BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat diperoleh kesimpulan sebagai berikut :

1. Sistem enkripsi menggunakan teknik *hybrid* kriptosistem *Vigenere Cipher* dan *Advanced Encryption Standard* 128 (AES) memiliki tahapan yang panjang untuk memperoleh cipherteks finalnya, karena setelah melalui tahap enkripsi menggunakan algoritma *Vigenere Cipher* maka dilanjutkan dengan proses enkripsi menggunakan algoritma *Advanced Encryption Standard* 128 bit yang tersusun menjadi 10 *round* proses, dimana setiap *round* nya terdiri dari *initial round*, *subbyte*, *shiftrow*, *mixcolumn*, dan *add round key*. Apabila terdapat sedikit perbedaan pada penulisan kuncinya, maka akan menghasilkan cipherteks yang berbeda. Sehingga dengan adanya perpaduan dua teknik kriptografi (*hybrid* kriptosistem) tersebut membuat chipherteksnya sulit untuk dipecahkan tanpa menggunakan kunci yang sesuai.
2. Algoritma *Advanced Encryption Standard* 128 (AES) merupakan algoritma enkripsi yang bersifat *case-sensitive*, dimana adanya perbedaan dalam penulisan kunci enkripsi dapat membuat pesan yang dienkripsi menjadi berbeda. Dan apabila kunci yang digunakan pada proses dekripsi salah, maka plainteks yang dihasilkan juga akan berbeda.
3. *Image* (citra digital) hasil dari proses penyisipan pesan menggunakan teknik steganografi *Pixel Value Differencing* (PVD) memiliki kualitas yang baik, hal tersebut dapat dibuktikan dengan melakukan perbandingan antara *cover-image* dengan *stego-image* yang tidak terlihat perbedaannya secara fisik atau visual.
4. *Image* hasil penyisipan pesan (*stego-image*) memiliki tingkat distorsi yang rendah. Hal tersebut dibuktikan dengan nilai *Mean Squared Error* (MSE) yang rendah (dapat diartikan bahwa nilai *error* yang ada pada *image* tersebut

rendah), sehingga nilai *Peak Signal to Noise Ratio* (PSNR) tinggi yaitu diatas 50 dB. Dengan nilai PSNR terbesarnya mencapai 93.38702 dB.

5. *Stego-image* hasil dari proses steganografi tidak tahan terhadap adanya modifikasi pada *file image* baik berupa perubahan *brightness*, *contras*, maupun proses kompresi *image* karena hal tersebut akan mempengaruhi nilai piksel yang ada didalam *stego-image* tersebut.

5.2 Saran

Sistem enkripsi dan dekripsi pada penelitian ini masih memiliki banyak kekurangan. Sehingga diperlukan adanya pengembangan pada *hybrid* kriptosistem *Vigenere Cipher* dan *Advanced Encryption Standard* 128 bit (AES) yang dipadukan dengan teknik steganografi *Pixel Value Differencing* (PVD) ini agar memiliki kinerja yang lebih baik lagi. Oleh karena itu, saran yang dapat peneliti berikan untuk pengembangan pada penelitian selanjutnya yaitu :

1. Media yang dapat digunakan sebagai *cover-image* tidak hanya citra *grayscale* dengan kedalaman 8bpp berekstensi .png tapi juga dapat berupa *file image*, video, dan audio.
2. Pada penelitian selanjutnya dapat difokuskan pada pembuatan aplikasi yang mengutamakan *user interface* (UI) dan *user experience* (UX) untuk sistem enkripsi dekripsi berbasis *mobile* maupun website yang menerapkan *hybrid* kriptosistem *Vigenere Cipher* dan *Advanced Encryption Standard* 128 bit (AES) yang dipadukan dengan teknik steganografi *Pixel Value Differencing* (PVD) dalam sekali pemrosesan, sehingga masyarakat dapat menerapkan sistem keamanan tersebut dalam kehidupan sehari-hari tanpa membutuhkan laptop atau komputer.
3. Pengiriman *stego-image* dapat dilakukan dengan menggunakan media tanpa proses kompresi, karena proses kompresi *file* dapat mengubah nilai *pixel* yang ada pada citra digital sehingga pesannya tidak dapat diekstrak kembali.