Jurnal Quancom
Vol.2, No.2, Desember 2024, pp. 17~22
e-ISSN: 2988-0998
P-ISSN: 2988-1005
DOI:https://doi.org/10.62375/jqc.v2i2.422

Pengujian dan Analisis Teknik Steganografi Menggunakan Metode Playfair, ElGamal, dan LSB untuk Penyembunyian Data pada Gambar Digital dalam Aplikasi Modern

Melvayana Manik [1], Sion Saut Parulian Pardosi [2], Irene Mutiara Situmorang [3]
[123] Sarjana Terapan Teknologi Rekayasa Perangkat Lunak
melvayana789@gmail.com[1]

Article Info

Article history:

Received 4 Desember 2024
Revised 12 Desember 2024
Accepted 20 Desember 2024

Keyword:

Steganografi, Least Significant Bit (LSB), ElGamal, Playfair, Penyembunyian Data.

ABSTRACT

The rapid advancement of information and communication technology has significantly transformed how individuals interact and share information, particularly through digital media such as images. While offering numerous benefits, the ease of digital media manipulation poses serious challenges, including cybercrimes like phishing and cyberbullying, highlighting the need for reliable data protection methods to maintain information confidentiality. This research focuses on steganography, the art of concealing messages in such a way that only the sender and recipient are aware of the hidden information. The study implements the Least Significant Bit (LSB) technique for embedding secret files within digital images and evaluates its effectiveness across various transmission scenarios, including email and instant messaging applications like WhatsApp, Instagram, and Telegram. Additionally, the research incorporates cryptographic algorithms such as Playfair and ElGamal to enhance data security. The findings aim to provide insights into the strengths and weaknesses of these methodologies, ultimately contributing to the development of secure digital communication practices.

This is an open access article under the CC Attribution 4.0 license.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam cara manusia berinteraksi dan berbagi informasi, terutama melalui media digital seperti gambar. Meskipun memberikan banyak manfaat, kemudahan manipulasi media digistal juga memunculkan tantangan serius, termasuk kejahatan dunia maya seperti phishing dan cyberbullying. Kondisi ini menekankan pentingnya metode perlindungan data yang andal untuk menjaga kerahasiaan informasi.[1]

Steganografi adalah seni menyembunyikan pesan teks sedemikian rupa sehingga hanya pengirim dan penerima yang mengetahui keberadaan informasi tersebut.[2] Dalam penerapannya, steganografi membutuhkan dua elemen utama, yaitu media penampung (carrier file) dan pesan rahasia (secret file). Teknik ini semakin penting untuk meningkatkan keamanan dalam proses pengiriman informasi. Umumnya, steganografi diterapkan dengan menggunakan dua media yang berbeda, di mana salah satu media berfungsi sebagai

wadah untuk menyimpan informasi, sementara media lainnya berisi informasi rahasia yang akan disembunyikan.[3]

Kriptografi adalah ilmu dan seni yang digunakan untuk menjaga kerahasiaan pesan dengan cara mengubahnya menjadi bentuk yang tidak dapat dipahami tanpa kunci dekripsi.[4] Salah satu algoritma asimetris dalam kriptografi adalah Algoritma ElGamal, yang menawarkan tingkat keamanan tinggi berdasarkan kesulitan dalam memecahkan masalah logaritma diskrit pada grup perkalian bilangan prima yang besar. Hal ini membuat upaya untuk mendekripsi pesan terenkripsi menjadi sangat sulit tanpa kunci yang sesuai.[5]

