BAB II

TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Penelitian yang telah dilakukan berpedoman dari hasil penelitian-penelitian terdahulu yang pernah dilakukan sebelumnya sebagai bahan perbandingan atau kajian. Adapun hasil - hasil penelitian yang dijadikan perbandingan dan tidak terlepas dari topik penelitian yaitu, tentang teknik steganografi menggunakan metode *least significant bit* dan *end of file*.

Penelitian yang telah dilakukan (Zhou, et al., 2014), perancangan aplikasi ini menggunakan metode *least significant bit*, dimana dalam proses menyembunyikan pesan rahasia kedalam sebuah gambar. Dimana algoritma ini dapat menerapkan keacakan pada *byte* tersembunyi dalam volume dan *bit*. Selain itu, algoritma ini dapat meningkatkan teknik modifikasi data. Hasil penelitian yang diperoleh adalah algortima dapat menyembunyikan gambar dengan baik dan memperkuat volume penyembunyian data yang dapat menahan serangan dari luar.

Penelitian yang telah dilakukan (Amin, 2014), menyembunyikan pesan berupa teks rahasia ke dalam citra digital *true colour* 24 *bit* dalam format RGB. Algoritma yang digunakan untuk menyisipkan pesan rahasia menggunakan algoritma LSB *(Least Significant Bit)* dengan mengganti *bit* terakhir atau *bit* ke-8 dalam setiap komponen warna RGB. Semakin besar ukuran file tersebut maka nilai MSE akan semakin besar dan nilai PSNR semakin kecil, begitu pula sebaliknya semakin kecil ukuran *file* pesan

maka nilai MSE semakin kecil dan nilai PSNR akan semakin besar. Jika nilai PSNR tersebut kecil maka dapat dikatakan kualitas citra semakin buruk itu artinya kualitas citra secara fisik buruk pula. Sedangkan apabila nilai PSNR besar maka kualitas citra tetap bagus, yang artinya kerusakan pada citra relatif sedikit.

Penelitian yang telah dilakukan (Sari, et al., 2012), dalam penelitiannya dibangun sebuah aplikasi menggunakan metode *least significant bit* (LSB), dalam penelitiannya teknik steganografi memiliki dua proses utama. Pada tahap pertama adalah proses *encode* yaitu cara untuk menyembunyikan pesan ke dalam media penampung pesan, dimana pesan yang disembunyikan ke dalam media di enkripsi terlebih dahulu. Pada tahap kedua adalah decode yaitu pengecekkan pesan rahasia dari media penampung pesan lalu ditampilkan. Berdasarkan hasil dari penelitian, dapat disimpulkan bahwa aplikasi steganografi berhasil diimplementasikan pada *android mobile*. Aplikasi ini dapat menyimpan jumlah karakter hingga 6.500 karakter sesuai dengan kebutuhan berdasarkan gambar yang telah dilakukan uji coba.

Penelitian yang telah dilakukan (Sembiring, 2013), dalam penelitian ini membahas tentang bagaimana cara merancang suatu aplikasi steganografi *end of file* dan bagaimana proses penyisipanya dalam gambar. Kesamaan dengan penelitian yang dilakukan sekarang adalah merancang aplikasi steganografi untuk menyisipkan pesan dalam media gambar. Perbedaannya adalah pada penelitian sebelumnya hanya menggunakan teknik steganografi dengan metode *end of file*, sedangkan pada penelitian sekarang teknik steganografi menggunakan metode *end of file* dikombinasikan dengan metode *least significant bit.*

Penelitian yang telah dilakukan (Edisuryana, et al., 2013), dalam penelitian ini di implementasikan teknik kriptografi dan steganografi pada citra berformat *bitmap* dengan menggunakan metode *end of file* (EOF). Penelitian sebelumnya dengan yang sekarang dilakukan memiliki persamaan yakni menerapkan teknik steganografi menggunakan metode *end of file*. Sedangkan perbedaannya adalah penelitian ini hanya menggunakan satu metode *end of file*, sedangkan pada penelitian sekarang teknik steganografi menggunakan dua metode *end of file* yang dikombinasikan dengan metode *least significant bit*. Selain itu perbedaan lainnya terdapat juga pada implementasinya. Penelitian sebelumnya menggunakan matlab R2008a, sedangkan pada penelitian sekarang implementasinya menggunakan aplikasi yang telah dibangun berdasarkan pada algoritma kedua metode berbasis *mobile.*

