Modem: Jurnal Informatika dan Sains Teknologi
Volume. 4, Nomor. 1 Januari 2026
E-ISSN .: 3046-7209; P-ISSN .: 3046-7217, Hal. 89-97
DOI: https://doi.org/10.62951/modem.v4i1.726
Tersedia: https://journal.aptii.or.id/index.php/Modem

Steganografi Video Adaptif Berbasis Multi-Bit LSB dengan Analisis Kecerahan, Tekstur, dan Gerakan Frame serta Robustness terhadap Kompresi dan Noise

Magfirotul Izza Intan Dwiyanti[1], Fiky Anggara[2*], Nur Maulida Putri[3], Nadiva Adelia Putri [4], Aprielliana Putri Supiandari[5]
[1-5]Sekolah Tinggi Teknologi Bontang, Indonesia
[*]*Penulis korespondensi: fikyanggara05@gmail.com[2]*

Abstack*: Steganography is a technique for hiding secret data within digital media such as images, audio, and video without causing noticeable visual changes. In video media, this technique offers advantages because each frame can be utilized dynamically, resulting in a larger data embedding capacity. However, conventional methods such as fixed-number Least Significant Bit (LSB) embedding still face limitations in balancing visual quality, embedding capacity, and resistance to compression or noise. To address these challenges, this study proposes an Adaptive Video Steganography Method based on Multi-Bit LSB that employs brightness, texture, and motion analysis for each frame to determine the number of embedding bits adaptively. The system adjusts the embedding capacity according to the local characteristics of the video: areas with high texture or rapid motion are assigned more bits, while static or low-texture areas use fewer bits to preserve visual quality. After the embedding process, the video quality is evaluated using PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index Measurement) to assess its similarity to the original video. Experimental results show a PSNR value of 45.86 dB and an SSIM value of 0.9441, Thus, the proposed adaptive method proves to be efficient, robust against disturbances, and capable of maintaining data security without compromising visual quality, making it highly suitable for implementation in multimedia-based information security systems.*

Keywords: *Adaptive Multi-Bit LSB; Frame Motion; PSNR; SSIM; Video Steganography*

Abstrak : Steganografi merupakan teknik penyembunyian data rahasia ke dalam media digital seperti gambar, audio, dan video tanpa menimbulkan perubahan visual yang mencolok. Pada media video, teknik ini memiliki keunggulan karena mampu memanfaatkan setiap frame secara dinamis sehingga kapasitas penyisipan data menjadi lebih besar. Namun, metode konvensional seperti *Least Significant Bit* (LSB) dengan jumlah bit tetap masih memiliki keterbatasan dalam menjaga keseimbangan antara kualitas visual, kapasitas penyisipan, serta ketahanan terhadap kompresi dan gangguan noise. Berdasarkan permasalahan tersebut, penelitian ini mengusulkan Metode Steganografi Video Adaptif Berbasis *Multi-Bit* LSB yang memanfaatkan analisis kecerahan, tekstur, dan gerakan pada setiap frame untuk menentukan jumlah bit penyisipan secara adaptif. Sistem menyesuaikan kapasitas penyisipan sesuai karakteristik lokal video, di mana area dengan tekstur tinggi atau pergerakan cepat diberikan kapasitas bit lebih besar, sedangkan area statis atau bertekstur rendah menggunakan bit lebih sedikit guna menjaga kualitas visual. Setelah proses penyisipan, kualitas video dievaluasi menggunakan PSNR *(Peak Signal-to-Noise Ratio)* dan SSIM *(Structural Similarity Index Measurement)* untuk mengukur kesamaan dengan video asli. Hasil pengujian menunjukkan nilai PSNR sebesar 45,86 dB dan SSIM sebesar 0,9441, Dengan demikian, metode adaptif ini terbukti efisien, tangguh terhadap gangguan, serta mampu menjaga keamanan data tanpa mengorbankan kualitas visual, sehingga berpotensi diterapkan pada sistem keamanan informasi berbasis multimedia.