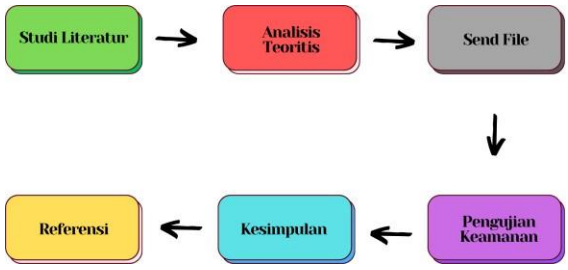
Salah satu keunggulan Algoritma ElGamal adalah kemampuannya menghasilkan ciphertext (pesan terenkripsi) yang berbeda untuk plaintext (pesan asli) yang sama pada setiap proses enkripsi.[6] Namun, saat proses dekripsi dilakukan, hasilnya tetap berupa plaintext yang sama seperti sebelum dienkripsi. Proses Algoritma ElGamal melibatkan tiga tahapan utama, yaitu: Pembentukan Kunci: Membuat pasangan kunci publik dan kunci privat. Proses Enkripsi: Mengubah plaintext menjadi ciphertext menggunakan kunci publik. Proses Deskripsi: Mengembalikan ciphertext menjadi plaintext menggunakan kunci privat.[7]

Algoritma ElGamal termasuk dalam kategori block cipher, di mana proses enkripsi dilakukan pada blok-blok data dari plaintext, yang kemudian menghasilkan blok-blok ciphertext.[8] Blok-blok ciphertext ini nantinya akan didekripsi kembali dan digabungkan untuk menghasilkan plaintext semula.Sementara itu, teknik Least Significant Bit (LSB) adalah salah satu metode paling sederhana dan cepat dalam steganografi.[9] Teknik ini menyisipkan pesan rahasia ke dalam elemen terkecil dari data digital, seperti bit paling tidak signifikan dari gambar, sehingga keberadaan pesan hampir tidak terdeteksi.

Penelitian ini bertujuan untuk mengimplementasikan metode LSB dalam menyembunyikan file pesan di dalam gambar digital, serta menguji efektivitasnya dalam berbagai skenario pengiriman, seperti melalui layanan email, dan aplikasi pesan instan seperti WhatsApp,Instagram dan telegram. Analisis terhadap kelebihan dan kekurangan metode ini diharapkan dapat memberikan wawasan mendalam mengenai penerapannya dalam memastikan komunikasi digital yang aman.[10]

METODE

Pada Gambar 1, ditampilkan metode penelitian yang diterapkan, serta akan menjelaskan langkah-langkah dalam menyelesaikan permasalahan yang dihadapi dalam penelitian ini.



Gambar 1.metode penelitian

Langkah-langkah atau metode yang diterapkan anatara lain:

A. *Studi Literatur*

Dalam penelitian ini, studi literatur dilakukan untuk mengumpulkan dan menganalisis berbagai sumber akademik yang relevan mengenai steganografi, terutama teknik Least Significant Bit (LSB).[11] Penelitian ini bertujuan untuk mengidentifikasi artikel dan jurnal yang membahas prinsip dasar steganografi, penerapan teknik LSB, serta analisis keamanan yang berkaitan.[12] Fokus utama adalah menilai kelebihan dan kelemahan metode LSB dibandingkan dengan teknik steganografi lainnya, serta mengevaluasi hasil pengujian yang telah dilakukan oleh peneliti sebelumnya.[13]

B. *Analisis Teoritis*

Analisis teoritis dilakukan untuk mengevaluasi mekanisme steganografi LSB secara matematis dan teknis. Proses ini mencakup perhitungan kapasitas penyimpanan data dalam sebuah gambar digital berdasarkan ukuran file dan jumlah piksel.[14] Analisis ini juga melibatkan simulasi algoritma LSB untuk memeriksa bagaimana bit paling rendah pada piksel dapat dimodifikasi tanpa menghasilkan distorsi visual yang terlihat.[15] Tahap ini memberikan pemahaman tentang bagaimana metode ini dapat dioptimalkan untuk meningkatkan keamanan dan efisiensi.

C. *Send File*

Tahapan berikutnya adalah proses pengiriman file atau data, yang melibatkan dua metode pengujian. Pada dilakukan dengan mengirim file steganografi image melalui alamat email. Sedangkan pada pengujian kedua, file steganografi image akan dikirim menggunakan aplikasi WhatsApp.

