JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Implementasi Penyembunyian Data pada Metadata PNG Menggunakan Enkripsi Fernet (AES) Berbasis Password dengan Python

Ulvia Rahmi[1*], Mutia Hafiza Quranul[2], Putri Dian[3], Rahmatul Amna[4]
[1,2,3,4] Universitas Malikussaleh, Indonesia
[1] ulvia.230170028@mhs.unimal.ac.id , [2]mutia.230170113@mhs.unimal.ac.id, [3]putri.230170009@mhs.unimal.ac.id, [4]rahmatul.230170034@mhs.unimal.ac.id

ABSTRACT

The rapid exchange of digital information necessitates robust security measures to protect sensitive data from unauthorized access. This research proposes a hybrid security model combining cryptography and steganography to hide information within PNG image metadata. The system utilizes Fernet symmetric encryption, which is built on top of AES-128, to secure the message before embedding it into the metadata fields. A password-based key derivation ensures that only authorized users can decrypt the content. By leveraging Python for implementation, the study demonstrates that metadata-based steganography provides a secure alternative to traditional pixel-based methods, as it does not alter the visual quality of the image. The results indicate that the encrypted metadata is resilient to basic image viewing while maintaining data integrity.

Kata Kunci/ Keywords:
Cryptography, Fernet Encryption, Metadata, PNG, Steganography.

PENDAHULUAN

Di era digital saat ini, kebutuhan akan sistem keamanan data semakin mendesak karena meningkatnya ancaman terhadap privasi, seperti penyadapan dan pencurian data (Set et al., 2025). Pertukaran informasi yang besar memerlukan pengawasan dan perlindungan yang lebih ketat (Indrayani et al., 2025). Salah satu celah keamanan yang sering dimanfaatkan adalah fitur unggah file pada aplikasi berbasis web. Metode validasi standar sering kali hanya memeriksa ekstensi file atau magic number, yang sebenarnya sangat mudah diubah oleh penyerang untuk menyisipkan skrip berbahaya. (Anwar et al., 2020).

Kriptografi berfungsi sebagai solusi utama untuk melindungi kerahasiaan, integritas, dan keaslian pesan (Amalia & Rosyani, 2018). Penggunaan algoritma seperti Advanced Encryption Standard (AES) telah terbukti ampuh dalam mengamankan data perusahaan serta dokumen penting lainnya (Khoirudin & Windarto, 2024). Namun, hanya dengan kriptografi saja tidak cukup, karena pesan yang telah dienkripsi tetap menarik perhatian. Oleh karena itu, perlu adanya penggabungan dengan steganografi untuk menyembunyikan keberadaan data rahasia tersebut (Imron & Pratama, 2022).

Penelitian ini mengkaji pemanfaatan metadata PNG sebagai tempat penyimpanan yang aman untuk data yang telah dienkripsi dengan metode Fernet berbasis Python, bertujuan menciptakan lapisan keamanan ganda yang kuat tetapi tetap efisien dalam hal komputasi (Pabokory et al., 2016).

TINJAUAN PUSTAKA

Kriptografi Fernet dan Keunggulan AES

Kriptografi merupakan ilmu yang berfokus pada perlindungan data dengan cara mengubahnya ke dalam format yang tidak dapat diakses tanpa kunci tertentu (Amalia & Rosyani, 2018). Algoritma AES, terutama varian 128-bit dan 256-bit, dianggap sebagai standar utama dalam enkripsi simetris karena ketahanannya terhadap serangan brute force serta efisiensi dalam waktu pemrosesannya (Indrayani et al., 2025);(Khoirudin & Windarto, 2024). Enkripsi Fernet adalah penerapan modern yang menggunakan dasar AES-128 dalam mode CBC dengan HMAC untuk memastikan autentikasi pesan. Penggunaan kata sandi sebagai dasar dalam pembuatan kunci menambah lapisan keamanan, sehingga hanya pengguna resmi yang memiliki kata sandi tersebut yang dapat melakukan proses dekripsi (Sultana et al., 2024).

