JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 3 Juni 2026, Page 292-298
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Penerapan Steganografi Video Menggunakan Algoritma Least Significant Bit (LSB) dan AES untuk Keamanan Data

Muhammad Hafiz[1], Yudi Prayudi[2]

[1,2)]Informatika, Universitas Islam Indonesia, Yogyakarta, Indonesia

Email: [1]21523228@students.uii.ac.id, [2]prayudi@uii.ac.id
Email Penulis Korespondensi: [1]21523228@students.uii.ac.id

Abstrak−Penerapan metode steganografi dan kriptografi pada media video menjadi salah satu pendekatan yang semakin relevan dalam upaya memperkuat perlindungan data di tengah meningkatnya ancaman terhadap keamanan informasi. Kombinasi algoritma Least Significant Bit (LSB) untuk penyembunyian pesan dan Advanced Encryption Standard (AES) untuk enkripsi memberikan mekanisme perlindungan berlapis, di mana pesan tidak hanya disisipkan secara tidak terlihat, tetapi juga diamankan melalui proses kriptografi yang kuat. Prosedur pengembangan sistem meliputi ekstraksi frame video, enkripsi pesan, penyisipan bit terenkripsi ke dalam frame menggunakan teknik LSB, hingga rekonstruksi ulang video hasil steganografi. Evaluasi kinerja dilakukan melalui pengukuran Peak Signal-to-Noise Ratio (PSNR) untuk menilai sejauh mana kualitas video tetap terjaga setelah proses penyisipan. Hasil pengujian menunjukkan bahwa metode yang diusulkan mampu mempertahankan kualitas visual video dengan nilai PSNR berkisar antara 51.25 dB hingga 56.11 dB pada berbagai resolusi video yang diuji. Sistem juga mampu menyisipkan pesan dengan kapasitas hingga 30 MB tanpa menyebabkan penurunan kualitas visual yang signifikan. Selain itu, proses ekstraksi pesan dari video steganografi berhasil dilakukan kembali secara utuh dengan tingkat keberhasilan 100%. Berdasarkan hasil tersebut, kombinasi algoritma LSB dan AES terbukti mampu meningkatkan keamanan data pada media video tanpa menurunkan kualitas visual secara signifikan.

Kata Kunci: Steganografi Video, Least Significant Bit (Lsb), Advanced Encryption Standard (Aes), Keamanan Data, Penyisipan Pesan, Psnr

Abstract−The application of steganography and cryptography methods in video media has become an increasingly relevant approach to strengthening data protection amid the growing threats to information security. The combination of the Least Significant Bit (LSB) algorithm for message embedding and the Advanced Encryption Standard (AES) for encryption provides a layered security mechanism, where messages are not only hidden invisibly but also protected through a strong cryptographic process. The system development procedure includes video frame extraction, message encryption, embedding encrypted bits into frames using the LSB technique, and reconstructing the steganographic video. Performance evaluation is conducted by measuring the Peak Signal-to-Noise Ratio (PSNR) to assess the extent to which video quality is maintained after the embedding process. The experimental results show that the proposed method is able to preserve the visual quality of the video with PSNR values ranging from 51.25 dB to 56.11 dB across various tested video resolutions. The system is also capable of embedding messages with a capacity of up to 30 MB without causing significant visual quality degradation. In addition, the extraction process successfully retrieves the hidden message from the steganographic video with a 100% success rate. Based on these results, the combination of the LSB and AES algorithms is proven to enhance data security in video media without significantly affecting visual quality.

Keywords: Video Steganography, Least Significant Bit (LSB), Advanced Encryption Standard (AES), Data Security, Message Embedding, PSNR.

1. PENDAHULUAN

Keamanan informasi menjadi kebutuhan yang semakin fundamental di era digital yang serba terbuka dan terhubung. Perkembangan teknologi komunikasi yang begitu cepat membawa dampak positif dalam mempermudah pertukaran data, namun juga meningkatkan risiko seperti pencurian data, penyadapan, manipulasi informasi, hingga serangan siber yang semakin canggih. Informasi rahasia atau data yang memiliki nilai strategis kini membutuhkan perlindungan berlapis agar tidak mudah diakses, dimodifikasi, atau dimanfaatkan oleh pihak yang tidak berwenang. Karena itulah, berbagai pendekatan keamanan terus dikembangkan untuk menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi, baik selama proses transmisi maupun penyimpanan.

Dua pendekatan penting yang sering dimanfaatkan dalam mengamankan data adalah kriptografi dan steganografi. Kriptografi berfungsi mengacak isi pesan melalui proses enkripsi sehingga tidak dapat dipahami tanpa kunci dekripsi yang benar[1]. Metode ini sangat efektif dalam mengamankan makna atau isi pesan. Sementara itu, steganografi bekerja berbeda karena berfokus menyembunyikan keberadaan pesan tersebut dengan menyisipkannya ke dalam media seperti citra, audio, atau video[2][3]. Tujuannya bukan hanya membuat pesan tidak dapat dibaca, tetapi juga tidak terdeteksi keberadaannya. Kombinasi keduanya menghasilkan sistem keamanan berlapis: meski pesan berhasil ditemukan, isinya tetap sulit diungkap karena telah terenkripsi terlebih dahulu.

