

Integrasi Steganografi LSB dan Enkripsi ROT13 untuk Penyisipan Pesan Teks pada Video Digital

Robby Aldi Suseno¹, Firahmi Rizky²

^{1,2}Program Studi Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara, Indonesia
Email: robbyaldi51@gmail.com; firahmirizky@umsu.ac.id

ABSTRAK

Perkembangan distribusi data digital melalui media video meningkatkan kebutuhan terhadap sistem keamanan informasi yang mampu melindungi pesan rahasia secara efektif. Penelitian ini bertujuan mengembangkan aplikasi penyisipan teks pada video menggunakan kombinasi metode *Least Significant Bit* (LSB) dan algoritma ROT13 serta mengevaluasi efektivitasnya dalam menjaga kerahasiaan pesan. Metode LSB digunakan untuk menyisipkan data teks terenkripsi ke dalam frame video dengan memodifikasi bit paling rendah piksel, sedangkan ROT13 berfungsi sebagai lapisan enkripsi awal sebelum proses penyisipan. Penelitian menggunakan pendekatan rekayasa sistem dengan tahapan analisis kebutuhan, perancangan sistem berbasis UML, implementasi aplikasi berbasis web, dan pengujian *black box*. Hasil pengujian menunjukkan bahwa aplikasi mampu menyisipkan dan mengekstrak pesan dengan akurasi tinggi tanpa menimbulkan perubahan visual signifikan pada video. Video hasil penyisipan tetap dapat diputar normal meskipun ukuran berkas meningkat. Integrasi metode steganografi dan kriptografi menghasilkan mekanisme keamanan berlapis yang meningkatkan kerahasiaan data. Temuan ini menunjukkan bahwa sistem yang dikembangkan efektif, ringan secara komputasi, dan berpotensi digunakan sebagai solusi praktis pengamanan informasi digital berbasis multimedia.

Kata Kunci: Steganografi; LSB; ROT13; Keamanan Data; Video Digital

ABSTRACT

The development of digital data distribution through video media increases the need for an information security system capable of effectively protecting confidential messages. This study aims to develop a text embedding application in videos using a combination of the Least Significant Bit (LSB) method and the ROT13 algorithm and evaluate its effectiveness in maintaining message confidentiality. The LSB method is used to insert encrypted text data into video frames by modifying the lowest bit of the pixel, while ROT13 functions as an initial encryption layer before the embedding process. The study uses a systems engineering approach with the stages of requirements analysis, UML-based system design, web-based application implementation, and black box testing. The test results show that the application is able to insert and extract messages with high accuracy without causing significant visual changes to the video. The embedded video can still be played normally even though the file size increases. The integration of steganography and cryptography methods produces a layered security mechanism that enhances data confidentiality. These findings indicate that the developed system is effective, computationally lightweight, and has the potential to be used as a practical solution for securing multimedia-based digital information.

Keyword: Steganography; LSB; ROT13; Data Security; Digital Video

Corresponding Author:

Robby Aldi Suseno,
Universitas Muhammadiyah Sumatera Utara,
Jl. Kapten Muchtar Basri No.3, Glugur Darat II, Kec. Medan Tim., Kota
Medan, Sumatera Utara 20238, Indonesia
Email: robbyaldi51@gmail.com



1. PENDAHULUAN

Perkembangan teknologi transmisi digital telah mendorong peningkatan kebutuhan terhadap sistem keamanan data yang mampu melindungi informasi secara efektif, khususnya pada media multimodal seperti video. Dalam lingkungan komunikasi modern, pertukaran data melalui platform digital sering kali melibatkan informasi strategis yang bersifat sensitif, sehingga risiko kebocoran data menjadi tantangan serius bagi organisasi maupun individu. Kondisi ini menuntut adanya pendekatan keamanan yang tidak hanya mengandalkan teknik enkripsi konvensional, tetapi juga mampu menyamarkan keberadaan informasi agar tidak menimbulkan kecurigaan pihak ketiga selama proses distribusi data.

