IMPLEMENTASI STEGANOGRAFI DENGAN METODE *LEAST SIGNIFICANT BIT* (LSB) UNTUK PENYISIPAN DALAM DATA GAJI PADA PT NUSA NETWORK PRATAMA

Freddi Moriston Alfa Doli[1], Lukman[2], Meri Chrismes Aruan[3]
Program Studi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer
Universitas Indraprasta PGRI
Jalan Raya Tengah No 80, Kelurahan Gedong, Pasar Rebo, Jakarta Timur
moristondollysirait@gmail.com[1], lkmnaja51@gmail.com[2], meriprincess08aruan@gmail.com[3]

Abstrak

Penelitian ini dilakukan dengan tujuan untuk meningkatkan keamanan informasi pada data gaji karyawan di PT Nusa Network Pratama melalui penerapan metode steganografi. Mengingat pentingnya kerahasiaan data gaji sebagai bagian dari informasi sensitif perusahaan, dibutuhkan sistem yang mampu menyembunyikan data tersebut tanpa terdeteksi secara visual maupun *digital* oleh pihak yang tidak berwenang. Metode yang digunakan dalam penelitian ini adalah steganografi berbasis *Least Significant Bit* (LSB), yaitu teknik penyisipan data dengan menggantikan *bit* paling tidak signifikan dari setiap piksel dalam citra *digital*. Pendekatan ini dipilih karena kemampuannya dalam menyisipkan data dengan cara yang tidak mempengaruhi kualitas visual gambar secara signifikan. Proses implementasi dilakukan dengan pengujian penyisipan dan ekstraksi data untuk memastikan bahwa data gaji dapat disembunyikan dan diambil kembali dengan akurasi yang tinggi. Hasil dari penelitian menunjukkan bahwa metode LSB dapat digunakan secara efektif untuk menyisipkan data gaji ke dalam citra tanpa merusak tampilan visual gambar. Data yang telah disisipkan dapat diekstraksi kembali dengan tingkat keberhasilan 100%, tanpa adanya kerusakan pada data asli maupun *file* gambar. Dengan demikian, implementasi steganografi LSB terbukti layak dan aman sebagai alternatif dalam mendistribusikan data gaji secara internal di lingkungan perusahaan.

Kata Kunci: Steganografi, *Least Significant Bit*, Keamanan Data, Data Gaji, Citra *Digital*, PT Nusa Network Pratama

Abstract

This research was conducted with the aim of enhancing information security for employee salary data at PT Nusa Network Pratama through the application of steganography methods. Given the importance of salary confidentiality as part of the company's sensitive information, a system is needed that can hide this data without being detected visually or digitally by unauthorised parties. The method used in this study is Least Significant Bit (LSB)-based steganography, a data-embedding technique that replaces the least significant bit of each pixel in a digital image. This approach was chosen for its ability to embed data without significantly affecting the visual quality of the image. The implementation process involved testing data embedding and extraction to ensure that salary data could be hidden and retrieved with high accuracy. The results of the study indicate that the LSB method can be effectively used to embed salary data into images without compromising the visual appearance of the image. The embedded data can be extracted with a 100% success rate, without any damage to the original data or the image file. Thus, the implementation of LSB steganography has proven to be feasible and secure as an alternative for distributing salary data internally within a corporate environment.

Keywords*: Steganography, Least Significant Bit, Data Security, Salary Data, Digital Image, PT Nusa Network Pratama*

PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat telah memberikan dampak signifikan terhadap pengelolaan data dalam dunia industri, termasuk dalam pengelolaan data internal perusahaan seperti data gaji karyawan. Informasi gaji merupakan data yang bersifat sensitif karena mencerminkan hak-hak finansial karyawan yang bersangkutan serta dapat berpotensi menimbulkan ketimpangan atau konflik internal apabila disebarluaskan tanpa izin (Irfan & Mulyadi, 2020). Pada perusahaan seperti PT Nusa Network Pratama, pengamanan data gaji