Kata kunci: Gerakan Frame; Multi-Bit LSB Adaptif; PSNR; SSIM; Steganografi Video

1. LATAR BELAKANG

Perkembangan teknologi informasi yang pesat telah mempermudah proses pertukaran data secara digital, baik dalam bentuk teks, gambar, maupun video. (Setyaningsih, 2023) Namun, kemudahan ini juga menimbulkan risiko kebocoran dan penyalahgunaan informasi, terutama dalam konteks keamanan data. (Rapina, 2025) Untuk mengatasi hal tersebut, diperlukan metode perlindungan informasi yang tidak hanya mengandalkan enkripsi, tetapi

Naskah Masuk: 14 November 2025; Revisi: 17 Desember 2025; Diterima: 10 Januari 2026;
Terbit: 13 Januari 2026

juga mampu menyembunyikan keberadaan data itu sendiri. (Wulandari, 2023) Salah satu teknik yang banyak digunakan untuk tujuan tersebut adalah steganografi, yaitu teknik menyisipkan pesan rahasia ke dalam media digital tanpa menimbulkan perubahan yang terlihat secara signifikan pada media penampungnya. (Jayakanth Kunhoth, 2023)

Dalam implementasinya, steganografi pada media video memiliki keunggulan dibandingkan media lain karena video terdiri dari banyak *frame*, sehingga kapasitas penyisipan data dapat lebih besar dan proses penyembunyian informasi menjadi lebih sulit dideteksi. (Ulan Ari Anti 1), 2017) Salah satu metode yang umum digunakan dalam steganografi adalah *Least Significant Bit* (LSB), di mana bit paling tidak signifikan dari setiap piksel diubah untuk menampung data rahasia. (Syifaur Rizqa Rahmatillah1), 2024). Meskipun sederhana dan memiliki tingkat keberhasilan yang cukup tinggi dalam menjaga tampilan visual, metode LSB konvensional masih memiliki keterbatasan, terutama dalam menjaga keseimbangan antara kualitas visual, kapasitas penyisipan, dan ketahanan terhadap gangguan seperti kompresi serta *noise*. (Jayakanth Kunhoth, 2023)

Metode LSB dengan jumlah bit tetap (seperti 1 bit atau 3 bit) sering kali menimbulkan dua kondisi ekstrem: jika menggunakan sedikit bit, kualitas video tetap baik tetapi kapasitas data rendah; sedangkan jika menggunakan lebih banyak bit, kapasitas meningkat namun kualitas video menurun signifikan. (Harjoko2, 2014) Oleh karena itu, dibutuhkan pendekatan yang lebih cerdas dan adaptif agar proses penyisipan data dapat menyesuaikan dengan karakteristik video itu sendiri. (Tuan Duc Nguyen, 2015)

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan metode Steganografi Video Adaptif Berbasis *Multi-Bit* LSB yang menganalisis kecerahan, tekstur, dan gerakan *frame* untuk menentukan jumlah *bit* optimal dalam penyisipan data. Pendekatan adaptif ini diharapkan mampu menghasilkan kualitas video yang tetap tinggi sekaligus meningkatkan kapasitas penyimpanan serta ketahanan terhadap kompresi dan *noise*. (Muhammad Turmudzi, 2025) Dengan demikian, metode ini diharapkan dapat menjadi solusi yang efektif dalam pengembangan sistem keamanan data berbasis video yang efisien, adaptif, dan tahan terhadap gangguan. (A.E. Ibrahim, 2016)

2. METODE PENELITIAN

Jenis dan Pendekatan Penelitian

Penelitian ini termasuk dalam kategori penelitian eksperimen kuantitatif, karena bertujuan untuk menguji efektivitas metode steganografi video adaptif berbasis *Multi-Bit* LSB melalui pengukuran parameter kuantitatif berupa PSNR (*Peak Signal-to-Noise Ratio*) dan

SSIM (*Structural Similarity Index Measurement*). (Berlian, 2024) Pendekatan yang digunakan adalah eksperimen komparatif, yaitu dengan membandingkan hasil metode yang diusulkan terhadap dua metode konvensional, yaitu metode 1 *Bit LSB* dan 3 *Bit LSB*.