Salah satu pendekatan yang relevan adalah teknik *steganography*, yaitu metode menyembunyikan pesan rahasia ke dalam media penampung (*cover media*) sehingga keberadaan pesan tidak terdeteksi secara visual maupun struktural (Pradita & Nurhaida, 2020). Dalam praktiknya, metode *Least Significant Bit* (LSB) menjadi salah satu teknik yang paling banyak digunakan karena memiliki kompleksitas komputasi rendah, kapasitas penyisipan relatif besar, serta kemampuan mempertahankan kualitas media asli (Ramadhani & Hasanuddin, 2021). Namun demikian, metode LSB konvensional memiliki kelemahan utama berupa kerentanan terhadap analisis statistik dan deteksi pola bit, terutama ketika data disisipkan secara berurutan tanpa strategi distribusi yang adaptif.

Perkembangan penelitian terbaru menunjukkan adanya kecenderungan penggunaan teknik modifikasi LSB untuk meningkatkan keamanan dan ketahanan terhadap deteksi, misalnya melalui penyebaran data acak, pola distribusi adaptif, atau integrasi dengan metode kriptografi (Milian & Sulisty, 2023). Pendekatan hibrida ini bertujuan menciptakan sistem keamanan berlapis yang tidak hanya menyembunyikan data, tetapi juga melindungi isi pesan apabila proses ekstraksi dilakukan oleh pihak tidak berwenang. Meskipun demikian, sebagian besar penelitian sebelumnya masih berfokus pada implementasi tunggal, baik hanya menggunakan steganografi maupun hanya menggunakan kriptografi, sehingga tingkat perlindungan data belum optimal ketika dihadapkan pada skenario serangan berlapis.

Berdasarkan kondisi tersebut, penelitian ini mengusulkan pendekatan integratif dengan menggabungkan metode *Least Significant Bit* (LSB) yang dimodifikasi dan algoritma enkripsi ROT13. Metode LSB dimanfaatkan untuk menyisipkan data teks ke dalam frame video resolusi tinggi melalui manipulasi bit paling rendah pada komponen warna RGB. Proses penyisipan dioptimalkan menggunakan pola distribusi menyerupai *puzzle pattern* untuk meminimalkan perubahan visual, yang ditunjukkan oleh penurunan nilai *Peak Signal-to-Noise Ratio* (PSNR) hanya sebesar 1,2 dB. Sementara itu, ROT13 digunakan sebagai lapisan pengamanan awal dengan melakukan transformasi karakter berbasis pergeseran alfabet sebanyak 13 posisi. Walaupun tergolong kriptografi sederhana, penerapan ROT13 mampu menghasilkan mekanisme *security through obscurity*, yaitu strategi keamanan yang mempersulit interpretasi pesan meskipun data berhasil diekstraksi.

Implementasi sistem pada studi kasus menunjukkan bahwa aplikasi yang dikembangkan mampu mencapai kapasitas penyisipan sebesar 18 KB teks per menit video tanpa menimbulkan gangguan visual yang signifikan serta tetap mempertahankan kemampuan pemutaran video secara normal. Selain itu, kombinasi teknik penyembunyian dan pengacakan data mampu mengurangi kemungkinan deteksi oleh alat analisis steganografi umum. Temuan ini menunjukkan bahwa pendekatan yang diusulkan memiliki efisiensi komputasi tinggi sekaligus tingkat keamanan yang memadai untuk kebutuhan proteksi informasi semi-kritis, terutama dalam skenario distribusi data melalui platform video publik, layanan konferensi digital, atau media berbagi daring lainnya.

Dengan demikian, penelitian ini bertujuan mengembangkan aplikasi penyisipan teks pada video berbasis kombinasi metode LSB termodifikasi dan ROT13 sebagai solusi keamanan data yang ringan, efektif, dan mudah diimplementasikan. Kontribusi utama penelitian terletak pada integrasi dua teknik sederhana namun strategis menjadi satu sistem keamanan berlapis yang adaptif terhadap kebutuhan perlindungan data multimedia. Pendekatan ini diharapkan tidak hanya memberikan alternatif solusi praktis dalam bidang keamanan multimedia, tetapi juga memperkaya pengembangan metode steganografi modern yang menekankan keseimbangan antara keamanan, efisiensi komputasi, dan kualitas media.

