Kombinasi Steganografi LSB dan Kriptografi AES dalam Sekuriti Teks Rahasia Pada Citra Berwarna

Chaerul Umam[1], Muslih[2], Daffa Fadillah[3]
[1,2,3] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
e-mail: [1]chaerul@dsn.dinus.ac.id, [2]muslih@dsn.dinus.ac.id, [3]dfffdllh20@gmail.com

ABSTRAK

Ketergantungan terhadap teknologi sebagai alat untuk melakukan dan membantu manusia dalam mengerjakan banyak hal dan instan, membuat penggunaan teknologi menjadi semakin massif dan seringkali terjadi penyalahgunaan terhadap teknologi. Penggunaan yang massif dalam skala besar-besaran dan tidak terkontrol membuat teknologi menjadi media yang rawan akan tindakan kriminal dan illegal. Faktor keamanan data menjadi suatu hal yang sangat penting dan harus dipertimbangkan terkait dengan semakin tingginya tingkat pertukaran data. Oleh sebab itu penulis memiliki gagasan dalam pengamanan data dengan menggabungkan teknologi kriptografi dan steganografi. Pemanfaatan algoritma kriptografi Advanced Encryption Standard *dan steganografi* Least Significant Bit *diharapkan mampu untuk membantu dalam pengamanan data di era saat ini.*

***Kata Kunci**: Stegamografi, Kriptografi, LBS, AES, Teks, Citra Berwarna*

1. PENDAHULUAN

Kemajuan teknologi dalam era globalisasi saat ini telah memberikan banyak manfaat diberbagai aspek termasuk dalam pertukaran informasi dan data-data yang bersifat publik (semua orang bisa melihat) ataupun data-data yang bersifat private (informasi atau data yang rahasia). Dengan dimanfaatkannya tenologi, pengolahan data dan pertukaran informasi menjadi sangat mudah. Informasi-informasi dan data yang ditukar tersebut tidak hanya berupa teks tulisan atau artikel dokumen. Media-media digital seperti video, audio, dan gambar juga merupakan media informasi karena bisa saja di dalam dokumen digital tersebut terdapat tulisan atau suara yang berisi informasi akan suatu hal [1], [2]. Ketergantungan terhadap teknologi sebagai alat untuk melakukan dan membantu manusia dalam mengerjakan banyak hal dan instan, membuat penggunaan teknologi menjadi semakin massif dan seringkali terjadi penyalahgunaan terhadap teknologi. Penggunaan yang massif dalam skala besar-besaran dan tidak terkontrol membuat teknologi menjadi media yang rawan akan tindakan kriminal dan illegal [3], [4].

Dari sekian banyak dan besar data dan informasi, mungkin data-data tersebut bisa saja berisi informasi penting yang bersifat privas. Karena bersifat private dan rahasia tidak menutup kemungkinan terjadinya tindak kejahatan teknologi seperti pencurian data melalui gawai yang diretas (sadap), pengubahan data terhadap informasi yang asli (valid) menjadi informasi yang palsu (invalid) dan tindak kejahatan digital lainnya yang dilakukan oleh orang yang tidak memiliki hak dan wewenang [5]–[7]. Demi melindungi data-data penting tersebut, dibutuhkan cara untuk menghindari tindakan-tindakan kejahatan digital atau cybercrime meskipun data disimpan secara lokal dan tidak didistribusikan atau dikirimkan tidak menutup kemungkinan dapat terjadinya tindakan kejahatan digital oleh pihak yang tidak memiliki hak-hak atas data tersebut. Faktor keamanan data menjadi hal yang sangat penting dan harus dipertimbangkan agar data tetap aman dan terhindar dari tindakan pencurian. Untuk menjaga keamanan, keaslian dan kerahasiaan data, dibutuhkan metode untuk menyembunyikan informasi asli namun dapat diakses oleh pihak-pihak tertentu yang memiliki wewenang khusus [8]–[10].

Kriptografi dan Steganografi adalah metode yang digunakan untuk proses pengamanan data. Kriptografi adalah ilmu yang mempelajari tentang kerahasian data, agar data tetap aman dan terjaga keaslianannya (valid) menggunakan metode enkripsi dan dekripsi. Sedangkan steganografi adalah ilmu yang melibatkan komunikasi data rahasia ke dalam pembawa multimedia sebagai media sampul atau penutup yang sesuai untuk menyembunyikan data atau informasi terhadap data digital. Kriptografi adalah salah satu metode untuk mengamankan dan menyembunyikan data dengan cara mengenkripsi dan mendekripsi informasi atau data menggunakan algoritma khusus. Kriptografi merupakan singkatan dari

"crypto" dan "graphia" yang dalam bahasa Yunani crypto yang artinya rahasia dan graphia yang memiliki arti tulisan. Dengan demikian secara umum kriptografi memiliki arti "tulisan rahasia". [2] Metode yang digunakan dalam proses kriptografi yaitu enkripsi dan dekripsi. Enkripsi adalah proses mengubah data asli menggunakan suatu algoritma tertentu menjadi sebuah data cipher atau data acak yang tidak dikenali oleh manusia maupun komputer. Dekripsi adalah proses pengembalian data menggunakan algoritma yang sama yang digunakan ketika proses enkripsi, mengembalikan data ciher menjadi data asli. Kata steganografi berasal dari bahasa Yunani. Steganografi merupakan singkatan dari kata Steganos dan Graptos. Steganos memiliki arti yaitu "menyembunyikan" dan Graptos yang secara harfiah memiliki arti "tulisan penutup". Dengan demikian, steganografi memanfaatkan media lain untuk menyembunyikan pesan rahasia yang disispkan ke dalam data yang lain. Steganografi berbeda dengan kriptografi karena steganografi hanya bersifat menyembunyikan data, informasi atau pesan rahasia tanpa mengubah strukturnya [11], [12]. Sedangkan, kriptografi adalah melindungi informasi yang akan dibagikan dengan mengubah struktur agar tidak dapat dipahami oleh orang lain selain orang yang semestinya menerima informasi tersebut.

