CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 8, No. 1, November 2025, hlm. 97-106

Analisis Pengaruh Kompresi File Pada Media Sosial Terhadap Ketahanan Image Steganografi Pada Metode *Least Significant Bit* (LSB)

Muhammad Na'im Al Jum'ah[1], Arifin[2]

[1,2]Ilmu Komputer Fakultas Teknologi Informasi, Universitas Sembilanbelas November Kolaka
Email: [1]muhnaimaljumah@usn.ac.id, [2]arifinusn019@gmail.com

Abstrak

Media sosial saat ini menjadi platform utama untuk pertukaran informasi di kalangan masyarakat luas. Platform seperti Facebook, Instagram, dan Twitter memungkinkan pengguna untuk berbagi gambar dengan audiens yang sangat besar. Namun, penggunaan media sosial ini juga menimbulkan kekhawatiran terkait privasi dan keamanan data, karena informasi yang dibagikan di platform ini rentan terhadap ancaman kejahatan. Metode Least Significant Bit (LSB) merupakan salah satu teknik steganografi yang paling sederhana dan paling banyak digunakan dalam penyembunyian data. Tujuan dari penelitian ini adalah untuk mengembangkan dan mengimplementasikan metode steganografi LSB yang lebih aman dan tahan terhadap serangan dan gangguan. Metode Least Significant Bit (LSB) merupakan salah satu teknik steganografi yang efektif untuk menyembunyikan pesan dalam media digital, termasuk gambar. Namun efektivitas metode ini dapat dianalisis berdasarkan beberapa parameter, seperti kapasitas penyimpanan, keterlihatan, dan ketahanan terhadap kompresi atau manipulasi gambar, khususnya pada platform media sosial seperti Telegram, Instagram, dan Facebook. Hasil pengujian yang dilakukan menunjukkan, file pesan yang telah disembunyikan dalam gambar tidak dapat ditemukan lagi akibat perubahan ekstensi dari file gambar yang telah di kirim serta penerapan metode kompresi lossy pada masing-masing platform media sosial juga mempengaruhi file stego yang ada.

Kata kunci: Digital Forensik, Sosial Media, Gambar, Steganografi, Least Significant Bit

Analysis Of The Effect Of File Compression On Social Media On Image Steganography Resilience In The Least Significant Bit (LSB) Method

Abstract

Social media is currently a major platform for information exchange among the wider community. Platforms such as Facebook, Instagram, and Twitter allow users to share images with a very large audience. However, the use of social media also raises concerns regarding privacy and data security, because information shared on these platforms is vulnerable to threats of crime. The Least Significant Bit (LSB) method is one of the simplest and most widely used steganography techniques in data hiding. The purpose of this study is to develop and implement a LSB steganography method that is more secure and resistant to attacks and interference. The Least Significant Bit (LSB) method is one of the effective steganography techniques for hiding messages in digital media, including images. However, the effectiveness of this method can be analyzed based on several parameters, such as storage capacity, visibility, and resistance to compression or image manipulation, especially on social media platforms such as Telegram, Instagram, and Facebook. Test results show that message files that have been hidden in images can no longer be found due to changes in the extension of the image file that has been sent. The application of lossy compression methods on each social media platform also affects the existing stego file..

***Keywords**:* Digital Forensics, Social Media, Image, Steganography, Least Significant Bit

1. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah memicu peningkatan signifikan dalam pertukaran data digital di berbagai bidang kehidupan, termasuk dalam sektor bisnis, pemerintahan, pendidikan, dan kehidupan sehari-hari. Hal ini menciptakan kebutuhan mendesak untuk perlindungan data guna memastikan kerahasiaan, integritas, dan keaslian informasi yang ditransmisikan. Salah satu metode yang populer untuk mencapai tujuan ini adalah dengan

menggunakan teknik steganografi, yang memungkinkan penyembunyian data dalam bentuk media digital seperti gambar, audio, atau video(Tri Handayani et al., 2021).

Steganografi adalah seni dan ilmu menyembunyikan informasi sedemikian rupa sehingga keberadaan informasi tersebut tidak diketahui oleh pihak yang tidak berwenang(Kaur & Rani, 2016). Berbeda dengan kriptografi, yang menyembunyikan isi pesan dengan mengubahnya menjadi format yang tidak dapat dimengerti, steganografi menyembunyikan keberadaan pesan itu sendiri. Teknik steganografi dapat diterapkan di berbagai media digital, dengan gambar digital menjadi salah satu media yang paling umum digunakan karena ketersediaannya yang luas dan kemampuan penyimpanan datanya yang tinggi(Nugroho & Muslihudin, 2022).

Media sosial saat ini menjadi platform utama untuk pertukaran informasi di kalangan masyarakat luas(Fitra Alfajri et al., 2019). Platform seperti Facebook, Instagram, dan Twitter memungkinkan pengguna untuk berbagi gambar dengan audiens yang sangat besar(Golbeck, 2015). Namun, penggunaan media sosial ini juga menimbulkan kekhawatiran terkait privasi dan keamanan data, karena informasi yang dibagikan di platform ini rentan terhadap ancaman kejahatan. Oleh karena itu, implementasi steganografi pada gambar yang dibagikan melalui media sosial dapat memberikan lapisan keamanan tambahan bagi pengguna(Ratnasari & Dwiyanto, 2020).

Metode *Least Significant Bit* (LSB) merupakan salah satu teknik steganografi yang paling sederhana dan paling banyak digunakan dalam penyembunyian data. Metode ini bekerja dengan menyisipkan bit-bit data rahasia ke dalam bit-bit paling tidak signifikan dari setiap piksel dalam gambar digital(Setiawan et al., 2020). Keunggulan metode LSB adalah kemudahannya dalam implementasi dan kemampuannya untuk menyembunyikan data tanpa menyebabkan perubahan visual yang signifikan pada gambar yang mengandung data rahasia (Widyastomo Anggoro Putro, 2016).

Beberapa penelitian telah dilakukan berkaitan dengan metode *Least Significant Bit* (Lsb), seperti yang dilakukan oleh (Al Jumah & Sarimuddin, 2024) yang melakukan pengujian file gambar yang di kirim melalui copy file dengan flashdisk, email dan pengiriman melalui whatsapp dengan model dokumen. Hasilnya menunjukkan bahwa dari file dari image stego masih bisa dilakukan ekstraksi data untuk mendapatkan pesan yang telah disembunyikan dalam gambar, namun ketika file image stego yang dikirimkan melalui whatsapps dengan model pengiriman image, image stego tersebut tidak bisa dilakukan ekstraksi. Penelitian lain juga dilakukan oleh (Laoli et al., 2020) dalam penerapan Hill Cipher dan *Least Significant Bit* (LSB) Untuk pengamanan pesan pada citra digital. Hasil penelitian ini menunjukkan pengamanan pesan pada citra digital aman dan tidak diketahui secara kasat mata, karena besar dari bitmap hasil steganografi tidak terlihat secara signifikan.