Penelitian sebelumnya menunjukkan efektivitas metode Least Significant Bit (LSB) dalam menyisipkan pesan ke dalam citra dengan tingkat distorsi visual yang sangat rendah [4][5]. Ada pula penelitian yang mengombinasikan LSB dengan algoritma kriptografi seperti RSA, di mana pesan dienkripsi terlebih dahulu sebelum disisipkan [6][7]. Kombinasi ini terbukti meningkatkan keamanan keseluruhan, karena ciphertext yang memiliki pola acak membuat penyisipan

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/10/2025**; Accepted: **29/04/2026**; Published: **16/06/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 3 Juni 2026, Page 292-298
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

menjadi lebih sulit dianalisis. Penelitian lain turut mengeksplorasi steganografi video, misalnya menggunakan pendekatan End of Frame (EOF) yang dikombinasikan dengan algoritma rijndael [8]. Berbagai studi tersebut memberi fondasi kuat bahwa penggabungan steganografi dan kriptografi mampu meningkatkan proteksi data secara signifikan.

Meskipun berbagai penelitian tersebut menunjukkan keberhasilan dalam menggabungkan teknik steganografi dan kriptografi, sebagian besar penelitian masih berfokus pada media citra statis atau hanya memanfaatkan sebagian kecil frame pada media video. Selain itu, pemanfaatan metode enkripsi modern seperti Advanced Encryption Standard (AES) pada skema steganografi video masih belum banyak dieksplorasi secara komprehensif. Oleh karena itu, diperlukan penelitian lebih lanjut yang memanfaatkan media video secara lebih optimal dengan mengombinasikan teknik penyisipan data dan mekanisme enkripsi yang kuat.

Video digital menjadi media yang sangat menarik untuk penelitian steganografi. Ukurannya yang besar, jumlah frame yang banyak, serta sifat redudansi informasi membuat video memiliki kapasitas penyisipan yang jauh lebih besar dibanding citra statis. Perubahan kecil pada sebagian frame video umumnya tidak mencolok, sehingga teknik steganografi dapat bekerja dengan efektif tanpa menurunkan kualitas visual secara signifikan. Hal ini menjadikan video sebagai media yang potensial untuk menampung pesan rahasia baik dalam jumlah kecil maupun besar, sekaligus mengurangi risiko deteksi.

Selain itu, steganografi di video pada dasarnya sangat mirip dengan steganografi pada gambar, hanya saja proses penyisipan dilakukan pada rangkaian frame yang membentuk video. Dengan kata lain, informasi rahasia tidak lagi ditanam pada satu citra, tetapi dapat disebar ke setiap frame video sehingga kapasitas data dan fleksibilitas embedding menjadi lebih besar. Namun, meskipun potensi video lebih tinggi dibanding gambar, sebagian besar penelitian sebelumnya masih memanfaatkan pendekatan sederhana, seperti hanya menyisipkan pesan pada satu frame atau beberapa frame saja. Bahkan dalam penelitian yang menggabungkan AES dan Rijndael pun, penyisipan umumnya dilakukan pada frame tertentu tanpa memanfaatkan keseluruhan struktur video[9].

Metode LSB menjadi salah satu teknik yang paling populer dalam domain spasial karena implementasinya sederhana dan memiliki performa yang baik[10]. LSB bekerja dengan mengganti bit paling tidak signifikan pada pixel atau frame video dengan bit-bit pesan. Perubahan ini sangat kecil sehingga tidak mengganggu tampilan visual. Meski begitu, LSB memiliki kelemahan karena relatif mudah dianalisis melalui teknik statistik seperti histogram analysis, chi-square attack, maupun steganalisis modern lainnya[11]. Tanpa lapisan keamanan tambahan, pesan yang disisipkan melalui LSB bisa berisiko dibongkar.

Karena itu diperlukan mekanisme pengamanan tambahan berupa enkripsi. Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris modern yang dikenal sangat kuat dan efisien[12][13]. Algoritma ini memanfaatkan struktur putaran kompleks dan prinsip substitusi–permutasi yang membuat proses pemecahan kunci menjadi sangat sulit. AES banyak digunakan dalam berbagai platform keamanan digital, mulai dari enkripsi data pada smartphone hingga perlindungan komunikasi jaringan. Ketika pesan dienkripsi menggunakan AES sebelum disisipkan dengan LSB, ciphertext yang dihasilkan memiliki distribusi bit acak sehingga lebih sulit dianalisis dan dideteksi.

Penggabungan LSB dan AES menawarkan pendekatan hybrid yang kuat. LSB membuat pesan tersembunyi di dalam video, sedangkan AES memastikan isi pesan tetap aman. Kombinasi ini tidak hanya menyulitkan proses deteksi, tetapi juga melindungi pesan apabila terjadi ekstraksi paksa. Pendekatan ini sangat relevan digunakan pada berbagai skenario, seperti komunikasi rahasia, pertukaran dokumen penting, keamanan multimedia, hingga perlindungan hak cipta.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan menerapkan steganografi video menggunakan metode LSB yang dikombinasikan dengan enkripsi AES. Fokus penelitian mencakup evaluasi kapasitas penyisipan, kualitas visual stego-video, dan tingkat keamanan pesan. Harapannya, metode hybrid ini dapat memberikan kontribusi nyata dalam pengembangan teknik pengamanan data yang lebih kuat, efisien, dan mudah diterapkan pada kebutuhan keamanan informasi modern.