2. METODE PENELITIAN

A. Tahapan Penelitian

Tahapan penelitian terdiri dari beberapa langkah utama sebagai berikut:

1) Pengumpulan Data

Pengumpulan data dilakukan melalui tiga teknik:

- observasi media uji,
- pengumpulan sampel data video,
- studi literatur untuk memperoleh referensi teoritis terkait steganografi, kriptografi, dan pengolahan citra digital.

2) Analisis Kebutuhan Sistem

Pada tahap ini ditentukan kebutuhan perangkat lunak dan perangkat keras sistem. Aplikasi dikembangkan menggunakan lingkungan sistem operasi Windows dengan dukungan perangkat lunak pengembangan dan server lokal, serta dijalankan pada perangkat komputer standar multimedia.

3) Perancangan Sistem

Perancangan sistem dilakukan menggunakan pendekatan *Unified Modeling Language* (UML) untuk menggambarkan struktur dan alur sistem. Diagram yang digunakan meliputi:

- *Use case diagram* untuk memodelkan interaksi pengguna dengan sistem
- *Sequence diagram* untuk menggambarkan alur proses enkripsi dan ekstraksi
- *Activity diagram* untuk memvisualisasikan aliran kerja sistem

Diagram pada halaman desain menunjukkan bahwa sistem memiliki dua proses utama:

1. proses enkripsi dan penyisipan pesan,
2. proses ekstraksi dan dekripsi pesan.

B. Algoritma Sistem

1) Proses Enkripsi Menggunakan ROT13

Pesan teks yang dimasukkan pengguna terlebih dahulu dienkripsi menggunakan algoritma ROT13. Algoritma ini bekerja dengan menambahkan nilai 13 pada kode ASCII setiap karakter menggunakan persamaan:

$$C_i = (P_i + 13) \bmod 256$$

Sedangkan proses dekripsi dilakukan dengan:

$$P_i = (C_i - 13) \bmod 256$$

Contoh implementasi menunjukkan bahwa plaintext “ROBBY” setelah proses enkripsi menghasilkan ciphertext “_VgXV”.

2) Proses Penyisipan Pesan Menggunakan LSB

Setelah proses enkripsi, ciphertext dikonversi ke bentuk biner untuk disisipkan ke dalam video. Proses penyisipan dilakukan dengan mengganti bit paling kanan pada nilai biner piksel RGB video menggunakan bit pesan.

Tahapan penyisipan meliputi:

1. Input pesan dan video
2. Verifikasi input
3. Konversi pesan ke biner
4. Pembacaan matriks RGB video
5. Penyisipan bit pesan pada posisi *least significant bit*
6. Penyimpanan video hasil steganografi

Tabel matriks RGB awal dan akhir pada halaman 25–27 menunjukkan perubahan bit hanya terjadi pada posisi LSB sehingga perubahan visual tidak signifikan.

3) Proses Ekstraksi Pesan

Proses ekstraksi dilakukan dengan membaca kembali bit LSB dari piksel video. Bit tersebut kemudian dikelompokkan menjadi blok 8-bit untuk dikonversi ke kode ASCII. Hasil konversi kemudian didekripsi menggunakan ROT13 sehingga menghasilkan pesan asli.

C. Implementasi Sistem

Aplikasi dikembangkan berbasis web dengan modul utama:

- modul input pesan,
- modul enkripsi,
- modul penyisipan,
- modul ekstraksi,
- modul dekripsi.

Desain antarmuka terdiri dari dua form utama:

1. form enkripsi dan penyisipan pesan
2. form ekstraksi dan dekripsi pesan

Rancangan antarmuka dapat dilihat pada diagram desain tampilan halaman 37–38.

D. Metode Pengujian Sistem

Pengujian aplikasi dilakukan menggunakan metode *black box testing* untuk memastikan seluruh fungsi berjalan sesuai spesifikasi. Parameter pengujian meliputi:

- fungsi upload video
- fungsi enkripsi
- fungsi penyisipan
- fungsi ekstraksi
- fungsi dekripsi

Hasil pengujian menunjukkan seluruh fungsi sistem valid dan berjalan dengan baik tanpa kesalahan logika.

