digunakan. Ukuran matriks citra  $m \times n$ ,  $B_1$  dan  $B_2$  merupakan matriks citra. Dengan kata lain Mean Square Error (MSE) adalah kesalahan kuadrat rata-rata sinyal-sinyal *pixel* citra hasil pemrosesan sinyal terhadap sinyal asli[2]. Untuk nilai terbaik MSE dalam segi enkripsi adalah semakin besar nilai dari MSE. Untuk menentukan nilai MSR digunakan persamaan berikut ini:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (B_1(i, j) - B_2(i, j))^2 \quad (4)$$

Dimana:

- $m$  : baris matriks citra hasil pemrosesan
- $n$  : kolom matriks citra hasil pemrosesan
- $B_1$  : *pixel* citra asli
- $B_2$  : *pixel* citra hasil pemrosesan

#### b. Peak Signal to Noise Ratio (PSNR) Image

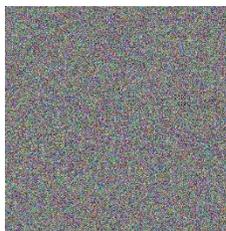
Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut, dalam satuan desibel (dB)[2]. Untuk nilai PSNR terbaik dalam segi enkripsi adalah semakin kecil nilai dari PSNR yang mana semakin tidak mirip dengan citra asli. Untuk menentukan nilai PSNR digunakan persamaan berikut ini:

$$PSNR = \frac{255^2}{MSE} \quad (5)$$

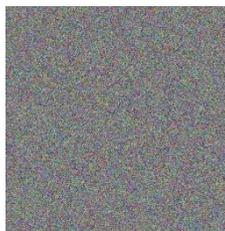
## 3. Hasil dan Pembahasan

### 3.1. Uji Coba Sistem

Dalam proses enkripsi citra menggunakan sistem yang sudah ada dengan menggunakan Bahasa pemrograman python, uji coba proses enkripsi dilakukan sebanyak 10 kali dengan algoritma hill cipher dan affine cipher yang menggunakan 5 citra yang berbeda pada setiap algoritma. Berikut merupakan hasil uji sistem proses enkripsi hill cipher dan affine cipher.



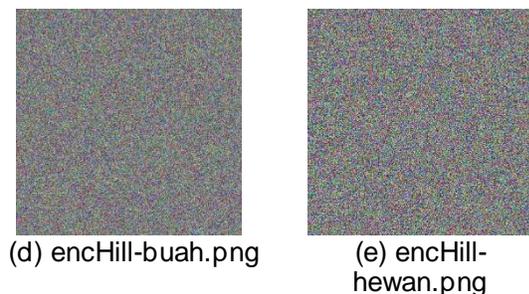
(a) encHill-windows.png



(b) encHill-lenna.png

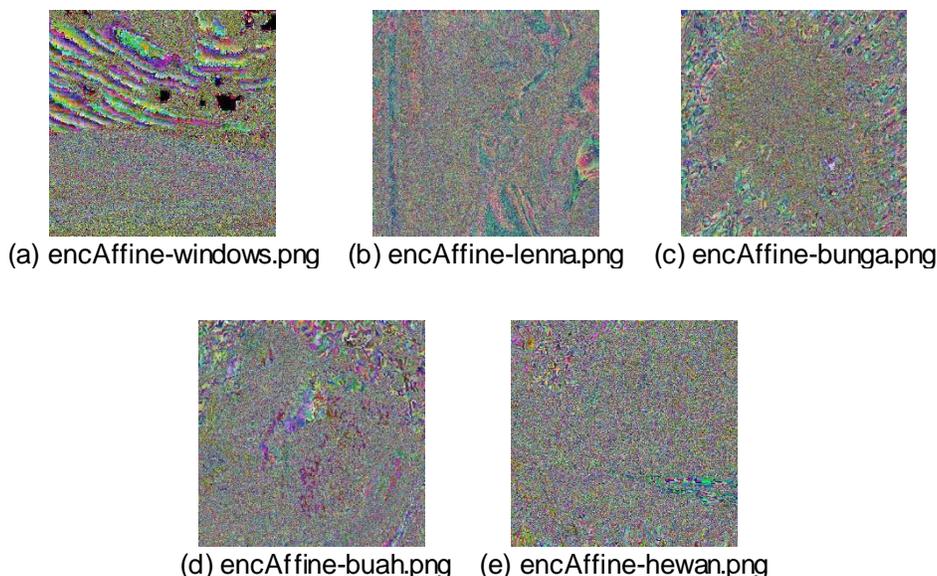


(c) encHill-bunga.png



**Gambar 2.** Hasil Enkripsi Citra dengan Algoritma Hill Cipher

Dapat dilihat pada gambar diatas terjadi perubahan pola menjadi acak dan tidak terlihat bagaimana bentuk citra aslinya, algoritma hill cipher memiliki bentuk kemiripan yang berbeda dengan citra aslinya.