Seperti yang dilakukan (Sitorus, 2015) dalam penelitiannya tentang implementasi Metode Least Significant Bit (LSB) menunjukkan bahwa dengan menggunakan teknik penyembunyian data ke dalam gambar dapat menjadi media untuk pengamanan data yang akan di kirim. Data rahasia berupa teks dapat di sisipkan ke dalam gambar dengan kunci yang di buat dan di mengerti oleh pengguna aplikasi. Steganography dapat di implementasikan untuk proses otentikasi data dan di gunakan untuk komunikasi atau pertukaran data yang rahasia. Penggunaan steganography dapat bermanfaat dan mencegah kebocoran informasi dari proses penyadapan. Hal yang serupa juga dilakukan oleh (Wiyata, 2016) dalam penelitianya yang mengimplementasikan metode LSB Serta pemrograman PHP untuk keamanan pesan gambar. Hasilnya menunjukkan bahwa metode LSB dapat menyembunyikan pesan yang sulit untuk dipecahkan. Kemudian citra digital yang disisipkan dengan metode LSB ditambah dengan enkripsi akan semakin sulit untuk dipecahkan oleh orang yang tidak berkepentingan.

Dalam penelitianya (Simbolon et al., 2016) menunjukkan kriptografi playfair cipher mengenkripsi pasangan huruf dengan tujuanmem buat analisis frekuensi menjadi sulit sebab frekuensi kemunculan huruf di dalam ciphertext akan menjadi datar. Penerapan kode ASCII juga akan membuat hasil enkripsi semakin sulit untuk dimengerti oleh pihak ketiga. Kombinasi steganografi menggunakan LSB dengan hasil file citra bitmap grayscale 8 bit per piksel dengan format biner akan menghindari kecurigaan. Dengan adanya penerapan kombinasi kriptografi dan steganografi dalam pengamanan data transkrip nilai mahasiswa dipastikan tidak akan diketahui oleh orang lain karena tidak akan mengandung kecurigaan.seperti yang dilakukan (Murdowo, 2020) tentang manual perhitungan menggunakan kriptografi klasik Playfair Cipher. Hasilnya menunjukkan bahwa algoritma Playfair Chiper dengan menggunakan kata kunci yang panjang dan menggunakan bujur sangkar 6X6. Mampu menghasilkan enkripsi pada satu kalimat plaintext yang cukup panjang menjadi chipertext yang cukup akurat dan cukup membingungkan bagi penerima pesan sebelum pesan tersebut dilakukan deskripsi.

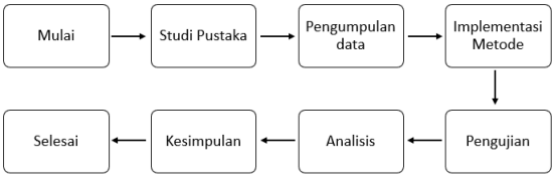
Namun, meskipun metode LSB sederhana dan efektif, teknik ini juga memiliki beberapa kelemahan. Salah satunya adalah kerentanannya terhadap serangan steganalisis, yaitu teknik yang digunakan untuk mendeteksi keberadaan pesan tersembunyi dalam media digital. Selain itu, metode LSB juga rentan terhadap kerusakan data apabila

gambar yang digunakan mengalami kompresi atau pemrosesan ulang (Langi et al., 2021).

Oleh karena itu, penelitian ini akan mengeksplorasi cara-cara untuk meningkatkan keamanan dan ketahanan metode LSB terhadap berbagai jenis serangan dan gangguan serta seberapa besar pengaruh kompresi media sosial terhadap integritas data tersembunyi, maka tujuan dari penelitian ini adalah untuk melakukan analisis dan pengujian tehadap pengaruh kompresi file pada media sosial terhadap ketahanan image steganografi serta menganalisis tingkat kerusakan data steganografi pada masing-masing platform media sosial. Platform media sosial yang digunakan pada penelitian ini adalah telegram, instagram dan Facebook.

2. METODE PENELITIAN

Adapun tahapan penelitian yang dilakukan pada penelitian ini adalah sebagai berikut:



Gambar 1. Tahapan Penelitian

2.1. Studi pustaka

Studi pustaka merupakan tahap awal dalam penelitian di mana peneliti mengumpulkan informasi dari berbagai sumber tertulis seperti jurnal ilmiah, buku, laporan penelitian, dan artikel terkait.

2.2. Pengumpulan data

Pada tahap ini, peneliti mengumpulkan data berupa gambar digital yang akan digunakan sebagai cover image untuk menyembunyikan pesan. Data juga mencakup pesan yang akan disembunyikan. Gambar digital yang digunakan harus memiliki resolusi dan format yang sesuai untuk mendukung metode LSB, misalnya format PNG atau BMP.

2.3. Implementasi metode

Pada tahapan ini Implementasi metode melibatkan pengkodean algoritma LSB ke dalam perangkat lunak yang digunakan, seperti Python atau MATLAB untuk di implementasikan untuk menyisipkan bit pesan ke dalam bit paling tidak signifikan dari piksel gambar.

2.4. Pengujian

Setelah implementasi, tahap pengujian dilakukan untuk menilai efektivitas dan keberhasilan metode LSB dalam menyembunyikan pesan.

2.5. Analisis

Pada tahap analisis, hasil pengujian dianalisis secara mendalam untuk mengukur efektivitas metode LSB. Analisis meliputi aspek ketahanan (robustness), kapasitas (capacity), dan keamanan (security) metode. Hasil pengujian visual dan ekstraksi dievaluasi untuk menilai sejauh mana gambar stego menyerupai gambar asli dan apakah metode LSB cukup aman dari deteksi oleh pihak ketiga. Analisis juga melibatkan perbandingan dengan metode steganografi lain jika diperlukan untuk mengukur keunggulan dan keterbatasan pendekatan ini.

