BAB I
PENDAHULUAN

1.1 Latar Belakang

Algoritma AES merupakan algoritma kriptografi menggunakan kunci simetris. Algoritma ini sangat efisien di dalam *software* maupun *hardware*. Algoritma ini memiliki ukuran blok tetap 128 bit serta ukuran kunci dengan kelipatan 32 bit, dengan minimum 128 dan maksimum 256 bit. Namun, algoritma AES ini memiliki kelemahan terhadap pengacakan kuncinya sehingga ekspansi kunci yang dihasilkan saling terkait dengan kunci aslinya (Geetha, et al., 2018). Untuk menyelesaikan permasalahan ini, dapat dilakukan modifikasi modul ekspansi kunci dari metode AES dengan *Symmetric Random Function Generator* (SRFG). SRFG menghasilkan *output* penyeimbang simetris dimana angka 1 dan 0 pada *string output* tidak berhubungan dengan *string input*. Sasaran utama dari penambahan SRFG ini adalah untuk menambahkan beberapa sifat pengacakan pada modul ekspansi kunci sehingga muncul istilah *Random Key Advanced Encryption Standard* (RK-AES). Selain kelemahan terhadap pengacakan kuncinya Metode AES juga memiliki perhitungan yang kompleks yaitu pada metode *MixColumns* sehingga membuat proses enkripsi dan dekripsi menjadi lebih lama. Untuk mengurangi kompleksitas tersebut digunakan metode *Bit Permutation* untuk menghindari perhitungan yang kompleks dan memberikan implementasi yang lebih mudah (Gamido, et al., 2018). Metode untuk mengganti *MixColumns* menjadi *Bit Permutation* ini dinamakan *Modified Advanced Encryption Standard* (MAES), dengan menggabungkan metode RK-AES dan MAES ini diharapkan agar data yang dilindungi menjadi lebih aman dan cepat dalam prosesnya.

Untuk lebih meningkatkan keamanan dari data yang dirahasiakan, maka dapat diterapkan metode steganografi untuk menyembunyikan data rahasia tersebut ke dalam sebuah media yang berupa citra digital. Salah satu metode steganografi yang paling umum digunakan adalah metode *Least Significant Bit* (LSB). Namun, metode ini memiliki kelemahan, yaitu sudah terlalu umum dan memiliki kompleksitas yang rendah dan metode ini hanya menyisipkan bit pesan ke dalam

cover image (citra sampul) sehingga dapat dideteksi dengan mudah (Batarius & Maslim, 2012). Untuk itu, maka perlu dilakukan modifikasi terhadap metode LSB yang disebut sebagai *Modified Least Significant Bit* (MLSB) (Nimje, et al., 2014). Metode MLSB sangat fleksibel dibandingkan metode LSB karena dapat ditentukan tempat atau cara dilakukan penyisipan data tersebut. Modifikasi ini bernama *Random Pixel Selection* yang akan dimulai dari proses segmentasi citra *input* dengan menggunakan metode *Different Size Image Segmentation* (DSIS) untuk memperoleh subblok citra dengan ukuran yang berbeda-beda dari *cover image* untuk menyebarkan data rahasia secara acak dan juga memiliki metode perhitungan bit sisip bernama *Number of Bits To be Hide* (NBTH) dimana nilai metode ini memiliki nilai 1 sampai 4. Kelebihan dari metode MLSB ini adalah data rahasia akan disisipkan secara acak dan nilai sisipnya tidak mudah untuk diprediksi sehingga tingkat keamanannya lebih baik daripada metode LSB (Shatanawi & Emam, 2015).

Dengan menggunakan penggabungan dari algoritma kriptografi RK-AES , MAES dan metode steganografi MLSB diharapkan akan memberikan proteksi yang lebih baik terhadap data. Mencermati hal-hal yang telah dipaparkan di atas maka diangkatlah topik tugas akhir dengan judul **"PENGAMANAN DATA MENGGUNAKAN ALGORITMA RANDOM KEY MAES DAN MLSB"**.