2. METODOLOGI PENELITIAN

Penelitian ini tergolong dalam kategori eksperimen terapan karena berfokus langsung pada penerapan metode steganografi dan kriptografi pada media video untuk mendukung keamanan data. Pendekatan eksperimen dipilih karena penelitian ini melibatkan proses penyisipan pesan ke dalam video secara nyata dan menilai hasilnya melalui berbagai parameter kuantitatif. Pengujian mencakup kualitas visual stego-video, keberhasilan ekstraksi pesan, waktu eksekusi proses, serta efektivitas mekanisme perlindungan data yang dihasilkan. Selain itu, penelitian ini juga mengevaluasi kapasitas panjang pesan yang dapat disisipkan ke dalam video, karena ukuran pesan memengaruhi kualitas visual, pola embedding, serta efisiensi dan keamanan sistem. Dengan demikian, penelitian tidak hanya menilai apakah proses penyisipan berhasil, tetapi juga menentukan batas optimal panjang pesan yang dapat ditampung tanpa menimbulkan degradasi kualitas maupun peningkatan risiko deteksi. Studi ini juga berada dalam ranah rekayasa perangkat lunak karena menghasilkan rancangan dan implementasi sistem steganografi–kriptografi berbasis kombinasi algoritma LSB dan AES.

Tahapan penelitian disusun secara sistematis, dimulai dari pengumpulan data berupa video yang digunakan sebagai media penampung, kemudian dilanjutkan dengan penerapan algoritma AES untuk proses enkripsi pesan, implementasi algoritma LSB sebagai metode penyisipan, hingga tahap pengujian dan evaluasi sistem. Seluruh hasil dari rangkaian proses tersebut dianalisis untuk menilai performa dan efektivitas metode yang diterapkan secara keseluruhan.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/10/2025**; Accepted: **29/04/2026**; Published: **16/06/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 3 Juni 2026, Page 292-298
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Pengujian sistem dilakukan pada perangkat komputer dengan prosesor Intel Core i7, RAM sebesar XX GB, serta GPU Intel Iris Xe Graphics. Sistem diimplementasikan menggunakan bahasa pemrograman Python versi 3.13.7 dengan memanfaatkan pustaka OpenCV untuk pengolahan citra dan FFmpeg untuk pemrosesan video.

2.1 Pengumpulan Data

Data yang digunakan dalam penelitian ini berupa video digital yang berfungsi sebagai media penampung (cover) untuk proses penyisipan pesan. Video yang digunakan memiliki format MP4 dengan codec H.264 berdurasi 2 detik. Pemilihan video dilakukan dengan mempertimbangkan kualitas visual serta variasi resolusi yaitu 144p, 240p, 360p, 480p, hingga 720p, dimana resolusi 144p hingga 480p memiliki fps sebesar 30 dan 720p memiliki fps sebesar 60, guna memungkinkan evaluasi kapasitas embedding dan kinerja metode pada berbagai tingkat ketajaman. Adapun pesan rahasia yang disisipkan berupa data teks.

2.2 Penerapan Algoritma AES

Sebelum pesan disisipkan ke dalam video, data teks rahasia terlebih dahulu diamankan melalui proses enkripsi menggunakan algoritma AES (Advanced Encryption Standard). Pada penelitian ini digunakan AES-256 dalam mode CBC, sebuah varian kriptografi simetris yang dikenal memiliki tingkat keamanan tinggi dan performa yang efisien untuk pengolahan data berukuran besar. Tahap ini memastikan bahwa teks asli diubah menjadi ciphertext, sehingga meskipun pesan berhasil diperoleh kembali dari stego-video, isinya tetap tidak dapat dipahami tanpa kunci dekripsi yang sesuai.

Proses enkripsi diawali dengan pembangkitan kunci 256-bit serta inisialisasi initialization vector (IV) yang diperlukan dalam mode CBC untuk menghasilkan pola enkripsi yang acak dan tidak repetitif. Setelah kunci dan IV terbentuk, AES menjalankan serangkaian transformasi kriptografis, yang terdiri dari AddRoundKey pada tahap awal, kemudian beberapa putaran utama yang mencakup operasi SubBytes, ShiftRows, MixColumns, serta AddRoundKey. Pada putaran akhir, AES kembali menjalankan SubBytes, ShiftRows, dan AddRoundKey tanpa MixColumns. Rangkaian proses ini mengubah teks asli menjadi ciphertext yang sama sekali tidak menyerupai data awal[12]. Ciphertext inilah yang kemudian digunakan sebagai input pada proses steganografi menggunakan metode LSB. Dengan demikian, data yang disisipkan ke dalam frame video tidak hanya tersembunyi secara visual, tetapi juga telah memperoleh perlindungan kriptografis berlapis berkat penggunaan AES-256-CBC.