Data Set Penelitian

Objek penelitian ini adalah video digital yang digunakan sebagai media penampung *(cover video)* untuk proses penyisipan data rahasia *(secret data)*. (Malese, 2021)Video yang digunakan dipilih dengan resolusi dan format tertentu (misalnya 720p, format MP4 atau AVI) agar hasil pengujian lebih terukur. Data rahasia yang disisipkan berupa file teks dengan ukuran tertentu yang akan dimasukkan ke dalam frame video menggunakan algoritma yang telah dirancang.

Data Set Penelitian https://github.com/wmk567/steganografi_video

Alat dan Bahan Penelitian

Penelitian ini menggunakan perangkat keras berupa komputer dengan spesifikasi minimal prosesor Intel i5, RAM 8 GB, dan sistem operasi Windows/Linux. Sedangkan perangkat lunak yang digunakan meliputi:

a. Bahasa Pemrograman Python atau MATLAB untuk implementasi algoritma.
b. OpenCV untuk pengolahan video dan ekstraksi *frame*.
c. NumPy dan Matplotlib untuk analisis numerik dan visualisasi data hasil eksperimen.

Selain itu, digunakan library tambahan untuk menghitung nilai PSNR dan SSIM sebagai parameter evaluasi.

Tahapan Penelitian

Analisis dan Perancangan Algoritma

Pada tahap ini dilakukan studi literatur terhadap metode LSB konvensional serta identifikasi kelemahannya. Berdasarkan hasil analisis, dirancang algoritma baru Steganografi Video Adaptif Berbasis *Multi-Bit LSB* dengan mempertimbangkan tiga parameter utama yaitu kecerahan, tekstur, dan gerakan *frame*.

Ekstraksi Frame Video

Video yang digunakan dipecah menjadi beberapa *frame* menggunakan teknik ekstraksi. Setiap *frame* kemudian dianalisis untuk menentukan area yang sesuai sebagai lokasi penyisipan data.

Analisis Karakteristik Frame

Setiap frame dianalisis berdasarkan kecerahan *(brightness)*, kompleksitas tekstur, dan tingkat pergerakan antar frame *(motion)*. Nilai dari hasil analisis tersebut akan menjadi dasar dalam menentukan jumlah *bit* yang digunakan untuk penyisipan data.

Proses Embedding (Penyisipan Data)

Data rahasia disisipkan ke dalam *frame* video dengan jumlah *bit* yang berbeda sesuai hasil analisis adaptif. Area dengan tekstur tinggi dan banyak pergerakan menggunakan *bit* lebih banyak, sedangkan area dengan tekstur halus menggunakan *bit* lebih sedikit.

Rekonstruksi Video Steganografi

Setelah seluruh *frame* disisipkan data, video hasil steganografi direkonstruksi kembali ke dalam format semula.

Proses Ekstraksi dan Evaluasi

Tahap ini dilakukan untuk menguji keberhasilan algoritma dalam mengekstraksi kembali data rahasia dari video hasil steganografi serta mengevaluasi kualitas visualnya menggunakan nilai PSNR dan SSIM.

Parameter Pengujian

PSNR (Peak Signal-to-Noise Ratio)

PSNR (*Peak Signal-to-Noise Ratio*) digunakan untuk mengukur tingkat distorsi antara video asli dan hasil steganografi. Nilai PSNR yang tinggi menunjukkan kualitas video yang baik. (Ilham Fauzi, 2025)

SSIM (Structural Similarity Index Measurement)

SSIM (*Structural Similarity Index Measurement*) digunakan untuk menilai tingkat kesamaan struktur visual antara video asli dan hasil steganografi. Nilai SSIM yang mendekati 1 menunjukkan bahwa struktur visual video tetap terjaga. (Muhammad Khozin, 2025)

Analisis Data

Data hasil eksperimen dianalisis dengan membandingkan nilai PSNR dan SSIM dari tiga metode: 1 *Bit LSB*, 3 *Bit LSB*, dan Metode Adaptif *Multi-Bit LSB*. Hasil perbandingan tersebut digunakan untuk menentukan tingkat efisiensi dan ketahanan metode yang diusulkan terhadap kompresi dan *noise*. Analisis dilakukan secara deskriptif kuantitatif untuk menilai keunggulan metode baru berdasarkan keseimbangan antara kualitas visual dan kapasitas penyisipan data. (Juriko Abdussamad, 2024)