2.6. Kesimpulan

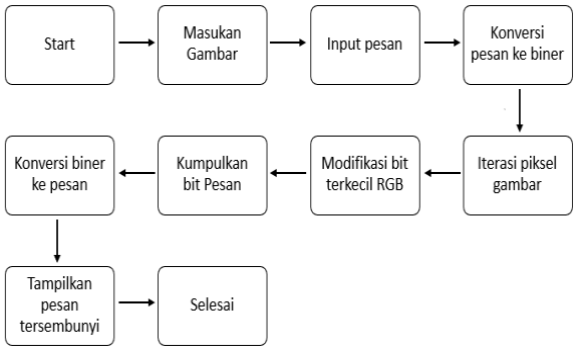
Kesimpulan merangkum temuan utama dari penelitian, termasuk keberhasilan metode LSB dalam menyembunyikan pesan secara efisien dan aman dalam gambar digital. Pada bagian ini, peneliti juga membahas keterbatasan penelitian

3. HASIL DAN PEMBAHASAN

3.1. Pengembangan Sistem

Dalam prosesnya pengembangan sistem, penelti menggunakan bahasa pemograman matlab. MATLAB digunakan karena memiliki fitur unggul dalam pemrosesan citra digital, kemudahan dalam pengelolaan data matriks, serta dokumentasi yang kaya terkait algoritme berbasis citra. Versi MATLAB yang digunakan pada penelitian ini adalah MATLAB Online. Dalam pengembangan sistem ini dilakukan proses Enkripsi dan Dekripsi pesan kedalam gambar.

3.1.1. Alur Proses Penyisipan (Embedding)

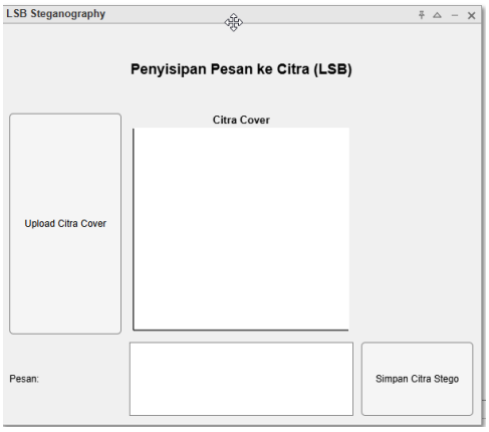


Gambar 2. Alur proses penyisipan

Proses in diawai dengan memilih gambar digital yang akan digunakan sebagai media penampung pesan. Selanjutnya dialkukan input pesan pesan yang ingin disembunyikan dalam gambar. Pesan yang dimasukkan diubah menjadi format biner. Setiap karakter dalam pesan dikonversi menjadi representasi biner 8-bit. Kemudian dilakukan iterasi melalui setiap piksel dalam gambar. Iterasi mengacu pada bagaimana gambar

diproses piksel demi piksel untuk menyisipkan atau mengekstrak pesan rahasia. Setiap piksel terdiri dari nilai RGB (Red, Green, Blue). Proses ini akan mengganti bit terkecil (least significant bit) dari setiap komponen warna (RGB) piksel dengan bit dari pesan biner.

Setelah pesan berhasil disisipkan ke dalam gambar setelah seluruh bit pesan biner ditempatkan pada bit terkecil RGB piksel. Selanjutnya gambar yang telah berisi pesan rahasia akan disimpan sebagai file baru. Gambar yang telah dimodifikasi dapat diunggah ke platform media sosial seperti Telegram, Facebook, dan Instagram. Berikut adalah tampilan untuk penyisipan pesan dalam gambar gambar:



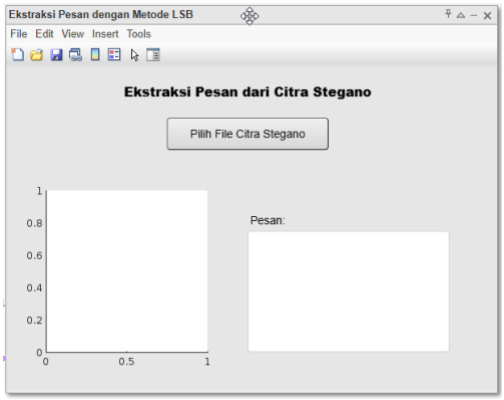
Gambar 3. Penyisipan pesan

3.1.2. Alur Proses Ekstraksi (Extraction)
Berikut ini merupakan alur dalam proses ekstraksi gambar.

Gambar 4. Alur proses ekstraksi

Proses ekstraksi ini dimulai dengan memilih gambar yang telah disiskan dengan metode LSB dan telah di kirim melalui media sosial. Gambar tersebut kemudian akan di ekstraksi gambar digital yang telah dimodifikasi dan berisi pesan tersembunyi untuk diekstraksi. Proses ekstraksi ini akan mengambil Bit terkesil dari RGB karena setiap bit terkecil (least significant bit) merupakan bagian dari pesan yang tersembunyi. Selanjutnya bit-bit yang diekstraksi dari komponen RGB setiap piksel dikumpulkan dan disusun secara berurutan untuk membentuk pesan biner.

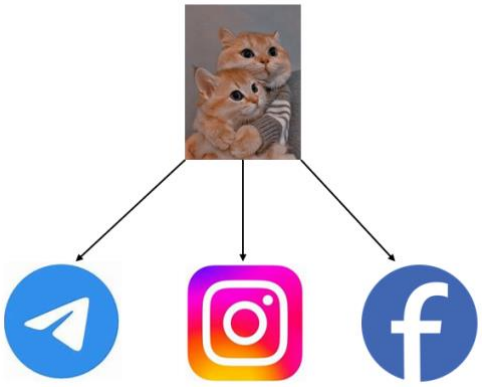
Setelah seluruh bit pesan terkumpul, bit-bit biner ini dikonversi kembali ke bentuk teks atau pesan asli. Proses ini melibatkan penggabungan bit-bit menjadi karakter ASCII atau format lain yang digunakan. Pesan yang telah berhasil diekstraksi dan dikonversi akan ditampilkan. Pesan adalah informasi yang awalnya disembunyikan dalam gambar. Berikut adalah tampilan untuk ekstraksi gambar:



Gambar 4. Ekstraksi gambar

3.2. . Implementasi pada Platform Media Sosial

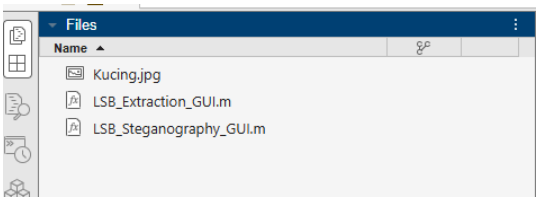
Setelah gambar telah melewati proses Penyisipan (Embedding) pesan, gambar yang telah berisi pesan tersebut akan dikirim menggunakan 4 jenis media sosial yaitu telegram, instagram, facebook dan X (Twitter). Proses pengiriman di media sosial ini dilakukan untuk mengetahui apakah gambar yang telah berisi pesan yang telah di enkripsi jika telah di kirim pada media sosial, data pesan tersebut masih bisa di kembalikan. pesan yang telah disisipkan, algoritma akan membaca bit paling tidak signifikan (LSB) dari setiap piksel gambar dapat disusun kembali menjadi pesan asli serta bagaimana pengaruh vulnerabilitas terhadap Kompresi.