Dengan latar belakang permasalahan tersebut, pada penelitian ini diusulkan sebuah solusi dalam proses pengamanan data digital menggunakan teknik kriptografi dan steganografi. Gagasan penulis dalam menentukan algoritma yang akan digunakan adalah Advanced Encryption Standard (AES) untuk proses pengamanan data dan menggunakan Least Significant Bit (LSB) untuk proses penyembunyian data. Tujuan dilakukan penelitian ini antara lain untuk mengetahui penerapan kombinasi kriptografi dan steganografi untuk mengamankan data digital; untuk mengetahui bagaimana proses implementasi penggabungan algoritma AES dan LSB dalam pengamanan data digital; dan untuk mengetahui tingkat keamanan data dari algoritma AES dan LSB dalam pengamanan data digital.

2. TINJAUAN PUSTAKA

2.1. Kriptografi

Kriptografi merupakan salah satu cara untuk menjaga keaslian data dengan cara mengacak data menjadi bentuk lain dan jauh dari bentuk aslinya [13], [14]. Kriptografi merupakan singkatan dari "crypto" dan "graphia" yang dalam bahasa Yunani crypto yang artinya "secret" atau rahasia dan "graphia" yang memiliki arti "writing" atau tulisan. Dengan demikian secara umum kriptografi memiliki arti "tulisan rahasia" [15]. Kriptografi adalah ilmu yang mempelajari tentang teknik penyandian dengan cara mengubah dan mengacak plaintext atau naskah asli menggunakan kunci dan algoritma khusus menjadi naskah acak yang sulit dikenali bahkan tidak bisa dibaca (ciphertext) oleh seseorang yang tidak memiliki kunci untuk mengembalikan informasi kembali ke naskah asli.

Proses untuk mengubah dan mengacak naskah asli menjadi naskah yang tidak dikenali disebut enkripsi, sedangkan dekripsi adalah sebuah proses mengembalikan naskah yang tidak dikenali menjadi naskah asli. Kedua proses utama kriptografi tersebut membutuhkan kunci untuk mengacak dan mengembalikan informasi. Sehingga ketika seseorang yang menerima data atau informasi tersebut tidak memiliki kunci, akan membutuhkan waktu yang sangat lama untuk mengembalikan ke bentuk asli dan kemungkinan tidak bisa dikembalikan sama sekali. Metode yang digunakan dalam teknik enkripsi kriptografi klasik menggunakan enkripsi simetris [16], [17]. Enkripsi simetris adalah proses enkripsi dimana kunci yang digunakan untuk dekripsi sama seperti dengan kunci yang digunakan untuk proses enkripsi. Kriptogarfi klasik menggunakan kunci yang dibuat melalui permutasi karakter atau subtitusi karakter.

2.2 Kriptografi Klasik

Kriptografi klasik adalah ilmu kriptografi yang dipakai pada zaman terdahulu dimana teknologi kalkulasi modern seperti komputer belum tercipta atau mungkin komputer sudah ditemukan tapi tidak secanggih saat sekarang ini. Kriptografi klasik menggunakan metode kalkulasi sederhana untuk proses pengacakan data seperti substitusi dan transposisi. Kriptografi klasik sendiri hanya terbatas pada karakter alfabet yaitu A-Z sehingga sangat tidak relevan apabila digunakan untuk mengamankan data di era perkembangan teknologi saat ini [15]. Karena tingkat pemecahan data yang relatif mudah dan dapat

ditembus dalam waktu singkat, kriptografi klasik sudah ditinggalkan dan telah digantikan kriptografi modern dengan proses kalkulasi yang lebih kompleks dan rumit. Ciri-ciri kriptografi klasik adalah:

- Terbatas karakter alfabet A - Z
- Menggunakan kalkulasi sederhana.
- Mudah ditebak hanya dengan melihat cipherteks (karena hanya menggunakan huruf abjad).

2.3 Kriptografi Modern

Kriptografi modern digolongkan menjadi 2 berdasarkan dengan jenis key nya yaitu Algoritma Asimetri atau algoritma kunci public dan Algoritma Simetri. Kriptografi modern membutuhkan komputasi komputer karena pada saat proses generasi kunci, enkripsi dan dekripsi menggunakan bilangan biner yang terdiri dari 1 (satu) dan 0 (nol) dan bilangan tersebut berjumlah sangat besar [11]. Setiap karakter kunci akan dikonversi menjadi sesuatu yang dipahami komputer yaitu setiap karakter akan diubah menjadi sederet bilangan 1 dan 0. Setiap karakter merupakan sederet bilangan biner dengan susunan yang unik sebesar 1 bit dimana setiap bit-nya berisi kombinasi bilangan 1 dan 0 sejumlah 8 karakter.