Gambar 2. Media pengujian file stego image

Pengiriman melalui WhatsApp akan dilakukan dengan dua cara: pertama, menggunakan media Photos, dan kedua, melalui Documents. Metode ini akan diuji untuk menentukan apakah data yang telah dienkripsi masih dapat ditemukan atau tidak setelah pengiriman. Hasil dari kedua metode tersebut kemudian akan dianalisis untuk membandingkan efektivitasnya.Yang ketiga file steganografi image akan

dikirim menggunakan aplikasi Instagram, dan yang keempat yaitu file steganografi image akan dikirim menggunakan aplikasi Telegram.

D. Pengujian Keamanan

Tahapan ini adalah inti dari proses, di mana pengujian dilakukan untuk mengevaluasi ketahanan metode LSB dalam berbagai kondisi nyata. Pengujian meliputi keberhasilan penyisipan pesan ke dalam gambar tanpa mempengaruhi kualitas visual, ketahanan terhadap manipulasi seperti kompresi gambar (misalnya, dari PNG ke JPEG), dan serangan steganalysis. Selain itu, integritas data diuji dengan memastikan bahwa informasi tersembunyi dapat diekstrak kembali dengan benar setelah gambar dikirim melalui aplikasi komunikasi seperti layanan email, dan aplikasi pesan instan seperti WhatsApp,Instagram dan Telegram.[4] Uji ketahanan ini memberikan informasi penting tentang keandalan metode LSB dalam skenario dunia nyata.

E. Kesimpulan

Tujuan dari kesimpulan ini adalah untuk menilai tingkat keamanan dan efektivitas metode steganografi LSB dalam menyembunyikan data pada gambar digital, serta merekomendasikan langkah-langkah penguatan, seperti penggunaan format gambar yang tepat dan enkripsi tambahan, agar metode ini dapat diimplementasikan secara aman dalam aplikasi komunikasi modern.[16]

F. Referensi

Semua literatur dan sumber yang digunakan dalam proses penelitian dicatat dalam referensi. Ini mencakup jurnal tentang steganografi, algoritma enkripsi tambahan, dan penelitian terkait deteksi steganografi. Referensi ini tidak hanya memberikan kredibilitas pada hasil penelitian tetapi juga membantu peneliti lain untuk memahami dan mereplikasi metode yang digunakan. [17]

HASIL DAN PEMBAHASAN

Hasil penelitian ini akan dijelaskan secara mendetail dalam proses ini. Setiap langkah yang telah diterapkan dalam penelitian akan dijelaskan secara rinci pada tahap ini.

Setelah proses enkripsi file pesan di dalam *cover image* selesai, pengiriman *stego image* dilakukan melalui dua metode, yaitu menggunakan email dan aplikasi WhatsApp. Pada pengiriman melalui WhatsApp, file dapat dikirim dalam bentuk gambar (*image*) atau dokumen (*document*). Pengiriman sebagai gambar memungkinkan berbagi cepat, namun berisiko mengalami kompresi, sedangkan pengiriman sebagai dokumen menjaga file tetap utuh tanpa perubahan kualitas. [5] Kedua metode ini dipilih berdasarkan kebutuhan akan kecepatan dan keamanan dalam pengiriman data.

A. *Mengirimkan File Stego Melalui Email*

Pengujian pertama dilakukan dengan mengirimkan file *stego image* melalui email. File *stego image* yang berisi data terenkripsi dikirim kepada penerima melalui email.

Gambar 3. Send stego dengan email

Gambar 3 menunjukkan proses pengiriman *stego image* menggunakan email, di mana file hasil enkripsi berhasil dikirimkan kepada penerima.

