BAB 6

KESIMPULAN DAN SARAN

Pada bab ini akan dibahas kesimpulan dari awal hingga akhir penelitian dan saran untuk penelitian selanjutnya.

6.1 Kesimpulan

Bagian ini akan membahas kesimpulan dari seluruh penelitian yang dilakukan pada skripsi ini. Kesimpulan diperoleh setelah melakukan beberapa langkah pengerjaan. Berikut merupakan langkah-langkah pengerjaan yang sudah dilakukan untuk memperoleh kesimpulan.

1. Mempelajari cara kerja metode steganografi *Least Significant Bit*
2. Mempelajari cara kerja metode steganografi *Pixel Indicator Technique*
3. Mengimplementasikan metode steganografi *Least Significant Bit*, *Pixel Indicator Technique*, dan metode *Modified Pixel Indicator Technique*

Berdasarkan langkah-langkah pengerjaan yang telah dilakukan dan berdasarkan pengujian pada Subbab 5.2, didapatkan kesimpulan bahwa perangkat lunak yang dibangun oleh penulis sudah dapat mengimplementasikan penyisipan *secret data* dengan metode *Least Significant Bit*, metode *Pixel Indicator Technique*, dan metode *Modified Pixel Indicator Technique*. Selain itu, perangkat lunak juga dapat mengimplementasikan ekstraksi *secret data* dengan ketiga metode tersebut.

Berdasarkan pengujian pada Subbab 5.3.1, diperoleh kesimpulan bahwa metode *Pixel Indicator Technique* kurang bagus untuk menyisipkan *secret data* dengan karakter yang cukup panjang. Hal ini disebabkan adanya penggunaan 8 byte nilai *channel* warna pertama pada *cover image* untuk menyisipkan panjang *secret data*. Terdapatnya panjang *secret data* di dalam *stego image* dapat berdampak buruk bagi kerahasiaan *secret data*, karena untuk melakukan ekstraksi pada metode *Pixel Indicator Technique* hanya dibutuhkan panjang *secret data*.

Berdasarkan pengujian pada Subbab 5.3.2, diperoleh kesimpulan bahwa metode *Least Significant Bit* menghasilkan *stego image* dengan kualitas gambar paling baik daripada metode lainnya. Hal ini dikarenakan penyisipan *secret data* dengan metode *Least Significant Bit* dilakukan dengan hanya mengganti satu bit terakhir dari setiap *channel* warna, sedangkan metode *Pixel Indicator Technique* dan metode *Modified Pixel Indicator Technique* melakukan penyisipan dengan mengganti 0 sampai 2 bit terakhir pada *channel* warna. Oleh karena itu, perbedaan nilai *channel* warna *stego image* dan *cover image* pada metode *Least Significant Bit* akan lebih kecil daripada kedua metode lainnya. Semakin kecil perbedaan nilai *stego image* dengan *cover image*, maka kualitas gambar (*stego image*) dapat dikatakan semakin baik.

Berdasarkan pengujian pada Subbab 5.3.3, diperoleh kesimpulan bahwa metode *Least Significant Bit* merupakan metode yang paling rentan dengan steganalisis *Chi-squared*. Metode *Least Significant Bit* memiliki nilai kemungkinan adanya *secret data* yang lebih besar daripada kedua metode lainnya. Seperti yang telah dibahas pada Subbab 2.2, bahwa metode *Least Significant Bit* melakukan penyisipan dengan cara mengganti bit terakhir pada setiap *channel* warna pada *cover image* dengan

bit *secret data* secara berurutan. Pola penyisipan ini tentunya membuat pihak-pihak yang tidak berkepentingan mudah untuk mendapatkan *secret data*. Oleh karena itulah terdapat pengembangan dari metode *Least Significant Bit*, yaitu metode *Pixel Indicator Technique* yang penyisipannya dilakukan dengan pola yang lebih acak.

6.2 Saran

Pada bagian ini akan dibahas saran dari penulis untuk pengembangan penelitian ini lebih lanjut. Berikut merupakan saran-saran tersebut.

- Pada penelitian ini, *secret data* yang digunakan hanya teks yang berupa String. Untuk penelitian lebih lanjut, penulis berharap perangkat lunak dapat dikembangkan sehingga *secret data* yang digunakan dapat berupa gambar, audio, video, ataupun *file* teks.
- Pada penelitian ini, *cover media* yang digunakan hanya berupa gambar (*cover image*). Untuk penelitian lebih lanjut, penulis berharap perangkat lunak dapat dikembangkan sehingga *cover media* yang digunakan tidak hanya berupa gambar, melainkan juga bisa video.

DAFTAR REFERENSI

[1] Gutub, A. (2010) Pixel indicator technique for rgb image steganography. *Journal of Emerging Technologies in Web Intelligence*, **1**, 1–10.

[2] Johnson, N. F. dan Jajodia, S. (1998) Exploring steganography: Seeing the unseen. *IEEE*, **31**, 1–4.

[3] Tiwari, N. dan Shandilya, M. (2010) Secure rgb image steganography from pixel indicator to triple algorithm-an incremental growth. *International Journal of Security and Its Applications*, **4**, 1–10.

[4] Anonymous (2012) Data link control: Error detection and correction. Technical Report 2. Indian Institute of Technology Kharagpur, India.

[5] S, A. dan S., N. B. (2012) Quality assessment of resultant images after processing. Technical Report 7. Dr. MGR Educational and Research Institute, India.

[6] Khalind, O. S., Hernandez-Castro, J. C., dan Aziz, B. (2014) Detecting 2-lsb steganography using extended pairs of values analysis. *SPIE-The International Society for Optional Engineering*, Baltimore, USA, 20-24 April, pp. 1–5. Baltimore, USA.

[7] Halim, I. F. (2016) Steganografi dengan pewarnaan graf. Skripsi. Universitas Katolik Parahyangan, Indonesia.