2.4 Kriptografi Berdasarkan Jenis Kunci

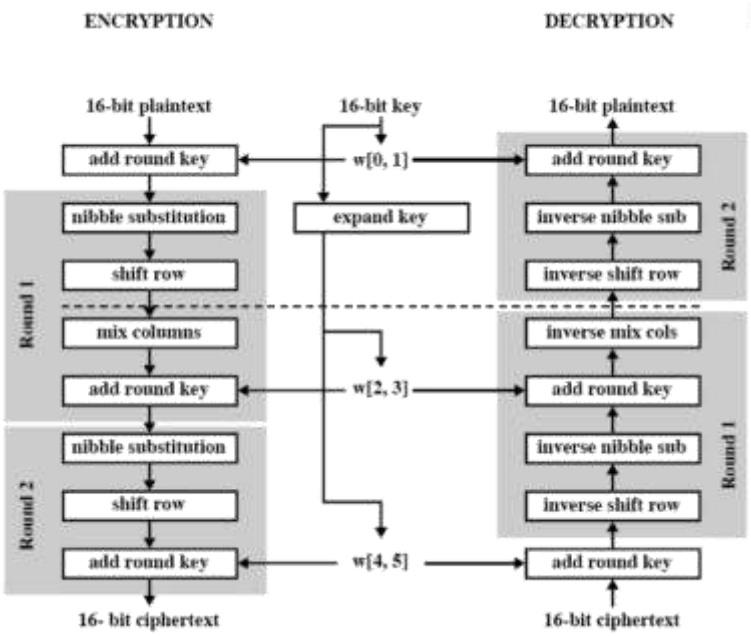
Kriptografi kunci simetris dan kirptografi kunci asimetris merupoakan bentuk kriptografi yang dikategorikan berdasarkan jenis kunci yang digunakan pada proses enkripsi dan dekripsi. Kriptografi kunci simetris merupakan algoritma yang dalam proses enkripsi dan dekripsi menggunakan metode dan kunci yang sama. Keamanan algoritma ini tergantung kunci tertentu yang telah disetujui oleh pihak pengirim dan penerima agar tetap bisa saling berkomunikasi dan bersifat rahasia [11], [18]. Dalam algoritma enkripsi simetris ketika kunci diketahui oleh orang yang tidak berkepentingan, maka orang tersebut memiliki akses untuk mendekripsi seluruh informasi. Algoritma yang termasuk simetris adalah DES, Rijndael (AES), Twofish, RC 5, OTP dan lain-lain. Algoritma simetris terdiri dari 2 jenis yaitu stream cipher dan block cipher. Stream cipher adalah algoritma simetris yang proses enkripsi dan dekripsinya dilakukan persatuan ukuran data seperti, bit, byte atau data dienkripsi setiap 10 bit. Sedangkan block cipher adalah algoritma yang enkripsi dan dekripsinya berupa satu buah blok data sebesar 64 bit dan atau 128 bit.

Kriptografi kunci asimetris merupakan algoritma yang telah dirancang secara kompleks untuk mengasilkan keamanan yang lebih tinggi karena kunci yang digunakan untuk dekripsi tidak sama dengan kunci yang digunakan untuk enkripsi. Dalam algoritma asimetri memiliki 2 buah kunci yaitu kunci publik dan kunci privat. Kunci publik dibuat dan dapat disebarluaskan hingga seluruh pihak dapat melihat kunci tersebut [19]. Untuk melakukan proses dekripsi, tharus menggunakan kunci privat dimana kunci privat merupakan pasangan kunci publik. Seperti kriptografi lainnya, kunci priat hanya dimiliki oleh pihak yang memiliki akses untuk melakukan proses dekripsi data. Beberapa algoritma yang termasuk algoritma asimetri adalah RSA yang diambil dari nama para perancangnya yakni Ron Rivest, Adi Shamir, dan Loenard Adleman. Algoritma RSA merupakan algoritma asimetri yang paling populer dari segi keamanan dan kekuatanya karena menggunakan proses eksponensial dan pemfaktoran bilangan menjadi 2 bilangan prima.