B. *Mengirimkan File Stego Melalui WhatsApp*

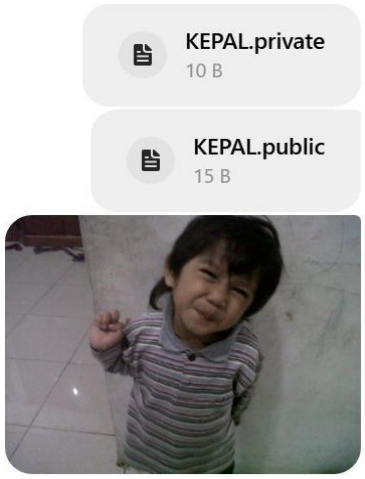
Pengujian kedua dilakukan dengan mengirimkan file *stego image* melalui email. File *stego image* yang berisi data terenkripsi dikirim kepada penerima melalui WhatsApp.

Gambar 4. Send stego dengan whatsapp

File *stego image* dikirim menggunakan dua jenis metode pengiriman. Metode pertama adalah sebagai *Image*, sementara metode kedua adalah sebagai *Dokumen*.

C. *Mengirimkan File Stego Melalui Instagram*

Pengujian ketiga dilakukan dengan mengirimkan file *stego image* melalui Instagram. File *stego image* yang berisi data terenkripsi dikirim kepada penerima melalui Instagram.



Gambar 5. Send stego dengan instagram

Gambar 5 menunjukkan proses pengiriman *stego image* menggunakan Instagram, di mana file hasil enkripsi berhasil dikirimkan kepada penerima.

D. *Mengirimkan File Stego Melalui Telegram*

Pengujian ketiga dilakukan dengan mengirimkan file *stego image* melalui Telegram. File *stego image* yang berisi data terenkripsi dikirim kepada penerima melalui Instagram.

Gambar 6. Send stego dengan telegram

Gambar 6 menunjukkan proses pengiriman *stego image* menggunakan telegram dimana file dalam bentuk zip.

Berikut adalah rincian pengujian keamanan, termasuk proses enkripsi dan dekripsi, pada teknik steganografi yang menggunakan metode Playfair, ElGamal, dan LSB untuk penyembunyian data pada gambar digital:

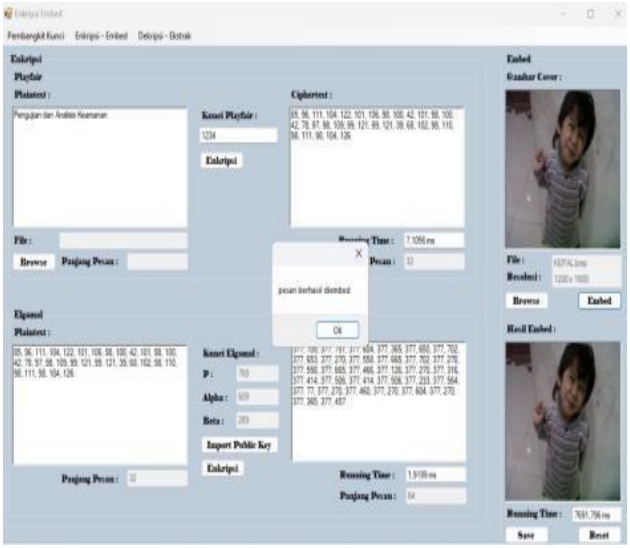
A. Implementasi LSB (Enkription File)

Pada penelitian ini, akan dilakukan implementasi metode Least Significant Bit (LSB) untuk enkripsi atau penyembunyian sebuah file ke dalam gambar. Berdasarkan gambar yang diunggah, berikut adalah penjelasan rinci mengenai proses enkripsi pada citra menggunakan metode Playfair, ElGamal, dan LSB (Least Significant Bit):