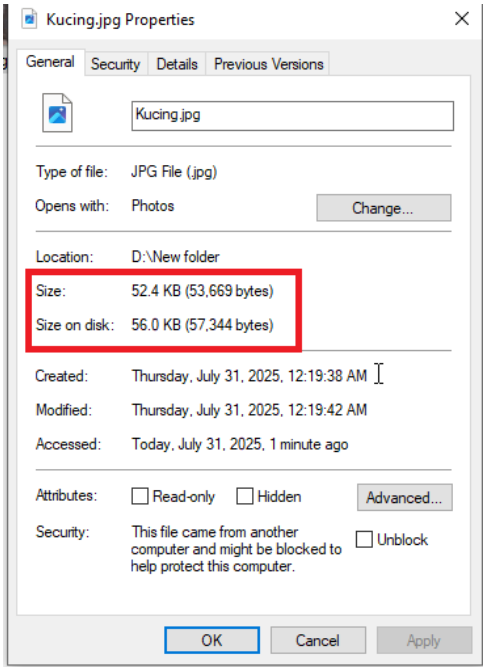
Gambar 5. Implementasi pada media sosial

3.2.1. Pengujian

Proses selanjutnya dilakukan proses pengujian. Pada proses ini akan dilakukan pengujian terhadap sistem yang telah di buat. Proses pertama yang dilakukan adalah melakukan penyisipan pesan pada gambar dengan menerapkan metode LSB. Proses in diawai dengan memilih gambar digital yang akan digunakan sebagai media penampung pesan. Gambar tesebut memiliki nama Kucing.jpg.



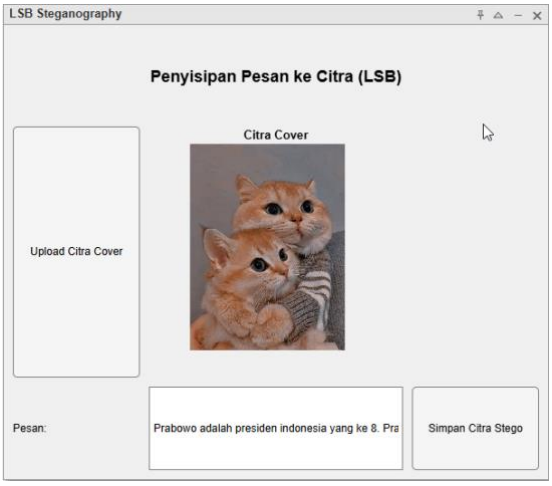
Gambar 6. Penamaan gambar



Gambar 7. Ukuran awal file gambar

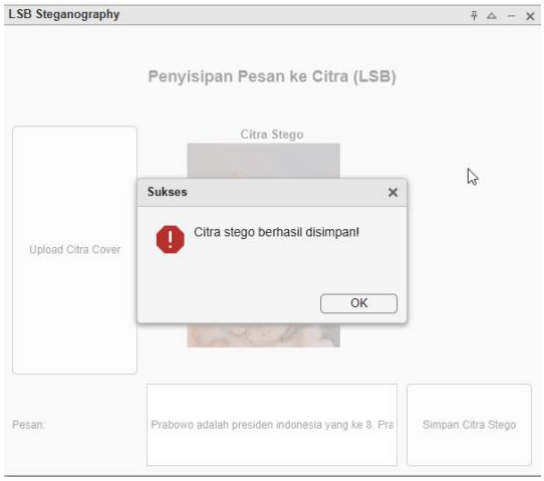
Sebelum dilakukan penyisipan pesan pada gambar dengan menerapkan metode LSB, dilakukan proses pengecekan detail file untuk melihat size awal pada gambar sebelum dilakukan penyisipan pesan. Dari dari pegecekan size gambar, gambar awal berukuran 52.4 KB (53,669 bytes).

Selanjutnya di lakukan upload cover gambar sebagai media yang akan digunakan untuk menyembunyikan pesan yang di inginkan. Pesan yang di sembunyikan adalah *"Prabowo adalah presiden indonesia yang ke 8. Prabowo berasal dari keluarga yang memiliki tradisi intelektual dan nasionalis. Ayahnya, Prof. Soemitro Djojohadikusumo, adalah seorang ekonom terkenal yang banyak berkontribusi pada pembangunan ekonomi Indonesia. Prabowo memiliki hubungan keluarga dengan pahlawan nasional Indonesia, Raden Mas Margono Djojohadikusumo. Prabowo menikah dengan Siti Hediati Hariyadi (Titiek Soeharto), putri dari Presiden Soeharto, namun pernikahan tersebut telah berakhir dengan perceraian."*



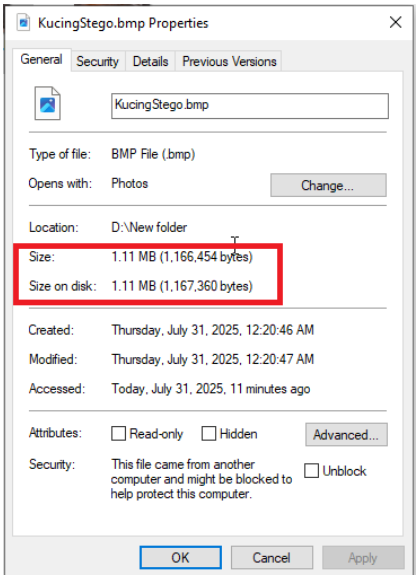
Gambar 8. penyisipan gambar ke citra (LSB)

Setiap karakter dalam pesan yang ingin disembunyikan dalam gambar dikonversi menjadi representasi biner 8-bit. Kemudian dilakukan iterasi melalui setiap piksel dalam gambar. Dalam setiap piksel gambar terdiri dari nilai RGB (Red, Green, Blue). Proses ini akan mengganti bit terkecil (least significant bit) dari setiap komponen warna (RGB) piksel dengan bit dari pesan biner. Misalnya, jika bit terakhir dari komponen warna biru adalah 0 dan bit pesan biner adalah 1, maka bit terakhir tersebut diubah menjadi 1. Pesan berhasil disisipkan ke dalam gambar setelah seluruh bit pesan biner ditempatkan pada bit terkecil RGB piksel.