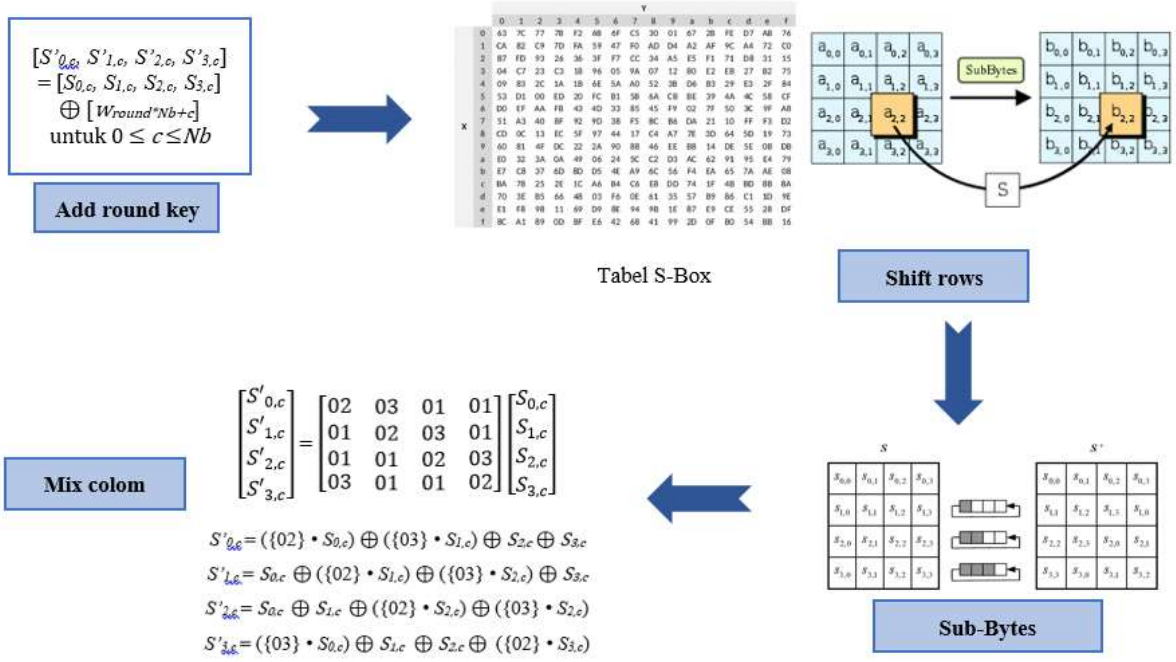
2.5 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) adalah algoritma kriptografi kunci simetris yang dibuat dan dirancang unttuk menggantikan algoritma DES atau Data Encryption Standard. Advanced Encryption Standard (AES) dipublikasikan secara resmi pada tahun 2001 oleh National Institute of Standard and Technology sebagai algoritma kunci simetris yang telah disepakati menjadi standar pada saat ini. Algoritma AES adalah algoritma kriptografi kunci simetris dimana kunci yang digunakan untuk dekripsi sama dengan kunci yang digunakan untuk enkripsi. AES memiliki 3 buah kategori kunci yakni AES 128 bit, 192 bit dan 256 bit [20], [21]. Pada algoritma AES 128 bit, setiap blok data asli sebesar 128 bit dirubah ke dalam bentuk state yaitu matriks heksadesimal berukuran 4x4. AES sendiri telah ditetapkan sebagai standar kriptografi blok cipher dengan kunci simetris sejak 2001 oleh NIST yang diperuntukkan untuk menggantikan algoritma DES karena mudah dibobol dan usang. Algoritma AES merupakan sebuah algoritma kunci simetris yang memiliki kemampuan enkripsi dan dekripsi data dengan varian kunci yang beragam yakni 128, 192, 256 bit. Blok data atau data asli tersebut berupa urutan data yang dikelompokan setiap blok nya terdiri dari 128

bit kemudian akan dilakukan proses enkripsi menjadi data cipher. Putaran enkripsi dan dekripsi pada algoritma AES dipengaruhi oleh panjang kunci. Sehingga ketika menggunakan kunci 128 bit, proses enkripsi atau dekripsi lebih cepat karena perputaran yang lebih sedikit. Algoritma AES dipilih karena memiliki kelebihan yaitu keamanan yang kuat dan kompatibel dengan segala macam perangkat lunak dan perangkat keras. AES memiliki kelebihan pada variasi kunci yang mempengaruhi perputaran enkripsi sesuai dengan penggunaan kunci. Semakin panjang kunci yang digunakan untuk algoritma AES, semakin banyak perputaran untuk mengenkripsi data tersebut.