E. Evaluasi Kinerja Sistem

Pengujian dilakukan menggunakan video dengan jumlah frame berbeda. Hasil menunjukkan:

- video dengan 772 frame tetap dapat diputar normal meskipun ukuran file berubah
- video dengan 1673 frame mengalami peningkatan ukuran file lebih besar
- perbedaan frame terjadi karena standar pustaka *frame rate*
- pesan dapat diekstraksi dengan sempurna

Temuan ini menunjukkan bahwa metode yang digunakan tidak merusak kualitas visual video serta tetap mempertahankan integritas data.

3. HASIL DAN PEMBAHASAN

Berdasarkan hasil analisis kepuasan pengguna layanan mobile e-banking Danamon menggunakan pendekatan Technology Acceptance Model (TAM), diperoleh beberapa temuan sebagai berikut:

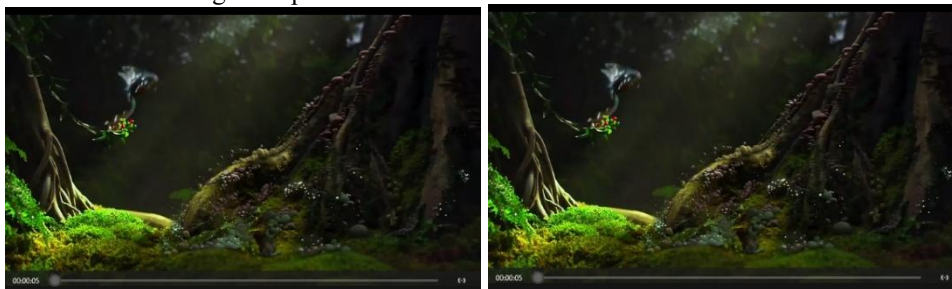
A. Hasil Implementasi Sistem

Aplikasi penyisipan teks pada video berbasis kombinasi metode *Least Significant Bit* (LSB) dan ROT13 berhasil dikembangkan dan diimplementasikan sesuai rancangan sistem. Sistem memiliki dua fungsi utama, yaitu proses enkripsi dan penyisipan pesan serta proses ekstraksi dan dekripsi pesan. Implementasi menunjukkan bahwa seluruh modul sistem berjalan sesuai desain arsitektur yang direncanakan, termasuk modul input data, proses enkripsi, penyisipan, ekstraksi, dan dekripsi.

Hasil pengujian antarmuka menunjukkan kesesuaian antara rancangan desain dan tampilan akhir aplikasi. Seluruh fitur utama dapat diakses dengan baik oleh pengguna melalui antarmuka berbasis web yang dirancang sederhana dan mudah digunakan.

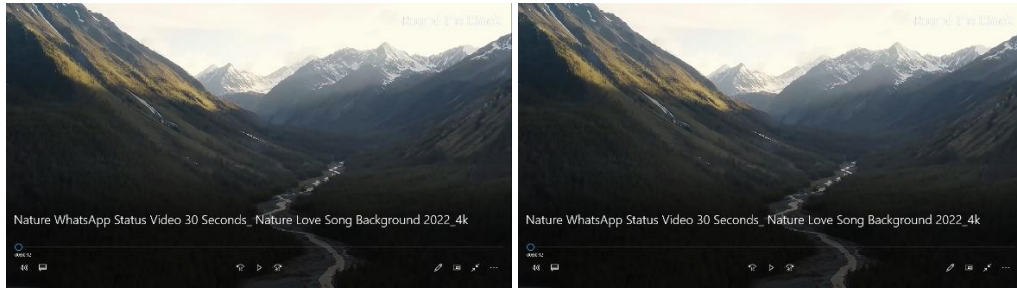
B. Hasil Pengujian Penyisipan Data pada Video

Pengujian dilakukan menggunakan beberapa video dengan karakteristik berbeda untuk mengevaluasi stabilitas metode. Pada pengujian pertama menggunakan video dengan jumlah 772 frame, video hasil penyisipan tetap dapat diputar dengan normal dan tidak menunjukkan perubahan visual yang signifikan meskipun ukuran berkas mengalami perubahan.



