



Implementasi Kriptografi *Advanced Encryption Standard* dan *Least Significant Bit* untuk Keamanan Pesan Email dalam Gambar

Repi Fahmi Sidiq¹, Raden Erwin Gunadhi Rahayu², Asep Deddy Supriatna³

Jurnal Algoritma
Institut Teknologi Garut
Jl. Mayor Syamsu No. 1 Jayaraga Garut 44151 Indonesia
Email : jurnal@itg.ac.id

¹1906014@itg.ac.id

²erwingunadhirahayu@itg.ac.id

³asepedddy@itg.ac.id

Abstrak – Email merupakan salah satu cara paling umum untuk berkomunikasi dan bertukar informasi di dalam dan luar kantor. *Manager* kantor Pos Garut selalu melakukan *meeting* dan kunjungan ke luar kota sehingga *manager* tidak selalu ada dikantornya, dikantor Pos Garut terdapat beberapa karyawan berdasarkan tingkatannya seperti karyawan tetap dan karyawan magang dalam melakukan penggajian karyawan tetap tidak perlu berkomunikasi dengan *manager* karena sudah tertera dikantor Pos Garut, tetapi untuk karyawan magang harus berkomunikasi dengan *managernya* sehingga hal ini sering dilakukan dengan pengiriman pesan email. Berdasarkan hasil wawancara yang dilakukan kepada *manager* kantor Pos Garut Menurutnya pesan melalui *Email* tidak selalu aman dalam mengirimkan informasi pribadi dan rahasia. Menurut sebuah studi 85% dari seluruh serangan *siber* yang terjadi pada perusahaan disebabkan oleh serangan *phishing* melalui *email*. Serangan *phishing* adalah teknik yang paling umum digunakan oleh peretas untuk mencuri informasi sensitif dari pengguna *email*. Kantor Pos Garut perlu memiliki Aplikasi Pengamanan Pesan *Email* dalam Gambar Menggunakan *Advanced Encryption Standard* (AES) dan *Least Significant Bit* (LSB) Berbasis *Website*, sehingga dapat meningkatkan tingkat keamanan dan privasi dalam pengiriman dan penerimaan pesan email untuk Karyawan Magang dan *Managernya*. Metodologi yang adalah metodologi *Extrime Programming* (XP), Untuk mengenkripsi pesan email menggunakan AES untuk keamanan, serta menyisipkan pesan yang dienkripsi ke dalam gambar dengan metode LSB agar tidak terlihat. Selain itu, penelitian ini ingin mengintegrasikan teknik ini ke dalam antarmuka website, menguji efektivitas keamanannya, dan memberikan kontribusi pada bidang keamanan informasi.

Kata Kunci – AES; Email; Kriptografi; LSB; Steganografi; Xtreme Programming.

I. PENDAHULUAN

Dalam era digital, email umum digunakan untuk berkomunikasi dan bertukar informasi di dalam dan luar kantor. Namun, rentannya email terhadap serangan yang mengancam kerahasiaan informasi seperti pencurian data atau penggunaan informasi secara tidak sah[1]. Penelitian dilakukan di Kantor Pos Garut, cabang PT Pos Indonesia (Persero) di Garut, Jawa Barat. *Manager* Kantor Pos Garut sering berada di luar kota, sehingga komunikasi melalui email penting, terutama dalam penggajian karyawan magang yang beragam. Pengiriman pesan email dari *manajer* kepada karyawan magang rentan terhadap risiko keamanan dan privasi karena pesan email tidak selalu aman. Oleh karena itu, Kantor Pos Garut perlu meningkatkan keamanan dan privasi pengiriman pesan email, terutama dalam pengiriman rincian penggajian karyawan magang, dengan aplikasi pengamanan email. *Manager* Kantor Pos Garut memiliki kekhawatiran terhadap pengiriman rincian gaji

karyawan magang melalui email yang tidak aman dan dapat membahayakan keamanan data dan reputasi perusahaan. Oleh karena itu, peningkatan keamanan dan privasi dalam pengiriman pesan email menjadi perlu, terutama melalui penggunaan aplikasi pengamanan email[2].

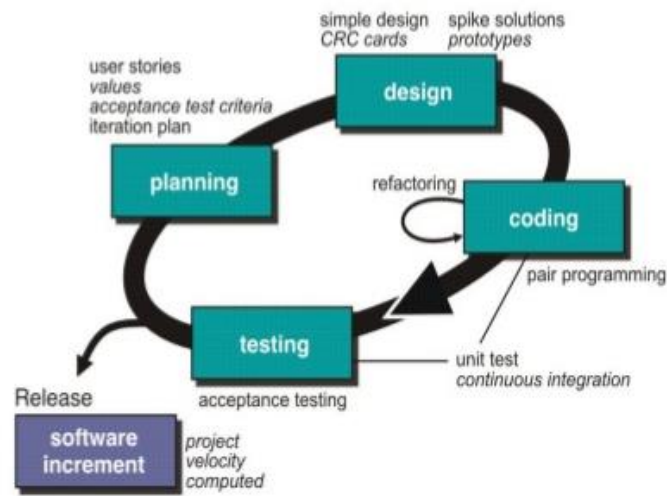
Untuk solusi ini, Kantor Pos Garut perlu menggunakan Aplikasi Pengamanan Pesan Email dalam Gambar berbasis website dengan Algoritma *Advanced Encryption Standard* (AES) dan *Least Significant Bit* (LSB). Kombinasi AES dan LSB telah terbukti efektif dalam meningkatkan keamanan pesan steganografi[3]. AES digunakan untuk mengenkripsi pesan sebelum disisipkan ke dalam gambar, sedangkan LSB memungkinkan pesan disisipkan tanpa merusak tampilan gambar asli. Hal ini memungkinkan pesan terenkripsi dan tersembunyi dengan baik, menjaga keamanan dan privasi pesan saat dikirim dan diterima oleh Manager dan Karyawan Magang di Kantor Pos Garut.