Playfair Cipher: Playfair Cipher digunakan dalam proses enkripsi awal untuk mengamankan teks atau plaintext.[7] Metode ini bekerja dengan cara membentuk matriks 5x5 yang didasarkan pada kunci yang diberikan, misalnya "1234". Teks yang akan dienkripsi dibagi menjadi pasangan huruf atau digraf, dan kemudian setiap pasangan tersebut dienkripsi menggunakan aturan matriks tersebut.[8] Hasil dari proses ini adalah ciphertext yang berupa urutan angka ASCII, yang tidak dapat dibaca langsung. Dengan demikian, Playfair memberikan lapisan perlindungan pertama pada teks rahasia, sehingga lebih sulit untuk dipahami oleh pihak yang tidak memiliki kunci enkripsi.[9]

ElGamal: Setelah melalui enkripsi dengan Playfair, langkah selanjutnya adalah menggunakan algoritma ElGamal untuk meningkatkan keamanan data. ElGamal adalah sistem enkripsi asimetris yang melibatkan kunci publik dan kunci privat.[10] Dalam proses ini, ciphertext yang dihasilkan oleh Playfair di enkripsi lebih lanjut menggunakan parameter kunci publik seperti P (bilangan prima), alpha (generator), dan beta (hasil perhitungan terkait kunci privat). Dengan cara ini, ciphertext yang sudah terenkripsi oleh Playfair menjadi lebih aman, karena hanya bisa didekripsi oleh pemegang kunci privat yang tepat. Algoritma ini mempunyai kerugian pada cipherteksnya yang mempunyai panjang dua kali lipat dari plainteksnya.Akan tetapi, algoritma ini mempunyai kelebihan pada enkripsi. [11] ElGamal memberikan tingkat keamanan yang lebih tinggi dengan menggunakan proses matematika yang kompleks, sehingga pesan tetap aman meskipun pihak lain bisa mengakses data yang telah dienkripsi.

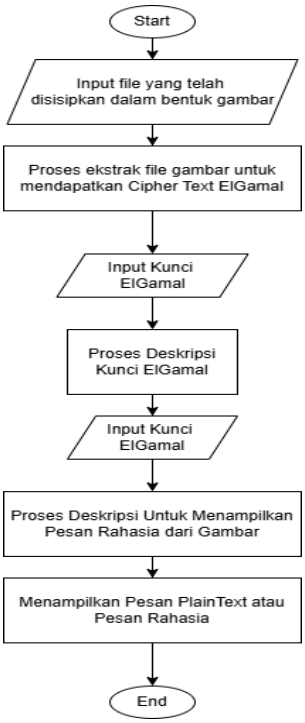
LSB (Least Significant Bit): Setelah ciphertext ElGamal dihasilkan,langkah terakhir adalah penyisipan data ke dalam gambar menggunakan metode LSB (Least Significant Bit). Least Significant Bit (LSB) merupakan teknik penyisipan pesan yang paling sederhana dan cepat dalam penggunaan metodesteganografi.[12] Dalam proses ini, bit terakhir dari setiap piksel gambar cover(misalnya gambar "KEPAL.bmp") diubah untuk menyisipkan bit data ciphertext tanpamengubah tampilan visual gambar secara signifikan. Metode LSB memungkinkan data rahasia disembunyikan dalam gambar dengan cara yang hampir tidak terlihat, sehingga gambar yang dihasilkan, yang disebut stego image, tetap tampak seperti gambar biasa meskipun mengandunginformasi terenkripsi di dalamnya. Proses ini membuat penggunaan gambar sebagai media penyimpanan data menjadi sangat efektif dalam menjaga kerahasiaan pesan.



Gambar 7. Enkripsi file stego image

Implementasi LSB (Description File), Metode LSB (Least Significant Bit) berfungsi untuk menyisipkan dan mengekstraksi data rahasia dari gambar dengan memanipulasi bit- bit terkecil tanpa merusak kualitas gambar.[13]ElGamal digunakan untuk mengenkripsi pesan rahasia sebelum disisipkan ke gambar, sehingga memastikan keamanan data selama penyimpanan. [14]Setelah data diekstraksi, PlayFair digunakan untuk mendekripsi pesan tahap akhir, mengungkapkan plaintext. Kombinasi ketiga metode ini memastikan kerahasiaan, keamanan, dan keberhasilan dalam pengolahan pesan rahasia pada file gambar.[15]