1.2 Rumusan Masalah

Berdasarkan uraian dari latar belakang di atas, rumusan masalah yang akan dibahas adalah:

1. Metode AES memiliki kelemahan pada pengacakan kuncinya.
2. Perhitungan MixColumns pada metode AES karena didalam perhitungan tersebut menggunakan perkalian *array*.
3. Metode LSB sudah terlalu umum dan memiliki tingkat kompleksitas yang rendah.

1.3 Tujuan

Adapun tujuan penelitian dalam tugas akhir ini adalah:

1. Membuat sebuah aplikasi yang dapat memberikan proteksi yang lebih baik terhadap data dengan menggabungkan algoritma *Random Key Modified Advanced Encryption Standard* (RK-MAES) dan metode steganografi *Modified Least Significant Bit* (MLSB).
2. Mengetahui keamanan kunci dan waktu proses enkripsi dan dekripsi dari RK-MAES dan juga mengetahui nilai PSNR dan MSE pada MLSB.

1.4 Manfaat

Manfaat dari penulisan tugas akhir ini adalah:

1. Tersedia aplikasi alternatif pengamanan data menggunakan kriptografi *Random Key Modified Advanced Encryption Standard* (RK-MAES) dan steganografi *Modified Least Significant Bit* (MLSB).
2. Sebagai bahan referensi bagi peneliti lain yang ingin membahas topik yang terkait dengan penelitian AES dan MLSB.

1.5 Batasan Masalah

Adapun batasan masalah dari tugas akhir ini adalah :

1. Media citra digital yang akan digunakan untuk penyembunyian pesan berformat bmp.
2. Data yang dienkripsi berupa teks yang berformat docx, doc, txt, dan rtf.
3. Kunci yang digunakan dalam metode RK-MAES adalah sebesar 128 bit.
4. Ukuran citra sampul dibatasi dengan minimal 100 x 100 piksel.
5. Data rahasia akan disisipkan pada *channel* R, G dan B dengan jumlah bit yang disisipkan ditentukan oleh nilai NBTH dari metode MLSB.

1.6 Metodologi Penelitian

Langkah-langkah dalam pengerjaan tugas akhir ini, sebagai berikut:

1. Mengumpulkan dan mempelajari materi yang berhubungan dengan topik yang dibahas yaitu mengenai algoritma Kriptografi AES, RK-MAES, Metode Steganogafi *Least Significant Bit (LSB)* dan *Modified Least Significant Bit*

(MLSB), serta pemrograman C#. serta referensi-referensi lainnya yang berhubungan dengan tugas akhir ini.

2. Pengembangan sistem dengan menerapkan metode *Waterfall* :
   a. Analisis Sistem

      Tahapan ini mencakup analisis masalah dan kebutuhan sistem secara fungsional dan non-fungsional. Analisis masalah dilakukan dengan melakukan analisa ulang terhadap algoritma-algoritma yang digunakan untuk mengidentifikasi potensi kesalahan perangkat lunak. Setelah itu, akan dilakukan analisa atau penjelasan tentang cara kerja algoritma yang digunakan. Terakhir, akan dilakukan pemodelan terhadap sistem yang akan dirancang dengan *Use Case Diagram*.

   b. Perancangan Sistem

      Pada tahap ini dilakukan perancangan tampilan antarmuka pada sistem (*user interface*) dengan aplikasi balsamiq Mockup. Perancangan tersebut akan dilakukan dengan bantuan perangkat lunak seperti Microsoft Visio 2007.

   c. Pembuatan Sistem

      Pada tahap ini dilakukan proses pengkodingan (*coding*) sistem dengan menggunakan bahasa pemrograman C#.

   d. Pengujian Sistem

      Sistem yang telah selesai dibuat akan diuji dengan tujuan untuk mengetahui bagaimana cara kerja metode RK-MAES dan MLSB yang telah diimplementasikan pada sistem. Proses pengujian yang akan dilakukan mencakup:

      1) Proses pengujian keamanan kunci dari RK-AES dengan melihat perubahan kunci yang diperoleh pada saat pengubahan 1 karakter pada kunci yang digunakan.
      2) Proses pengujian kecepatan proses enkripsi dan dekripsi dari metode MAES dengan metode AES.
      3) Proses pengujian terhadap kualitas citra stego yang dihasilkan oleh metode MLSB akan menggunakan metode MSE dan PSNR.