Berdasarkan berbagai penelitian terdahulu, telah diketahui bahwa penerapan aplikasi pengamanan pesan email dalam bentuk gambar menggunakan algoritma AES dan LSB dapat memberikan manfaat besar bagi organisasi. Sebuah penelitian oleh [4] kerahasiaan data rekam medis, termasuk pemeriksaan fisik dan kegiatan tenaga Kesehatan, pengembangan Aplikasi Pengamanan Data Rekam Medis Pasien dan keterbatasan metode *Vigenere Cipher* dalam menghadapi serangan modern. Orisinalitas dapat dilihat dari penerapan metode tersebut dalam konteks rekam medis, penelitian yang dilakukan oleh [5] Penelitian ini menerapkan steganografi dan kriptografi pada pesan SMS dalam gambar menggunakan metode *Least Significant Bit* (LSB) dan algoritma kriptografi *Advanced Encryption Standard* (AES) pada platform Android, pengembangan aplikasi Android untuk meningkatkan keamanan pesan teks SMS, evaluasi kinerja dan kekuatan enkripsi dari metode yang diusulkan, [6] penelitian ini berkaitan dengan steganografi audio menggunakan metode LSB dan meningkatkan keamanan dengan algoritma kriptografi AES, mengenkripsi pesan tersembunyi dalam data audio, pengembangan metode steganografi audio yang dioptimasi dengan AES dan melibatkan analisis seberapa kuat metode ini terhadap serangan terkini. penelitian oleh [7] Penelitian ini berfokus pada pengamanan lampiran dalam komunikasi email berbasis TLS menggunakan algoritma AES dan LSB, panduan praktis untuk mengamankan lampiran dalam komunikasi email dan melibatkan evaluasi terhadap kerentanan email berbasis TLS yang belum diatasi. Penelitian yang terakhir oleh [8] penelitian ini menggabungkan steganografi LSB dan kriptografi AES pada citra berwarna untuk mengamankan teks rahasia, pengembangan metode kombinasi tersebut untuk penyisipan pesan pada citra berwarna, dan melibatkan perbandingan dengan metode serupa dan analisis keunggulan dari pendekatan tersebut.

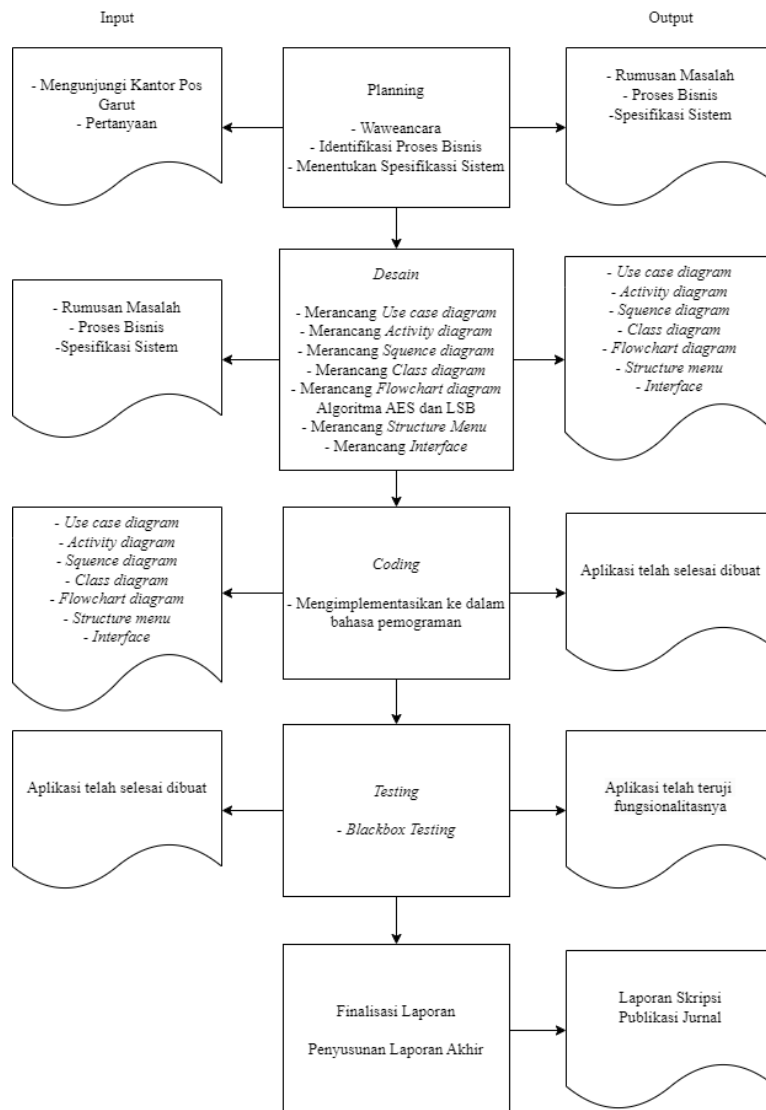
Berdasarkan permasalahan pada latar belakang dapat diambil rumusan masalah yang akan menjadi pembahasan penelitian yaitu, Bagaimana cara untuk Meningkatkan tingkat keamanan dan privasi dalam pengiriman dan penerimaan pesan email di Kantor Pos Garut, terutama dalam pengiriman rincian penggajian karyawan magang, sehingga dapat menjaga kerahasiaan informasi yang dikirimkan dan diterima oleh manager dan karyawan magangnya. Dalam penelitian ini, kami bertujuan untuk merancang dan membangun aplikasi Pengamanan Pesan Email dalam gambar yang menggunakan algoritma AES dan metode LSB berbasis *website* untuk meningkatkan tingkat keamanan dan privasi dalam pengiriman dan penerimaan pesan email di Kantor Pos Garut, terutama dalam pengiriman rincian penggajian karyawan magang, sehingga dapat menjaga kerahasiaan informasi yang dikirimkan dan diterima oleh karyawan.