Berikut merupakan diagram alur DescriptionFile:

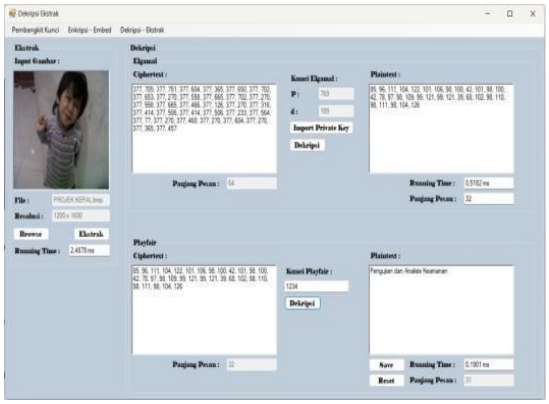


Gambar 8. Diagram alur description

Menyisipkan dan mengekstraksi pesan dari gambar. File gambar dimasukkan, dan sistem mengekstraksi ciphertext tersembunyi menggunakan teknik LSB. Pengguna kemudian memasukkan kunci ElGamal untuk mendekripsi ciphertext tersebut, menghasilkan data terenkripsi kedua. Selanjutnya, kunci PlayFair digunakan untuk mendekripsi data ini menjadi plaintext. LSB digunakan untuk penyembunyian pesan, sementara ElGamal dan PlayFair menjaga keamanan dan integritas dekripsi pesan.

A. *Mengirimkan File Image Melalui Email*

Pada pengujian Pertama dilakukan proses deskripsi *file stego image* yang diterima melalui email.



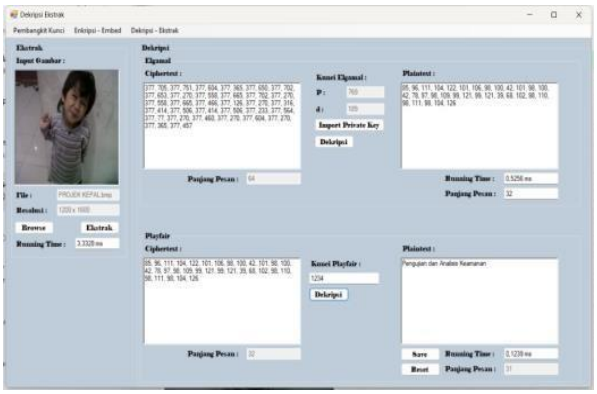
Gambar 9. Deskripsi File Stego Image dari Email

Dari hasil pengujian yang dilakukan seperti pada Gambar 9, *file stego image* yang dikirimkan melalui Email

didapatkan isi pesan yang sesuai setelah di enkripsi dalam file gambar.

B. *Mengirimkan File Image Melalui Email*

Pada pengujian kedua dilakukan prosesdekripsi *file stego image* yang diterima melalui WhatsApp.

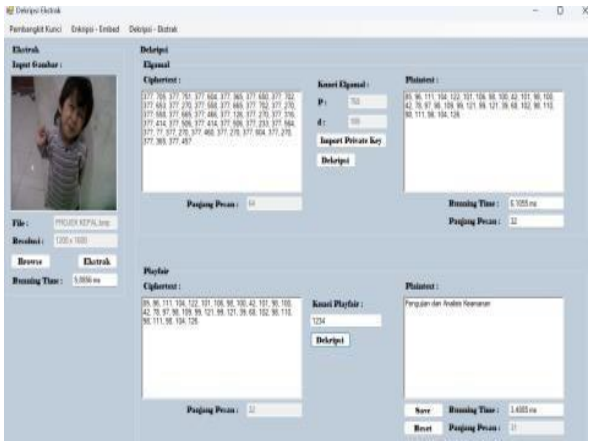


Gambar 10. Deskripsi file stego image dari whatsapp

Dari hasil pengujian yang dilakukan seperti pada Gambar 10, *file stego image* yang dikirimkan melalui WhatsApp didapatkan isi pesan yang sesuai setelah di enkripsi dalam file gambar.