menjadi aspek penting dalam menjaga kerahasiaan dan integritas informasi karyawan. Meski telah banyak sistem keamanan seperti enkripsi yang digunakan, tidak menutup kemungkinan bahwa data tetap dapat diakses oleh pihak tidak berwenang melalui berbagai celah (Rahman et al., 2021). Perkembangan teknologi digital juga meningkatkan risiko terhadap keamanan dan privasi data, sehingga perlindungan terhadap data sensitif menjadi semakin penting dalam berbagai aktivitas organisasi (Prasetya et al., 2024). Selain itu, ancaman seperti peretasan dan kebocoran data menunjukkan bahwa sistem keamanan informasi harus terus dikembangkan agar mampu menghadapi serangan siber yang semakin kompleks (Futri & Parhusip, 2023) . Penggunaan teknik enkripsi dan kontrol akses yang tepat menjadi salah satu solusi untuk menjaga kerahasiaan data dari pihak yang tidak berwenang (Judijanto et al., 2025) . Di sisi lain, kasus kebocoran data di Indonesia menunjukkan adanya kelemahan pada sistem keamanan dan kesiapan infrastruktur, yang berpotensi menimbulkan kerugian ekonomi dan menurunkan kepercayaan publik (Bua & Idris, 2024). Oleh karena itu, dibutuhkan pendekatan tambahan yang bersifat menyembunyikan data, bukan hanya mengamankannya. Steganografi merupakan teknik yang memungkinkan penyisipan informasi rahasia ke dalam media digital, seperti gambar, suara, atau video, tanpa terdeteksi secara visual (Lestari & Nugroho, 2019). Salah satu metode steganografi yang umum digunakan adalah Least Significant Bit (LSB), yaitu teknik yang menyisipkan data ke dalam bit terkecil suatu piksel citra digital sehingga tidak menyebabkan perubahan signifikan terhadap tampilan visual gambar (Rahmat et al., 2021. Pendekatan ini dinilai efektif karena tidak hanya menyembunyikan data tetapi juga menjaga tampilan citra tetap sama, sehingga keberadaan informasi tersembunyi tidak mencurigakan. Melalui penerapan metode LSB, perusahaan diharapkan dapat mendistribusikan atau menyimpan data gaji secara tersembunyi dan aman tanpa mengganggu struktur sistem yang ada (Pratama & Wijaya, 2024). Hal ini sangat relevan di era digital saat data dapat dengan mudah ditransmisikan dan terekspos oleh pihak luar. Rumusan masalah dalam penelitian ini adalah bagaimana cara menyisipkan data gaji menggunakan metode steganografi *Least Significant Bit* (LSB) dalam citra *digital*, sejauh mana tingkat keberhasilan dan keamanan metode LSB dalam menyisipkan dan mengekstraksi kembali data gaji tanpa kerusakan data. Tujuan dari penelitian ini adalah untuk mengimplementasikan metode steganografi LSB dalam proses penyisipan data gaji karyawan pada citra *digital*. Untuk mengevaluasi efektivitas dan akurasi metode LSB dalam proses penyisipan dan ekstraksi data gaji tanpa merusak kualitas citra maupun data asli. Manfaat hasil penelitian dari penelitian ini diharapkan dapat menjadi solusi tambahan dalam menjaga kerahasiaan data sensitif, khususnya data gaji karyawan, dari pihak yang tidak berwenang. Memberikan kontribusi dalam pengembangan dan penerapan steganografi *digital* dalam dunia nyata, khususnya di bidang keamanan informasi. Menjadi referensi dalam membangun sistem keamanan data dengan pendekatan steganografi. Memberikan pemahaman tentang pentingnya perlindungan data sensitif dalam era *digital*.

PENELITIAN RELEVAN

Putra, A., & Wijaya, D. (2022), Implementasi Metode LSB pada Gambar *Digital* untuk Keamanan Data Akademik. Jurnal Informatika. Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa metode *Least Significant Bit* (LSB) efektif digunakan untuk menyisipkan data akademik ke dalam citra *digital* tanpa mengubah tampilan visual gambar secara signifikan. Implementasi metode ini mampu menjaga kerahasiaan data akademik dengan menyembunyikan informasi penting dalam media yang sulit terdeteksi oleh pihak tidak berwenang. Selain itu, LSB memiliki keunggulan dalam hal kemudahan implementasi dan efisiensi penyimpanan, sehingga cocok digunakan pada sistem keamanan informasi akademik yang membutuhkan penyamaran data tanpa mengganggu struktur asli *file*. Oleh karena itu, metode LSB dapat menjadi solusi alternatif dalam menjaga keamanan dan integritas data di lingkungan akademik.