Steganografi Metadata vs LSB

Teknik steganografi yang umum digunakan sering kali memanfaatkan Least Significant Bit (LSB) untuk menyembunyikan data di dalam piksel gambar. Namun, metode LSB dapat menimbulkan perubahan visual jika data yang disisipkan terlalu besar (Set et al., 2025). Sebagai solusi, steganografi yang berbasis metadata menggunakan area non-visual dalam struktur file, seperti teks atau komentar dalam file PNG dan MP4 (Darwis et al., 2025). Metadata pada PNG sangat bermanfaat karena tidak mengubah kualitas gambar asli dan sering diabaikan oleh alat pemindai keamanan standar (Anwar et al., 2020). Dengan memanfaatkan metadata, kita dapat memastikan bahwa integritas visual gambar tetap sepenuhnya 100% sama dengan aslinya (Darwis et al., 2025).

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Penggabungan Metode (Hybrid Security)

Integrasi antara kriptografi dan steganografi menghasilkan tingkat keamanan berlapis yang sangat tinggi (Shwaysh et al., 2024). Dalam sistem hibrida, meskipun pihak ketiga dapat mendeteksi teknik steganografi, informasi yang disimpan tetap tidak dapat diakses karena masih dalam keadaan terenkripsi (Pabokory et al., 2016). Penggabungan algoritma enkripsi yang cepat dengan media penyimpanan metadata yang tersembunyi adalah strategi optimal dalam melindungi kerahasiaan e-dokumen dan komunikasi digital (Imron & Pratama, 2022).

METODE PENELITIAN

Penelitian ini menggunakan metodologi eksperimental terapan dengan langkah-langkah sistematis yang meliputi:

Analisis dan Perancangan:

Mengidentifikasi arsitektur sistem yang melibatkan modul enkripsi Fernet dan modul manipulasi metadata PNG menggunakan pustaka Python seperti Pillow dan cryptography. Hal ini bertujuan untuk menciptakan sistem yang tidak hanya kuat tetapi juga mudah diimplementasikan (Amalia & Rosyani, 2018).

Proses Pembangkitan Kunci:

Sistem meminta input password dari pengguna. Password ini diolah menggunakan fungsi derivasi kunci (KDF) untuk menghasilkan kunci Fernet yang unik. Keamanan kunci sangat krusial dalam skema enkripsi simetris (Shwaysh et al., 2024).

Proses Enkripsi (Cryptography Layer):

Pesan teks yang ingin disembunyikan dienkripsi menjadi ciphertext. Penggunaan Fernet menjamin bahwa jika ada perubahan satu bit saja pada data, proses dekripsi akan gagal, sehingga integritas data terjamin (Sultana et al., 2024).

Penyisipan Data (Steganography Layer):

Ciphertext hasil enkripsi kemudian disisipkan ke dalam kolom metadata khusus pada file PNG (misalnya blok 'tEXt' atau 'zTXt'). Berbeda dengan modifikasi piksel, metode ini tidak mengubah nilai warna gambar (Darwis et al., 2025);(Set et al., 2025).

Pengujian dan Validasi:

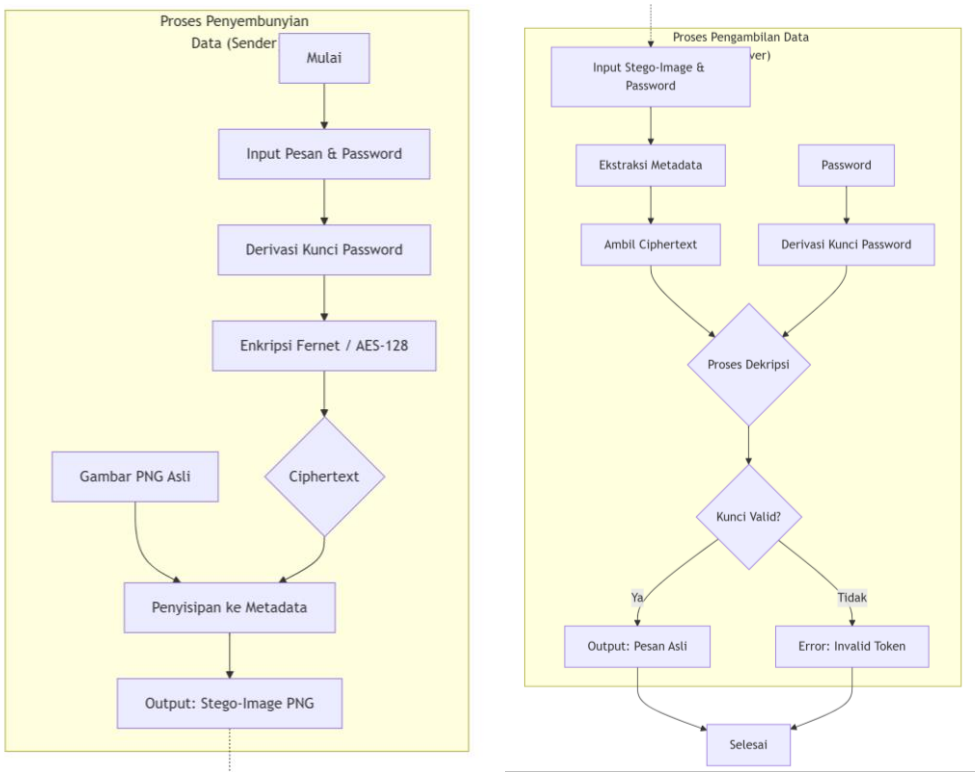
- **Uji Integritas:**
  Memastikan pesan dapat diekstraksi dan didekripsi kembali dengan sempurna tanpa kehilangan data (Indrayani et al., 2025).
- **Analisis Visual:**
  Melakukan perbandingan visual antara file PNG asli dan file PNG yang telah disisipkan data untuk memastikan tidak ada artefak visual (Pabokory et al., 2016).
- **Analisis Metadata:**
  Memeriksa apakah data yang disembunyikan bertahan setelah proses unggah/unduh standar pada aplikasi web (Anwar et al., 2020).

HASIL DAN PEMBAHASAN

Analisis Alur Kerja dan Keamanan Hibrida

Sistem yang diimplementasikan menggabungkan dua disiplin keamanan informasi: kriptografi untuk melindungi isi pesan, dan steganografi untuk menyembunyikan keberadaan pesan tersebut. Alur kerja dimulai dengan proses derivasi kunci menggunakan *Password-Based Key Derivation Function* (PBKDF2) yang terintegrasi dalam pustaka Fernet.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

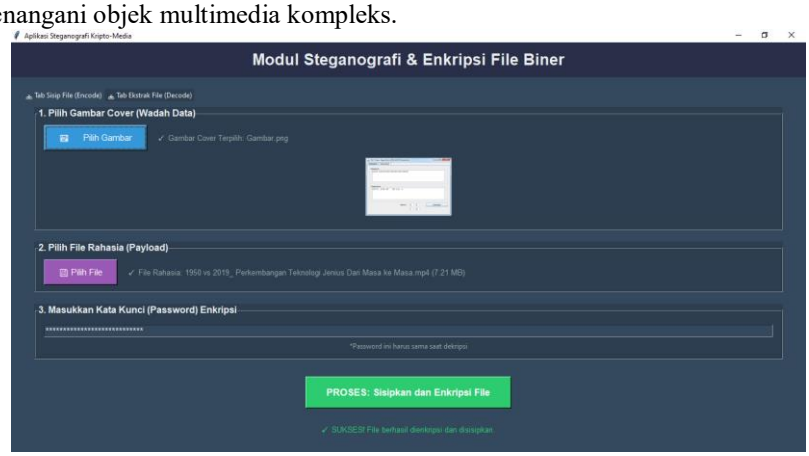


Gambar 1. Arsitektur Sistem: (a) Alur Enkripsi dan Penyisipan Metadata dan Arsitektur Sistem: (b) Alur Ekstraksi dan Dekripsi Metadata

Penggunaan algoritma Fernet memberikan jaminan keamanan pada tingkat tinggi karena berbasis AES-128 dalam mode CBC dengan autentikasi HMAC. Hal ini memastikan bahwa jika data di dalam metadata diubah oleh pihak ketiga, proses dekripsi akan gagal total, sehingga integritas data terjamin.