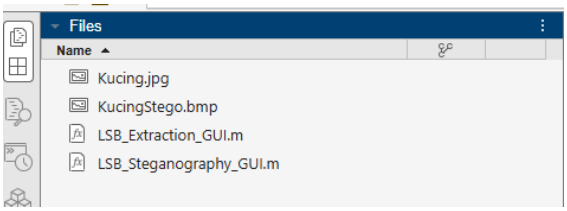
Gambar 9. Citra stego berhasil di simpan

Setelah dilakukan penyisipan pesan pada gambar dengan menerapkan metode LSB, dilakukan proses pengecekan detail gambar untuk melihat size gambar setelah penyisipan pesan. Dari hasil pengecekan detail, terjadi perubahan size gambar menjadi 1.11 MB (1,166,454 bytes) seperti yang telihat pada gambar 10.



Gambar 10. Perubagan size gambar

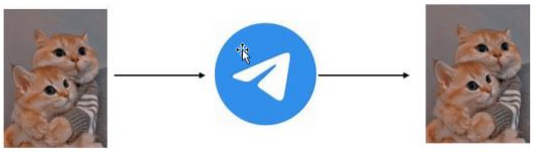
Selanjutnya gambar yang telah berisi pesan rahasia akan disimpan sebagai file baru dengan nama KucingStego.bmp



Gambar11. Gambar hasil penyisipan pesan

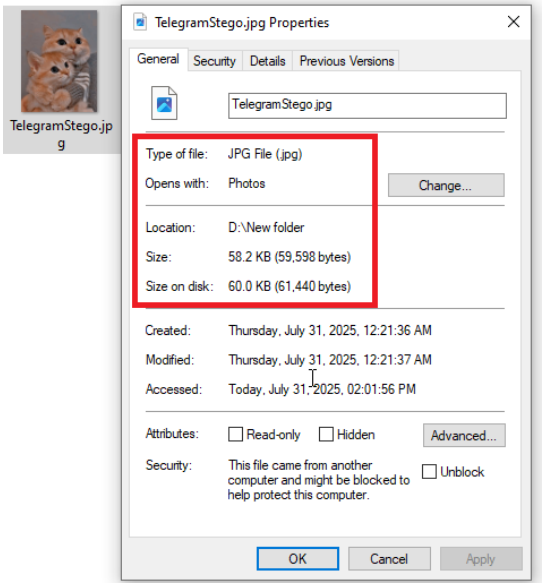
3.2.2. Telegram

Proses pengujian pertama adalah melakukan pengiriman gambar pada media sosial telegram. Hal ini dilakukan untuk melakukan analisis terhadap gambar yang telah berisi pesan yang telah di enkripsi jika telah di kirim pada media sosial, apakah data pesan tersebut masih bisa di kembalikan atau tidak.



Gambar 11. Pengujian dengan telegram

Setelah file stego dibuat menggunakan metode LSB, pengujian dilakukan dengan mengirimkan file tersebut melalui aplikasi Telegram. Telegram akan berfungsi sebagai medium untuk mengirimkan file hasil stego dan melakukan analisis terhadap perubahan yang terjadi.Langkah awal yang dilakukan adalah melakukan download terhadap gambar yang telah di kirim melalui telegram.



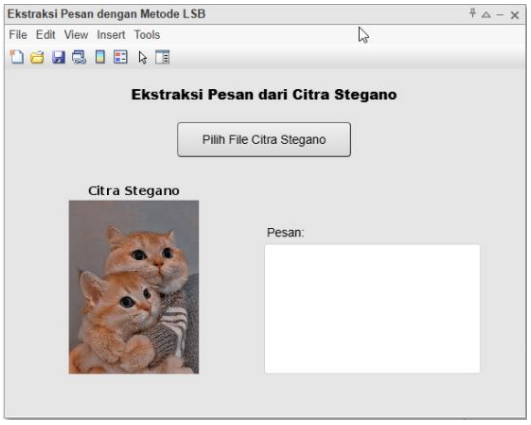
Gambar 12. Detail gambar dari telegram

Dari hasil download file tersebut dilakukan proses pengecekan detail gambar dari telegram seperti gambar 12. dari hasil analisis detail gambar, terjadi perubahan ektensi file. File yang di kirim memiliki file ekstensi .bmt, akan tetapi setelah di download oleh penerima file, ekstensi tersebut kemudian berubah menjadi ekstensi .jpg.. Hasil analisis juga terlihat bahwa size gambar berubah menjadi lebih kecil menjadi 58.2 KB (59,598 bytes) di bandingkan dengan size gambar pada gambar stego.

Selanjutnya dilakukan analisis apakah file tetap dapat diakses atau dibuka dengan benar setelah dikirim melalui telegram. Proses ini termasuk memeriksa apakah file gambar dapat dilihat tanpa gangguan berarti. Selanjutnya memeriksa apakah ada perubahan visual atau suara yang terjadi pada file setelah pengiriman. Perubahan yang dihasilkan oleh LSB biasanya sangat minim, tetapi terkadang ada distorsi yang dapat dideteksi, terutama jika informasi yang disembunyikan cukup besar.

Gambar 13. File hasil download telegram

Proses Selanjutnya dilakukan proses ektraksi terhadap file gambar dari telegram yang telah di download.



Gambar 14. ekstraksi pada file TelegramStego.jpg

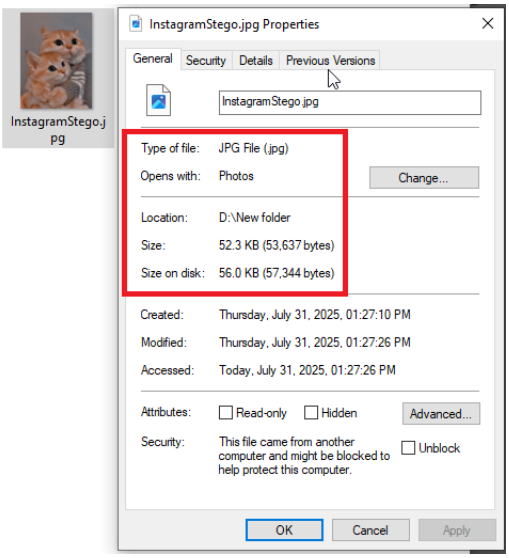
Hasil analisis setelah dilakukan proses ekstraksi pada file gambar TelegramStego.jpg, tidak ditemukan pesan rahasia yang telah disisipkan. Hal ini diakibatkan oleh file gambar telah mengalami kompresi atau perubahan melalui aplikasi Telegram, hasil pengujian ini menunjukkan bahwa teknik LSB memiliki keterbatasan dalam menjaga integritas file. Dalam proses implementasinya sangat penting untuk mempertimbangkan platform yang digunakan untuk pengiriman file dan memeriksa potensi kompresi atau perubahan yang mungkin mempengaruhi keberhasilan steganografi.