Maharani, L., & Saputra, H. (2022). Steganografi pada *file citra menggunakan teknik Least Significant Bit* (LSB). Penelitian ini menunjukkan bahwa teknik steganografi menggunakan metode Least Significant *Bit* (LSB) pada *file* citra dapat digunakan secara efektif untuk menyembunyikan informasi rahasia tanpa mengubah kualitas visual gambar secara signifikan. Teknik LSB memanfaatkan *bit* terkecil pada tiap piksel citra *digital* sehingga perubahan data yang disisipkan tidak

dapat dikenali oleh mata manusia. Dengan karakteristik tersebut, metode ini cocok diterapkan dalam sistem yang membutuhkan keamanan data tinggi, seperti dokumen rahasia atau informasi sensitif. Hasil uji coba juga menunjukkan bahwa metode LSB memiliki tingkat akurasi yang baik dalam proses ekstraksi data tersembunyi, selama format dan resolusi citra dipertahankan. Oleh karena itu, teknik ini dapat menjadi solusi sederhana namun andal dalam mendukung sistem keamanan informasi *digital*.

Hidayat, R., & Amelia, T. (2023). Aplikasi steganografi dengan LSB untuk menyimpan data pribadi. Penelitian ini membuktikan bahwa aplikasi steganografi dengan metode *Least Significant Bit* (LSB) merupakan solusi efektif untuk menyimpan dan melindungi data pribadi dalam *file* citra *digital*. Teknik ini menyisipkan informasi ke dalam *bit* paling tidak signifikan dari setiap piksel gambar tanpa menimbulkan perbedaan yang terlihat secara visual. Hasil pengujian menunjukkan bahwa data pribadi dapat disembunyikan dan diambil kembali (ekstraksi) dengan akurasi tinggi selama tidak terjadi kompresi atau manipulasi gambar setelah penyisipan. Selain itu, aplikasi berbasis LSB memiliki keunggulan dari sisi kemudahan implementasi, kecepatan proses, serta efisiensi ruang penyimpanan. Dengan demikian, metode ini sangat tepat digunakan untuk meningkatkan keamanan data pribadi dalam era *digital* yang rentan terhadap kebocoran informasi.

Firdaus, M., & Nurhadi, E. (2023). Pengamanan Data dengan Metode Steganografi *Least Significant Bit*. Metode steganografi dengan pendekatan *Least Significant Bit* (LSB) terbukti mampu memberikan lapisan pengamanan tambahan terhadap data *digital* dengan cara menyisipkan informasi rahasia ke dalam media citra tanpa memengaruhi kualitas visual secara signifikan. Penelitian ini menunjukkan bahwa data yang disisipkan menggunakan teknik LSB tetap tersembunyi dari pengamatan biasa dan dapat diambil kembali (diekstrak) secara utuh, selama *file* citra tidak mengalami kompresi atau modifikasi. Keunggulan utama dari metode ini terletak pada kesederhanaan implementasi, kecepatan proses, serta kemampuannya dalam menjaga kerahasiaan dan integritas data. Oleh karena itu, teknik ini sangat relevan untuk diaplikasikan dalam sistem pengamanan informasi di berbagai bidang, termasuk keuangan, akademik, dan komunikasi pribadi.

Yuliani, D., & Akbar, R. (2024). Analisis Teknik LSB dalam Penyisipan Informasi Rahasia pada Citra *Digital*. Hasil analisis menunjukkan bahwa teknik *Least Significant Bit* (LSB) merupakan salah satu metode steganografi yang paling efisien dan sederhana untuk menyisipkan informasi rahasia ke dalam citra *digital*. Dengan memanfaatkan *bit* terkecil dari setiap piksel, informasi dapat disembunyikan tanpa memengaruhi tampilan visual gambar secara signifikan, sehingga tidak menimbulkan kecurigaan. Penelitian ini juga membuktikan bahwa akurasi dalam proses penyisipan dan ekstraksi data sangat tinggi, selama *file* citra tidak mengalami perubahan format atau kompresi. LSB efektif untuk kebutuhan keamanan informasi berukuran kecil hingga sedang, namun memiliki keterbatasan terhadap serangan steganalisis dan pengolahan ulang gambar. Oleh karena itu, teknik ini sangat sesuai digunakan dalam lingkungan yang mengutamakan kerahasiaan data dengan media visual sebagai penyamaran, khususnya pada komunikasi privat, sistem penggajian, dan distribusi data akademik rahasia.