Implementasi Enkripsi dan Efisiensi Payload (Encoding)

Pada tahap pengujian, sistem diuji menggunakan *payload* biner berupa file video MP4 sebesar **7.21 MB**. Penggunaan file biner sebagai data rahasia menunjukkan bahwa sistem tidak terbatas pada pesan teks sederhana, melainkan mampu menangani objek multimedia kompleks.



Gambar 2. Antarmuka proses enkripsi dan penyisipan file biner ke metadata gambar

Berdasarkan Gambar 2, terdapat beberapa poin teknis yang perlu dicatat:

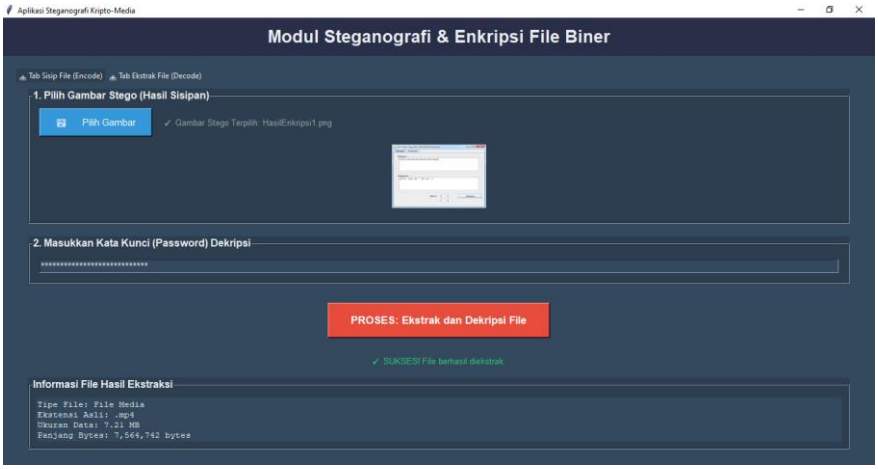
- **Pengolahan Metadata:** Data rahasia disisipkan ke dalam blok metadata khusus pada struktur file PNG. Kelebihannya, metadata dapat menampung kapasitas data yang cukup besar selama sistem operasi dan aplikasi pembaca gambar dapat menangani ukuran file tersebut.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

- **Keamanan Kunci:** Penggunaan password yang di-masking mencegah *shoulder surfing* dan memastikan hanya pemilik otoritas yang dapat membangkitkan kunci dekripsi yang tepat.
- **Feedback Berbasis Event:** Notifikasi sukses yang muncul menunjukkan bahwa penulisan ulang struktur *hexadecimal* pada file PNG telah selesai dilakukan tanpa merusak *magic number* file penampung.

Validasi Integritas Data dan Ekstraksi (Decoding)

Keberhasilan sistem diukur dari kemampuannya mengembalikan data ke bentuk semula tanpa kehilangan satu bit pun (*lossless*).



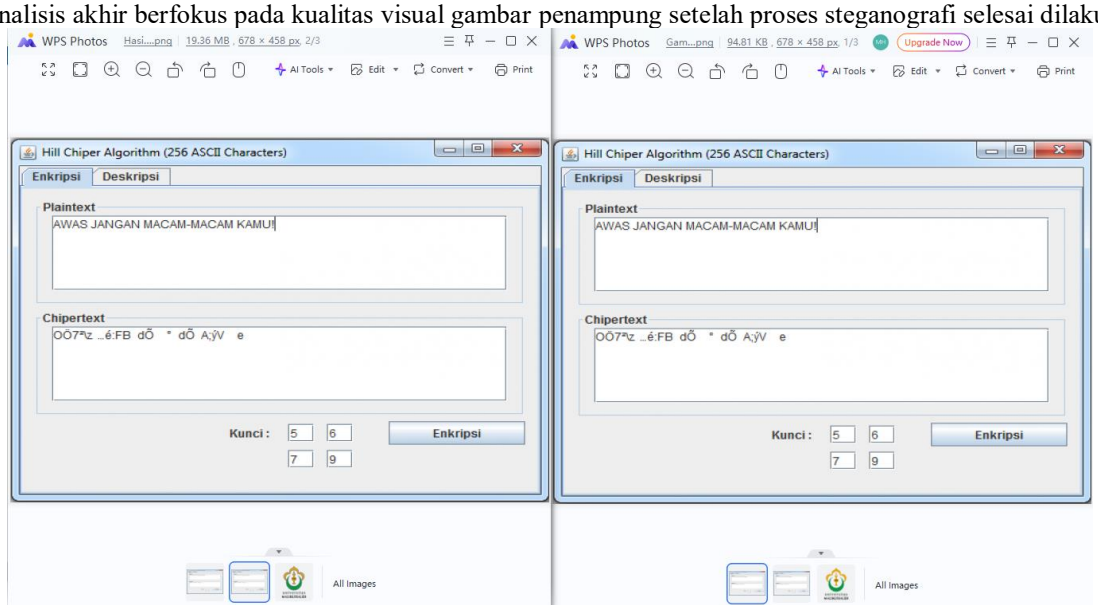
Gambar 3. Antarmuka keberhasilan ekstraksi file rahasia dari metadata gambar