2.3 Penerapan Algoritma LSB

Setelah data rahasia dienkripsi menggunakan AES, proses berlanjut pada tahap penyisipan ke dalam video menggunakan teknik Least Significant Bit (LSB). Pendekatan ini dipilih karena mampu menyisipkan data tanpa mengganggu kualitas visual secara berarti. Sebelum proses embedding dimulai, video dipisahkan terlebih dahulu dari audionya, kemudian bagian visual diuraikan menjadi rangkaian frame citra berformat RGB. Pemisahan ini dilakukan agar manipulasi hanya terjadi pada komponen visual tanpa mengubah struktur audio asli.

Ciphertext hasil enkripsi kemudian diubah ke dalam representasi biner sehingga siap untuk dimasukkan ke dalam nilai piksel. Setiap frame yang telah diekstrak menyediakan ruang penyisipan melalui tiga kanal warna—Red, Green, dan Blue. Ketiga kanal ini memungkinkan kapasitas embedding yang lebih besar karena tiap piksel memiliki tiga LSB yang dapat dimodifikasi secara bergantian. Prosesnya berjalan dengan mengganti bit paling rendah pada setiap kanal dengan bit-bit data rahasia secara berurutan. Pergantian ini hanya mengubah bagian terkecil dari nilai warna, sehingga tampilan frame tetap tampak sama bagi pengamat.

Ilustrasinya sederhana, bayangkan satu piksel memiliki tiga angka warna, misalnya R=10110010, G=11100101, dan B=10011000. Bit terakhir dari masing-masing nilai inilah yang diubah untuk menyimpan bagian kecil dari pesan terenkripsi[13]. Karena perubahan terjadi di posisi paling rendah, pergeseran warnanya sangat kecil dan hampir tidak mungkin dibedakan secara visual. Proses ini diulangi untuk setiap piksel dalam frame hingga bagian pesan yang dialokasikan untuk frame tersebut selesai disisipkan.

Setelah seluruh frame dimodifikasi, semuanya dirangkai kembali menjadi sebuah video baru yang kini membawa pesan rahasia di dalam struktur pikselnya. Tahap akhir adalah menggabungkan kembali video tersebut dengan audio asli, menghasilkan berkas video utuh yang tampak normal namun menyimpan informasi terenkripsi yang hanya dapat diambil melalui proses ekstraksi dengan metode LSB yang sama.

2.4 Pengujian dan Evaluasi

Setelah proses enkripsi dan penyisipan pesan selesai dilakukan, penelitian berlanjut pada tahap pengujian untuk menilai performa sistem secara menyeluruh. Evaluasi berfokus pada tiga aspek pokok, yaitu kapasitas penyisipan, kualitas visual stego-video, serta tingkat keamanan pesan. Kapasitas penyisipan dipahami melalui analisis seberapa banyak data dapat ditanamkan ke dalam video pada berbagai resolusi tanpa menimbulkan gangguan visual. Penilaian ini melibatkan pengamatan keterkaitan antara ukuran pesan, jumlah frame, serta total ruang bit yang tersedia pada ketiga kanal warna di setiap piksel. Dengan cara ini, batas optimal penyisipan dapat diketahui sehingga tidak mengorbankan kualitas tampilan.

Kualitas visual stego-video dievaluasi dengan membandingkan frame asli dan frame hasil penyisipan menggunakan dua parameter kuantitatif, yaitu Mean Squared Error (MSE) dan Peak Signal-to-Noise Ratio (PSNR). Nilai MSE dihitung menggunakan persamaan:

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: 19/10/2025; Accepted: 29/04/2026; Published: 16/06/2026

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 3 Juni 2026, Page 292-298
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left[I(i,j) - K(i,j) \right]^2 \quad (1)$$

$I(i,j)$ = nilai piksel pada frame asli
$K(i,j)$ = nilai piksel pada frame hasil steganografi
$M \, dan \, N$ = ukuran frame video

Dengan $I(i,j)$ sebagai nilai piksel pada frame asli dan $K(i,j)$ sebagai nilai piksel pada frame hasil embedding, sedangkan M dan N merupakan dimensi frame. Nilai ini menggambarkan rata-rata tingkat perbedaan kuadrat antar piksel semakin kecil MSE, semakin kecil perubahan visual yang terjadi. Nilai PSNR kemudian dihitung berdasarkan MSE melalui persamaan:

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

MAX = nilai maksimum intensitas piksel
MSE = nilai Mean Squared Error

Dengan MAX sebagai nilai maksimum intensitas piksel (misalnya 255 untuk citra 8-bit). PSNR memberikan indikasi seberapa baik kualitas visual dipertahankan setelah penyisipan; nilai PSNR yang tinggi menunjukkan bahwa video hasil embedding tetap sangat mirip dengan video asli. Kedua metrik ini memberikan gambaran objektif mengenai dampak modifikasi LSB terhadap tampilan akhir video.