Wulandari, S., & Hakim, F. (2024). Implementasi Steganografi LSB pada Data Keuangan Perusahaan. Penelitian ini menunjukkan bahwa implementasi metode *Least Significant Bit* (LSB) pada *file* citra *digital* dapat digunakan secara efektif untuk menyembunyikan data keuangan perusahaan secara aman dan tidak mencolok. Dengan memanfaatkan *bit* paling tidak signifikan pada setiap piksel gambar, informasi keuangan seperti laporan laba-rugi, rincian gaji, atau arus kas dapat disisipkan ke dalam gambar tanpa mengubah kualitas visual yang tampak. Hasil pengujian menunjukkan bahwa data dapat disisipkan dan diekstraksi kembali dengan akurasi tinggi selama *file* citra tidak dimodifikasi pasca penyisipan. Teknik ini memberikan solusi alternatif dalam menjaga kerahasiaan data internal perusahaan dari akses tidak sah, terutama dalam proses distribusi atau penyimpanan digital. Dengan karakteristiknya yang ringan, efisien, dan sulit terdeteksi secara kasatmata, metode LSB layak diterapkan sebagai strategi perlindungan data sensitif di lingkungan korporasi.

METODE PENELITIAN

Metode penelitian yang dilakukan adalah berdasarkan desain penelitian, Desain penelitian mencakup (1) Tujuan Penelitian, (2) Hipotesis, (3) Variabel Penelitian, (4) Metode Penelitian, (5) Populasi dan Sampel, (6) Instrumen Penelitian, (7) Prosedur Pengumpulan Data, (8) Analisis Data. Tempat penelitian ini dilakukan di PT Nusa Network Prakasa, dengan alamat Jl. Kamal Raya Outer Ring Road Blok A17, RT.6/RW.14, Cengkareng Tim, Kecamatan Cengkareng, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta 11730. Teknik pengumpulan data dilakukan melalui studi kepustakaan, studi lapangan terdiri dari observasi, wawancara.

HASIL DAN PEMBAHASAN

Berdasarkan hasil pengamatan dan observasi yang telah dilakukan, berikut permasalahan yang menjadi faktor penghambat antara lain:

1. Belum adanya sistem proteksi tambahan untuk data gaji karyawan di PT Nusa Network Pratama.
2. Ancaman kebocoran data internal dan eksternal semakin meningkat setiap tahunnya.
3. Penggunaan sistem pengamanan berbasis enkripsi saja tidak cukup menjamin kerahasiaan saat data berpindah media.
4. Kurangnya pemahaman dan penerapan teknologi *steganografi* di lingkungan perusahaan.
5. Minimnya integrasi metode penyembunyian data dalam sistem manajemen keuangan perusahaan.
6. Kebutuhan akan metode pengamanan data yang tidak hanya kuat, namun juga tidak mencolok dan mudah diimplementasikan.

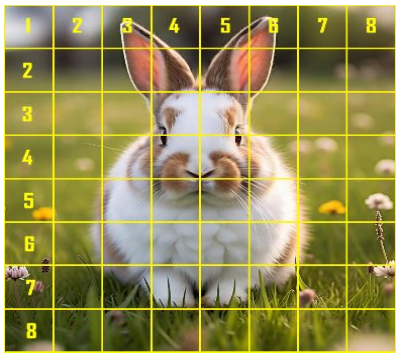
Berdasarkan permasalahan diatas, setelah mendapatkan data informasi yang dibutuhkan melalui wawancara, maka selanjutnya data yang diperoleh di analisis melalui implementasi *Steganografi* dengan Metode *Least Significant Bit* (LSB).

