Blantika: Multidisciplinary Jornal
Volume 3 Number 7, Januari, 2025
p- ISSN 2987-758X e-ISSN 2985-4199

Penerapan Steganografi LSB dan Enkripsi AES untuk Keamanan Data Rahasia pada Gambar Digital

Faustina Maria C. Baria Set, Citra Maria N. Bana, Maria Angliadi Anunut, Demetriana Da Costa, Yulita Niis
Universitas Timor, Indonesia
Email author: bariasettiara@gmail.com, citrabana8@gmail.com, anunutanglyadi@gmail.com, tridemetri@gmail.com, junnyyuni@gmail.com

ABSTRAK

Di era digital, kebutuhan akan sistem perlindungan data semakin mendesak seiring meningkatnya ancaman terhadap privasi, seperti penyadapan dan pencurian informasi. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem perlindungan data yang menggabungkan metode steganografi berbasis Least Significant Bit (LSB) dan enkripsi menggunakan algoritma Advanced Encryption Standard (AES-256) untuk menjaga keamanan data rahasia dalam citra digital. Penelitian ini menggunakan pendekatan eksperimen kuantitatif terapan dengan desain laboratorium, melibatkan proses enkripsi teks menggunakan AES-256 dan penyisipan hasil enkripsi ke dalam citra berformat PNG melalui teknik LSB. Evaluasi dilakukan dengan mengukur kualitas citra menggunakan PSNR dan MSE, serta menilai keberhasilan ekstraksi, dekripsi, dan efisiensi waktu proses. Hasil penelitian menunjukkan bahwa sistem berhasil menjaga kualitas visual citra dengan nilai PSNR di atas 58 dB, yang mengindikasikan tidak adanya perubahan visual signifikan. Proses ekstraksi dan dekripsi mencapai tingkat keberhasilan 100%, sementara waktu eksekusi untuk masing-masing proses kurang dari 0,02 detik, menunjukkan efisiensi tinggi. Kombinasi steganografi dan enkripsi terbukti mampu memberikan perlindungan berlapis yang efektif terhadap data rahasia. Kesimpulannya, sistem ini layak diterapkan sebagai solusi keamanan data digital berbasis citra, dengan potensi untuk dikembangkan lebih lanjut melalui metode steganografi adaptif dan integrasi algoritma enkripsi lainnya..

Kata Kunci: Steganografi, Enkripsi AES, Keamanan Data, Citra Digital, Least Significant Bit, Perlindungan Informasi

ABSTRACT

In the digital era, the need for data protection systems has become increasingly urgent due to growing threats to privacy, such as eavesdropping and information theft. This study aims to design and implement a data protection system that combines Least Significant Bit (LSB)-based steganography with Advanced Encryption Standard (AES-256) encryption to secure confidential data within digital images. This research employs an applied quantitative experimental approach with a laboratory design, involving the encryption of text data using AES-256, followed by embedding the encrypted data into PNG-format images using the LSB technique. Evaluation is conducted by measuring image quality using PSNR and MSE, as well as assessing the success of data extraction, decryption, and process efficiency. The results show that the system successfully maintains the visual quality of the image, with PSNR values exceeding 58 dB, indicating no significant visual alterations. Data extraction and decryption achieved a 100% success rate, while the execution time for each process was less than 0.02 seconds, demonstrating high efficiency. The combination of steganography and encryption proves to provide an effective layered protection mechanism for confidential data. In conclusion, this system is feasible for implementation as a digital image-based data security solution, with potential for further development through adaptive steganography methods and the integration of additional encryption algorithms.

Keywords: *Steganography, AES Encryption, Data Security, Digital Image, Least Significant Bit, Information Protection*

Manuscript accepted: 27-05-2025 Revised: 15-06-2025 Date of publication: 30-06-2025

PENDAHULUAN

Di era digital saat ini, keamanan data menjadi salah satu aspek yang sangat krusial. Informasi pribadi, data keuangan, hingga dokumen sensitif banyak dipertukarkan melalui berbagai media digital seperti media sosial, email, dan platform daring lainnya. Akan tetapi, pertukaran data digital ini menghadirkan tantangan serius terkait potensi pencurian, penyadapan, dan penyalahgunaan informasi oleh pihak-pihak yang tidak bertanggung jawab (Bainus & Rachman, 2023). Oleh karena itu, diperlukan upaya yang lebih canggih untuk melindungi data agar tetap rahasia dan hanya dapat diakses oleh pihak yang berwenang.