Aspek keamanan pesan dinilai dari efektivitas algoritma AES-256-CBC dalam melindungi isi data yang disisipkan. Ciphertext yang tersimpan di dalam frame harus tetap tidak dapat dibaca tanpa kunci dekripsi yang valid. Dengan memastikan bahwa hasil ekstraksi tanpa kunci tetap berupa data tak bermakna, sistem menunjukkan bahwa ia tidak hanya menyembunyikan pesan melalui LSB, tetapi juga memberikan perlindungan kriptografis yang kuat. Melalui kombinasi pengujian tersebut, sistem dapat dievaluasi dari sisi daya tampung, ketajaman visual stego-video, hingga ketahanan pesan terhadap akses yang tidak sah.

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil eksperimen serta analisis menyeluruh mengenai kinerja sistem steganografi–kriptografi yang dikembangkan menggunakan kombinasi algoritma AES-256-CBC dan teknik penyisipan Least Significant Bit (LSB) pada media video digital. Seluruh tahapan uji yang dilakukan dirancang berdasarkan metodologi yang sebelumnya dijelaskan, yaitu evaluasi kapasitas penyisipan, kualitas visual setelah embedding, tingkat keamanan pesan, serta efisiensi waktu proses. Hasil-hasil eksperimen dianalisis secara kritis untuk memahami bagaimana rancangan sistem berperilaku saat menerima variasi resolusi video dan ukuran pesan yang beragam. Dengan demikian, pembahasan pada bagian ini tidak hanya menunjukkan keberhasilan penyisipan, tetapi juga menilai batas optimal sistem, pola perubahan kualitas visual, serta perilaku sistem terhadap tekanan beban data yang berbeda.

3.1 Hasil Pengujian Lengkap Sistem Steganografi–Kriptografi

Untuk memperoleh gambaran menyeluruh mengenai kinerja sistem, dilakukan serangkaian pengujian pada berbagai resolusi video dan panjang pesan yang berbeda. Setiap pengujian menghasilkan beberapa parameter penting, mulai dari kapasitas penyisipan, waktu enkripsi, waktu embedding, ukuran file stego, hingga nilai PSNR sebagai indikator kualitas visual. Selain itu, dicatat pula apakah proses penyisipan berhasil atau mengalami kegagalan ketika pesan melebihi kapasitas penyimpanan video. Tabel berikut menyajikan seluruh hasil pengujian secara lengkap dan menjadi dasar analisis pada subbagian-subbagian berikutnya.

Tabel 1. Hasil Pengujian

Resolusi	Kapasitas	Panjang Pesan	Status Penyisipan	Waktu Penyisipan	Keakuratan Pesan Setelah Ekstraksi	Ukuran Video Awal (KB)	Ukuran Video Akhir (KB)	PSNR
144p	829.440	300.000	Berhasil	7,87	100	140	1.990	54,24
	829.440	400.000	Berhasil	7,15	100	140	2.110	53

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/10/2025**; Accepted: **29/04/2026**; Published: **16/06/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 3 Juni 2026, Page 292-298
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Resolusi	Kapasitas	Panjang Pesan	Status Penyisipan	Waktu Penyisipan	Keakuratan Pesan Setelah Ekstraksi	Ukuran Video Awal (KB)	Ukuran Video Akhir (KB)	PSNR
	829.440	470.000	Berhasil	8,15	100	140	2.180	52,31
	829.440	600.000	Berhasil	9,56	100	140	2.310	51,25
	829.440	700.000	Gagal	-	-	-	-	-
240p	2.300.400	1.000.000	Berhasil	13,85	100	316	5.250	53,48
	2.300.400	1.300.000	Berhasil	16,3	100	316	5.570	52,35
	2.300.400	1.500.000	Berhasil	22,72	100	316	5.800	51,72
	2.300.400	2.000.000	Gagal	-	-	-	-	-
360p	5.184.000	2.500.000	Berhasil	29,74	100	595	11.100	53,03
	5.184.000	3.000.000	Berhasil	35,58	100	595	11.600	52,24
	5.184.000	4.000.000	Gagal	-	-	-	-	-
480p	9.223.200	4.000.000	Berhasil	50,88	100	884	18.500	53,5
	9.223.200	5.000.000	Berhasil	66,55	100	884	19.700	52,53
	9.223.200	6.000.000	Berhasil	71,26	100	884	20.900	51,74
	9.223.200	7.000.000	Gagal	-	-	-	-	-
720p	41.472.000	10.000.000	Berhasil	175,15	100	2210	67.300	56,11
	41.472.000	20.000.000	Berhasil	428,4	100	2210	81.900	53,08
	41.472.000	30.000.000	Berhasil	481,97	100	2210	94.500	51,31

3.2 Kapasitas Penyisipan Pesan pada Setiap Resolusi Video

Evaluasi kapasitas penyisipan dilakukan untuk mengetahui seberapa besar pesan terenkripsi dapat dimasukkan ke dalam video tanpa menimbulkan kegagalan embedding maupun gangguan visual yang signifikan. Kapasitas penyisipan secara langsung berkaitan dengan jumlah piksel dalam frame video—yang berarti resolusi video menjadi faktor yang sangat menentukan. Sesuai dengan pendekatan LSB yang memodifikasi bit paling rendah pada kanal R, G, dan B secara berurutan, semakin besar resolusi video maka semakin banyak ruang bit yang tersedia untuk menyimpan cipher hasil enkripsi AES.