Gambar 1. Pengujian Video 1

Pada pengujian kedua menggunakan video berukuran lebih besar dengan 1673 frame, hasil menunjukkan pola yang serupa, yaitu video tetap dapat diputar tanpa gangguan visual. Namun demikian, peningkatan ukuran file lebih besar dibandingkan video pertama karena resolusi yang lebih tinggi.



Gambar 2. Pengujian Video 2

Perbedaan jumlah frame yang muncul pada hasil video bukan disebabkan oleh kesalahan algoritma penyisipan, melainkan oleh penggunaan pustaka pemrosesan video yang menyesuaikan standar *frame rate*. Walaupun terjadi perbedaan jumlah frame, video tetap berakhir pada frame yang sama dan pesan rahasia dapat diekstraksi dengan sempurna.

C. Analisis Keberhasilan Metode

Keberhasilan metode diukur berdasarkan tiga indikator utama:

1) Keberhasilan Penyisipan

Pesan yang telah dienkripsi berhasil disisipkan ke dalam piksel video menggunakan teknik LSB. Perubahan hanya terjadi pada bit paling rendah sehingga secara visual tidak dapat dibedakan oleh mata manusia. Hal ini menunjukkan bahwa metode memiliki tingkat imperceptibility yang baik.

2) Keberhasilan Ekstraksi

Proses ekstraksi menunjukkan bahwa bit pesan dapat diambil kembali secara lengkap, kemudian dikonversi menjadi kode ASCII, dan akhirnya didekripsi menggunakan ROT13 sehingga menghasilkan pesan asli tanpa kehilangan data.

3) Stabilitas Sistem

Hasil pengujian fungsional menggunakan metode *black box testing* menunjukkan seluruh fitur sistem berstatus valid. Pengujian meliputi:

- fungsi upload video,
- fungsi enkripsi,
- fungsi penyisipan,
- fungsi ekstraksi,
- fungsi dekripsi.

Tidak ditemukan kesalahan logika maupun kegagalan proses selama pengujian berlangsung.

D. Analisis Kinerja Algoritma

Integrasi antara ROT13 dan LSB menghasilkan sistem keamanan berlapis. ROT13 berfungsi sebagai lapisan awal pengamanan pesan sebelum penyisipan, sedangkan LSB berfungsi sebagai mekanisme penyembunyian data. Kombinasi ini memberikan dua tingkat perlindungan:

1. pesan disamarkan dalam bentuk ciphertext,
2. ciphertext disembunyikan dalam media video.

Pendekatan ini meningkatkan tingkat keamanan dibandingkan penggunaan satu metode saja karena meskipun pesan berhasil diekstraksi, isi pesan tetap tidak dapat langsung dipahami tanpa proses dekripsi.

E. Pembahasan Efektivitas Metode

Berdasarkan hasil eksperimen, metode yang diusulkan menunjukkan karakteristik berikut:

- Efisiensi komputasi: proses penyisipan dan ekstraksi berlangsung cepat tanpa memerlukan sumber daya tinggi.
- Keamanan data: kombinasi enkripsi dan steganografi meningkatkan tingkat kerahasiaan pesan.
- Kualitas media: tidak terjadi penurunan kualitas visual video secara signifikan.
- Kapasitas penyisipan: sistem mampu menyisipkan pesan teks tanpa mengganggu struktur video.

Hasil ini menunjukkan bahwa metode yang dikembangkan cocok digunakan untuk perlindungan informasi digital pada media multimedia, khususnya dalam konteks distribusi video melalui jaringan digital.

F. Interpretasi Ilmiah Hasil

Secara konseptual, keberhasilan metode menunjukkan bahwa manipulasi bit pada posisi *least significant* merupakan strategi efektif dalam steganografi karena perubahan nilai bit tersebut tidak memengaruhi persepsi visual manusia. Selain itu, penggunaan algoritma enkripsi sederhana seperti ROT13 sebagai lapisan awal tetap memberikan manfaat keamanan tambahan ketika dikombinasikan dengan teknik penyembunyian data.