Penelitian yang telah dilakukan (Rahayu, et al., 2012), Dalam penelitiannya keamanan data menjadi suatu hal yang paling terpenting demi terjaminnya kerahasiaan data dalam sebuah *file*. Metode yang digunakan dalam penelitian ini adalah *end of file.* Metode *end of file* merupakan salah satu metode yang digunakan dalam teknik steganografi, metode ini digunakan dengan cara menambahkan data pada bit terakhir dalam *file*. Dalam penelitiannya akan dibangun sebuah aplikasi yang menerapkan steganografi metode *end of file* dan *Rijndael*. Persamaan dengan penelitian sekarang adalah dalam penerapan metode *end of file* untuk menyisipkan pesan, sedangkan perbedaannya terletak pada metode enkripsi yang digunakan. Pada penelitian sebelumnya menggunakan enkripsi *Rijndael* sedangkan pada penelitian sekarang

menggunakan dua metode yaitu *least significant bit* dan *end of file* untuk dibandingkan berdasarkan kualitas citra yang terbaik.

2.2 Perbandingan Penelitian

Pada Tabel 1. dapat dilihat perbandingan penelitian yang dilakukan penulis dengan penelitian yang telah ada berdasarkan judul, metode, platform yang digunakan dan tujuan dari penelitian yang dilakukan.

Tabel 1. Perbandingan Penelitian				
No.	**Judul dan Penulis**	**Metode**	**Platform**	**Tujuan Penelitian**
1.	Aplikasi *mobile* menggunakan metode *Least Significant Bit* dan *End Of File* untuk steganografi (Malo, F.X. Kurniawan, 2017)	*Least Significant Bit dan End of File*	Android	Tujuan yang ingin dicapai dalam penelitian ini adalah membandingkan dua metode steganografi pada citra dengan menggunakan metode *least significant bit* dan metode *end of file* berbasis *mobile*.
2.	*Improved LSB algorithm of image hiding based on randomness* (Zhou, et al., 2014)	*Least Significant Bit*	Visual Studio C#	Tujuan dari penelitian ini adalah menerapkan metode *least significant bit* dalam gambar yang tersembunyi menggunakan domain spasial berdasarkan keacakan dalam gambar.
3.	Image steganography dengan metode *least significant bit* (Amin, 2014)	*Least Significant Bit*	Visual Basic 6.0	Tujuan dalam penelitian ini yaitu menerapkan teknik steganografi menggunakan metode *least significant bit* dengan perangkat lunak *visual basic 6.0*, sehingga proses penyembunyian pesan aman dan tidak mempengaruhi kualitas dari *cover image* secara *significant*.
4.	Implementasi steganografi menggunakan metode *Least Significant Bit* dan *Kriptografi Advanced Encryption Standard* (Sari, et al., 2012)	*Least Significant Bit*	Android	Tujuan yang diharapkan dalam penelitian ini adalah implementasi dari teknik kriptografi dan teknik steganografi dengan menggunakan tempat atau media penampung pesan yang berformat *png* dan dapat diintegrasikan ke dalam sistem operasi berbasis *mobile* android.
5.	Perancangan aplikasi steganografi untuk menyisipkan pesan teks pada gambar dengan metode *End of File* (Sembiring, 2013)	*End of File*	Visual Basic 6.0	Tujuan yang dingin dicapai adalah merancang sebuah aplikasi menggunakan teknik steganografi dengan menerapkan metode *end of file* pada aplikasi steganografi yang telah dirancang.
6.	Aplikasi steganografi pada citra berformat *Bitmap* dengan menggunakan metode *End Of File* (Edisuryana, et al., 2013)	*End of File*	Matlab R2008a	Dalam penelitiannya menerapkan algoritma dengan teknik steganografi menggunakan metode *end of file* (EOF) dengan perangkat yang digunakan yaitu MATLAB R2008a, serta menguji setiap tingkat perubahan citra pada *file* yang telah disisipkan pesan.
7.	Implementasi steganografi teknik *End Of File* dengan enkripsi *Rijndael* (Rahayu, et al., 2012)	*End of File*	*XAMPP* 1.7.3.	Tujuan dalam penelitian ini adalah menerapkan teknik steganografi dan kriptografi dalam proses penyisipan pesan dengan melakukan enkripsi dan deskripsi sehingga memiliki kualitas dan kuantitas *file* yang baik.