3. HASIL DAN PEMBAHASAN

Hasil Pengujian Sistem

Penelitian ini melakukan pengujian terhadap tiga metode steganografi video, yaitu 1 Bit LSB**,** 3 Bit LSB**,** dan Metode *Multi-Bit LSB* Adaptif yang diusulkan. Video uji menggunakan resolusi 720p dengan format MP4 berdurasi 10 detik. Data rahasia berupa file

teks berukuran 50 KB disisipkan ke dalam video menggunakan algoritma masing-masing metode.

Tabel 1. Hasil Perbandingan Nilai PNSR dan SSIM.

Metode Steganografi	PSNR (dB)	SSIM
1 *Bit LSB*	49.32	0.9712
3 *Bit LSB*	39.41	0.8817
Multi-Bit LSB Adaptif	45.86	0.9441

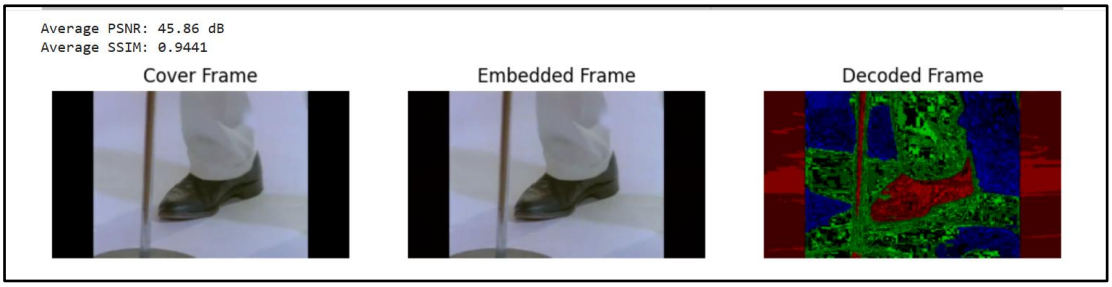
Berdasarkan hasil tersebut, metode *Multi-Bit LSB* Adaptif menghasilkan nilai PSNR dan SSIM yang lebih seimbang antara kualitas visual dan kapasitas penyisipan. Meskipun sedikit menurun dari metode 1 *Bit*, namun peningkatan enskripsi mencapai hasil yang lebih baik dibandingkan metode 1 *Bit*, serta kualitas visual jauh lebih baik dibandingkan metode 3 *Bit*.

Analisis Visual Kualitas Video

Analisis visual dilakukan untuk membandingkan kualitas *frame* video sebelum dan sesudah proses penyisipan data. Berdasarkan hasil pengamatan, *cover frame* dan *embedded frame* menunjukkan tampilan visual yang hampir identik, sehingga perubahan bit pada frame tidak menimbulkan distorsi yang dapat terlihat oleh mata manusia. Hal ini menunjukkan bahwa metode *Multi-Bit LSB* adaptif mampu mempertahankan kualitas visual video dengan baik.

Sementara itu, *decoded frame* digunakan untuk menampilkan perbedaan struktur piksel akibat proses *embedding*. Visualisasi ini menunjukkan area yang mengalami perubahan, terutama pada bagian yang memiliki tekstur kompleks dan pergerakan tinggi. Perbedaan tersebut hanya terlihat melalui teknik *decoding* dan tidak tampak pada tampilan video biasa.

Secara visual, hasil video steganografi adaptif menunjukkan bahwa perbedaan antara video asli dan hasil steganografi hampir tidak terlihat oleh mata manusia. Hal ini karena algoritma adaptif mampu menyesuaikan jumlah *bit* yang digunakan berdasarkan karakteristik lokal *frame*. Area dengan tekstur tinggi dan pergerakan cepat menggunakan *bit* lebih banyak, sedangkan area statis dan halus menggunakan *bit* lebih sedikit.