II. METODOLOGI PENELITIAN

Metode Penelitian *Extreme Programming* (XP) didasarkan pada serangkaian ide sederhana dari masa lalu, yang menyajikan pendekatan inovatif dalam pengembangan aplikasi. Namun, *Kent Beck* menegaskan bahwa XP tidak sesuai untuk semua proyek pengembangan perangkat lunak; namun, keunggulan utamanya terletak pada proyek-proyek dengan persyaratan dinamis atau ketidakjelasan dalam kebutuhan dari klien [9]. Metode XP merupakan metode yang responsif terhadap perubahan[10].



Gambar 1: Tahapan *Extrime Programming* (XP)



Gambar 2: Krangka Penelitian

Berdasarkan dari gambar diatas pada proses pembuatan sistem XP mengadopsi empat tahapan utama dalam pengembangan perangkat lunak, antara lain:

1. Langkah pertama, *Planning*/Perencanaan, memulai dengan memahami pada tahap konteks bisnis aplikasi, dilakukan definisi keluaran dan fitur-fitur yang akan diimplementasikan dalam aplikasi. Selain itu, langkah ini bertujuan untuk menentukan fungsi utama aplikasi, serta merencanakan alur pengembangan aplikasi.
2. Kemudian, tahap *Design*/Perancangan menitikberatkan pada pentingnya desain aplikasi yang sederhana. Metode yang digunakan dalam tahap ini mencakup diagram *usecase*, *class diagram*, *activity diagram*, *Sequence diagram*, dan *flowchart* Algoritma AES dan LSB.
3. Tahap *Coding*/Pengkodean merupakan inti dari pengembangan aplikasi dengan XP, yang mana *pair programming* digunakan secara intensif. Dalam *pair programming*, dua atau lebih *programmer* bekerja bersama-sama dalam pembuatan program.
4. Terakhir *Testing*/Pengujian fokus pada menguji fitur-fitur aplikasi untuk memastikan bahwa tidak ada kesalahan (*error*) dan aplikasi sesuai dengan proses bisnis dari klien (pelanggan).

III. HASIL DAN PEMBAHASAN

A. Hasil Penelitian

Pada bagian ini, dipersembahkan hasil penelitian yang telah dilakukan tentang perancangan aplikasi keamanan email dengan gambar menggunakan algoritma AES dan algoritma LSB menggunakan metode *Extreme Programming* (XP). Demikian hasil diskusi penelitian kegiatan yang tertuang dalam metodologi XP.

1. *Planning*

Tahap ini Penelitian ini dimulai dengan mengkaji berbagai sumber literatur, termasuk referensi dokumen dan jurnal terkait, guna memahami penelitian-penelitian sebelumnya yang relevan. Melalui langkah ini, berhasil diidentifikasi kesenjangan yang akan menjadi fokus penelitian selanjutnya. Selanjutnya, dilakukan wawancara dengan bagian Staff IT di Kantor Pos Garut untuk mendapatkan wawasan tentang konteks bisnis dari aplikasi yang akan dikembangkan. Pada tahap ini, keluaran, karakteristik, dan fungsionalitas dari aplikasi yang diimplementasikan didefinisikan dengan jelas. Pada Langkah perencanaan ini dilakukan pendefinisian proses bisnis dan pendefinisian spesifikasi kebutuhan sistem.

a. Identifikasi proses bisnis

Menganalisa kegiatan Mengidentifikasi proses bisnis dilakukan untuk memahami dengan lebih jelas bagaimana proses bisnis yang sedang berlangsung di Kantor Pos Garut mengenai bagaimana proses bisnis aplikasi yang akan dirancang, sehingga dapat memberikan gambaran untuk aplikasi yang akan dibuat. Berikut merupakan hasil dari wawancara yang dilakukan dalam rangka mengidentifikasi proses bisnis.