Hasil pengujian pada Gambar 3 menunjukkan akurasi yang sangat tinggi:

- **Presisi Ukuran:** Data yang diekstraksi tetap berukuran **7,564,742 bytes**. Konsistensi ukuran ini membuktikan bahwa proses enkripsi Fernet dan penyimpanan pada metadata tidak menyebabkan korupsi data.
- **Identifikasi Metadata:** Sistem secara otomatis mendeteksi ekstensi asli (.mp4), yang menunjukkan bahwa informasi *header* file rahasia turut disimpan secara aman di dalam metadata. Hal ini memudahkan pengguna karena tidak perlu melakukan penggantian ekstensi file secara manual setelah proses ekstraksi.

Analisis Imperceptibility dan Perbandingan Fisik

Analisis akhir berfokus pada kualitas visual gambar penampung setelah proses steganografi selesai dilakukan.



Gambar 4. Analisis perbandingan visual antara citra asli (kanan) dan citra stego (kiri)

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Perbandingan pada Gambar 4 memberikan hasil analisis sebagai berikut:

- **Integritas Visual:** Secara kasat mata, tidak terdapat degradasi kualitas, perubahan saturasi, atau *noise* pada citra stego. Hal ini merupakan keunggulan utama steganografi berbasis metadata dibandingkan metode *Least Significant Bit* (LSB) yang cenderung mengubah nilai warna pada piksel gambar.
- **Analisis Overhead Ukuran File:** Meskipun visualnya identik, terdapat perbedaan signifikan pada ukuran fisik file. File asli berukuran **~94 KB**, sedangkan file stego membengkak menjadi **~19 MB**. Peningkatan ini disebabkan oleh penggabungan ukuran gambar asli, ukuran file video (7.21 MB), dan penambahan karakter akibat proses encoding Base64 yang dilakukan oleh Fernet (menambah beban sekitar 33% dari data asli).
- **Ketahanan terhadap Perangkat Lunak:** File hasil tetap dapat dibuka oleh aplikasi pembaca gambar standar (seperti WPS Photos pada gambar di atas), membuktikan bahwa modifikasi metadata tidak merusak kompatibilitas file PNG.

KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dipaparkan, dapat disimpulkan bahwa sistem keamanan hibrida yang menggabungkan kriptografi Fernet dan steganografi metadata PNG telah berhasil menjalankan fungsinya dengan sangat baik. Penelitian ini menunjukkan bahwa penggunaan metadata sebagai media penyimpanan data rahasia memiliki keunggulan signifikan dibandingkan metode konvensional seperti *Least Significant Bit* (LSB). Hal ini dibuktikan melalui analisis visual yang menunjukkan integritas citra stego tetap terjaga 100% tanpa adanya degradasi kualitas atau artefak visual, meskipun membawa beban data (*payload*) biner yang cukup besar yakni file video berukuran 7.21 MB.