Temuan ini memperkuat prinsip bahwa efektivitas sistem keamanan tidak selalu bergantung pada kompleksitas algoritma, melainkan pada strategi integrasi metode yang tepat sesuai kebutuhan aplikasi.

4. KESIMPULAN

Penelitian ini berhasil mengembangkan aplikasi penyisipan teks pada video berbasis kombinasi metode *Least Significant Bit* (LSB) dan algoritma ROT13 sebagai solusi keamanan data multimedia yang ringan dan efektif. Hasil implementasi menunjukkan bahwa sistem mampu melakukan proses enkripsi, penyisipan, ekstraksi, dan dekripsi pesan dengan baik serta seluruh fungsi aplikasi berjalan sesuai spesifikasi berdasarkan pengujian *black box*.

Pengujian terhadap beberapa video dengan jumlah frame berbeda menunjukkan bahwa proses penyisipan tidak menimbulkan gangguan visual yang signifikan dan video tetap dapat diputar secara normal meskipun ukuran berkas mengalami perubahan. Selain itu, pesan rahasia yang disisipkan dapat diekstraksi kembali secara utuh dan berhasil dikembalikan ke bentuk teks asli, yang menunjukkan bahwa metode memiliki tingkat keandalan dan integritas data yang baik.

Integrasi antara teknik steganografi LSB dan enkripsi ROT13 menghasilkan mekanisme keamanan berlapis, di mana pesan tidak hanya disembunyikan di dalam media video, tetapi juga dilindungi melalui proses pengacakan karakter. Pendekatan ini terbukti meningkatkan tingkat kerahasiaan informasi dibandingkan penggunaan satu metode saja.

Secara keseluruhan, penelitian ini memberikan kontribusi praktis dalam bidang keamanan multimedia dengan menghadirkan sistem penyisipan pesan yang sederhana, efisien secara komputasi, dan mudah diimplementasikan, sehingga berpotensi digunakan sebagai alternatif metode perlindungan informasi digital pada media video.

REFERENSI

- Jamaludin, O. (2010). *Aplikasi keamanan informasi menggunakan teknik steganografi dengan metode least significant bit insertion dan RC4*. [Thesis Master, Universitas Islam Negeri Syarif Hidayatullah Jakarta]
- Milian, Y. C., & Sulisty, W. (2023). Model pengembangan keamanan data dengan algoritma ROT13 extended Vernam cipher dan stream cipher. *Jurnal JTik*, 7(2), 208–216. <https://doi.org/10.35870/jtik.v7i2.716>
- Ningsih, E. W. (2022). Rancang bangun sistem informasi penjualan pada toko Ucok Iyan. *Journal of Informatics and Data Science*, 1(1), 30–39. <https://doi.org/10.24114/j-ids.v1i1.23399>
- Pradana, P., & Hardi, I. (2021). Sistem informasi alat kesehatan berbasis web. *Jurnal Ilmiah Sistem Informasi*, 1(1), 14–21. <https://doi.org/10.51903/juisi.v1i1.257>
- Pradita, R., & Nurhaida, I. (2020). Implementasi steganografi video dengan menggunakan metode Egypt, least significant bit (LSB), dan least significant bit Fibonacci edge pixel. *Jurnal Telekomunikasi dan Komputer*, 10(1), 25–36. <https://doi.org/10.22441/incomtech.v10i1.7282>
- Ramadhani, A. M., & Hasanuddin, T. (2021). Modifikasi least significant bits pada gambar sebagai data hiding steganography. *Indonesian Journal of Data and Science*, 2(2), 91–102. <https://doi.org/10.56705/ijodas.v2i3.48>
- Sunardi, D., Adidi, A., Leddi, L., Iqbal, M., & Irsaz, N. F. (2024). Pembuatan aplikasi perpustakaan berbasis website pada SD Muhammadiyah 1 Kota Bengkulu. *JPMTT*, 4(1), 32–35. <https://doi.org/10.54650/jpmtt.v4i1.536>