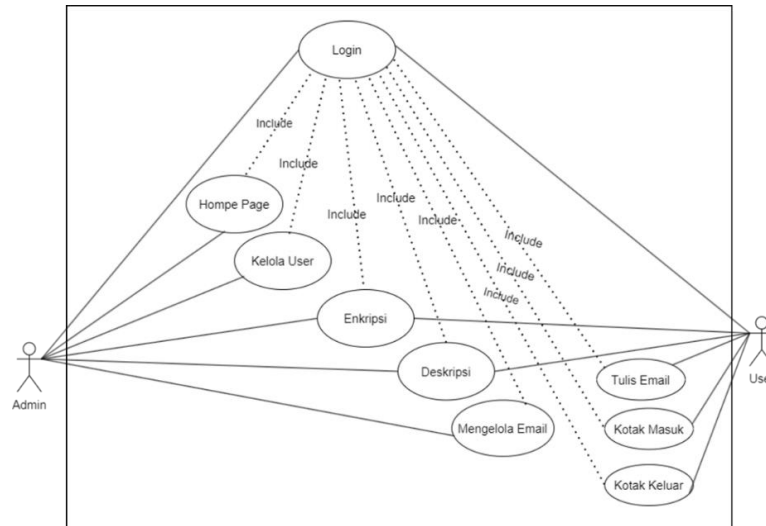
b. Identifikasi spesifikasi sistem

Penyusunan spesifikasi sistem guna memenuhi kebutuhan yang mendukung dalam pembangunan aplikasi dilakukan melalui beberapa tahapan analisis kebutuhan fungsional dan non-fungsional. Tujuan dari analisis ini adalah untuk mengumpulkan informasi yang diperlukan dan mengkonseptualisasikan aplikasi yang akan dilakukan.

2. *Design*

Perancangan ini diawali dengan mengidentifikasi para pelaku (aktor) dan menyusun diagram kasus pengguna (use case diagram) berdasarkan hasil dari wawancara yang telah dilaksanakan. Perancangan bermula dengan melakukan Mengidentifikasi *actor*, *Flowchart* algoritma AES dan LSB, dan perancangan *interface*.

- a. Mengidentifikasi *actor* Mengidentifikasi *actor* dilakukan untuk menentukan target yang akan melakukan aktivitas pada sistem yang sedang dibangun.

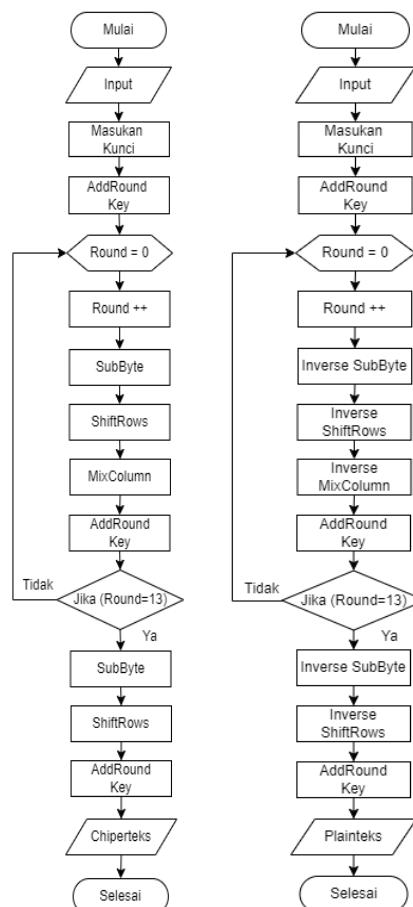


Gambar 4: Usecase diagram Sistem Pengamanan Pesan Email Dalam Gambar menggunakan Algoritma AES dan LSB

b. Flowchart Kriptografi Algoritma AES dan LSB

1) Perancangan sistem algoritma AES

Untuk menyembunyikan pesan dalam gambar dengan menggunakan *cipherteks*, diperlukan perencanaan dalam berbagai tahapan proses. Rincian langkah-langkah tersebut akan diilustrasikan melalui sebuah diagram alir, juga dikenal sebagai *flowchart*. *Flowchart* tersebut akan menjelaskan proses untuk tahapan *enkripsi*, penyisipan, *encrypt*, dan *dekrypt*:



Gambar 5: Flowchart Proses Encrypt dan Decrypt Algoritma AES

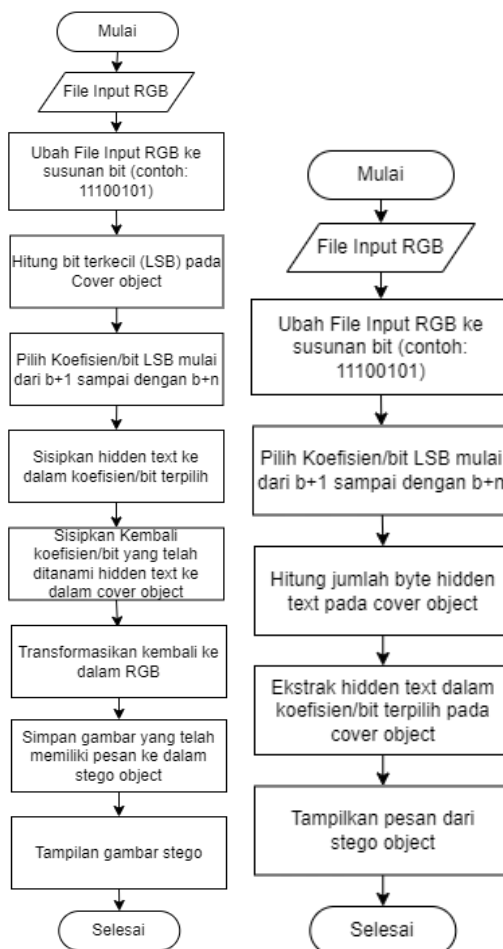
2) Proses *Encrypt* Algoritma AES

Gambar 5 sebelah kiri pada diagram tersebut mengilustrasikan proses enkripsi menggunakan algoritma AES (*Advanced Encryption Standard*). Tahap pertama dalam proses *encoding* adalah memasukkan data yang akan dienkripsi, dalam penelitian ini data yang digunakan berupa gambar. Kemudian, kunci input diproses, menggunakan algoritma AES256 dengan panjang kunci 256 bit. Tahap selanjutnya adalah menjalankan prosedur *AddRoundKey*, yaitu operasi XOR antara teks biasa dan kunci, Proses enkripsi ini melibatkan empat jenis *transformasi byte*, yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* [11]. Pada tahap awal enkripsi, saat (*Round* = 0), data melewati konversi byte *AddRoundKey*. Selain itu, state yang akan mengalami transisi berulang *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* paling banyak pada (*Round* = 13), Jika (*Round* = 14), maka hanya akan dilakukan tiga transisi, yaitu *SubBytes*, *ShiftRows*, dan *AddRoundKey*, dan menghasilkan teks terenkripsi. Dengan demikian, proses enkripsi dapat diselesaikan.

3) Proses *Decrypt* Algoritma AES

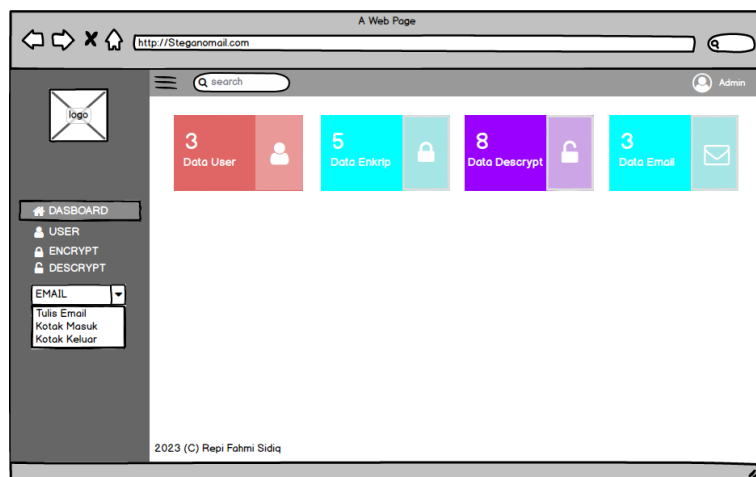
Diagram alur pada gambar 5 sebelah kanan : diatas memaparkan tahapan *enkripsi* dengan menggunakan algoritma kriptografi AES. Pada Langkah awal dalam proses *enkripsi*, data harus melalui empat jenis *transformasi byte*, yaitu *InverseSubByte*, *InverseShiftRows*, *InverseMixcolumn*, dan *AddRoundKey*. Pada tahap awal *dekripsi* atau *Round* =0, *inputistate* akan mengalami *transformasi byte AddRoundKey*. Selanjutnya, *state* akan mengalami *transformasi InverseSubBytes*, *InverseShiftRows*, *InverseMixColumns*, dan *AddRoundKey* berulang sebanyak *Round*=13. Jika *Round* = 14, maka akan dilakukan tiga proses *transformasi InverseSubBytes*, *InverseShiftRows*, dan *AddRoundKey*, menghasilkan *plainteks* atau data asli, proses *dekripsi* akan selesai.

4) Perancangan sistem algoritma LSB



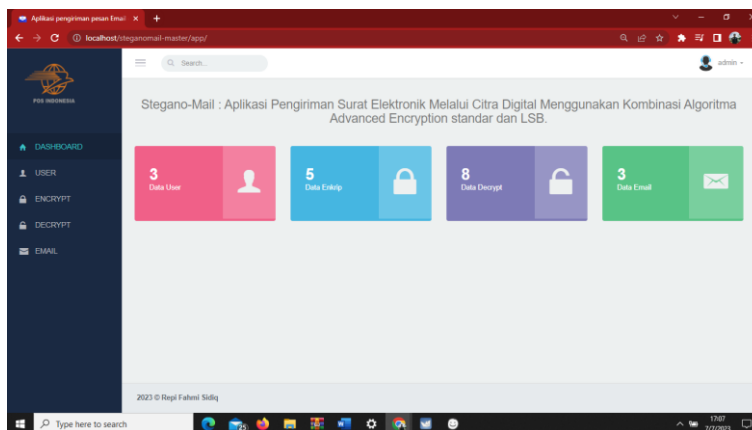
Gambar 6: *Flowchart* Proses *Encrypt* dan *Decrypt* Algoritma LSB