**Gambar 3.** Hasil Enkripsi Citra dengan Algoritma Affine Cipher

Citra hasil enkripsi menggunakan algoritma affine cipher memiliki perubahan pola yang acak, namun masih terlihat beberapa kesamaan antara citra terenkripsi dengan citra aslinya, dimana adanya sedikit kemiripan pada beberapa citra.

### 3.2. Perbandingan Hasil Nilai MSE dan PSNR

Untuk mendapatkan nilai MSE dan PSNR *Image* menggunakan sistem yang sudah ada dengan menggunakan bahasa pemrograman python, dimana program dalam sistem tersebut menggunakan menyesuaikan dengan perhitungan MSE pada persamaan (4) dan PSNR pada persamaan (5).

**Tabel 2.** Nilai MSE dan PSNR dengan Algoritma Hill Cipher

Nama Citra	Uji MSE	Uji PSNR (dB)
encHill-windows.png	6064.21	10.30
encHill-lenna.png	3715.03	12.43

encHill-bunga.png	5538.38	10.69
encHill-buah.png	7073.40	9.63
encHill-hewan.png	6891.99	9.74

**Tabel 3.** Nilai MSE dan PSNR dengan Algoritma Affine Cipher

Nama Citra	Uji MSE	Uji PSNR (dB)
encAffine-windows	5538.38	10.69
encAffine-lenna.png	4572.87	11.52
encAffine-bunga.png	5373.84	10.82
encAffine-buah.png	6917.35	9.73
encAffine-hewan.png	7029.37	9.66

Pada tabel diatas menunjukkan bahwa nilai MSE dan PSNR dari masing-masing algoritma memiliki perbedaan. Perbedaan nilai tersebut dipengaruhi oleh *pixel* yang ditampung oleh citra tersebut. Nilai MSE terbaik dalam proses enkripsi adalah semakin besar nilainya dan sedangkan nilai PSNR terbaik dalam proses enkripsi adalah semakin kecil nilainya. Pada tabel tersebut dapat dilihat bahwa dari semua nilai pengujian tersebut, algoritma hill cipher rata-rata mencapai nilai MSE dan PSNR yang sesuai dengan syarat pengujian dengan nilai terbaik MSE 7073.40 dan PSNR *image* 9.63 dB, sedangkan nilai yang paling jauh dengan syarat pengujian yaitu dengan MSE 3715.03 dan PSNR *image* 12.43 dB.

#### 4. Kesimpulan

Berdasarkan hasil pembahasan dan penelitian yang telah dilakukan. dapat disimpulkan bahwa secara visual algoritma hill cipher menghasilkan citra enkripsi berupa pola acak dan tidak terlihat bentuk citra aslinya, sedangkan pada algoritma affine cipher menghasilkan pola acak namun pada beberapa citra terdapat beberapa kemiripan antara citra enkripsi dengan citra aslinya. Pada pengujian hasil enkripsi, algoritma yang mencapai syarat dari pengujian yaitu algoritma hill cipher dengan nilai terbaik MSE 7073.40 dan PSNR *image* 9.63 dB.

#### Referensi

- [1] W. Sari *et al.*, "Analisa Algoritma Elgamal Dalam Penyandian Data," vol. 2, no. 1, pp. 60–70, 2018.
- [2] S. Y. Doo, S. Tena, and V. M. Ndolu, "Implementasi Pengamanan Data Menggunakan Metode Kriptografi Hill Cipher Dan Steganografi Least Significant Bit (Lsb) Pada Media Citra Digital," *J. Media Elektro*, vol. VIII, no. 2, pp. 93–99, 2019, doi: 10.35508/jme.v0i0.1778.
- [3] B. Firmanto, D. Putri, K. Ningrum, A. Bramanto, and W. Putra, "Perbandingan Hasil Performa Optimasi Transposisi Hill Cipher dan Vigenere Cipher pada Citra Digital," *SMARTICS J.*, vol. 7, no. 2, pp. 65–71, 2021, [Online]. Available: <https://doi.org/10.21067/smartics.v7i2.5931>
- [4] D. S. Ginting, J. Simanulang, and M. Zarlis, "Kriptografi Simetris Dengan Kombinasi Hill cipher Dan Affine Cipher Di Dalam Matriks Cipher Transposisi Dengan Menerapkan Pola Alur Bajak Sawah," *Semin. Nas. Teknol. Inf.*, no. The Future of Computer Vision, pp. 191–198, 2017.