3.2.3. Instagram

Proses pengujian pertama adalah melakukan pengiriman gambar pada media sosial Instagram. Hal ini dilakukan untuk melakukan analisis terhadap gambar yang telah berisi pesan yang telah di enkripsi jika telah di kirim pada media sosial, apakah data pesan tersebut masih bisa di kembalikan atau tidak.

Gambar 15. Pengujian dengan Instagram

Setelah file stego dibuat menggunakan metode LSB, pengujian dilakukan dengan mengirimkan file tersebut melalui aplikasi Telegram. Telegram akan berfungsi sebagai medium untuk mengirimkan file hasil stego dan melakukan analisis terhadap perubahan yang terjadi.Langkah awal yang dilakukan adalah melakukan download terhadap gambar yang telah di kirim melalui telegram.



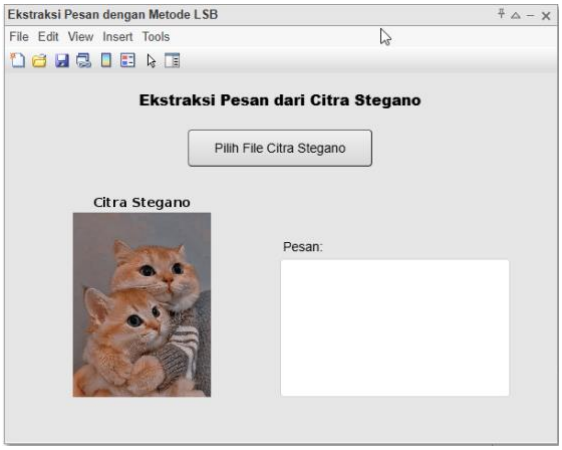
Gambar 16. Detail gambar dari Instagram

Dari hasil download file tersebut dilakukan proses pengecekan detail gambar seperti gambar 17. dari hasil analisis detail gambar, terjadi perubahan ektensi file. File yang di kirim memiliki file ekstensi .bmt, akan tetapi setelah di download oleh penerima file, ekstensi tersebut kemudian berubah menjadi ekstensi.jpg. Dari hasil analisis juga terlihat bahwa size gambar berubah menjadi lebih kecil menjadi 52.3 KB (53,637 bytes) di bandingkan dengan size gambar pada gambar stego

Setelah itu dilakukan analisis apakah file tetap dapat diakses atau dibuka dengan benar setelah dikirim melalui Telegram. Proses ini termasuk memeriksa apakah file gambar dapat dilihat tanpa gangguan berarti. Selanjutnya memeriksa apakah ada perubahan visual atau suara yang terjadi pada file setelah pengiriman. Perubahan yang dihasilkan oleh LSB biasanya sangat minim, tetapi terkadang ada distorsi yang dapat dideteksi, terutama jika informasi yang disembunyikan cukup besar.

Gambar 17. File hasil download instagram

Selanjutnya dilakukan proses ektraksi terhadap file gambar dari telegram yang telah di download.

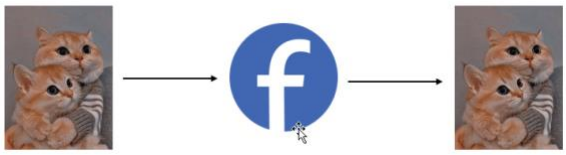


Gambar 18. ektraksi pada file InstagramStego.jpg

Setelah dilakukan proses ekstraksi pada file gambar InstagramStego.jpg, tidak ditemukan pesan rahasia yang telah disisipkan. Hal ini diakibatkan oleh file gambar telah mengalami kompresi atau perubahan melalui aplikasi Instagram, hasil pengujian ini menunjukkan bahwa teknik LSB memiliki keterbatasan dalam menjaga integritas file. Dalam proses implementasinya sangat penting untuk mempertimbangkan platform yang digunakan untuk pengiriman file dan memeriksa potensi kompresi atau perubahan yang mungkin mempengaruhi keberhasilan steganografi.

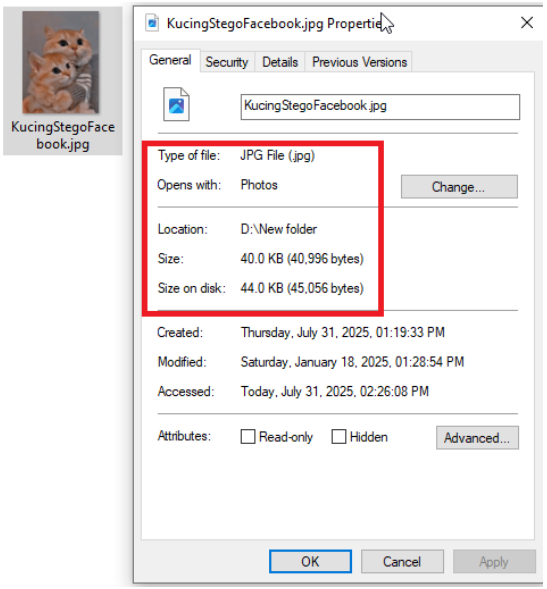
3.2.4. Facebook

Proses pengujian pertama adalah melakukan pengiriman gambar pada media sosial Facebook. Hal ini dilakukan untuk melakukan analisis terhadap gambar yang telah berisi pesan yang telah di enkripsi jika telah di kirim pada media sosial, apakah data pesan tersebut masih bisa di kembalikan.



Gambar 19. Pengujian dengan Facebook

Setelah file stego dibuat menggunakan metode LSB, pengujian dilakukan dengan mengirimkan file tersebut melalui aplikasi Telegram. Telegram akan berfungsi sebagai medium untuk mengirimkan file hasil stego dan melakukan analisis terhadap perubahan yang terjadi.Langkah awal yang dilakukan adalah melakukan download terhadap gambar yang telah di kirim melalui telegram.