Pembahasan Metode *Least Significant Bit* (LSB

Tahap awal implementasi pada metode *least significant bit* (LSB) dimulai dengan konversi data pesan ke dalam bentuk ASCII dan biner. Setiap karakter direpresentasikan dalam 8 bit, sehingga memungkinkan penyisipan data pada bit terakhir (*Least Significant Bit*). Selanjutnya menyiapkan gambar yang akan digunakan, Gambar/*Image* yang akan digunakan sebagai media untuk menyisipkan pesan itu harus berada satu folder dengan aplikasi yang akan dijalankan.
Berikut ini adalah media gambar awal yang akan digunakan dalam proses *steganografi*:

Gambar 1. Gambar Kelinci

Dari gambar yang disiapkan dibagi pada 8 piksel, dimana setiap piksel terdiri dari tiga komponen warna, yaitu *Red, Green, Blue* (RGB). Masing-masing komponen diwakili oleh 8 *bit* (1 byte). *Bit* ke-8 (terakhir) dari tiap komponen digunakan untuk menyimpan *bit* dari data rahasia.



Gambar 2. Gambar Kelinci dalam 8 Piksel

Hasil yang diperoleh dari gambar pada matrik RGB dalam 8 Piksel dalam sebuah matrik, sebagai berikut :

Tabel 1. matrik RGB dalam 8 Piksel

Untuk *Channel Red* (R), diperoleh:	**Untuk *Channel Green* (G), diperoleh:**	**Untuk *Channel Blue* (B), diperoleh:**
[[157, 129, 128, 82, 87, 116, 113, 88], [108, 95, 134, 145, 145, 145, 89, 104], [157, 168, 172, 184, 213, 179, 168, 161], [138, 149, 181, 158, 176, 210, 167, 157], [138, 153, 187, 143, 140, 223, 167, 140], [129, 121, 152, 158, 158, 203, 126, 101], [83, 66, 76, 117, 120, 129, 113, 108], [72, 72, 62, 82, 102, 99, 122, 148]]	[[158, 125, 115, 76, 66, 92, 87, 105], [105, 93, 108, 109, 107, 108, 89, 93], [148, 158, 159, 175, 199, 163, 157, 150], [134, 146, 171, 142, 153, 188, 157, 150], [133, 147, 188, 141, 132, 210, 156, 134], [124, 119, 155, 165, 161, 188, 120, 100], [83, 73, 82, 121, 119, 123, 106, 105], [75, 80, 72, 81, 101, 103, 118, 137]]	[[165, 131, 103, 62, 54, 66, 44, 73], [74, 65, 79, 97, 95, 76, 52, 60], [74, 80, 85, 174, 196, 93, 78, 76], [56, 62, 134, 140, 143, 150, 75, 66], [44, 62, 192, 138, 121, 200, 70, 58], [50, 54, 160, 173, 161, 175, 57, 41], [40, 25, 57, 111, 95, 64, 34, 32], [37, 34, 21, 32, 25, 10, 40, 81]]

*S*elanjutnya nilai-nilai tersebut dikonversi ke biner, setiap nilai dalam matriks RGB dikonversi ke 8 *digit* biner. Sebagai contoh:
Nilai *Red* : 158 → Biner: 10011110
Nilai *Green* : 129 → Biner: 10000001
Nilai *Blue* : 87 → Biner: 01010111
Dan seterusnya

Selanjutnya menyusun pesan yang akan disisipkan (Contoh: Data Gaji),
NIK : 123
Nama : Freddi
Gaji : 5000000

Setiap karakter dalam *String* dikonversi kedalam representasi ASCII, masukan desimalnya dan masukan nilai biner nya agar memudahkan dalam proses konversi dan penyisipan data. maka diperoleh tabel sebagai berikut:

Tabel 2. Konversi *String* dalam ASCII

Karakter	**ASCII (Desimal)**	**Binner**
1	49	00110001
2	50	00110010
3	51	00110011
;	59	00111011
F	70	01000110
R	114	01110010
E	101	01100101

D	100	01100100
D	100	01100100
I	105	01101001
;	59	00111011
5	53	00110101
0	48	00110000
0	48	00110000
0	48	00110000
0	48	00110000
0	48	00110000
0	48	00110000

Pada tabel pesan diawali dengan nik yaitu 123, maka biner awal yaitu angka 1 adalah 00110001, biner ini disisipkan pada biner *Image* sebanyak 8 baris, maka akan disipkan pada biner dari tabel *Image*

Tabel 3. Proses Penyisipan Pesan angka 1 dengan metode LSB

Desimal	Biner Awal	Biner Pesan (angka 1)	Biner akhir setelah LSB	Keterangan Nilai
157	1001110**1**	0	1001110**0**	Berubah
129	1000000**1**	0	1000000**0**	Berubah
128	1000000**0**	1	1000000**1**	Berubah
82	0101001**0**	1	0101001**1**	Berubah
87	0101011**1**	0	0101011**0**	Berubah
116	0111010**0**	0	0111010**0**	Tetap sama
113	0111000**1**	0	0111000**0**	Berubah
88	0101100**0**	1	0101100**1**	Berubah

Selanjutnya dilakukan langkah yang sama hingga penyisipan pesan terakhir yaitu angka 0 (dari 5000000) dengan nilai biner adalah 00110000.

