**IMPLEMENTASI KRIPTOGRAFI RIJNDAEL DAN STEGANOGRAFI LSB PADA TEKS DAN CITRA BERWARNA**

1. **Latar Belakang**

Kriptografi merupakan ilmu mengenai teknik pengamanan atau penyembunyian komunikasi diatara dua pihak. Berdasarkan jenis kunci yang digunakan, algoritma kriptografi terbagi menjadi 2 yaitu kriptografi kunci simetri dan kriptogrfi kunci asim etri (Geta Putri et al., 2015). Dimana, kunci simetri ini menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, sedangkan kunci asimetri ini menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Pengukuran kekuatan suatu algoritma kriptografi bisa dilakukan dengan cara melihat nilai perubahan kecil baik pada *plaintext* maupun kunci yang dapat mempengaruhi *chipertext* atau biasa disebut sebagai *Avalanche Effect*. Kriteria algoritma kriptografi yang memiliki *Avalanche Effect* yang memuaskan adalah pada saat *chipertext* yang dihasilkan mengalami perubahan paling sedikit sebanyak 50% akibat terjadinya perubahan satu bit pada *plaintext* ataupun kunci (Singh & Singh, 2015). Semakin tinggi nilai *avalanche effect* maka semakin bagus algoritma kriptografi tersebut.

Terdapat beberapa penelitian mengenai *avalanche effect* untuk mengukur keamanan suatu algoritma kriptografi. Efek yang lebih berpengaruh kuat adalah ketika terjadi perubahan pada *plaintext* dibandingkan adanya perubahan pada kunci. Tetapi, pada penelitian ini hanya menggunakan *plaintext* yang relatif pendek.

Steganografi adalah teknik yang digunakan untuk menyembunyikan keberadaan data dalam berbagai format seperti teks, gambar, audio, atau video (Anshori et al., 2019). Steganografi mentransmisikan data dengan menyembunyikan keberadan adanya informasi sehingga orang lain selain orang yang ditujukan tidak dapat mengidentifikasi adanya keberadaan informasi tersebut.

Algoritma steganografi diantaranya *Least Significant Bit* (LSB), dan *End of File* (EOF). Keunggulan lebih banyak didapatkan pada metode LSB dibandingkan dengan metode EOF dikarenakan citra hasil penyisipan (citra stego/*stego image*) hanya mengalami sedikit penurunan kualitas yang tidak begitu berpengaruh secara signifikan bila dilihat oleh mata manusia, sedangkan metode EOF mengalami perubahan yang signifikan pada ukuran citra. Sehingga untuk metode penyisipan pada citra algoritma LSB lebih baik untuk digunakan.

Pada penelitian ini akan dilakukan penggabungan teknik kriptografi dengan metode Rijndael dan teknik steganografi dengan metode *Least Significant Bit* (LSB) dalam penyisipan teks pada citra berwarna.

1. **Rumusan Masalah**

Permasalahan yang akan dibahas pada penelitian ini adalah bagaimana proses mengimplementasikan penggabungan algoritma kriptografi Rijndael dalam pengamanan teks pesan dan penyisipannya di dalam citra menggunakan algoritma steganografi *Least Significant Bit* (LSB), bagaimana kualitas citra yang dihasilkan setelah proses penyisipan serta perbedaan kualitas citra stego yang dihasilkan yang ditentukan oleh hasil perhitungan nilai *Peak Signal-to-Noise Ratio* (PSNR). Selain itu, akan diukur lama waktu yang digunakan dalam proses penyisipan untuk tiap skema penyisipan.