Gambar 1. Perbandingan Cuplikan Frame Antara Video Asli dan Hasil Steganografi Adaptif.

Pembahasan

Hasil pengujian menunjukkan bahwa metode Steganografi Video Adaptif Berbasis *Multi-Bit LSB* memiliki kinerja yang lebih unggul dibandingkan metode LSB konvensional. Keunggulan tersebut terlihat pada tiga aspek utama, yaitu efisiensi kapasitas penyisipan**,** kualitas visual**,** dan ketahanan terhadap kompresi maupun noise**.**

Dari aspek kualitas visual**,** nilai PSNR sebesar 45,86 dB dan SSIM sebesar 0,9441 menunjukkan bahwa video hasil steganografi memiliki kesamaan struktur yang sangat tinggi dengan video asli. Nilai ini menggambarkan bahwa perubahan yang terjadi pada piksel bersifat minimal dan tidak dapat dibedakan oleh mata manusia. Analisis *visual frame* juga menunjukkan bahwa tampilan *embedded frame* tetap identik dengan *cover frame* tanpa munculnya distorsi atau artefak yang mengganggu. Hal ini menunjukkan bahwa mekanisme adaptif mampu memilih area yang tepat untuk penyisipan data sehingga kualitas visual tetap terjaga.

Pada aspek kapasitas penyisipan, metode adaptif memberikan peningkatan kapasitas dibandingkan metode 1 *Bit LSB*. Peningkatan ini dicapai melalui proses analisis terhadap kecerahan, tekstur, dan gerakan pada setiap *frame*. Area dengan tekstur kompleks atau pergerakan tinggi mampu menampung *bit* penyisipan lebih banyak tanpa menurunkan kualitas visual. Sebaliknya, area halus atau statis hanya diberikan sedikit *bit* untuk menghindari distorsi. Pendekatan adaptif ini menghasilkan keseimbangan yang tidak dapat dicapai oleh metode konvensional yang menggunakan jumlah *bit* tetap pada semua piksel.

Metode konvensional menunjukkan performa yang lebih rendah, sehingga dapat disimpulkan bahwa metode adaptif lebih mampu mempertahankan integritas data rahasia meskipun video mengalami proses penyimpanan ulang atau gangguan selama transmisi. Kemampuan ini diperoleh dari cara algoritma menempatkan *bit* penyisipan pada area yang lebih stabil secara statistik.

Secara keseluruhan, metode yang dikembangkan dalam penelitian ini berhasil menggabungkan tiga parameter utama ,kecerahan, tekstur, dan gerakan untuk menentukan jumlah *bit* yang optimal pada setiap area *frame*. Pendekatan ini memberikan peningkatan kualitas, kapasitas, dan ketahanan secara simultan. Dengan hasil tersebut, metode adaptif ini memiliki potensi besar untuk digunakan dalam berbagai aplikasi keamanan informasi berbasis multimedia, termasuk pengiriman video rahasia, penyisipan *watermark*, dan sistem komunikasi yang membutuhkan perlindungan data tingkat tinggi. Keunggulan dalam menghadapi kompresi dan *noise* juga menjadikan metode ini cocok untuk *platform* berbasis internet yang menggunakan proses *transcoding* otomatis.

4. KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa metode Steganografi Video Adaptif Berbasis *Multi-Bit LSB* dengan analisis kecerahan, tekstur, dan gerakan *frame* mampu meningkatkan efisiensi penyisipan data tanpa mengorbankan kualitas visual video secara signifikan. Nilai PSNR sebesar 45,86 dB dan SSIM sebesar 0,9441 menunjukkan bahwa kualitas visual video hasil steganografi tetap tinggi dan hampir tidak dapat dibedakan dari video asli. Dengan demikian, metode Steganografi Video Berbasis *Multi-Bit LSB* ini terbukti lebih efisien, tangguh, dan mampu menjaga keamanan data dalam media video. Metode ini juga potensial untuk diterapkan pada berbagai sistem keamanan informasi berbasis multimedia yang memerlukan perlindungan data secara tersembunyi dan dinamis.