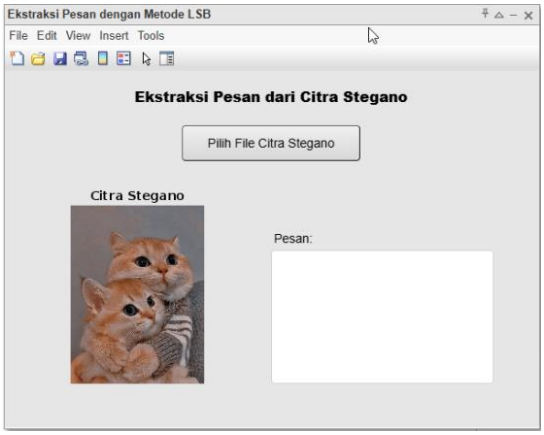
Gambar 20. Detail gambar dariFacebook

Dari hasil download file tersebut dilakukan proses pengecekan detail gambar seperti gambar 21. dari hasil analisis detail gambar, terjadi perubahan ektensi file. File yang di kirim memiliki file ekstensi .bmt, akan tetapi setelah di download oleh penerima file, ekstensi tersebut kemudian berubah menjadi ekstensi.jpg. Dari hasil analisis juga terlihat bahwa size gambar berubah menjadi lebih kecil menjadi 40.0 KB (40,996 bytes) di bandingkan dengan size gambar pada gambar stego

Setelah itu dilakukan analisis apakah file tetap dapat diakses atau dibuka dengan benar setelah dikirim melalui Telegram. Proses ini termasuk memeriksa apakah file gambar dapat dilihat tanpa gangguan berarti. Selanjutnya memeriksa apakah ada perubahan visual atau suara yang terjadi pada file setelah pengiriman. Perubahan yang dihasilkan oleh LSB biasanya sangat minim, tetapi terkadang ada distorsi yang dapat dideteksi, terutama jika informasi yang disembunyikan cukup besar.

Gambar 21. File hasil download Facebook

Selanjutnya dilakukan proses ektraksi terhadap file gambar dari telegram yang telah di download.



Gambar 22. ektraksi pada file FacebookStego.jpg

Setelah dilakukan proses ekstraksi pada file gambar FacebookStego.jpg, tidak ditemukan pesan rahasia yang telah disisipkan. Hal ini diakibatkan oleh file gambar telah mengalami kompresi atau perubahan melalui aplikasi Facebook. Hasil pengujian ini menunjukkan bahwa teknik LSB memiliki keterbatasan dalam menjaga integritas file. Dalam proses implementasinya sangat penting untuk mempertimbangkan platform yang digunakan untuk pengiriman file dan memeriksa potensi kompresi atau perubahan yang mungkin mempengaruhi keberhasilan steganografi.

3.3. Pembahasan

Berdasarkan hasil pengujian yang telah dilakukan pada tiga jenis media sosial yaitu Telegram, Instagram dan Facebook, setelah dilakukan proses ektrasi pesan terhadap gambar stego yang berisi pesan rahasia tidak ditemukan pesan rahasia yang telah di sisipkan sebelumnya. Hal ini terjadi karena terjadi resistensi terhadap gambar yang telah dikirimkan melalui ketiga media sosial tersebut. Resistensi terhadap kompresi gambar dan manipulasi lainnya merupakan salah satu tantangan terbesar bagi efektivitas metode LSB.

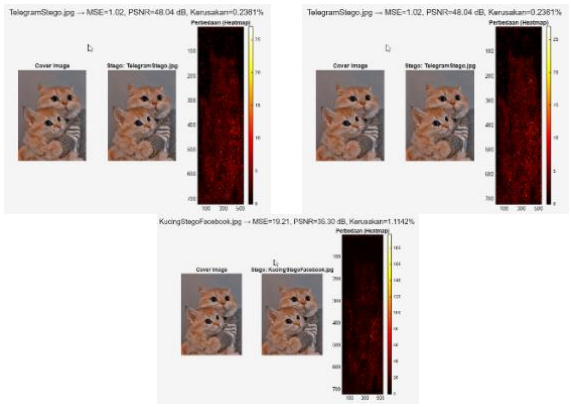
Platform media sosial seperti Instagram dan Facebook secara otomatis menerapkan kompresi lossy pada gambar yang diunggah, yang dapat merusak atau menghapus data tersembunyi. Pada facebook memiliki jenis kompresi yang mengubah nilai piksel, sehingga bit-bit LSB sering kali hilang atau rusak, menyebabkan pesan steganografi tidak dapat dipulihkan, sedangkan pada Instragram kompresi lossy pada gambar dilakukan untuk mengurangi kapasitas file yang di upload pada media tersebut.

Sebaliknya, Telegram, yang mendukung pengiriman berkas dalam format aslinya tanpa kompresi, sangat cocok untuk metode LSB. Memotong, mengubah ukuran, mengedit, atau manipulasi gambar lainnya dapat merusak integritas data tersembunyi, sehingga mustahil merekonstruksi pesan sepenuhnya. Akan tetapi pada kasus ini, hasil pesan yang dikirimkan melalui telegram juga tidak ditemukan, Hal ini diakibatkan oleh file gambar telah mengalami kompresi lossy akibat pengiriman file serta format file yang tidak di dukung oleh telegram, dimana telegram mendukung format file .png dalam pengiriman file steganografi.

Hasil pengujian juga menunjukkan hasil data persentase kerusakan dan perbandingan metrik tingkat kerusakan seperti yang di tunjukan pada tabel 4.1. dari tiga media sosial yang dilakukan pengujian terlihat bahwa facebook memiliki presentase kerusakan yang paling tinggi dibandingkan media sosial lain yaitu sebesar 1.1825%.

Tabel 4.1 Hasil pengujian pada media sosial

No	Jenis Media Sosial	Pesan Hasil Ekstraksi		Preseentase Kerusakan		
		Ya	Tidak	MSE	PSNR	%
1	Telegram		✓	1.0211	48.04 dB	0.2361 %
2	Instagram		✓	0.0021	74.87 dB	0.0008 %
3	Facebook		✓	23.1046	34.49 dB	1.1825 %



Gambar 23. persentase kerusakan dan perbandingan metrik

Metode bit signifikan terkecil (LSB) merupakan teknik steganografi yang efektif untuk menyembunyikan pesan dalam media digital seperti gambar. Efektivitas metode ini dapat dianalisis berdasarkan beberapa parameter, seperti kapasitas penyimpanan, visibilitas, dan ketahanan terhadap kompresi dan manipulasi gambar. Khususnya, platform media sosial seperti Telegram, Instagram, dan Facebook telah melaporkan bahwa dalam hal kapasitas penyimpanan, metode LSB memungkinkan penyisipan pesan yang relatif besar, terutama untuk gambar dengan resolusi tinggi dan kedalaman warna tinggi (misalnya, 24 bit).). Ada keuntungannya. Namun, kapasitas penyimpanan juga dipengaruhi oleh format gambar yang digunakan. Gambar dalam format BMP atau PNG, yang tidak dikompresi secara destruktif, memungkinkan penyisipan pesan lebih baik daripada format JPEG, yang menggunakan kompresi lossy.