Dua pendekatan populer dalam mengamankan data adalah steganografi dan enkripsi. Steganografi merupakan teknik penyembunyian informasi ke dalam media lain, seperti gambar digital, tanpa menarik perhatian pihak luar. Salah satu metode yang sering digunakan dalam steganografi adalah Least Significant Bit (LSB), yang menyisipkan data pada bit-bit paling rendah dari setiap piksel gambar. Teknik ini mampu menjaga tampilan visual gambar sehingga perubahan tidak mudah terdeteksi secara kasat mata (Arya & Soni, 2018).

Namun demikian, meskipun steganografi efektif dalam menyembunyikan data, metode ini tetap rentan terhadap teknik deteksi dan analisis steganalisis (Kautsar & Ikhsan, 2025; Pratama & Fachri, 2025). Untuk meningkatkan keamanannya, steganografi perlu dikombinasikan dengan metode enkripsi. Salah satu algoritma enkripsi yang terbukti aman dan banyak diadopsi adalah Advanced Encryption Standard (AES). AES merupakan algoritma kriptografi simetris yang mampu mengenkripsi data dengan kecepatan tinggi dan tingkat keamanan yang tinggi, sehingga sangat cocok digunakan untuk melindungi data sensitif (Sari et al., 2022).

Dalam penelitian ini, dikembangkan sebuah sistem yang menggabungkan teknik steganografi berbasis LSB dan enkripsi menggunakan algoritma AES. Sistem ini bekerja dalam dua tahap: pertama, data rahasia dienkripsi menggunakan AES untuk memastikan tingkat kerahasiaan yang tinggi; kedua, data hasil enkripsi disisipkan ke dalam citra digital menggunakan metode LSB. Dengan pendekatan ini, data tidak hanya tersembunyi tetapi juga dienkripsi, sehingga menawarkan lapisan keamanan ganda terhadap upaya peretasan maupun pencurian data (Ahuja et al., 2016).

Urgensi penelitian ini terletak pada meningkatnya intensitas serangan siber dan kebutuhan akan sistem perlindungan data yang tidak hanya mengandalkan satu lapis keamanan, tetapi mengintegrasikan pendekatan ganda yang mampu menangkal eksploitasi data oleh pihak tidak sah. Dalam banyak kasus kebocoran data, metode enkripsi saja tidak cukup karena keberadaan data terenkripsi itu sendiri dapat memicu upaya dekripsi dari pihak luar. Oleh karena itu, diperlukan sistem yang mampu menyembunyikan keberadaan data sekaligus menjaga isinya tetap terenkripsi.

Kebaruan dari penelitian ini terletak pada penggabungan algoritma AES yang kuat dalam hal kriptografi dengan metode LSB yang dikenal ringan dan efisien dalam steganografi digital. Meski masing-masing metode telah banyak diteliti, kombinasi kedua pendekatan ini dalam satu sistem yang terintegrasi untuk konteks pengamanan data gambar digital masih jarang dieksplorasi secara sistematis, terutama dengan fokus pada keseimbangan antara kualitas gambar (imperceptibility) dan ketahanan terhadap serangan (robustness). Penelitian ini juga berkontribusi dalam pengujian kualitas sistem secara menyeluruh, baik dari sisi visual maupun teknis, yang belum banyak dilakukan pada studi sebelumnya.

Tujuan dari penelitian ini adalah untuk merancang dan mengimplementasikan sistem perlindungan data yang memadukan metode steganografi dan enkripsi AES, serta mengevaluasi efektivitas sistem tersebut dalam menjaga kualitas gambar dan ketahanan data yang tersembunyi. Kontribusi dari penelitian ini adalah menunjukkan penerapan gabungan metode steganografi dan enkripsi untuk meningkatkan keamanan data dalam citra digital.

Dengan demikian, sistem ini diharapkan dapat memberikan kontribusi terhadap pengembangan solusi keamanan data yang lebih komprehensif di era digital.

