BAB I
PENDAHULUAN

1.1 Latar Belakang

Laju pertukaran informasi yang semakin pesat di era digital saat ini membawa tantangan besar dalam menjaga kerahasiaan dan keamanan data, khususnya pada media gambar yang sering digunakan sebagai sarana pertukaran dan penyimpanan informasi penting. Ancaman seperti penyadapan, pencurian data, serta modifikasi tidak sah terhadap data digital menuntut adanya solusi keamanan yang tidak hanya mampu melindungi isi pesan, tetapi juga menyamarkan keberadaan pesan tersebut dari pihak yang tidak berwenang (Amanda, 2023).

Kriptografi dan steganografi merupakan dua cabang ilmu yang berkembang pesat untuk menjawab kebutuhan tersebut. Kriptografi berperan sebagai teknik penyamaran data dengan cara mengubah informasi asli (plainteks) menjadi bentuk yang tidak dapat dikenali (cipherteks) melalui proses enkripsi, sehingga hanya pihak yang memiliki kunci tertentu yang dapat mengembalikan data ke bentuk semula melalui proses dekripsi (Mulyadi, 2019). Salah satu algoritma kriptografi yang banyak diadopsi karena kekuatan dan efisiensinya adalah *Advanced Encryption Standard* (AES). AES dalam pengamanan data dapat diimplementasikan terhadap pesan teks, file dan isi dokumen (Pabokory, 2015). AES juga dapat diimplementasikan terhadap pesan dalam bentuk audio (Sihombing, 2019), selain audio terdapat juga implementasi terhadap gambar dengan menggunakan AES (Pangestu, 2022).

AES merupakan algoritma blok cipher simetris yang digunakan secara luas untuk melindungi data sensitif karena tingkat keamanannya yang tinggi dan ketahanannya terhadap berbagai serangan kriptanalisis (Pabokory, 2015). Algoritma ini diresmikan sebagai standar kriptografi oleh *National Institute of Standards and Technology* (NIST) pada tahun 2001, menggantikan *Data Encryption Standard* (DES) yang sudah dianggap tidak aman. AES mampu melakukan proses enkripsi dan dekripsi data dengan panjang kunci yang bervariasi, yaitu 128-bit, 192-bit, dan 256-bit, sehingga fleksibel dalam

penerapannya untuk berbagai kebutuhan keamanan informasi (Voni, 2009). Menurut Fredianto (2018) AES-128 memiliki keunggulan utama dalam kecepatan eksekusi karena hanya memerlukan 10 putaran enkripsi, sedangkan AES-192 dan AES-256 masing-masing memerlukan 12 dan 14 putaran. Hal ini membuat AES-128 lebih cepat dan efisien, Meskipun panjang kuncinya lebih pendek, AES-128 tetap sangat aman dengan ruang kunci 2^{128} yang tidak dapat dipecahkan secara praktis sehingga pada AES-128, AES-192, serta AES-256 tidak memiliki perbedaan performa yang signifikan, cocok untuk aplikasi kinerja tinggi dan perangkat dengan keterbatasan sumber daya, sehingga peneliti disini memilih untuk menggunakan AES-128.

Namun, penggunaan kriptografi saja seringkali masih menimbulkan kecurigaan karena bentuk cipherteks yang dihasilkan cenderung acak dan tidak wajar. Untuk mengatasi hal ini, steganografi hadir sebagai solusi pelengkap dengan menyembunyikan pesan yang telah dienkripsi ke dalam media digital seperti gambar, sehingga keberadaan pesan tidak mudah terdeteksi oleh pihak luar (Sulviyani, 2022), sehingga dapat diketahui bahwa kriptografi merupakan teknik menyamarkan informasi sedangkan steganografi merupakan teknik menyembunyikan informasi. Salah satu metode steganografi yang efektif untuk media gambar adalah *Pixel Value Differencing* (PVD). PVD dalam menyembunyikan data dapat diimplementasikan terhadap media gambar (Gustiawan, 2023).

Metode PVD memanfaatkan perbedaan nilai antar piksel bertetangga untuk menentukan seberapa banyak bit pesan yang dapat disisipkan tanpa mengganggu kualitas visual gambar secara signifikan (Gustiawan, 2023). Pada area gambar dengan kontras tinggi, kapasitas penyisipan pesan dapat ditingkatkan, sementara pada area kontras rendah, perubahan diminimalisir agar tidak terdeteksi oleh indera manusia (Tseng & Leng, 2013).

Kombinasi antara kriptografi AES dan steganografi PVD memberikan dua lapis perlindungan terhadap informasi. Pertama, isi pesan diamankan dengan enkripsi yang kuat. Kedua, pesan yang telah terenkripsi disisipkan ke dalam

gambar sehingga tidak menimbulkan kecurigaan dan sulit dideteksi keberadaannya. Pendekatan ini telah terbukti mampu meningkatkan kerahasiaan, integritas, serta otentikasi data, sekaligus menjaga kualitas media gambar yang digunakan sebagai penampung pesan (Pabokory, 2015).

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada penerapan algoritma AES, khususnya AES-128, untuk mengenkripsi pesan, serta metode steganografi PVD untuk menyisipkan pesan terenkripsi ke dalam media gambar. Dengan demikian, diharapkan kombinasi kedua teknik ini mampu memberikan solusi keamanan data yang lebih optimal, baik dalam hal perlindungan isi pesan maupun penyamaran keberadaan pesan dalam media gambar.

1.2 Rumusan Masalah

Berdasarkan Latar belakang tersebut, rumusan masalah yang dapat diperoleh adalah sebagai berikut :

1. Bagaimana skema proses penerapan dari kombinasi kriptografi AES-128 dan steganografi PVD ke dalam media gambar?
2. Bagaimana konstruksi program aplikasi untuk menerapkan kombinasi kriptografi AES-128 dan steganografi *Pixel Value Differencing* menggunakan bahasa pemrograman *Python*?
3. Bagaimana kualitas dari *stego-image* yang diperoleh dari kombinasi kriptografi AES-128 dan steganografi PVD?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, dapat dituliskan tujuan dari penelitian ini adalah sebagai berikut :

1. Mengetahui skema proses penerapan kombinasi antara kriptografi AES-128 dan steganografi PVD pada media gambar.
2. Mengonstruksikan program aplikasi untuk menerapkan kombinasi kriptografi AES-128 dan steganografi *Pixel Value Differencing* menggunakan bahasa pemrograman *Python*.

3. Mengetahui kualitas *stego-image* yang diperoleh dari kombinasi antara kriptografi AES-128 dan steganografi PVD dengan membandingkan hasil uji kualitas gambar antara *cover-image* dengan *stego-image*.

1.4 Manfaat Penelitian

Adapun beberapa manfaat dari penelitian ini yang diharapkan dapat berguna dalam berbagai hal, diantaranya yaitu:

1. Berkontribusi dalam bidang kriptografi dan steganografi, khususnya dalam perkembangan kriptografi dan steganografi melalui kombinasi kriptografi AES-128 dan steganografi PVD pada media gambar.
2. Program Aplikasi yang dikembangkan dapat dimanfaatkan untuk pengamanan dan penyembunyian plainteks dengan menggunakan kombinasi kriptografi AES-128 dan steganografi PVD pada media gambar.

1.5 Batasan Masalah

Adapun batasan masalah dari penelitian ini adalah sebagai berikut :

1. Data informasi yang disamarkan berupa data teks.
2. Kriptografi AES yang digunakan adalah AES-128.
3. Media gambar yang digunakan sebagai *cover-media* dalam format (.PNG).