Saran

Optimasi waktu komputasi perlu dilakukan agar proses analisis dan penyisipan data dapat berjalan lebih cepat tanpa menurunkan akurasi analisis *frame*. Pengembangan algoritma dapat diarahkan untuk format video beresolusi tinggi (Full HD atau 4K) agar dapat menguji skalabilitas metode adaptif terhadap ukuran data yang lebih besar. Dapat dilakukan integrasi dengan teknik enkripsi tambahan sebelum proses penyisipan untuk meningkatkan tingkat keamanan ganda. Pengujian lanjutan disarankan dengan beragam jenis *noise* dan metode kompresi agar performa metode dapat dinilai lebih menyeluruh terhadap kondisi nyata. Perlu dikembangkan versi *real-time embedding*, sehingga metode ini dapat diterapkan langsung pada sistem komunikasi video *streaming* yang aman.

DAFTAR REFERENSI

A.E. Ibrahim, M. E. (2016). Video Stegonography UsingLeast Significant BIT In Frequency Domain. *International Journal of Intelligent Computing and*.

Berlian, A. A. (2024). Penambahan Kode Bit Ringan untuk Menyisipkan Informasi pada File Suara. *Jurnal Informatika Press*.

Harjoko2, M. Y. (2014). Penyembunyian Data pada File Video Menggunakan Metode LSB dan DCT . *Indonesian Journal Of Computing and Cybernetic System*, 81-90.

Ilham Fauzi, M. K. (2025). Analisis Perbandingan Kapasitas Penyisipan Data dan Kualitas Citra Dalam Teknik Steganografi LSB dan MSB Menggunakan Peak to Signal to Noise Ratio dan Mean Squared Error. *Jurnal Ilmu Komputer dan Sistem Informasi*.

Jayakanth Kunhoth, N. S.-M. (2023). *Video Steganography: Recent Advances and Challenges.* Multimedia Tools and Applications.

Juriko Abdussamad, I. S. (2024). *Metode Penelitian Kuantitatif, kualititatif, dan Mixed Methode.* Medan: PT Media Penerbit Indonesia.

Malese, L. P. (2021). Penyembunyian Pesan Rahasia Pada Citra Digital dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB). *Jurnal Ilmiah Wahana Pendidikan*.

Muhammad Khozin, D. N. (2025). Peningkatan Keamanan Steganografi Citra Berbasis Least Significant Bit dengan Integrasi Algoritma Deep Learning Convolutional Neural Network (CNN). *Jurnal Surya Informatika*.

Muhammad Turmudzi, A. W. (2025). *Jaringan Multimedia Menguasai Ekosistem Multimedia Produksi Konten, Distribusi Jaringan, dan Aplikasi Industri.* Penerbit Ilmu Literasi dan Riset (Pilar).

Rapina, I. F. (2025). Analisis Risiko Keamanan Data Pribadi Pada Penggunaan Media Sosial Instagram Dengan Menggunakan Metode DREAD. *JurnalSains, Nalar, dan Aplikasi Teknologi Informasi*, 149-156.

Setyaningsih, E. (2023). Perkembangan Multimedia Digital dan Pembelajaran. *Indonesian Journal of Learning and Instructional Innovatio*, 24-34.

Syifaur Rizqa Rahmatillah1), M. T. (2024). STEGANOGRAFI:KEAMANANDATADENGANMETODELEASTSIGNIFICANT BITMENGGUNAKANPYTHON. *JURSISTEKNI(JurnalSistemInformasidanTeknologiInformasi)*, 439-447.

Tuan Duc Nguyen, S. A.-i.-i. (2015). *An adaptive multi bit-plane image steganography using block data-hiding.* Multimedia Tools and Applications.

Ulan Ari Anti 1), A. H. (2017). STEGANOGRAFI PADA VIDEO MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN END OF FILE (EOF). *Jurnal Informatika Mulawarman* , 104-110.

Wulandari, I. W. (2023). PERAN SISTEM INFORMASI AKUNTANSI DALAMPENGAPLIKASIAN ENKRIPSI TERHADAPPENINGKATAN KEAMANAN PERUSAHAAN. *Jkpim:Jurnal Kajian dan Penalaran IlmuManajemen*, 11-25.