Hasil pengujian kapasitas penyisipan maksimal tiap resolusi disajikan pada Tabel 2.

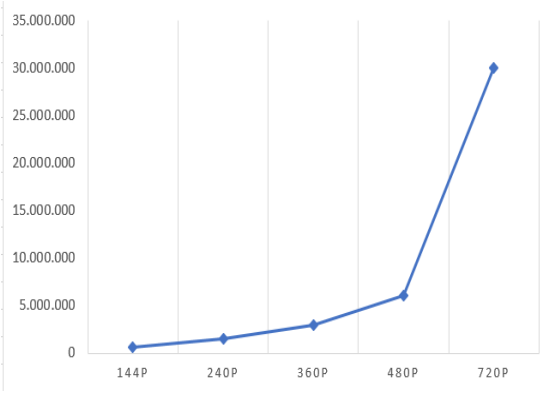
Tabel 2. Kapasitas Penyisipan Maksimum Tiap Resolusi

Resolusi	Kapasitas Video (Byte)	Maks. Pesan Berhasil (Byte)
144p	829.440	600.000
240p	2.300.400	1.500.000
360p	5.184.000	3.000.000
480p	9.223.200	6.000.000
720p	41.472.000	30.000.000

This is an open access article under the CC–BY-SA license

Submitted: **19/10/2025**; Accepted: **29/04/2026**; Published: **16/06/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 3 Juni 2026, Page 292-298
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin



Gambar 1. Grafik Kapasitas Penyisipan Pesan terhadap Resolusi Video

Dari hasil tersebut terlihat bahwa kapasitas penyisipan meningkat hampir sejalan dengan jumlah piksel yang dimiliki masing-masing resolusi. Pola ini sesuai dengan prediksi teoretis yang telah dibahas pada bagian metode, bahwa setiap piksel menyediakan tiga bit yang dapat dimodifikasi tanpa memberikan perubahan visual signifikan. Dengan demikian, video 144p yang mengandung 829.440 piksel hanya mampu menampung sekitar 600.000 byte ciphertext, sedangkan video 720p yang memiliki 41 juta piksel mampu menampung hingga 30.000.000 byte ciphertext.

Kegagalan embedding terjadi ketika ciphertext yang hendak dimasukkan melebihi batas kapasitas bit yang tersedia dalam video. Pada saat terjadi kegagalan, penyisipan tidak dapat dilanjutkan karena mekanisme LSB tidak dapat mengakomodasi bit tambahan tanpa menimpa data atau menyebabkan pergeseran struktur piksel. Kondisi ini menegaskan bahwa kapasitas penyisipan merupakan faktor kritis yang harus diperhitungkan ketika menentukan ukuran pesan yang akan dienkripsi dan disisipkan.

Temuan ini sejalan dengan penelitian sejenis yang menyatakan bahwa LSB sangat efektif dalam menyimpan data selama batas kapasitas piksel tidak dilampaui. Namun, berbeda dari citra statis, video memberikan keuntungan berupa jumlah frame yang umumnya lebih banyak, sehingga total kapasitas penyimpanan menjadi jauh lebih besar. Hal ini menjadikan video sebagai media yang ideal untuk menyisipkan pesan berukuran besar.

3.3 Analisis Kualitas Visual Stego-Video

Setelah pesan disisipkan, evaluasi dilanjutkan pada aspek kualitas visual. Parameter utama yang digunakan adalah Mean Squared Error (MSE) dan Peak Signal-to-Noise Ratio (PSNR), sesuai kerangka yang telah dijelaskan pada Metode Penelitian. Pengukuran MSE memberikan gambaran mengenai rata-rata perbedaan nilai piksel antara video asli dan stego-video, sedangkan PSNR menilai tingkat kemiripan visual antara keduanya.

Rentang nilai PSNR untuk setiap resolusi ditunjukkan pada Tabel 3.

Tabel 3. Rentang Nilai PSNR pada Berbagai Resolusi

Resolusi	Panjang Pesan (Byte)	PSNR (dB)
144p	300k – 600k	54.24 – 51.25
240p	1M – 1.5M	53.48 – 51.72
360p	2.5M – 3M	53.03 – 52.24
480p	4M – 6M	53.50 – 51.74
720p	10M – 30M	56.11 – 51.31

Seluruh nilai PSNR berada di atas 50 dB, yang berarti kualitas stego-video masih masuk kategori sangat baik dan perubahan visual tidak dapat dideteksi oleh manusia. Dalam literatur steganografi, nilai PSNR di atas 40 dB sudah dianggap sangat baik; oleh karena itu hasil ini berada jauh di atas batas minimal tersebut. Temuan ini menunjukkan bahwa modifikasi bit pada kanal RGB melalui teknik LSB bekerja sesuai ekspektasi: meskipun bit paling rendah diubah, pergeseran nilai warna yang terjadi sangat kecil dan tidak memengaruhi persepsi visual.