- a) *Proses Encrypt Algoritma LSB*
Gambar 6 sebelah kiri : menggambarkan proses penyisipan pesan kedalam wadah gambar dengan menggunakan metode LSB, Prosesnya dimulai dengan mengimpor berkas RGB (file gambar *bitmap*) sebagai input. Kemudian berkas input RGB diubah menjadi *array bit* (contoh:11100100) dan menghitung *bit* terkecil (LSB) dari *cover image*. Langkah berikutnya Langkah berikutnya yaitu memilih koefisien bit LSB mulai dari (b+1) hingga (b+n) untuk menyelipkan teks tersembunyi (pesan). Setelah itu, teks tersembunyi disisipkan ke dalam koefisien bit yang telah terpilih, dan kemudian gambar sampel dikembalikan ke keadaan semula. Hasilnya, gambar tersebut diubah kembali menjadi gambar yang diperoleh dari nilai RGB terbaru *stego* (pesan disisipkan ke dalam gambar) disimpan[12].
- b) *Proses Decrypt Algoritma LSB*
Gambar 6 sebelah kanan : menggambarkan proses ekstraksi menggunakan Teknik LSB digunakan dalam proses ini. Tahap awal melibatkan penerapan pada berkas RGB, diikuti dengan pemrosesan berkas tersebut, kemudian file RGB diubah menjadi susunan bit (contoh: 11100100)[13], Selanjutnya dilakukan pemilihan *byte* LSB terpilih dari (b+1) hingga (b+n). Setelah itu, dihitung jumlah *byte hidden text* pada gambar *cover*. Proses berikutnya ialah mengekstrak *hidden text byte* terpilih dari gambar objek, sehingga menghasilkan pesan yang telah disisipkan sebelumnya pada gambar *cover*.
- c. *Merancang Interface*
Perancangan Antarmuka merupakan representasi secara keseluruhan dari situs web yang akan dibangun, merancang *interface* berguna untuk efisiensi kerja saat implementasi ke bahasa pemrograman.



Gambar 9: *Interface Dashboard*

3. *Coding*
Analisis dan rancangan desain telah diimplementasikan ke dalam bahasa pemrograman. Sistem pengamanan pesan *email* dalam gambar menggunakan algoritma AES dan LSB berbasis *website* dibangun dengan bahasa pemrograman PHP *Native*.



Gambar 10: Tampilan *Dashboard*



4. *Testing*

Langkah ini menitikberatkan pada pengujian fitur-fitur yang sudah ada dalam aplikasi, dengan tujuan mencegah terjadinya kesalahan (error) dan memastikan bahwa aplikasi yang dikembangkan sesuai dengan proses bisnis klien (pelanggan).

a. Pengujian Proses Kriptografi AES dan Steganografi LSB

Pengujian yang dilakukan meliputi pengujian enkripsi, pengujian *embedding* pesan, pengujian *extracting* pesan dan pengujian dekripsi. Pengujian kualitas *stego-image* yang dihasilkan aplikasi, digunakan PSNR. Gambar penampung (*cover image*) yang digunakan dapat dilihat pada Tabel 1.

Tabel 1: Gambar Penampung yang Digunakan

No	Gambar	Nama Gambar	Dimensi	Size
1		blackandwhite vaping.jpg	3456 x 4320	1100 KB
2		hexohm_black.jpg	1280 x 1280	155 KB

b. Pengujian enkripsi

Pada proses enkripsi dapat dilihat penggunaan RAM dan CPU semakin meningkat secara teratur seiring panjangnya pesan yang diproses, kecuali pada waktu proses yang terlihat tetap stabil. Hasil pengamatan pada proses enkripsi dapat dilihat pada Tabel 2.

Tabel 2: Hasil Pengujian Proses Enkripsi

Gambar	Panjang Pesan	RAM	CPU	Waktu Proses	keterangan
1	19 karakter	0,2 mb	0,1%	18 ms	Berhasil
1	108 karakter	0,8 mb	0,3%	25 ms	Berhasil
2	138 karakter	0,10 mb	0,4%	27 ms	Berhasil
2	65 karakter	0,5 mb	0,2%	21ms	Berhasil

c. Pengujian Penyisipan Pesan

Ciphertext yang dihasilkan dari proses enkripsi diubah menjadi *bit* untuk dimasukkan ke dalam *pixel* gambar dengan menggunakan metode LSB. Hasil pengamatan pada proses penyisipan pesan dapat dilihat pada Tabel 3.

