

III. METODOLOGI PENELITIAN

A. Jenis Penelitian

Penelitian ini menggunakan metode penelitian kepustakaan atau studi pustaka. Kutipan informasi diperoleh dari buku, artikel atau skripsi-skripsi terdahulu dan dikumpulkan sesuai dengan judul.

B. Jenis dan Sumber Data

Data yang digunakan dalam penelitian ini berupa data citra digital yang berukuran 256×256 piksel dan format citra *.png yang diperoleh dari *standard image test*.

C. Waktu dan Tempat Pengambilan Data

Data penelitian tersebut diambil dari *standard image test*, pada bulan Juni 2025.

D. Prosedur Penelitian

Adapun langkah – langkah yang dilakukan untuk mendapatkan tujuan penelitian dengan menggunakan metode kriptografi Advance Hill Cipher dengan kunci terenkripsi El Gamal yaitu:

1. Persiapan Data
 - a. Mengumpulkan beberapa citra digital berwarna yang akan digunakan sebagai data uji coba.
2. Penerapan Algoritma
 - a. Pembangkitan Kunci
 - 1) Membangkitkan matriks kunci untuk algoritma Advance Hill Cipher yang invertibel modulo 256.

2) Menghasilkan pasangan kunci publik dan privat untuk algoritma ElGamal.

b. Proses Enkripsi

1) Mengenkripsi citra digital menggunakan Advance Hill Cipher dengan matriks kunci.

2) Mengenkripsi matriks kunci menggunakan ElGamal.

c. Proses Dekripsi

1) Mendekripsi matriks kunci menggunakan ElGamal.

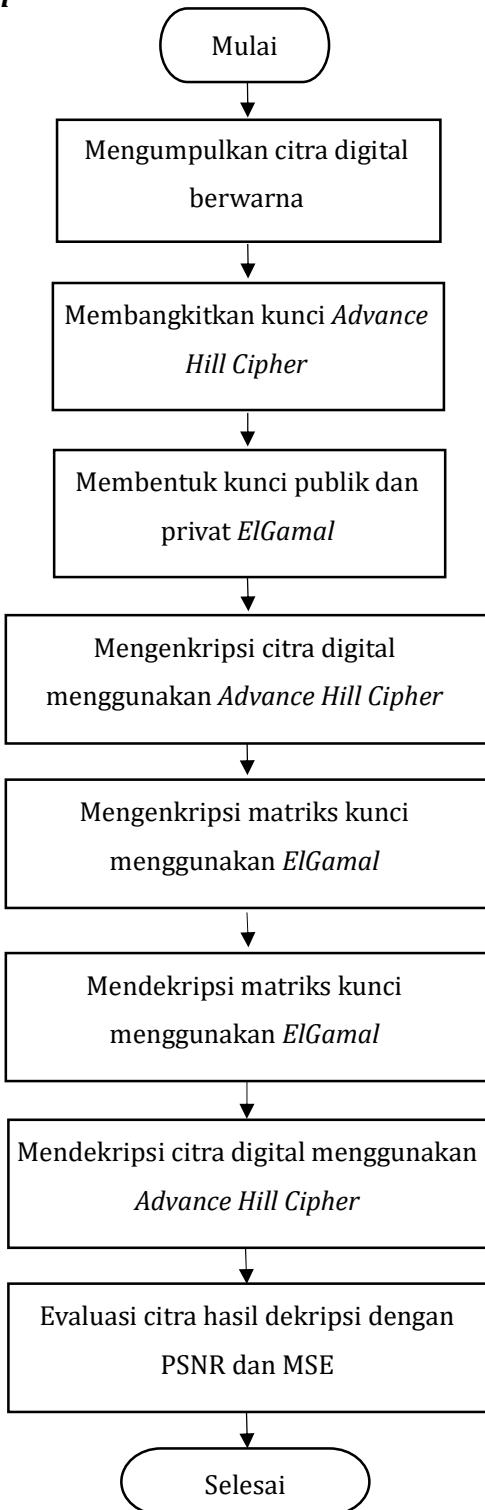
2) Mendekripsi citra menggunakan Advance Hill Cipher dengan matriks kunci dekripsi.

3. Evaluasi Hasil

a. Menilai kualitas citra hasil dekripsi menggunakan PSNR dan MSE.

b. Mengamati hasil visual untuk memastikan citra dapat dikenali.

E. Flowchart Penelitian



DAFTAR PUSTAKA

- Acharya, B., Panigrahy, S. K., Patra, S. K., Kumar Panigrahy, S., & Panda, G. (2009). Image Encryption Using Advanced Hill Cipher Algorithm. In *International Journal of Recent Trends in Engineering* (Vol. 1, Issue 1). <https://www.researchgate.net/publication/229012891>
- APJII. (2024). *Laporan Survei Pengguna Internet APJII 2024*.
- Azam, T. (2020). *Cryptanalysis of the Encryption Scheme based on Advanced Hill Cipher Algorithm*.
- Fadlilah, S. N., Turmudi, T., & Khudzaifah, M. (2022). Penggabungan Algoritma Hill Cipher dan ElGamal untuk Mengamankan Pesan teks. *Jurnal Riset Mahasiswa Matematika*, 1(5), 230–235. <https://doi.org/10.18860/jrmm.v1i5.14496>
- Gonzalez, R. C. (2009). *Digital image processing*. Pearson education india.
- Hakim, M. L. (2021). *Implementasi algoritma Hill Cipher dan Arnold cat map dalam pemanfaatan enkripsi dan dekripsi citra digital berbasis website*.
- Jamaludin, J. (2018). Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem. *Sinkron: Jurnal Dan Penelitian Teknik Informatika*, 2(2), 86–93.
- Khazaei, S., & Ahmadi, S. (2017). Ciphertext-only attack on $d \times d$ Hill in $O(d^3d)$. *Information Processing Letters*, 118, 25–29. <https://doi.org/10.1016/j.ipl.2016.09.006>
- Wulandari, M. (2017). Index Quality Assesment Citra Terinterpolasi (SSIM dan FSIM). *Jurnal Terapan Teknologi Informasi*, 1(1).