BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang sudah dilakukan, maka didapat kesimpulan sebagai berikut:

1. Skema pengamanan *plaintext* dengan penggabungan kriptografi skema (t, w) dan steganografi *LSB* menggunakan *pseudorandom Hitzl-Zele* pada *file* audio *wav* berhasil dirancang. Terdapat 2 skema, yaitu *Dealer* dan *Participant*. *Dealer* adalah pihak pengirim *plaintext* yang berperan untuk mengenkripsi *plantext* menjadi beberapa *share* dan *embedding share* ke file audio *wav* berdasarkan *pseudorandom Hitzl-Zele*, sehingga diperoleh beberapa file audio, disebut sebagai *stego-audio* untuk dibagikan. *Participant* adalah pihak penerima *stego-audio* yang berperan untuk *extracting share* dari *stego-audio* berdasarkan *pseudorandom Hitzl-Zele* dan mendekripsi *plaintext* menggunakan *share* tersebut.
2. Algoritma dan program aplikasi yang diberi nama "*(t, w)-Threshold Scheme and LSB Hitzl-Zele*" telah dikonstruksi menggunakan bahasa pemrograman Python 3.12. Program aplikasi tersebut berisi 2 menu primer, pertama adalah Menu *Dealer* untuk enkripsi dan *embedding* dan Menu *Participant* untuk *extracting* dan dekripsi. Selain itu, terdapat menu sekunder untuk menjalankan tes *PSNR*.
3. Program aplikasi divalidasi dengan 3 cara, yaitu validasi perhitungan manual, validasi perumuman, dan validasi dengan tes *PSNR*. Pada validasi perhitungan manual, program aplikasi berhasil mengonstruksi kembali *plaintext* dengan seluruh hasil program aplikasi dan program perhitungan manual sudah sama. Untuk validasi perumuman, program aplikasi tetap berjalan pada $t, w,$ dan *plaintext* yang relatif besar. Sementara itu, hasil validasi tes *PSNR* menunjukkan program aplikasi memperlihatkan performa yang lebih baik dalam menyisipkan pesan berdasarkan nilai *PSNR* dibandingkan dengan penelitian Al-Hooti, dkk. (2016).

5.2 Saran

Setelah penelitian ini dilakukan, terdapat saran untuk dikembangkan dan diperbaiki pada penelitian selanjutnya, di antaranya:

1. Menemukan dan mengembangkan metode supaya kriptografi skema (t, w) dan steganografi *LSB* dengan menggunakan *pseudorandom Hitzl-Zele* dapat memproses *plaintext* yang berbentuk media lain, misalnya teks, gambar, audio, atau video.
2. Meneliti penggunaan algoritma *pseudorandom* lain untuk melihat perbandingan efektivitas dan keamanan dalam penerapan kriptografi skema (t, w) dan steganografi *LSB*.
3. Melakukan kriptanalisis untuk menguji kekuatan dan kelemahan dari implementasi kriptografi skema (t, w) dan steganografi *LSB* menggunakan *pseudorandom Hitzl-Zele*. Tujuan dari kriptanalisis ini adalah untuk mengidentifikasi potensi serangan dan mencari cara untuk meningkatkan keamanan algoritma yang digunakan.