Tabel 3: Hasil Pengujian Proses Penyisipan Pesan Rahasia

Gambar	Panjang Pesan	RAM	CPU	Waktu Proses	Size	keterangan
1	19 karakter	0,8 mb	1,2%	21 ms	8.20 MB	Berhasil
1	108 karakter	0,13 mb	2,7%	28 ms	8.20 MB	Berhasil
2	138 karakter	0,15 mb	3,2%	35 ms	1.39 MB	Berhasil
2	65 karakter	0,10 mb	2,1%	26 ms	1.39 MB	Berhasil

Pengujian yang dilakukan pada proses penyisipan *chiphertext* ke dalam gambar memperlihatkan rata-rata penggunaan RAM, CPU dan waktu proses yang meningkat. Dari pengamatan ini dapat dilihat bahwa panjang *chiphertext* yang disisipkan ke dalam gambar mempengaruhi RAM, CPU dan waktu proses penyisipan pesan rahasia pada gambar.

d. Pengujian Ekstraksi Pesan Rahasia

Dari hasil pengamatan yang ditampilkan pada Tabel 4 dapat dilihat bahwa panjang *chiphertext* yang terdapat pada gambar mempengaruhi waktu proses dalam melakukan ekstraksi. Penggunaan RAM dan CPU menunjukkan pola yang meningkat pada setiap pengujian.

Tabel 4: Hasil Pengujian Ekstraksi Pesan Rahasia

Gambar	Panjang Pesan	RAM	CPU	Waktu Proses	keterangan
1	19 karakter	0,8 mb	1,7%	29 ms	Berhasil
1	108 karakter	0,13 mb	3,1%	37 ms	Berhasil
2	138 karakter	0,15 mb	3,5%	41 ms	Berhasil
2	65 karakter	0,10 mb	2,8%	32 ms	Berhasil

e. Pengujian Dekripsi

Proses dekripsi merupakan proses mengubah *chiphertext* yang telah diekstrak dari gambar menjadi *plaintext*. Hasil pengamatan proses dekripsi dapat dilihat pada Tabel 5.

Tabel 5: Hasil Pengujian Dekripsi

Gambar	Plaintext	Akurasi	keterangan
1	19 karakter	10 ms	Berhasil
1	108 karakter	10 ms	Berhasil
2	138 karakter	10 ms	Berhasil
2	65 karakter	10 ms	Berhasil

Dari hasil pengujian yang dilakukan pada proses dekripsi memiliki tingkat akurasi sebesar 100%, untuk gambar dengan nama *blackandwhite vaping.jpg* dengan dimensi 1.54cm x 2.91cm memiliki ambang batas tampung maksimal 1450 karakter (*plaintext*), sedangkan untuk gambar *hexohm_black.jpg* dengan dimensi 1.5cm x 3.19cm memiliki ambang batas tampung maksimal 1500 karakter (*plaintext*).

f. Pengukuran Kualitas Gambar menggunakan metode MSE dan PSNR

Pengukuran kualitas gambar dilakukan dengan menggunakan rumus PSNR. Gambar asli akan dibandingkan dengan *stego-image*. Gambar yang diukur masih menggunakan gambar yang dipakai tahap pengujian yang telah dijelaskan sebelumnya. Untuk mendapatkan nilai PSNR maka diperlukan untuk melakukan perhitungan *Mean Square Error* (MSE) terlebih dahulu. Rumus yang digunakan

untuk menghitung nilai MSE dapat dilihat pada persamaan [14], dan rumus untuk menghitung nilai PSNR dapat dilihat pada persamaan [15].

$$MSE = \frac{1}{M \times N} \sum_{x=1}^M \sum_{y=1}^N (S_{xy} - C_{xy})^2 \quad \dots\dots(1)$$

Dengan ketentuan:

x, y : Koordinat suatu titik pada gambar

M, N : Dimensi dari gambar

S : Gambar tersisipi (stego-image)

C : Gambar asli (cover image)

$$PSNR = 10 \cdot \log_{10} \left(\frac{C_{\max}^2}{MSE} \right) \quad \dots\dots(2)$$

Berikutnya, pada Tabel 6 ditampilkan hasil perhitungan MSE dan PSNR. Dari hasil ini, dapat diketahui bahwa panjang pesan rahasia berpengaruh terhadap nilai MSE dan PSNR. Pada baris 2 dan 2 untuk nilai MSE dan PSNR yang diperoleh tidak begitu jauh berbeda, hal ini disebabkan panjang karakter pesan untuk gambar baris ke 2 dan 3 tidak jauh berbeda, demikian juga untuk baris ke 1 dan 4 tidak terlalu jauh berbeda panjang karakter pesan yang dimasukkan.

Tabel 6: Hasil Perhitungan MSE dan PSNR

Gambar	Panjang Pesan	MSE	PSNR
1	19 karakter	0.00002678	128.85
1	108 karakter	0.00002688	122.75
2	138 karakter	0.0000268399	94.88
2	65 karakter	0.0024488955	74.23

B. Pembahasan Hasil

Dalam pembahasan hasil implementasi kriptografi untuk mengamankan pesan email dalam gambar menggunakan algoritma AES dan LSB berbasis website memberikan wawasan penting terhadap perlindungan data sensitif melalui pesan email. Temuan ini mengarah pada penggunaan AES yang andal dalam menjaga kerahasiaan pesan, serta penerapan metode LSB untuk menyisipkan pesan secara *visual* dalam gambar. Penelitian ini memperluas pemahaman kita tentang kombinasi kriptografi dan steganografi, yang sebelumnya telah diterapkan pada berbagai jenis data seperti rekam medis, pesan SMS, dan data audio. keunggulan gabungan kriptografi dan steganografi dalam mengamankan komunikasi pesan email dalam gambar ini, khususnya pada jenis data yang berbeda dengan penelitian sebelumnya, meliputi alternatif efektif untuk mengamankan pesan email secara tidak terlihat, meningkatkan keamanan komunikasi digital, dan berpotensi diintegrasikan dengan konsep lain atau pendekatan baru untuk mengatasi tantangan keamanan data yang semakin kompleks di masa depan.

