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). Untuk memperoleh kelebihan dari metode RK-AES dan MAES, maka akan digabungkan metode RK-AES dan MAES.

Sementara itu, 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 dengan Random Pixel Selection**".

1.2 Perumusan Masalah

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

1. Bagaimana menghilangkan keterkaitan ekspansi kunci yang dihasilkan dengan kunci aslinya pada metode AES.
2. Bagaimana mempercepat proses enkripsi dari metode AES.
3. Bagaimana meningkatkan keamanan dari data yang dirahasiakan, agar tidak dapat terdeteksi dengan mudah.

1.3 Tujuan dan Manfaat

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 dengan metode *avalanche effect* dan waktu eksekusi proses enkripsi dan dekripsi dari RK-MAES serta juga mengetahui nilai PSNR dan MSE pada MLSB.

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.

1.4 Pembatasan 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.

1.5 Keterbaruan

Penelitian sejenis yang pernah dilakukan sebelumnya yaitu: “Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES”. Hasil penelitian ini yaitu “modified LSB digunakan untuk menyisipkan bit-bit cipherteks ke dalam diagonal matriks pixel komponen warna pada citra. Sistem ini dikembangkan dengan menggunakan bahasa pemrograman c#. Pengujian yang dilakukan pada penelitian ini yaitu dengan

melihat aspek *imperceptibility* dan aspek *recovery* pada metode *modified* LSB. Penelitian ini menegaskan bahwa kombinasi dari algoritma AES dan modified LSB dapat digunakan dalam meningkatkan keamanan data" (Syaiful Anwar, 2017).

Penelitian lainnya yaitu "Aplikasi Pengamanan Informasi Menggunakan Metode *Least Significant Bit* (LSB) dan Algoritma Kriptografi *Advanced Encryption Standard* (AES)". Hasil dari penelitian ini adalah "semua aspek keamanan data dapat dicapai, termasuk ketika melewati proses pengiriman data melalui media seperti *internet*" (Dian Novianto dan Yohanes Setiawan, 2018).

Penelitian lainnya lagi yaitu "Algoritma Kriptografi Triple DES dan Steganografi LSB sebagai Metode Gabungan dalam Keamanan Data". Hasil dari penelitian ini adalah "algoritma kriptografi Triple DES dan steganografi LSB sanggup memberikan keamanan ganda karena pesan bukan hanya tersembunyi dalam gambar tetapi juga terenkrip menggunakan algoritma kriptografi Triple DES" (Parma Hadi Rantelinggi dan Eka Saputra, 2020).

Penelitian lainnya lagi seperti "Steganografi pada Citra dengan Metode MLSB dan Enkripsi Triple Transposition Vigenere Cipher". Hasil pengujian menunjukkan bahwa "kecepatan dan kualitas citra hasil steganografi bergantung pada berapa banyak karakter dan keacakan dari karakter yang akan diinput. Kualitas citra steganografi dengan metode ini menunjukkan kualitas yang baik, karena nilai PSNR di atas 40Db" (Ali Akbar Lubis, Ng Poi Wong, Irfan Arfiandi, V. Immanuel Damanik dan Adithya Maulana, 2015).

Perubahan yang ditawarkan dalam penelitian ini, mencakup:

1. Meningkatkan keamanan kunci dari metode AES dengan memodifikasi modul ekspansi kunci dari metode AES.
2. Meningkatkan kecepatan enkripsi dan dekripsi dari metode AES dengan menggunakan metode *Bit Permutation*.
3. Meningkatkan keamanan data dari metode LSB dengan menentukan tempat atau cara dilakukan penyisipan data.