METODE PENELITIAN

Penelitian ini termasuk dalam jenis penelitian eksperimen kuantitatif terapan (applied quantitative experimental research). Penelitian eksperimen digunakan karena peneliti melakukan serangkaian prosedur implementasi sistem secara langsung terhadap objek digital (gambar), serta mengamati dan mengevaluasi hasilnya berdasarkan parameter kuantitatif seperti kualitas citra (PSNR, MSE), tingkat keamanan, dan efisiensi waktu proses. Penelitian ini juga bersifat rekayasa perangkat lunak (software engineering research) karena menghasilkan rancangan dan implementasi sistem keamanan data digital berbasis kombinasi algoritma steganografi dan enkripsi.

Desain penelitian yang digunakan adalah eksperimen laboratorium dengan pendekatan sistematis melalui beberapa tahapan implementasi dan pengujian system. Penelitian ini bertujuan untuk menerapkan kombinasi antara teknik steganografi berbasis Least Significant Bit (LSB) dan enkripsi menggunakan algoritma Advanced Encryption Standard (AES) untuk melindungi data rahasia dalam citra digital.

Pengumpulan Data

Data yang digunakan dalam penelitian ini berupa gambar digital yang akan digunakan sebagai media pembawa (cover image) untuk menyembunyikan data rahasia. Gambar ini dipilih dengan kualitas yang baik, seperti format .PNG atau .JPEG, yang memiliki resolusi cukup untuk menampung data rahasia. Data rahasia yang akan disembunyikan adalah teks yang akan dienkripsi.

Untuk memperoleh data gambar, sumber gambar bisa berupa citra dari internet yang memiliki lisensi bebas atau citra yang dihasilkan oleh perangkat lunak pemrograman (Sabrina, 2021; Siregar & Sundari, 2016). Citra ini akan digunakan sebagai tempat untuk menyembunyikan data teks yang telah dienkripsi.

Preprocesing Citra

Pada tahap preprocessing, gambar yang digunakan akan dipersiapkan untuk mempermudah proses penyembunyian data rahasia (Mulyati et al., 2014). Beberapa langkah preprocessing yang dilakukan adalah sebagai berikut:

1. Mengubah Gambar ke Format RGB: Gambar yang digunakan akan dikonversi terlebih dahulu ke format RGB (Red, Green, Blue), jika gambar tersebut dalam format lain. Format RGB memudahkan pemanipulasian tiap piksel gambar, yang penting dalam proses steganografi.
2. Pengubahan Ukuran Gambar: Jika ukuran gambar terlalu besar, maka gambar tersebut bisa dikurangi agar lebih efisien dalam proses penyembunyian dan pengolahan data.

Implementasi Steganografi

Pada tahap ini, data rahasia (teks) akan disembunyikan dalam gambar menggunakan teknik Least Significant Bit (LSB), yang merupakan salah satu teknik steganografi paling sederhana dan efektif (Darwis, 2017).

Proses Steganografi:

1. Konversi Teks ke Biner: Data rahasia yang berupa teks akan diubah terlebih dahulu menjadi representasi biner. Setiap karakter pada teks akan dikodekan menjadi bilangan biner yang sesuai dengan kode ASCII karakter tersebut.
   Teks→Kode ASCII→Biner
   Sebagai contoh, karakter 'A' dalam ASCII adalah 65, yang dalam biner menjadi 01000001.
2. Penyembunyian Data dalam Piksel Gambar: Setelah data rahasia diubah menjadi biner, data ini akan disembunyikan ke dalam gambar dengan cara mengganti Least Significant

Bit (LSB) pada setiap piksel gambar dengan satu bit dari data rahasia. Metode LSB sangat efisien karena perubahan pada bit paling sedikit (terakhir) tidak terlalu memengaruhi kualitas visual gambar.

Proses ini bisa dijelaskan dengan rumus berikut:

$$I(x,y) = I(x,y)\&{\sim}1 + data[k]$$

Di mana:

1. $I(x,y)$ adalah nilai warna piksel pada posisi (x,y).
2. $\&{\sim}1$ digunakan untuk menghapus bit LSB.
3. $data[k]$ adalah bit dari data rahasia yang akan disembunyikan.
3. Hasil: Gambar yang dihasilkan ini hampir tidak berbeda dari gambar aslinya, tetapi kini sudah menyimpan data rahasia yang hanya dapat diakses jika mengetahui metode yang digunakan untuk menyembunyikannya.

Implementasi Enkripsi AES

Setelah data disembunyikan dalam citra menggunakan steganografi, data tersebut akan dienkripsi menggunakan algoritma AES (Advanced Encryption Standard) untuk meningkatkan tingkat perlindungannya. AES adalah algoritma enkripsi simetris yang sangat aman dan banyak digunakan untuk melindungi data sensitif.