Setelah seluruh pesan berhasil dilakukan penyisipan ke LSB gambar, maka menyimpan gambar baru yang telah disisipi pesan, dimana matriks RGB yang sudah dimodifikasi digabung kembali menjadi gambar baru, disimpan sebagai *file* **.PNG** untuk mempertahankan integritas data.
Terakhir ekstraksi gambar. Dimana gambar dibuka, matriks RGB dipisahkan kembali, untuk setiap nilai RGB, *bit* paling kanan (LSB) diambil, Setiap 8 *bit* yang terkumpul direkonstruksi menjadi 1 karakter:
157 : 1001110**0** → ambil 0
129 : 1000000**0** → ambil 0
128 : 1000000**1** → ambil 1
82 : 0101001**1** → ambil 1
87 : 0101011**0** → ambil 0
116 : 0111010**0** → ambil 0

113 : 01110000 → ambil 0
88 : 01011001 → ambil 1

00110001 → Nilai Desimal ASCII = 49 → '**1**' (angka pertama dalam nik 123)
Proses dilakukan sampai seluruh pesan berhasil diekstrak.

Dari hasil penyisipan pesan dan proses LSB diatas, telah diketahui *Image* yang telah mengalami perubahan biner, namun dalam hal ini, karena perubahan yang dilakukan yaitu merubah nilai *bit* akhir, maka tidak akan terlihat perubahan warna *Image* yang signifikan, melainkan tak kasat mata, sekilas terlihat mrip dan sama, hanya saja ketika *Image* di masukan dalam sebuah aplikasi yang mampu mengekstrak sebuah pesan, maka secara otomatis akan menampilkan pesan yang tersembunyi dalam sebuah *Image*. Berikut adalah tampilan *Image* sebelum dan sesudah disisipi pesan, dapat dilihat pada gambar dibawah:

***Image* / Gambar Sebelum Disisipi Pesan**	***Image* / Gambar Sesudah Disisipi Pesan**
	

Gambar 3. Tampilan *Image* sebelum dan setelah disisipi pesan

Tampilan Layar

Gambar 4. Tampilan *Form Menu* Utama

Gambar diatas merupakan tampilan menu utama aplikasi implementasi steganografi menggunakan metode *Least Significant Bit* (LSB) pada PT Nusa Network Prakarsa. Aplikasi ini memiliki beberapa menu seperti seperti buka file, proses, laporan, dan keluar, yang menunjukkan fungsi pengolahan data atau penyisipan informasi tersembunyi dalam media digital. Secara keseluruhan, aplikasi ini dirancang untuk mendukung keamanan data dengan teknik penyembunyian informasi dalam bentuk yang tidak mudah terdeteksi.

Gambar 5. Tampilan *Form Menu* Penyisipan pesan pada Gambar

Gambar diatas merupakan tampilan menu penyisipan pesan pada gambar. Pengguna dapat memilih gambar melalui tombol “Ambil Gambar”, lalu menyisipkan pesan dengan memilih data karyawan dan menekan tombol “Sisip Pesan”, sebelum akhirnya menyimpan hasilnya melalui “Simpan Gambar Berpesan”. Antarmuka ini juga menyediakan opsi cetak dan kembali, serta menampilkan informasi karyawan yang dipilih, sehingga memudahkan proses penyisipan pesan tersembunyi ke dalam gambar secara terstruktur.

Gambar 6. Tampilan *Form Menu* Ekstak Gambar

Gambar diatas merupakan tampilan untuk proses ekstraksi pesan tersembunyi dari gambar yang telah disisipi menggunakan metode steganografi LSB. Pengguna dapat memuat gambar melalui tombol “Ambil Gambar”, kemudian menekan tombol “Ekstrak” untuk menampilkan isi pesan yang tersembunyi pada bagian “Isi Pesan”. Halaman ini berfungsi sebagai tahap akhir dalam membaca kembali informasi yang telah disisipkan ke dalam gambar.