Dapat diamati bahwa semakin besar pesan yang disisipkan, nilai PSNR cenderung menurun. Namun penurunannya sangat moderat. Pada resolusi 720p, penyisipan pesan sebesar 30 juta byte masih mempertahankan PSNR sebesar 51.31 dB, yang berarti perubahan visual tetap tidak signifikan. Dengan demikian, metode LSB tetap dapat diandalkan untuk penyisipan pesan berukuran besar karena toleransi visual manusia terhadap perubahan bit rendah sangat tinggi.

Selain itu, penelitian ini juga menunjukkan bahwa nilai PSNR tidak hanya bergantung pada panjang pesan tetapi juga pada struktur distribusi bit dalam ciphertext. Karena ciphertext AES-256-CBC sangat acak, distribusi bitnya tidak memberikan pola tertentu yang dapat memengaruhi kanal gambar secara konsisten, sehingga penyisipan menjadi lebih aman dan tidak menciptakan pola visual abnormal.

This is an open access article under the CC–BY-SA license

Submitted: **19/10/2025**; Accepted: **29/04/2026**; Published: **16/06/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 3 Juni 2026, Page 292-298
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

3.4 Keamanan Pesan Melalui Enkripsi AES dan Integritas Ekstraksi

Aspek keamanan pesan adalah komponen penting dalam penelitian ini. Keamanan tidak hanya dipahami sebagai kemampuan menyembunyikan pesan secara visual (imperceptibility), tetapi juga memastikan bahwa isi pesan tetap terlindungi dari pihak yang tidak berwenang. Untuk itu, sebelum penyisipan dilakukan, pesan teks dienkripsi menggunakan AES-256-CBC sesuai prosedur yang dijelaskan pada bagian metode.

Keberhasilan ekstraksi ciphertext dari stego-video menjadi indikator integritas sistem. Hasil ekstraksi ditampilkan dalam Tabel 1. Seluruh penyisipan yang berstatus "berhasil" menunjukkan akurasi ekstraksi sebesar 100%, artinya setiap bit ciphertext yang dimasukkan dapat dikeluarkan kembali secara utuh tanpa kerusakan. Keberhasilan ekstraksi ini menandakan bahwa mekanisme LSB bekerja stabil dan tidak menyebabkan bit loss selama proses embedding maupun rekonstruksi frame menjadi video. Hal ini juga menunjukkan bahwa reassembly frame dan rejoining audio tidak memengaruhi data yang telah disisipkan.

Dari sisi kriptografi, AES-256-CBC memastikan bahwa pesan tetap aman meskipun seorang penyerang dapat memperoleh ciphertext dari stego-video. Tanpa kunci dan initialization vector (IV) yang sesuai, ciphertext tetap tidak bermakna. Hal ini memberi dua lapisan perlindungan yaitu pertama perlindungan visual melalui LSB, dan kedua perlindungan berbasis enkripsi melalui AES.

Kombinasi keduanya memberikan tingkat keamanan yang lebih tinggi dibandingkan menggunakan LSB tanpa enkripsi, karena ancaman berupa analisis statistik terhadap pola bit tidak lagi efektif saat ciphertext memiliki distribusi bit yang acak.

4. KESIMPULAN

Penelitian ini berhasil mengimplementasikan dan mengevaluasi sistem steganografi–kriptografi berbasis kombinasi algoritma AES-256-CBC dan teknik penyisipan Least Significant Bit (LSB) pada media video digital. Berdasarkan rangkaian eksperimen dan analisis yang telah dilakukan, beberapa kesimpulan utama dapat diambil sebagai berikut.

Pertama, metode LSB terbukti memiliki kemampuan penyisipan yang sangat bergantung pada resolusi video. Semakin tinggi resolusi, semakin besar kapasitas penyimpanan yang tersedia. Pengujian menunjukkan bahwa video 144p mampu menampung sekitar 600.000 byte ciphertext, sedangkan video 720p mampu menyisipkan hingga 30.000.000 byte sebelum terjadi kegagalan. Hal ini menegaskan bahwa pemanfaatan LSB pada kanal RGB memberikan ruang penyimpanan yang memadai untuk kebutuhan penyembunyian data berskala besar.

Kedua, kualitas visual stego-video tetap berada dalam kategori sangat baik pada seluruh variasi resolusi dan panjang pesan yang diuji. Nilai PSNR yang diperoleh selalu lebih dari 50 dB, yang menandakan bahwa perubahan visual akibat proses embedding bersifat imperceptible dan tidak dapat dibedakan oleh pengamat manusia. Dengan demikian, metode LSB terbukti efektif mempertahankan kualitas tampilan video meskipun digunakan untuk menyisipkan ciphertext berukuran besar.

Ketiga, kombinasi antara LSB dan AES-256-CBC memberikan tingkat keamanan yang tinggi terhadap pesan rahasia. Seluruh ciphertext yang disisipkan dapat diekstraksi kembali secara utuh dengan akurasi 100%, menandakan bahwa tidak ada kehilangan bit maupun kerusakan data selama proses embedding maupun rekonstruksi video. Sementara itu, mekanisme enkripsi AES menjamin bahwa pesan tetap terlindungi meskipun bit-bit embedding berhasil diidentifikasi pihak yang tidak berwenang, karena ciphertext tidak dapat dibaca tanpa kunci yang benar.