Proses Enkripsi AES:

1. Pembuatan Kunci Enkripsi: Sebelum data dienkripsi, sebuah kunci enkripsi harus dibuat. Kunci AES memiliki panjang 128-bit, 192-bit, atau 256-bit. Kunci ini akan digunakan untuk mengenkripsi dan mendekripsi data rahasia.
2. Proses Enkripsi: Data yang disembunyikan dalam gambar akan dienkripsi dengan menggunakan algoritma AES. Proses enkripsi AES dilakukan melalui serangkaian rounds yang melibatkan transformasi bit dan penggantian byte.

Proses enkripsi AES dapat dijelaskan dengan langkah-langkah berikut:

1. Initial Round: Lakukan AddRoundKey dengan kunci awal.
2. Rounds Utama: Lakukan SubBytes, ShiftRows, MixColumns, dan AddRoundKey untuk setiap round (untuk AES-128, ada 10 rounds).
3. Final Round: Lakukan SubBytes, ShiftRows, dan AddRoundKey.
4. Output: Setelah data terenkripsi, data yang sudah tersembunyi dalam gambar akan lebih aman dan hanya dapat dibaca dengan kunci enkripsi yang benar. Citra yang ter-enkripsi akan tampak berbeda, dan hanya dapat dibuka dengan proses dekripsi yang sesuai.

Pengujian dan Evaluasi

Setelah proses steganografi dan enkripsi selesai, sistem akan diuji untuk mengevaluasi beberapa aspek penting:

1. Kualitas Gambar: Pastikan bahwa kualitas gambar tetap terjaga meskipun data telah disembunyikan. Pengujian dilakukan dengan mengukur PSNR (Peak Signal-to-Noise Ratio) dan MSE (Mean Squared Error) antara gambar asli dan gambar yang sudah diproses.

$$PSNR = 10log_{10}\left(\frac{MAXC^2}{MSE}\right)$$

Dimana:

- MAX adalah nilai maksimum yang mungkin dari piksel.
- MSE adalah kesalahan kuadrat rata-rata antara gambar asli dan gambar yang diproses.

2. Keamanan Data: Evaluasi dilakakukan dengan mengukur seberapa kuat enkripsi AES dalam melindungi data rahasia dari potensi serangan.

3. Kecepatan Enkripsi dan Dekripsi: Waktu yang diperlukan untuk mengenkripsi dan mendekripsi data akan diukur untuk menilai efisiensi sistem

Tingkat Keberhasilan: Pengujian dilakukan dengan memastikan bahwa data yang disembunyikan dapat dipulihkan kembali melalui proses dekripsi dan ekstraksi steganografi.

HASIL DAN PEMBAHASAN

Hasil Implementasi

Dalam penelitian ini, proses implementasi melibatkan dua tahap utama:

1. **Tahap pertama**: Melakukan enkripsi data menggunakan algoritma **AES-256**.
2. **Tahap kedua**: Menyisipkan hasil enkripsi ke dalam citra digital menggunakan metode **Steganografi LSB (Least Significant Bit)**.

Uji coba dilakukan menggunakan beberapa citra berformat **PNG** beresolusi **512×512 piksel**. Data yang digunakan berupa teks sensitif sepanjang 128 karakter, yang kemudian dienkripsi sebelum proses penyisipan.

Berikut untuk langkah-langkah Implementasi:

Tabel 1. Langkah-langkah implementasi

No	Proses	Penjelasan
1	Enkripsi Data	Data teks dienkripsi menggunakan AES-256 dengan mode CBC (Cipher Block Chaining).
2	Penyisipan Data	Ciphertext hasil enkripsi disisipkan ke dalam citra menggunakan LSB pada channel warna RGB.
3	Ekstraksi Data	Data dienkripsi diambil kembali dari citra stego menggunakan teknik LSB reverse.
4	Dekripsi Data	Data hasil ekstraksi didekripsi kembali ke bentuk teks aslinya menggunakan kunci AES.

Evaluasi Kualitas Citra

Untuk mengevaluasi dampak penyisipan data terhadap kualitas gambar, digunakan dua metrik:

a. PSNR (Peak Signal-to-Noise Ratio)

PSNR digunakan untuk mengukur perbedaan antara citra asli dan citra stego (Handoyo et al., 2018; Zulfikar, 2020). Semakin tinggi nilai PSNR, maka semakin kecil perubahan yang terjadi pada gambar.

