BAB V
KESIMPULAN DAN SARAN

Dari konstruksi dan analisis algoritma kriptografi max plus wavelet yang sudah dilakukan, dapat diambil kesimpulan serta diberikan saran untuk perbaikan dan pengembangan penelitian selanjutnya.

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari pengerjaan tesis ini adalah:

1. Pada tesis ini berhasil dikonstruksi algoritma kriptografi berdasarkan transformasi max plus wavelet. Transformasi max plus wavelet yang digunakan adalah tipe A, B, C, D dan E. Algoritma ini termasuk dalam algoritma kriptografi *stream cipher*. Sedangkan berdasarkan jenis kunci termasuk kriptografi asimetris, karena kunci enkripsi berbeda dengan kunci deripsi. Kunci enkripsi terdiri dari dua bagian yaitu tipe max plus wavelet dan kanal yang digunakan. Kunci dekripsi terdiri dari kunci enkripsi ditambah dengan kode sinyal detail. Proses enkripsi didasarkan pada proses analisis, sedangkan proses dekripsi didasarkan pada proses sintesis.

2. Berdasarkan analisis hasil uji coba diketahui bahwa algoritma kriptografi ini mempunyai nilai korelasi *plaintext* dan *ciphertext* yang kecil, artinya *plaintext* dan *ciphertext* mempunyai hubungan linier yang sangat rendah. Algoritma ini juga memiliki nilai kualitas enkripsi yang baik. Hal-hal tersebut menunjukkan bahwa algoritma ini mempunyai enkripsi yang baik.

3. Dari penghitungan *running time* dan analisis kompleksitas diketahui bahwa kompleksitas algoritma ini adalah O(n) atau kompleksitas linier. Hasil tersebut menunjukkan bahwa Algoritma kriptografi ini efisien dalam hal waktu proses.

4. Algoritma kriptografi ini dalam prosesnya hanya melibatkan integer dan tidak melibatkan *floating point*, sehingga mempunyai beberapa kelebihan yaitu lebih sederhana, *running time* lebih cepat, penggunaan memori lebih kecil dan tidak menghasilkan error penghitungan.

5. Penggunaan kelima tipe MP-Wavelet dapat memperbesar *key space* sehingga semakin banyak kemungkinan kunci dan semakin sulit untuk menemukan kunci yang sebenarnya. Kunci kanal juga mempersulit upaya pemecahan kunci karena harus menemukan faktor-faktor dari suatu bilangan dan semua kemungkinan kanal yang digunakan. Disarankan menggunakan kunci enkripsi yang akan menghasilkan *ciphertext* dengan banyak karakter bukan bilangan prima agar kunci sulit untuk ditebak.

6. Kunci kanal pertama mempunyai pengaruh yang besar terhadap hasil enkripsi. Dengan menggunakan tipe max plus wavelet yang sama, jika kunci kanal pertama sama maka hasil enkripsi sebagian besar adalah sama. Jika kunci kanal pertama berbeda maka hasil enkripsi juga memiliki banyak perbedaan.

5.2 Saran

Saran-saran yang dapat diberikan setelah pengerjaan tesis ini adalah:

1. Banyaknya karakter yang digunakan diperbanyak, tidak hanya terbatas 95 karakter.

2. Proses enkripsi dilakukan lebih dari satu kali, sehingga akan lebih mengaburkan *ciphertext*.

3. Sebelum dilakukan proses analisis, *plaintext* diacak terlebih dahulu. Hal ini juga akan lebih mengaburkan *ciphertext*.

4. Penggunaan transformasi max plus wavelet untuk algoritma kriptografi citra, audio dan lain sebagainya.