Penerapan algoritma Fernet berbasis AES-128 memberikan jaminan keamanan data yang kuat melalui enkripsi simetris dan autentikasi HMAC, sehingga data tidak hanya tersembunyi, tetapi juga terlindungi dari upaya modifikasi oleh pihak ketiga. Manfaat praktis dari penelitian ini adalah tersedianya solusi proteksi data yang efisien untuk pertukaran e-dokumen sensitif, di mana kerahasiaan terjaga melalui penyamaran (*steganography*) dan isi data tetap aman melalui enkripsi (*cryptography*).

Meskipun sistem ini sangat efektif dalam menjaga kualitas visual, penelitian ini memiliki keterbatasan pada peningkatan ukuran fisik file (*overhead*) yang cukup signifikan, di mana file membengkak hingga ~19 MB akibat proses *encoding* Base64 dan ukuran *payload* asli. Untuk pengembangan selanjutnya, direkomendasikan untuk mengintegrasikan algoritma kompresi sebelum tahap enkripsi guna mereduksi ukuran file akhir. Selain itu, pengujian ketahanan terhadap proses kompresi otomatis pada platform media sosial atau aplikasi pesan instan menjadi poin penting yang perlu ditingkatkan agar data di dalam metadata tetap bertahan (*persistent*) dalam berbagai skenario transmisi digital.

REFERENSI

Amalia, R., & Rosyani, P. (2018). Implementasi Algoritma AES dan Algoritma XOR pada Aplikasi Enkripsi dan Dekripsi Teks Berbasis Android. *Faktor Exacta, 11*(4), 370. https://doi.org/10.30998/faktorexacta.v11i4.2878

Anwar, F., Fadlil, A., & Riadi, I. (2020). Analisis Validasi Image PNG File Upload menggunakan Metadata pada Aplikasi Berbasis Web. *Edu Komputika Journal, 7*(1), 10–15. https://doi.org/10.15294/edukomputika.v7i1.38722

Darwis, D., Fernando, Y., Mehta, A. R., Wamiliana, ., & Setiawansyah, . (2025). Metadata-Based Video Steganography: Development of a New Model for Secure Information Embedding. *Engineering, Technology & Applied Science Research*, *15*(5), 27076–27088. https://doi.org/10.48084/etasr.11937

Imron, M., & Pratama, A. (2022). Pengamanan E-Dokumen Berbasis Steganografi Dengan KombinasiAdvanced Encryption Standard (AES) 128 Bit. *InfoTekJar : Jurnal Nasional Informatika Dan Teknologi Jaringan*, *6*, 253–257. https://doi.org/10.30743/infotekjar.v6i2.4346

Indrayani, R., Ferdiansyah, P., & Koprawi, M. (2025). Analisis Penggunaan Kriptografi Metode AES 256 Bit pada Pengamanan File dengan Berbagai Format. *Digital Transformation Technology*, *4*(2), 1245–1251. https://doi.org/10.47709/digitech.v4i2.5457

Khoirudin, N. H., & Windarto, W. (2024). Penerapan Algoritme Advanced Encryption Standard (AES-512) untuk Pengamanan File Berbasis Web. *KRESNA: Jurnal Riset Dan Pengabdian Masyarakat*, *4*(1), 62–71. https://doi.org/10.36080/kresna.v4i1.104

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *10*(1), 20. https://doi.org/10.30872/jim.v10i1.23

Set, F. M. C. B., Bana, C. M. N., Anunut, M. A., Costa, D. Da, & Niis, Y. (2025). Penerapan Steganografi LSB dan Enkripsi AES untuk Keamanan Data Rahasia pada Gambar Digital. *Blantika: Multidisciplinary Journal*, *3*(7), 1040–1047. https://doi.org/10.57096/blantika.v3i7.382

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Shwaysh, M. M., Alani, S., Saad, M. A., & Abdulhussein, T. A. (2024). Image Encryption and Steganography Method Based on AES Algorithm and Secret Sharing Algorithm. *Ingenierie Des Systemes d'Information*, *29*(2), 705–714. https://doi.org/10.18280/isi.290232

Sultana, H., Deena Faria, & A.H.M. Kamal. (2024). Image Steganography based on Fernet Symmetric Encryption and Odd-Even Pixel Modification. *International Journal of Engineering and Computer Science*, *13*(08), 26325–26337. https://doi.org/10.18535/ijecs/v13i08.4874