C. *Mengirimkan File Image Melalui Instagram*

Pada pengujian ketiga dilakukan proses dekripsi *file stego image* yang diterima melalui Telegram.

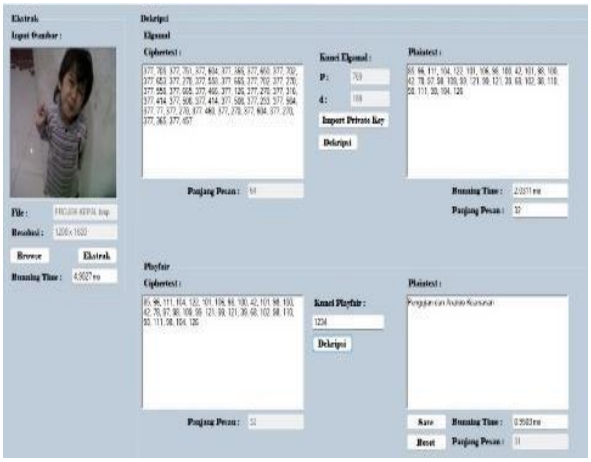


Gambar 11. Deskripsi file stego dari instagram

Dari hasil pengujian yang dilakukan seperti pada Gambar 11, *file stego image* yang dikirimkan melalui Instagram didapatkan isi pesan yang sesuai setelah di enkripsi dalam file gambar.

D. *Mengirimkan File Image Melalui Telegram*

Pada pengujian keempat dilakukan proses dekripsi *file stego image* yang diterima melalui telegram.



Gambar 12. Deskripsi file stego image dari telegram

Dari hasil pengujian yang dilakukan seperti pada Gambar 12, *file stego image* yang dikirimkan melalui telegram didapatkan isi pesan yang sesuai setelah di enkripsi dalam file gambar.

SIMPULAN

Berdasarkan hasil penelitian ini menegaskan bahwa penelitian ini telah berhasil mencapai tujuannya, yaitu memvalidasi keamanan dan keandalan dengan Teknik Steganografi Menggunakan Metode Playfair, ElGamal, dan LSB untuk Penyembunyian Data pada Gambar Digital.

TABEL I
HASIL PENGUJIAN

Media Pengujian	Hasil yang diharapkan	Hasil Pengujian	Kesimpulan
WhatsApp	Pengujian dan Analisi Keamanan	Pengujian dan Analisi Keamanan	Valid
Email	Pengujian dan Analisi Keamanan	Pengujian dan Analisi Keamanan	Valid
Telegram	Pengujian dan Analisi Keamanan	Pengujian dan Analisi Keamanan	Valid
Instagram	Pengujian dan Analisi Keamanan	Pengujian dan Analisi Keamanan	Valid

DAFTAR PUSTAKA

[1] A. Gustiawan, J. Wahyudi, and E. Suryana, "Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Metode Pixel Value Differencing," *JUKI J. Komput. dan Infromatika*, vol. 5, pp. 151–163, 2023.

[2] F. Yanti and K. Budayawan, "Implementasi Steganografi Menggunakan Metode Least Significant Bit (LSB) dalam Pengamanan Informasi pada Citra Digital," *Voteteknika*