Secara keseluruhan, penelitian ini membuktikan bahwa pendekatan steganografi–kriptografi berbasis AES-256-CBC dan teknik LSB dapat memberikan performa yang sangat baik dari sisi kapasitas penyisipan, kualitas visual, integritas pesan, dan keamanan data. Metode ini dapat diterapkan secara efektif pada berbagai skenario komunikasi rahasia, perlindungan data, maupun penyimpanan pesan aman berbasis video digital.

Keberhasilan penelitian ini juga menegaskan pentingnya integrasi antara teknik kriptografi dan steganografi untuk menghasilkan sistem keamanan berlapis yang lebih kuat dan sulit dideteksi.

REFERENCES

[1] M. Minarni, A. Ikram, I. Warman, and G. Y. Swara, "Implementasi Algoritma Vigenere Cipher Dan End Of File Pada Steganografi Video," *J. Minfo Polgan*, 2023, [Online]. Available: https://www.jurnal.polgan.ac.id/index.php/jmp/article/view/12418.

[2] M. N. Al Jumah and S. Sarimuddin, "Implementasi Steganografi Metode Least Significant Bit (LSB) untuk Menyembunyikan File Pesan dalam Gambar," *J. Inform. ...*, 2024, [Online]. Available: https://publikasiilmiah.unwahas.ac.id/JINRPL/article/view/10143.

[3] J. Jurnal, "Teknik Steganography untuk Menyisipkan Pesan pada Sebuah Citra Menggunakan Metode Least Significant Bit (LSB)," 2022, *academia.edu*. [Online]. Available: https://www.academia.edu/download/91000692/pdf.pdf.

[4] M. Yunus and A. Harjoko, "Penyembunyian Data pada File Video Menggunakan Metode LSB dan DCT," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 8, no. 1, p. 81, 2014, doi: 10.22146/ijccs.3498.

[5] L. P. Malese, "Penyembunyian Pesan Rahasia Pada Citra Digital dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB)," *J. Ilm. Wahana Pendidik.*, 2021, [Online]. Available: http://jurnal.peneliti.net/index.php/JIWP/article/view/976.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/10/2025**; Accepted: **29/04/2026**; Published: **16/06/2026**

[6] L. A. Fitriani, "Analisa Keamanan Data Teks Dengan Menerapkan Kriptografi RSA Dan Steganografi LSB," 2020, *download.garuda.kemdikbud.go.id*. [Online]. Available: http://download.garuda.kemdikbud.go.id/article.php?article=1604485&val=18036&title=Analisa Keamanan Data Teks Dengan Menerapkan Kriptografi RSA Dan Steganografi LSB.

[7] M. Agus, "Analisis Pengaruh Citra Terhadap Kombinasi Kriptografi RSA dan STEGANOGRAFi LSB," 2022, *pdfs.semanticscholar.org*. [Online]. Available: https://pdfs.semanticscholar.org/fc3a/27fbc166749f66321b7294507e004951d85d.pdf.

[8] I. Riadi, S. Sunardi, and D. Aryanto, "Algoritma End of File dan Rijndael pada Steganografi Video," *JRST (Jurnal Ris. Sains ...*, 2021, [Online]. Available: https://jurnalnasional.ump.ac.id/index.php/JRST/article/view/9187.

[9] I. Riadi, S. Sunardi, and D. Aryanto, "Steganografi Video Digital dengan Algoritma LSB (Least Significant Bit) dan Rijndael," 2020, *download.garuda.kemdikbud.go.id*. [Online]. Available: http://download.garuda.kemdikbud.go.id/article.php?article=2070624&val=18481&title=Steganografi Video Digital dengan Algoritma LSB Least Significant Bit dan Rijndael.

[10] A. P. Ratnasari and F. A. Dwiyanto, "Metode steganografi citra digital," 2020, *academia.edu*. [Online]. Available: https://www.academia.edu/download/108503079/pdf.pdf.

[11] A. Syaima'Fadel, R. D. Saputra, Y. Fatma, and ..., "Analisis keamanan steganografi teks dengan metode lsb (least significant bit) pada citra digital," *... (Computer Sci. ...*, 2024, [Online]. Available: https://ejurnal.umri.ac.id/index.php/coscitech/article/view/6759.

[12] E. Nirmala, "Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) Dan Algoritma Kriptografi Advanced Encryption Standard (AES)," 2020, *academia.edu*. [Online]. Available: https://www.academia.edu/download/72551649/pdf.pdf.

[13] F. Set, C. M. N. Bana, M. A. Anunut, and ..., "Penerapan Steganografi LSB dan Enkripsi AES untuk Keamanan Data Rahasia pada Gambar Digital," *Blantika ...*, 2025, [Online]. Available: https://blantika.publikasiku.id/index.php/bl/article/view/382.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **19/10/2025**; Accepted: **29/04/2026**; Published: **16/06/2026**