1. **Penelitian yang Terkait**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Tahun | Authors | Objek | Metode Digunakan | Hasil Analisa |
| 1. | 2019 | Yusuf Anshori, A.Y. Erwin Dodu, Megawati Purwaningsih | Citra Digital | *Least Significant Bit* (LSB) | - Proses penyisipan pesan dapat dilakukan dengan tiga jenis pesan rahasia berupa teks, gambar, dan *file* berbentuk rar.  - Metode LSB dapat menyembunyikan pesan dengan cara mengganti bit paling kanan cover dengan bit pesan rahasia.  - Steganografi ini hanya dapat melakukan *embed* dan ekstrak gambar yang memiliki piksel 24 bit. |
| 2. | 2018 | Geby Geta Putri, Wiwin Styorini, Rizki Dian Rahayani | Citra Digital | Kriptografi AES dan RSA | - Pada algoritma AES, proses enkripsi dan dekripsi dipengaruhi oleh panjang kunci, semakin panjang kunci maka proses enkripsi dan dekripsi akan memakan waktu lebih lama.  - Pada algoritma RSA, proses enkripsi dan dekripsi dipengaruhi oleh pasangan kunci, semakin panjang kunci public maka proses enkripsi semakin lama dan semakin panjang kunci privat maka proses dekripsi akan memakan waktu lebih lama.  - Algoritma RSA lebih unggul pada kualitas dekripsi dan kecepatan proses enkripsi dan dekripsi, sedangkan algoritma AES lebih unggul pada kualitas enkripsi.  - Disarankan untuk dapat menggunakan penggabungan kedua algoritma untuk melakukan enkripsi dan dekripsi. |
| 3. | 2018 | Dian Novianto, Yohanes Setiawan | Informasi digital | LSB dan AES | - Penerapan steganografi LSB dapat dikombinasikan bersama kriptografi AES dikarenakan data yang berhasil dienkripsi dapat disisipkan kedalam gambar tanpa mengurangi kualitas citra secara signifikan.  - Ukuran gambar dengan ekstensi .bmp lebih konsisten terhadap penyisipan informasi dikarenakan tidak terjadi perbedaan ukuran gambar, tetapi pada gambar dengan ekstensi .png terjadi perbedaan ukuran ketika terjadi penyisipan pesan di dalamnya. |
| 4. | 2015 | Amritpah Singh, Harpal Singh | Citra Digital | *Least Significant Bit* (LSB) | - Metode Least Significant bit (LSB) untuk penyisipan pesan rahasia dibuat berdasarkan sensitivitas mata manusia terhadap berbagai panjang gelombang warna. Pendekatan selektif ini menginduksi noise yang lebih rendah dan keamanan yang tinggi untuk mentransfer gambar.  - Tetapi metode LSB yang digunakan ini menghasilkan kualitas gambar yang lebih baik, aman dan andal karena gambar dibagi menjadi tiga bidang, yaitu merah, hijau dan biru. Kemudian setelah dibagi menjadi tiga, pesan dimasukkan di setiap bidang berdasarkan sensitivitas warna. |
| 5. | 2019 | Tiepsi, Kristian Siregar | Teks | Rijndael (AES) | - Algoritma Rijndael memproses blok data 128-bit dengan panjang kunci 128 bit, 192 bit, dan 256 bit.  - Proses pengamanan algoritma Rijndaeldapat dilakukan dengan langkah-langkah antara lain *SubBytes*, *ShiftRows*, *MixColumns*, dan *addRoundkey*. |

**DAFTAR PUSTAKA**

Anshori, Y., Dodu, A. Y. E., & Purwaningsih, M. (2019). *SATIN – Sains dan Teknologi Informasi Aplikasi Steganografi pada Media Citra Digital Menggunakan Metode Least Significant Bit ( LSB )*. *5*(1), 1–10.

Geta Putri, G., Styorini, W., & Dian Rahayani, R. (2015). Ethos (Jurnal Penelitian dan Pengabdian Masyarakat): 197-207 Analisis Kriptografi Simetris AES dan Kriptografi Asimetris RSA Pada Enkripsi Citra Digital. *Ethos (Jurnal Penelitian Dan Pengabdian Masyarakat)*, *3*(8), 197–207.

Singh, A., & Singh, H. (2015). An improved LSB based image steganography technique for RGB images. *Proceedings of 2015 IEEE International Conference on Electrical, Computer and Communication Technologies, ICECCT 2015*, 1–4. https://doi.org/10.1109/ICECCT.2015.7226122

Nama : Jessica Julia Paradina Siregar

NIM : 09021281722032