SIMPULAN

Berdasarkan pemelitian yang telah dilakukan dapat disimpulkan bahwa metode *Least Significant Bit* (LSB) terbukti efektif digunakan untuk menyembunyikan data gaji karyawan ke dalam citra digital tanpa menimbulkan perubahan visual yang signifikan, sehingga sulit dideteksi secara kasat mata. Proses penyisipan dan ekstraksi yang dilakukan menunjukkan bahwa data dapat disimpan dan dikembalikan dengan akurat, sehingga menjaga integritas informasi. Selain itu, metode ini memiliki keunggulan dalam kemudahan implementasi dan efisiensi penggunaan sumber daya, meskipun masih memiliki keterbatasan dalam hal keamanan terhadap manipulasi citra. Oleh karena itu, metode LSB layak digunakan sebagai solusi tambahan dalam pengamanan data, dengan potensi pengembangan lebih lanjut melalui kombinasi dengan teknik keamanan lainnya.

DAFTAR PUSTAKA

Bua, M., & Idris, M. (2024). Analisis kebocoran data dan dampaknya terhadap kepercayaan publik di Indonesia. *Jurnal Desentralisasi*, 5(2), 45–55.

Firdaus, M., & Nurhadi, E. (2023). Pengamanan data dengan metode steganografi Least Significant Bit. *Jurnal Teknologi Informasi*, 7(1), 23–30.

Futri, A., & Parhusip, J. (2023). Analisis ancaman keamanan siber pada sistem informasi digital. *Jurnal Informatika dan Keamanan*, 6(2), 101–110.

Hidayat, R., & Amelia, T. (2023). Aplikasi steganografi dengan LSB untuk menyimpan data pribadi. *Jurnal Sistem Informasi*, 8(1), 55–62.

Irfan, M., & Mulyadi, D. (2020). Keamanan data dalam sistem informasi perusahaan. *Jurnal Manajemen Informatika*, 4(2), 77–85.

Judijanto, L., Nugraha, A., & Santoso, B. (2025). Analisis keamanan data dan perlindungan privasi dalam pengelolaan big data. *Jurnal Teknologi Digital*, 9(1), 12–20.

Lestari, D., & Nugroho, A. (2019). Steganografi sebagai metode penyembunyian data pada media digital. *Jurnal Ilmu Komputer*, 3(1), 15–22.

Maharani, L., & Saputra, H. (2022). Steganografi pada file citra menggunakan teknik Least Significant Bit (LSB). *Jurnal Informatika*, 6(1), 34–40.

Prasetya, R., Wibowo, A., & Santika, D. (2024). Perlindungan data sensitif dalam era digital. *Jurnal Sistem Informasi dan Teknologi*, 10(1), 66–74.

Pratama, Y., & Wijaya, R. (2024). Implementasi steganografi LSB dalam keamanan data digital. *Jurnal Komputasi*, 8(2), 88–95.

Putra, A., & Wijaya, D. (2022). Implementasi metode LSB pada gambar digital untuk keamanan data akademik. *Jurnal Informatika*, 5(2), 41–48.

Rahman, F., Siregar, H., & Putri, N. (2021). Analisis celah keamanan pada sistem informasi perusahaan. *Jurnal Teknologi Informasi*, 5(1), 11–18.

Rahmat, A., Firmansyah, D., & Kurniawan, E. (2021). Penerapan metode Least Significant Bit (LSB) pada citra digital. *Jurnal Informatika Terapan*, 4(2), 29–36.

Sari, N., Putri, L., & Ramadhan, F. (2023). Analisis efektivitas steganografi dalam penyembunyian data. *Jurnal Keamanan Informasi*, 7(2), 59–67.

Wulandari, S., & Hakim, F. (2024). Implementasi steganografi LSB pada data keuangan perusahaan. *Jurnal Teknologi Informasi*, 9(2), 102–110.

Yuliani, D., & Akbar, R. (2024). Analisis teknik LSB dalam penyisipan informasi rahasia pada citra digital. *Jurnal Informatika Modern*, 8(1), 73–81.