Rumus PSNR:

$$PSNR = 10 \times log_{10}\left(\frac{255^2}{MSE}\right)$$

Rumus MSE (Mean Squared Error):

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{i} . \sum_{j=1}^{n} (I\ (i,j) - K(i,j))^2$$

Keterangan:
- $I\ (i,j)$: piksel pada gambar asli
- $K(i,j)$ piksel pada gambar stego
- m dan n dimensi gambar

b. Hasil Pengujian PSNR

Tabel 2. Hasil Pengujian PNSR

No	Gambar	MSE	PSNR (dB)	Keterangan
1	Pemandangan Alam	0.092	58.49	Sangat Baik
2	Gedung Modern	0.087	58.72	Sangat Baik
3	Citra Abstrak	0.094	58.35	Sangat Baik

Analisis:
Semua nilai PSNR di atas 50 dB, membuktikan bahwa perubahan akibat penyisipan data tidak signifikan dan tidak terdeteksi secara visual. Ini sejalan dengan penelitian Berliani, (2025) yang menyatakan bahwa metode LSB mempertahankan kualitas gambar dengan PSNR > 50 dB.

Evaluasi Keamanan Data

a. Keberhasilan Ekstraksi dan Dekripsi

Dalam semua pengujian:
- Proses ekstraksi data dari citra stego berhasil 100%.
- Proses dekripsi data menghasilkan teks asli tanpa kesalahan (akurasi 100%).
  Ini menunjukkan bahwa kombinasi steganografi dan enkripsi AES sangat efektif untuk menjaga kerahasiaan dan integritas data, sebagaimana juga dilaporkan oleh Rizqa et al., (2022)

b. Perlindungan Berlapis
- **Lapisan 1:** Data disembunyikan menggunakan steganografi → orang tidak menyadari adanya data.
- **Lapisan 2:** Data dienkripsi → meskipun data ditemukan, tidak dapat dibaca tanpa kunci dekripsi.

Tabel 3. Proses Eksekusi Waktu

Proses	Rata-rata Waktu (detik)
Enkripsi (AES-256)	0.0031

Penyisipan (LSB)	0.0142
Ekstraksi (LSB)	0.0127

Sehingga tingkat keamanan meningkat dibandingkan penggunaan salah satu metode saja.

Waktu Eksekusi Proses

Waktu yang dibutuhkan untuk setiap proses sangat cepat, hal ini menunjukkan bahwa metode gabungan ini efisien dan dapat digunakan untuk aplikasi real-time (Suhanjoyo & Nugroho, 2020).

KESIMPULAN

Berdasarkan hasil implementasi dan pengujian, sistem perlindungan data yang menggabungkan metode steganografi berbasis Least Significant Bit (LSB) dan enkripsi Advanced Encryption Standard (AES-256) terbukti efektif dalam menjaga kerahasiaan data dalam citra digital. Kombinasi kedua metode ini menghadirkan perlindungan berlapis, di mana data rahasia tidak hanya tersembunyi secara visual dalam gambar, tetapi juga diamankan secara kriptografis. Hal ini memastikan bahwa meskipun citra stego berhasil diakses oleh pihak yang tidak berwenang, isi pesan tetap tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Nilai PSNR yang melebihi 58 dB menunjukkan bahwa kualitas visual gambar tidak terganggu secara signifikan oleh proses penyisipan data, sehingga gambar tetap tampak alami dan tidak mencurigakan. Selain itu, sistem ini menunjukkan keberhasilan ekstraksi dan dekripsi mencapai 100%, serta efisiensi waktu proses yang tinggi (kurang dari 0,02 detik per proses), yang menjadikannya layak diterapkan dalam konteks aplikasi real-time.