Dalam hal visibilitas, metode LSB memiliki keuntungan menghasilkan perubahan yang hampir tidak terlihat oleh mata manusia. Perubahan bit yang besar pada posisi terkecil tidak secara nyata mempengaruhi kualitas optik gambar. Hal ini

membuat metode ini sulit dideteksi dengan mata telanjang, terutama pada gambar dengan warna dan tekstur yang kompleks. Namun, memanipulasi gambar Anda, seperti menambahkan filter atau menyesuaikan warna, seperti yang umum dilakukan pada platform seperti Instagram dan Facebook, dapat mengurangi visibilitasnya.

Secara keseluruhan, efektivitas metode LSB sangat bergantung pada media sosial yang digunakan, format file gambar, dan jenis manipulasi atau kompresi yang diterapkan. Untuk memastikan keberhasilan teknik ini, pilih platform yang mendukung pengunggahan gambar yang tidak dikompresi. Penggunaan format gambar lossless juga merupakan faktor penting di Telegram. Untuk aplikasi yang memerlukan ketahanan yang lebih besar, metode LSB dapat dikombinasikan dengan teknik steganografi lain atau format data yang lebih kuat dapat digunakan untuk lebih melindungi pesan tersembunyi.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian yang telah di lakukan, maka kesimpulan yang dapat di ambil dari penelitian ini adalah Metode Least Significant Bit (LSB) merupakan salah satu teknik steganografi yang efektif untuk menyembunyikan pesan dalam media digital, termasuk gambar. Namun efektivitas metode ini dapat dianalisis berdasarkan beberapa parameter, seperti kapasitas penyimpanan, keterlihatan, dan ketahanan terhadap kompresi atau manipulasi gambar, khususnya pada platform media sosial seperti Telegram, Instagram, dan Facebook. Hasil pengujian yang dilakukan menunjukkan, file pesan yang telah disembunyikan dalam gambar tidak dapat ditemukan lagi akibat perubahan ekstensi dari file gambar yang telah di kirim serta penerapan metode kompresi lossy pada masing-masing platform media sosial juga mempengaruhi file stego yang ada.

DAFTAR PUSTAKA

Al Jumah, M. N., & Sarimuddin, S. (2024). Implementasi Steganografi Metode Least Significant Bit (LSB) untuk Menyembunyikan File Pesan dalam Gambar. *Jurnal Informatika Dan Rekayasa Perangkat Lunak*, *6*(1), 102–108.

Fitra Alfajri, M., Adhiazni, V., & Aini, Q. (2019). Pemanfaatan Social Media Analytics Pada Instagram Dalam Peningkatan Efektivitas Pemasaran. In *Jurnal Ilmu Komunikasi* (Vol. 8, Issue 2).

Golbeck, Jennifer. (2015). *Introduction to social media investigation : a hands-on approach*. Syngress.

Kaur, H., & Rani, J. (2016). A Survey on different techniques of steganography. *MATEC Web of Conferences*, *57*. https://doi.org/10.1051/conf/2016

Langi, E. R., Sambul, A. M., & Kambey, F. D. (2021). Perbandingan Metode Least Significant Bit Dan Discrete Wavelet Transform Dalam Teknik Steganografi Pada Citra Batik Bentenan. *Jurnal Teknik Informatika*.

Laoli, D., Sinaga, B., & Sindar, A. (2020). Penerapan Algoritma Hill Cipher Dan Least Significant Bit (LSB) Untuk Pengamanan Pesan Pada Citra Digital. In *JANUARI* (Vol. 4, Issue 3).

Murdowo, S. (2020). Manual Perhitungan Menggunakan Kriptografi Klasik Playfair Chiper. *Jurnal Infokam*, *16*(1).

Nugroho, C., & Muslihudin, M. (2022). Steganografi Pada Pengiriman Teks Pesan Gambar dengan Metode Least Significant Bit & Steghide. *Jurnal Ilmu Siber*, *1*(2).

Ratnasari, A. P., & Dwiyanto, F. A. (2020). Metode Steganografi Citra Digital. *Sains, Aplikasi, Komputasi Dan Teknologi Informasi*, *2*(2), 52.

Setiawan, A. E., Pasaribu, A., & Pratama, R. C. (2020). Penerapan Steganografi Pada Citra Digital Menggunakan Metode Least Significant Bit (LSB) Kombinasi RC4 Berbasis Mobile Android. *Aisyah Journal of Informatics and Electrical Engineering*, *2*(1). http://jti.aisyahuniversity.ac.id/index.php/AJIEE

Simbolon, R. W., Mbp, A., Jurusan, M., & Informatika, M. (2016). *Pengamanan Transkrip Nilai Mahasiswa Menggunakan Kriptografi Playfair Cipher Dan Steganografi Dengan Teknik Least Significant Bit (LSB)* (Vol. 5, Issue 1).

Sitorus, M. (2015). Teknik Steganography Dengan Metode Least Significant Bit (LSB). *Jurnal Ilmiah Fakultas Teknik LIMIT'S*, *11*(2). https://doi.org/10.13140/RG.2.2.14942.23362

Tri Handayani, Tri Yuliati, & Patimah, S. (2021). Implementasi Steganografi Dengan Metode End Of File (EOF) Untuk Menyisipkan Pesan Teks Pada Gambar. *JURNAL FASILKOM*, *11*(3), 143–149. https://doi.org/10.37859/jf.v11i3.3124

Widyastomo Anggoro Putro, B. (2016). Aplikasi Watermarking Dengan Metode Least Significant Bit Menggunakan Matlab. In *Jurnal Informatika dan Komputer* (Vol. 21, Issue 3).

Wiyata, W. (2016). Implementasi Steganografi Metode LSB Menggunakan Program PHP untuk Keamanan Pesan Gambar. *Jurnal ICT Learning*, *2*(2).

.