IV. KESIMPULAN

Berdasarkan dari hasil dan pembahasan penelitian yang dilakukan maka dapat disimpulkan Untuk meningkatkan keamanan email melalui enkripsi AES dan penyisipan pesan dalam gambar menggunakan metode LSB di website. Untuk melindungi pesan, mengintegrasikan teknik ini dalam antarmuka website, menguji keamanannya, dan berkontribusi pada keamanan informasi secara keseluruhan. Dengan demikian, penelitian ini berfokus untuk mengamankan komunikasi email dengan menggabungkan kriptografi dan steganografi dalam konteks online.

DAFTAR PUSTAKA

- [1] S Tangade, SS Manvi, "Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs," *Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs*, vol. 69, no. 5, pp. 5232–5243, 2020, doi: 10.1109/TVT.2020.2981127.
- [2] M. S. Rumetna, "Kombinasi Gnu Privacy Guard Dan Hamming Distance Untuk Keamanan Email Serta Jalur Sertifikasi Combination of Gnu Privacy Guard and Hamming Distance for Email Security and Certification Paths," *Elektro Luceat [November]*, vol. 7, no. 2, pp. 151–160, 2021.
- [3] V. Swathi and M. P. Vani, "Privacy-Cheating Discouragement: A New Homomorphic Encryption Scheme for Cloud Data Security," *International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, p. 87, 2020, doi: 10.1109/ICCCNT49239.2020.9225481.
- [4] E. Gunadhi and A. Sudrajat, "Pengamanan Data Rekam Medis Pasien Menggunakan Kriptografi Vigènere Cipher," *Jurnal Algoritma*, vol. 13, no. 2, pp. 295–301, 2017, doi: 10.33364/algoritma/v.13-2.295.
- [5] E. Nirmala, "Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android," *Jurnal Informatika Universitas Pamulang*, vol. 5, no. 1, p. 36, 2020, doi: 10.32493/informatika.v5i1.4646.
- [6] S. Achmady and J. Salat, "Steganografi Audio dengan Metode Least Significant Bit (LSB) dan Keamanan dan Dioptimasi Dengan Advanced Encryption Standard (AES)," *Prosiding Seminar Nasional Universitas Jabal Ghafur*, vol. 1, no. 1, pp. 235–240, 2021.
- [7] L. B. Handoko and C. Umam, "Kombinasi Vigenere-Aes 256 dan Fungsi Hash Dalam Kriptografi Aplikasi Chatting," *Prosiding Sains Nasional dan Teknologi*, vol. 12, no. 1, p. 390, 2022, doi: 10.36499/psnst.v12i1.7068.
- [8] Chaerul Umam, Muslih Muslih, and Daffa Fadillah, "Kombinasi Steganografi LSB dan Kriptografi AES dalam Sekuriti Teks Rahasia Pada Citra Berwarna," *Seminar Nasional Teknologi dan Multidisiplin Ilmu (SEMNASTEKMU)*, vol. 2, no. 1, pp. 109–118, 2022, doi: 10.51903/semnastekmu.v2i1.160.
- [9] I. G. N. Suryantara, *Merancang Aplikasi dengan Metodologi Extreme Programming*. Bandung: Elex Media Komputindo, 2017. doi: 6020421023.
- [10] F. Sulianta, *Strategis Merancang Arsitektur Sistem Informasi Masa Kini. PT. Alex Media Komputindo*. Jakarta: PT Elex Media Komputindo, Jakarta, 2019.
- [11] S. Aisa and N. Aini, "Implementasi Metode Advance Encryption Standard dan Least Significan Bit pada Kriptografi Citra Digital," *CSRID Journal*, vol. 11, no. 2, pp. 105–117, 2019.
- [12] N. Mumbai, "International Research Journal of Engineering and Technology (IRJET) Security in Ad-Hoc Network Using Encrypted Data Transmission and Steganography Prof . Ravindra Ghugare , Ankita Patil , Ajay Jha , Dhiraj Kuslekar Dhiraj Kuslekar , Dept of Computer En," pp. 63–69, 2021.
- [13] G. W. Bhaudhayana and I. M. Widiartha, "Implementasi Algoritma Kriptografi AES 256 dan Metode Steganografi LSB Pada Gambar Bitmap," *Jurnal Ilmu Komputer*, vol. 8, no. 2, pp. 9–25, 2020.
- [14] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 3, pp. 1168–1175, 2019, doi: 10.12928/TELKOMNIKA.V17I3.12230.
- [15] A. S. Ansari, M. S. Mohammadi, and M. T. Parvez, "A multiple-format steganography algorithm for color images," *IEEE Access*, vol. 8, no. April, pp. 83926–83939, 2020, doi: 10.1109/ACCESS.2020.2991130.