Melihat hasil yang dicapai, sistem ini memiliki potensi besar dalam mendukung keamanan pertukaran informasi digital, terutama dalam era di mana ancaman terhadap privasi dan kebocoran data semakin meningkat. Namun demikian, penelitian ini juga membuka ruang pengembangan lebih lanjut. Beberapa rekomendasi yang dapat dilakukan dalam penelitian lanjutan meliputi penerapan metode steganografi adaptif yang lebih tangguh terhadap kompresi atau manipulasi gambar, peningkatan kapasitas penyisipan data agar lebih optimal tanpa mengorbankan kualitas citra, serta integrasi dengan algoritma enkripsi lain seperti RSA atau ChaCha20 guna memperkuat sistem dengan lapisan keamanan tambahan. Upaya-upaya tersebut diharapkan dapat semakin menyempurnakan solusi keamanan data digital berbasis citra yang tidak hanya andal, tetapi juga efisien dan mudah diimplementasikan pada berbagai platform.

REFERENSI

Ahuja, R., Ramrakhyani, M., Manchundiya, B., & Shroff, S. (2016). Dual layer secured password manager using Blowfish and LSB. *International Journal of Computer Applications*, *143*(3), 5–10.

Arya, A., & Soni, S. (2018). Performance evaluation of secrete image steganography techniques using least significant bit (LSB) method. *Int. J. Comput. Sci. Trends Technol*, *6*(2), 160–165.

Bainus, A., & Rachman, J. B. (2023). Hubungan Internasional Digital (Digital International Relations). *Intermestic: Journal of International Studies*, *8*(1), 1–18.

Berliani, D. Z. (2025). Penerapan Kriptografi Aes Dan Steganografi Gambar Dengan Metode Spread Spectrum Untuk Pengaman Data Teks. *EProceedings of Engineering*, *12*(2), 1–7.

Darwis, D. (2017). Teknik Steganografi untuk Penyembunyian Pesan Teks Menggunakan Algoritma GIFSHUFFLE. *Jurnal Teknoinfo*, *11*(1), 19–24.

Handoyo, A. E., Rachmawanto, E. H., Sari, C. A., & Susanto, A. (2018). Teknik penyembunyian dan enkripsi pesan pada citra digital dengan kombinasi metode LSB dan RSA. *Jurnal Teknologi Dan Sistem Komputer*, *6*(1), 37–43.

Kautsar, A., & Ikhsan, M. (2025). Implementation of the Advanced Encryption Standard (AES) Algorithm and Bit Plane Complexity Segmentation (BPCS) Steganography Technique for Enhancing Text File Security. *SISTEMASI*, *14*(2), 956–968.

Mulyati, S., Amini, S., & Juliasari, N. (2014). Perancangan Data Warehouse Untuk Pengukuran Kinerja Pengajaran Dosen (Studi Kasus: Fakultas Teknologi Informasi Universitas Budi Luhur). *Jurnal Telematika MKOM*, *6*(1).

Pratama, Y. B., & Fachri, F. (2025). Analisis Keamanan Steganografi Pada Gambar Yang Diunggah Ke Media Sosial Menggunakan Least Significant Bit (LSB). *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(1), 725–732.

Rizqa, I., Safitri, A. N., & Harkespan, I. (2022). Kriptostegano Menggunakan Data Encryption Standard dan Least Significant Bit dalam Pengamanan Pesan Gambar. *Jurnal Masyarakat Informatika*, *13*(2), 111–120.

Sabrina, F. N. (2021). Aplikasi Steganografi Pada Media Gambar Menggunakan Algoritma Least Significan Bit. *Jurnal Tera*, *1*(2), 185–201.

Sari, M., Purnomo, H. D., & Sembiring, I. (2022). Algoritma Kriptografi Sistem Keamanan SMS di Android. *Journal of Information Technology*, *2*(1), 11–15.

Siregar, S. R. S., & Sundari, P. (2016). Rancangan Sistem Informasi Pengelolaan Data Kependudukan Desa (Studi Kasus di Kantor Desa Sangiang Kecamatan Sepatan Timur). *Jurnal Sisfotek Global*, *6*(1).

Suhanjoyo, B. W., & Nugroho, A. (2020). Perancangan Aplikasi Gugus Penjualan Terintegrasi ERP dengan Metode Gabungan Prototype Agile. *Dalam Conference on Innovation and Application of Science and Technology (CIASTECH 2020). Malang: Universitas Widyagama. Http://Publishing-Widyagama. Ac. Id/Ejournalv2/Index. Php/Ciastech/Article/View/1902/1342*.

Zulfikar, D. H. (2020). Quality Factor terhadap Kapasitas Pesan Rahasia pada Steganografi Citra JPEG dan Kualitas Citra Stego. *JUSIFO (Jurnal Sistem Informasi)*, *6*(2), 89–100.