Gambar 1. Alur enkripsi dekripsi AES



Gambar 2. Ilustrasi tahapan enkripsi AES

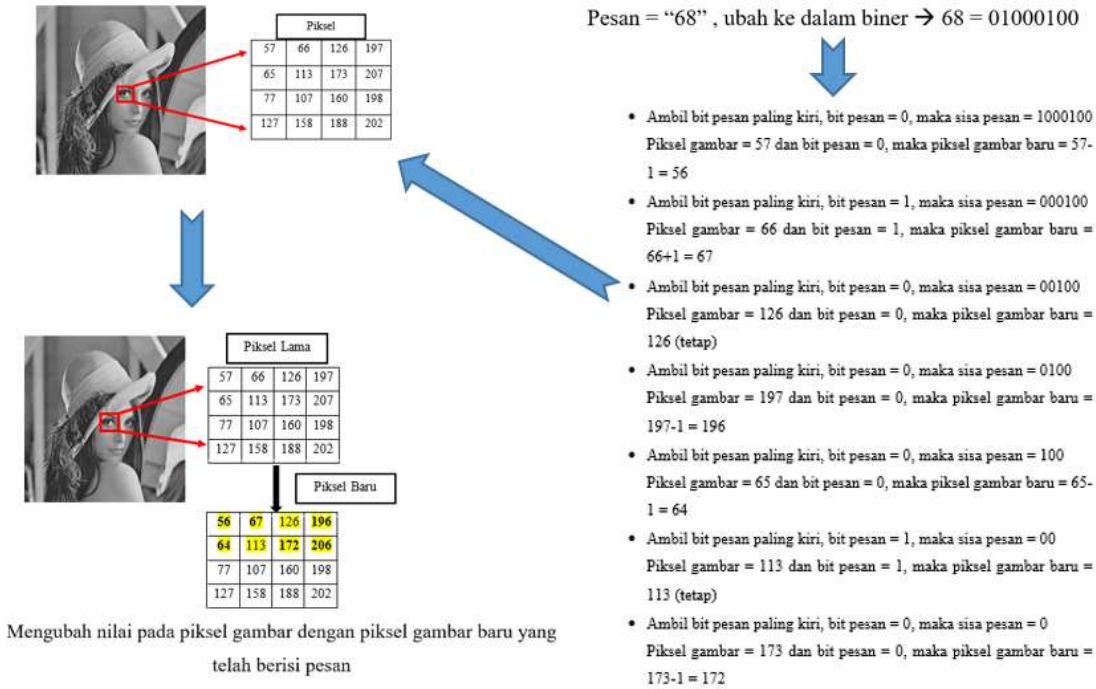
2.6 Steganografi

Steganografi merupakan singkatan dari kata Steganos dan Graptos. Steganos memiliki arti yaitu "menyembunyikan" dan Graptos yang secara harfiah memiliki arti "tulisan penutup". Kata steganografi berasal dari bahasa Yunani. Steganografi adalah ilmu yang melibatkan komunikasi data rahasia ke dalam pembawa multimedia sebagai media sampul atau penutup yang sesuai untuk menyembunyikan data atau informasi, misalnya file gambar, audio, video, dan sebagainya. Secara umum kata steganografi dikenal sebagai komunikasi yang tidak dapat dilihat oleh indera manusia. Steganografi berbeda dengan kriptografi karena steganografi hanya bersifat menyembunyikan data, informasi atau pesan rahasia tanpa mengubah strukturnya [11], [22]. Sedangkan, kriptografi adalah melindungi informasi yang akan dibagikan dengan mengubah struktur agar tidak dapat dipahami oleh orang lain selain orang yang semestinya menerima informasi tersebut. Salah satu media yang banyak digunakan ialah media gambar. Data, informasi atau pesan rahasia yang telah disembunyikan atau disematkan ke dalam gambar yang digunakan sebagai wadah sampul menghasilkan gambar stego. Gambar stego nantinya dapat dibagikan tanpa menimbulkan kecurigaan karena gambar stego menyerupai gambar cover (gambar asli sebelum disisipkan pesan rahasia).

Cara kerja pada steganografi adalah proses embedding dan proses extraction. Proses embedding adalah proses dimana pesan rahasia disisipkan pada suatu gambar yang digunakan agar pesan tersebut tidak dapat terlihat. Kemudian gambar stego dikirimkan ke pihak yang diinginkan tanpa harus takut diketahui oleh pihak ketiga. Setelah gambar stego diterima oleh penerima, terjadi proses extraction yang mana penerima dapat dengan mudah melakukan ekstraksi pada gambar tersebut. Pada proses ekstraksi dapat dilakukan secara langsung atau dengan menggunakan kunci stego (stego key), tergantung pada saat proses embedding. Pada gambar 8 menunjukkan cara kerja steganografi tanpa menggunakan kunci stego.

2.7 Least Significant Bit (LSB)

Least Significant Bit adalah metode steganografi yang dapat menyembunyikan pesan hanya dengan cara memasukkan setiap bit pesan ke dalam bit dari setiap piksel. Karena terjadi perubahan yang sangat kecil, mata manusia tidak dapat mengenali atau mendeteksi perubahan. Dikarenakan hal itu, metode LSB dapat menghasilkan gambar stego dengan kualitas impeceptibilitas yang baik [8]. Metode LSB merupakan salah satu algoritma dari domain spasial steganografi yang sangat sederhana. Metode ini melakukan perubahan gambar sampul secara berurutan.



Gambar 3. Ilustrasi embedding dengan LSB

3. METODE

3.1 Jenis Data

Dataset file citra yang akan digunakan untuk penelitian ini berupa file citra berjumlah 5 gambar citra dan keseluruhan file citra berupa file citra warna. Pada awalnya setiap file citra memiliki ukuran dan resolusi yang berbeda. Agar file citra memiliki ukuran dan resolusi yang sama untuk mempermudah proses perhitungan dan memenuhi syarat untuk diuji, file citra dimodifikasi dan diubah sedemikian rupa agar memenuhi syarat dengan cara melakukan proses cropping (pemotongan) dan resize (pengubahan ukuran). File citra yang diuji memiliki resolusi yang sama sebesar 512x512 piksel dan memiliki ukuran tidak lebih dari 2MB.

3.2 Alur Penelitian

Alur Penelitian ini dijabarkan secara singkat pada poin-poin di bawah ini:

1. Akuisisi Dataset Citra
   Pada penelitian ini, dataset citra yang digunakan diperoleh dari beberapa sumberyang beredar di internet. Total jumlah citra yang digunakan pada penelitian ini berjumlah 5 gambar dan memiliki resolusi berukuran 512x512 piksel dan berukuran tidak lebih dari 2MB.
2. Proses Enkripsi dan Penyisipan File
   Pada proses enkripsi file, pengujian dilakukan sebanyak 3 kali dengan 3 variasi panjang kunci yaitu 8, 16 dan 32 karakter. Kunci berupa alfabet A - Z dan angka 0 – 9 termasuk menggunakan karakter spesial seperti simbol, operator perhitungan dan karakter asing. Proses dilakukan dengan mengeksekusi Algoritma AES dan proses penyisipan dieksekusi denga algoritma LSB.
3. Proses Dekripsi dan Pembongkaran File
   Proses dekripsi file, dilakukan secara berkebalikan dari proses enkripsi dan menggunakan kunci yang sama persis dengan kunci yang digunakan saat proses enkripsi yaitu dengan menjalankan proses pembongkaran menggunakan LSB terlebih dahulu kemudian dilanjutkan dengan dekripsi algoritma AES.
4. Evaluasi
   Metode evaluasi yang dipakai pada penelitian ini menggunakan pengukuran nilai PSNR untuk file citra.