(Vocational Tek. Elektron. dan Inform., vol. 11, no. 1, p. 63, 2023, doi: 10.24036/voteteknika.v11i1.121968.
[3] Taufan Maynard Prananda Sancaka1 and Veronica Lusiana, "Penerapan Metode Playfair Cipher Dalam Aplikasi Enkripsi-Dekripsi File Teks," *Elkom J. Elektron. dan Komput.*, vol. 15, no. 2, pp. 260–270, 2022, doi: 10.51903/elkom.v15i2.937.
[4] E. W. Purwanto and S. S. S. T, "Algoritma Kriptografi El-Gamal Untuk Pengamanan Pesan Pada Steganografi Citra Domain Discrete Cosine Transform Dengan Teknik Penyisipan Least Significant Bit," *e-Proceeding Eng.*, vol. 5, no. 1, pp. 116–123, 2018.
[5] M. M. Syarif, "Rancang Bangun Aplikasi Steganografi Menggunakan Metode Least Significant Bit untuk Penyembunyian Pesan Teks ke dalam Gambar Digital," 2019.
[6] Danang Tri Massandy, "Algoritma elgamal dalam pengamanan pesan rahasia," *Inst. Teknol. Bandung*, pp. 1–5, 2009, [Online]. Available: www.informatika.stei.itb.ac.id
[7] E. Saragih, D. Siregar, and H. Dafitri, "Implementasi Penyisipan Pesan Teks Terenkripsi Menggunakan Kriptografi ElGamal pada Citra Digital Menggunakan Steganogarafi LSB," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 22, no. 2, p. 464, 2023, doi: 10.53513/jis.v22i2.8755.
[8] Z. Niswati, "Steganografi Berbasis Least Significant Bit (Lsb) Untuk Menyisipkan Gambar Ke Dalam Citra Gambar," *Fakt. Exacta*, vol. 5, no. 2, pp. 181–191, 1979, [Online]. Available: https://journal.lppmunindra.ac.id/index.php/Faktor_Exacta/article/download/194/185
[9] T. E. Putri, M. R. Al Fauzan, and P. A. Sejati, "Perbaikan Algoritma Steganografi Teknik Least Significant Bits Untuk Aplikasi Keamanan Data," *J. Online Phys.*, vol. 3, no. 1, pp. 27–32, 2018, doi: 10.22437/jop.v3i1.5343.
[10] N. F. Hasan, C. N. Dengen, and D. Ariyus, "Analisis Histogram Steganografi Least Significant Bit Pada Citra Grayscale," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 1, pp. 20–29, 2020, doi: 10.31849/digitalzone.v11i1.3413.
[11] I. Putra Sinaga, "Implementasi Kriptografi Hybrid Algoritma Elgamal Dan Double Playfair Cipher Dalam Pengamanan File Jpeg Berbasis Dekstop," *J. Informatics, Electr. Electron. Eng.*, vol. 1, no. 2, pp. 67–74, 2021, [Online]. Available: https://djournals.com/jieeeJIEEE,
[12] M. N. Al Jumah and S. Sarimuddin, "Jurnal Informatika dan Rekayasa Perangkat Lunak Implementasi Steganografi Metode Least Significant Bit (LSB) untuk Menyembunyikan File Pesan dalam Gambar," vol. 6, no. 1, pp. 102–108, 2024.
[13] P. H. Rantelinggi and E. Saputra, "Algoritma Kriptografi Triple Des dan Steganografi LSB sebagai Metode Gabungan dalam Keamanan Data," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 4, p. 661, 2020, doi: 10.25126/jtiik.2020741838.
[14] Z. Rifai and S. Huda, "Aplikasi Pengamanan Data Email," *Techno.Com*, vol. Vol. 12, no. No. 2, pp. 73–81, 2013.
[15] Sudarta, "**済無**No Title No Title No Title," vol. 16, no. 1, pp. 1–23, 2022.
[16] A. Hafiz, "Steganografi Berbasis Citra Digital Untuk Menyembunyikan DataMenggunakan Metode Least Significant Bit (Lsb)," *J. Cendikia Vol. XVII Cendikia 2019 Bandar Lampung, April 2019* , vol. 17, pp. 194–198, 2019.
[17] R. Santi, "Implementasi Algoritma Enkripsi Playfair pada File Teks," *None*, vol. 15, no. 1, p. 246766, 2010.