3.3 Hasil Analisa Pemrosesan

Hasil keluaran yang dihasilkan dari sistem ini adalah berupa beberapa file yaitu :

1. Plain file adalah file normal atau file asli yang belum atau tidak mengalami perubahan apapun.
2. Cipher File adalah file hasil dari proses enkripsi dan penyisipan pesan namun file masih dapat dikenali dan dibuka. Namun pesan tersembunyi tidak dapat dibaca atau dilihat.

3.4 Usulan Metode

Metode yang diusulkan dalam penelitian ini yaitu menggunakan algoritma AES (Advanced Encryption Standard) dan Least Significant Bit, proses pemodelannya adalah sebagai berikut :

1. Peneliti melakukan pengujian menggunakan file-file yang tercantum pada Batasan Masalah.
2. Melakukan pencatatan atribut-atribut file seperti ukuran file dalam satuan paling terkecil (byte) untuk selanjutnya sebagai pembanding dengan file yang telah dienkripsi & disispkan dan proses didekripsi .
3. Percobaan enkripsi dilakukan sebanyak 3 kali menggunakan kunci berupa alfabet A – Z dan angka 0 - 9 tanpa menggunakan karakter spesial seperti simbol dengan jumlah karakter 8, 16, dan 32 karakter dari masing-masing kunci menggunakan sata sebanyak 5 citra. Proses enkripsi dilakukan dengan memproses algoritma AES kemudian dilanjutkan dengan proses penyisipan pesan menggunakan LSB.
4. Plainteks dengan panjang 500 karakter termasuk dengan spasi, abjad, numerik, dan simbol unik.
5. Plainteks dienkripsi dengan algoritma Advanced Encryption Standard, kemudian akan menghasilkan cipherteks.
6. Cipherteks tersebut kemudian disisipkan ke dalam gambar yang diunggah.

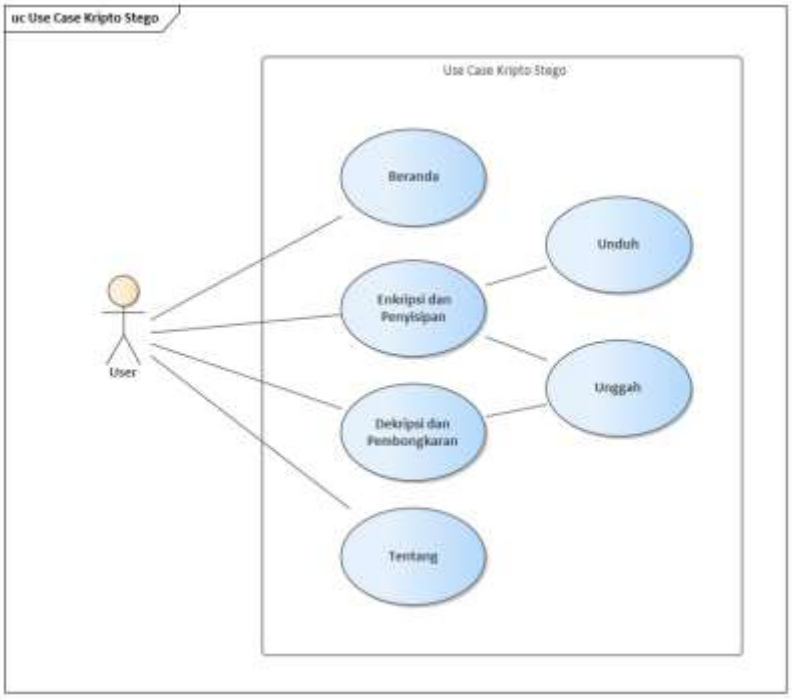
7. Setelah proses enkripsi selesai dijalankan menghasilkan file gambar berupa gambar yag telah disisipkan dengan algoritma LSB.
8. Melakukan pencatatan atribut-atribut file yang telah dienkripsi seperti ukuran file dalam satuan paling terkecil (byte) dan waktu yang telah dihabiskan untuk enkripsi untuk selanjutnya sebagai pembanding.
9. Proses dekripsi dilakukan dengan mengunggah gambar yang telah disisipkan sebelumnya kemudian memasukkan password yang sama seperti ketika proses enkripsi dilakukan.
10. Hasil dari proses dekripsi berupa plainteks identik seperti yang digunakan pada saat proses enkripsi.
11. Melakukan penghitungan dan perbandingan atribut file seperti ukuran file dalam satuan paling terkecil (byte) dan waktu yang telah dihabiskan untuk dekripsi untuk mengetahui apakah ada perbedaan atau tidak.

3.5 Metode Pengujian Hasil

Pengujian dilakukan pada tahap akhir dalam penelitian ini menggunakan Visual Studio Code sebagai aplikasi pengkodean dan aplikasi xampp sebagai side-server untuk mengolah Bahasa php. Tahapan yang dilakukan adalah menerapkan teknik pengacakan plainteks menjadi cipherteks dengan ilmu kriptografi. Penelitian ini bertujuan untuk menggabungkan 2 metode pada kriptografi dan steganografi. Objek yang digunakan dalam penelitian ini adalah file digital yaitu citra digital atau file gambar.

3.6 Use Case Diagram

Gambar 1. Ilustrasi dari proses konversi citra RGB menjadi Grayscale



Gambar 4. Use Case Diagram

4. HASIL DAN PEMBAHASAN

Tahapan ini merupakan tahap pembuatan sistem Pengamanan Data Menggunakan Kriptografi AES dan Steganografi Menggunakan Metode LSB dengan menerapkan analisis dan perancangan yang telah dilakukan untuk menghasilkan suatu sistem pendukung keputusan. Sistem pendukung keputusan ini diimplementasikan dengan web based untuk menjalankan aplikasi dibutuhkan xampp sebagai server local.

(a) (b)

Gambar 5. (a) tampilan enkripsi pesan, (b) tampilan dekrpsi pesan

Gambar 5(a) merupakan hasil implementasi halaman enkripsi dimana bila user memilih untuk melakukan proses enkripsi, maka sistem akan menampilkan halaman seperti ini, sedangkan Gambar 5 (b) hasil implementasi halaman dekripsi dimana bila user memilih untuk melakukan proses dekripsi, maka sistem akan menampilkan halaman seperti ini. Pada Gambar 6, dapat diilustrasikan hasil implementasi halaman hasil dekripsi dimana bila user telah selesai melakukan proses dekripsi, maka sistem akan menampilkan halaman hasil.

Gambar 6. Tampilan hasil dekripsi

Berikut ini merupakan percobaan menggunakan 5 buah citra berbeda ukuran dengan file pesan yang sama seperti pada Gambar 6. File citra berukuran 128x128 piksel sebanyak 2 citra, 256x256 piksel sebanyak 2 citra dan ukuran 512x512 piksel sebanyak 1 citra. Hasil enkripsi dan dekripsi juga dilihat dari waktu tempuh. Berdasarkan hasil eksperimen pada Tabel 1, dapat dilihat bahwa keseluruhan file tidak mengalami kendala saat proses enkripsi dekripsi.

Tabel 1. Waktu tempuh enkripsi dan dekripsi (dalam detik)

Nama File	Ukuran piksel citra	Enkripsi	Dekripsi
Lena.bmp	128x128 piksel	0.00654	0.00712
Gril.bmp	128x128 piksel	0.00932	0.00983
Plane.jpg	256x256 piksel	0.01985	0.01997
Flower.bmp	256x256 piksel	0.02450	0.02469
House.tiff	512x512 piksel	0.03888	0.03911
Rata-rata		0.019818	0.020114

Waktu yang dibutuhkan untuk pemrosesan cukup singkat meskipun pada Tabel 2 dapat dilihat bahwa 2 dari 5 citra berubah ukuran, dimana ukuran setelah enkripsi menjadi sedikit lebih besar dibanding citra asli. Berdasarkan Tabel 2, dapat diketahui bahwa dari 5 file percobaan, hanya terdapat 3 file yang tidak berubah ukuran selah proses enkripsi yaitu pada citra girl.bmp dan house.tiff. Perubahan file pada 3 citr alain mungkin disebabkan oleh ukuran citra cover yang kecil, namun di sisipi pesan yang cukup panjang dengan demikian berpengaruh pada ukuran file setelah proses enkripsi. Pada proses dekripsi, ukuran file kembali seperti semula.

Tabel 2. Ukuran file asli setelah enkripsi dan dekripsi

Nama File	Ukuran piksel citra	File Size		
		File Asli	File Setelah Enkripsi	File Setelah Dekripsi
Lena.bmp	128x128 piksel	32KB	34KB	32KB
Gril.bmp	128x128 piksel	32KB	32KB	32KB
Plane.jpg	256x256 piksel	68KB	70KB	68KB
Flower.bmp	256x256 piksel	69KB	70KB	69KB
House.tiff	512x512 piksel	124KB	124KB	124KB

5. KESIMPULAN

Dari hasil percobaan pada penelitian ini, telah didapatkan hasil sebagai berikut :

1. Dari hasil percobaan yang telah dilakukan pada aplikasi ini, program dapat mengamankan data dengan aik menggunakan algoritma AES dan LSB.
2. Dengan melakukan kombinasi algoritma AES dan LSB pengamanan pesan dan penyembunyian data menjadi lebih baik ketika dikirim dan dibagikan daripada mengirim data secara polos.
3. Meskipun data berhasil diambil dan diekstrak, pihak yang tidak bertanggung jawab akan sangat merasa kesulitan dan tidak dapat membaca pesan tersebut karena pesan telah dienkripsi.

6. SARAN

Dari hasil percobaan pada penelitian ini, penulis merasa dalam penulisan ini masih memiliki kekurangan antara lain :

1. Dalam proses enkripsi untuk saat ini hanya dapat berupa citra gambar. Diharapkan ketika penelitian ini dilanjutkan, sistem dapat melakukan proses penyisipan tidak hanya file citra (gambar), melainkan file yang lain.
2. Program masih dalam tahap pengembangan sehingga mungkin akan ada kendala ketika digunakan dalam jangka panjang. Peneliti berharap untuk peneliti selanjutnya untuk melakukan penyempurnaan terhadap program.

DAFTAR PUSTAKA

[1] D. Arisandi, M. B. Yusuf, and S. Sukri, “Pemeriksaan Integritas Dokumen Dengan Digital Signature Algorithm,” *JOISIE (Journal Inf. Syst. Informatics Eng.*, vol. 4, no. 1, p. 1, 2020.

[2] T. S. Permana, C. A. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and E. R. Subhiyakto, “Implementasi Pengamanan Citra Digital Berbasis Metode Kriptografi Vernam Cipher,” *Techno.Com*, vol. 16, no. 4, pp. 337–347, 2017.

[3] F. Muharram, H. Azis, and A. R. Manga, “Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES),” *Pros. Semin. Nas. Ilmu Komput. dan Teknol. Inf.*, vol. 3, no. 2, pp. 112–115, 2018.

[4] F. Al Isfahani and F. Nugraha, “Implementasi Steganografi LSB dengan Enkripsi Base64 Pada Citra dengan Ruang Warna CMYK,” *Sci. Comput. Sci. Informatics J.*, pp. 1–8, 2019.

[5] A. P. N. Nurdin, “Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia,” *Jesik*, vol. 3, no. 1, pp. 1–11, 2017.

[6] E. Rachmawanto, C. Sari, Y. Astuti, and L. Umaroh, “KRIPTOGRAFI VERNAM CIPHER UNTUK MENCEGAH PENCURIAN DATA PADA SEMUA EKSTENSI FILE,” in *PROSIDING SEMINAR NASIONAL MULTI DISIPLIN ILMU & CALL FOR PAPERS UNISBANK (SENDI_U) KE-2 Tahun 2016*, 2016, pp. 46–51.

[7] T. Zebua and E. Ndruru, “Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma RC4,” *J. Teknol. Inf.*

dan Ilmu Komput., vol. 4, no. 4, pp. 275–282, 2017.
[8] C. A. Sari, E. H. Rachmawanto, and E. J. Kusuma, "Good Performance Images Encryption Using Selective Bit T-Des on Inverted Lsb Steganography," *J. Ilmu Komput. dan Inf.*, vol. 12, no. 1, p. 41, 2019.
[9] E. H. Rachmawanto and C. A. Sari, "Keamanan File Menggunakan Teknik Kriptografi Shift Cipher," *Techno.COM*, vol. 14, no. 4, pp. 329–335, 2015.
[10] I. U. W. Mulyono, A. Susanto, T. Anggraeny, and C. A. Sari, "Encryption of Text Message on Audio Steganography Using Combination Vigenere Cipher and LSB (Least Significant Bit)," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 4, no. 1, pp. 63–74, 2018.
[11] E. J. Kusuma, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption," in *International Conference on Innovative and Creative Information Technology (ICITech)*, 2017, pp. 1–5.
[12] I. Suryanto, C. Suhery, and Y. Brianorman, "Pengembangan Aplikasi Chat Messenger dengan Metode Advanced Encryption Standard (AES) pada Smartphone," *J. Coding Sist. Komput. Untan*, vol. 03, no. 2, pp. 1–10, 2017.
[13] A. Putera and U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," *Int. J. Sci. Res.*, vol. 5, no. 7, pp. 1149–1152, Jul. 2016.
[14] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data Security Using Vigenere Cipher and Goldbach Codes Algorithm," *Int. J. Eng. Res. Technol.*, vol. 6, no. 01, pp. 360–363, 2017.
[15] D. Sinaga, C. Umam, D. R. I. M. Setiadi, and E. H. Rachmawanto, "Teknik Super Enkripsi Menggunakan Transposisi Kolom Berbasis Vigenere Cipher Pada Citra Digital," *Din. Rekayasa*, vol. 14, no. 1, p. 57, 2018.
[16] P. Saha, "A comprehensive study on digital signature for internet security," *Accent. Trans. Inf. Secur.*, vol. 1, no. 1, pp. 1–6, 2016.
[17] R. Aulia, A. Sembiring, A. Zakir, and B. A. U. Siregar, "Penyandian Texts Chat Via Internet Dengan Algoritma Vigenere Cipher," *JSIK (Jurnal Sist. Inf. Kaputama)*, vol. 3, no. 2, pp. 28–34, 2019.
[18] G. Ardiansyah, C. A. Sari, D. Setiadi, and E. H. Rachmawanto, "Hybrid Method using 3-DES , DWT and LSB for Secure Image Steganography Algorithm," in *International Conference on Information Technology, Information Systems, and Electrical Engineering*, 2017, pp. 248–253.
[19] H. Abdel-nabi and A. Al-haj, "Efficient Joint Encryption and Data Hiding Algorithm for Medical Images Security," in *Efficient Joint Encryption and Data Hiding Algorithm for Medical Images Security*, 2017, pp. 147–152.
[20] S. M. A. Ali and H. F. Hasan, "Novel encryption algorithm for securing sensitive information based on feistel cipher," *Test Eng. Manag.*, vol. 2019, no. November, pp. 10–16, 2019.
[21] M. T. Elkandoz, W. Alexan, and H. H. Hussein, "Double-Layer Image Security Scheme with Aggregated Mathematical Sequences," in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2019, pp. 1–7.
[22] A. K. Agrahari, M. Sheth, and N. Praveen, "Comprehensive Survey on Image Stegnography Using LSB With AES," vol. 13, no. 8, pp. 5841–5844, 2018.