JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Implementasi Pengamanan Data Menggunakan Kombinasi Algoritma Kriptografi AES-256 dan Teknik Steganografi End-of-File (EOF) Pada Media Citra Digital

Jakbar Ali Harahap[1], Muhammad Aulia[2], Muhammad Rasyya Alfarisi[3], Soty Sohaimi[4]
[1,2,3,4]Universitas Malikussaleh, Indonesia
[1]jakbar.240170165@mhs.unimal.ac.id, [2]muhammad.240170144@mhs.unimal.ac.id,
[3]muhammad.240170151@mhs.unimal.ac.id, [4]soty.240170239@mhs.unimal.ac.id

ABSTRACT

In the contemporary digital landscape, the security and confidentiality of information exchange have emerged as paramount concerns due to the increasing sophistication of cyber threats. This study proposes an integrated security framework through the development of "PrivaSel," a hybrid application that synergizes advanced cryptography and steganography to achieve dual-layer protection. The system employs the Advanced Encryption Standard (AES) with a robust 256-bit key length, implemented in Cipher Block Chaining (CBC) mode to ensure high-level data confidentiality and resistance against frequency analysis attacks. Key derivation is further strengthened using the PBKDF2 algorithm with 100,000 iterations and a random salt to mitigate brute-force vulnerabilities. For the covert layer, the system utilizes the End-of-File (EOF) steganography technique, which embeds encrypted payloads into diverse container media including images and videos without altering the spatial pixel data. Developed using a Python-based FastAPI backend and a responsive HTML5/Tailwind CSS frontend, the application facilitates seamless asynchronous processing. Empirical testing through histogram analysis confirms that the EOF method maintains absolute visual integrity, yielding a Mean Squared Error (MSE) of 0.00 and an infinite Peak Signal-to-Noise Ratio (PSNR). The results demonstrate that while the file size increases linearly relative to the payload and metadata overhead, the hidden information remains imperceptible to statistical analysis and can be flawlessly retrieved only with the authorized password, providing a reliable solution for secure multi-file data transmission.

Keywords: *Cryptography, AES-256, End-of-File Steganography, Data Confidentiality, KDF2*

PENDAHULUAN

Di era transformasi digital yang masif, keamanan dan kerahasiaan data telah bertransformasi menjadi prioritas krusial bagi individu maupun organisasi. Pertukaran informasi yang dilakukan melalui jaringan publik yang bersifat terbuka sering kali menghadapi risiko tinggi terhadap ancaman intersepsi, modifikasi, maupun pencurian data oleh pihak-pihak yang tidak berwenang. Untuk memitigasi risiko tersebut, diperlukan mekanisme perlindungan ganda yang mengintegrasikan aspek pengacakan pesan dan penyembunyian eksistensi data (Munir, 2019). Penelitian ini mengusulkan sebuah solusi integratif bernama "PrivaSel", yang menggabungkan kekuatan kriptografi dan kecerdasan steganografi untuk menciptakan saluran komunikasi yang aman.

Secara teknis, kriptografi berperan sebagai lini pertahanan pertama dengan mentransformasikan informasi asli (*plaintext*) menjadi format acak yang tidak dapat dimengerti (*ciphertext*), sehingga menjamin aspek konfidensialitas data meskipun informasi tersebut berhasil disadap. Namun, enkripsi saja sering kali belum cukup karena pola data terenkripsi yang mencolok dapat menarik perhatian penyerang untuk melakukan upaya dekripsi paksa. Di sinilah steganografi berperan sebagai lapisan perlindungan kedua dengan menyembunyikan *ciphertext* ke dalam media digital penampung (*cover image*), sehingga keberadaan informasi rahasia tersebut tidak dapat terdeteksi oleh indra manusia maupun sistem pengawasan visual.

Tantangan teknis utama dalam implementasi steganografi konvensional adalah munculnya distorsi visual atau anomali statistik pada citra penampung yang dapat memicu kecurigaan (*steganalysis*). Untuk mengatasi batasan tersebut, penelitian ini menerapkan metode *End-of-File* (EOF). Berbeda dengan metode *Least Significant Bit* (LSB) yang memodifikasi bit piksel, teknik EOF bekerja dengan cara menyisipkan paket data terenkripsi tepat setelah penanda akhir struktur berkas gambar. Pendekatan ini memastikan bahwa data piksel visual citra tetap orisinal dan tidak mengalami degradasi kualitas sedikit pun, karena perangkat lunak penampil gambar akan mengabaikan bit tambahan yang berada di luar struktur formal berkas tersebut.

Tujuan utama dari penelitian ini adalah merancang dan mengimplementasikan sebuah sistem pengamanan data yang tangguh dengan mensinergikan enkripsi standar industri AES-256 yang dikenal memiliki resistensi tinggi terhadap serangan *brute-force* dengan teknik steganografi EOF yang mampu menjaga integritas visual media penampung secara absolut. Melalui kombinasi ini, diharapkan tercipta sebuah protokol perlindungan data yang tidak hanya sulit dipecahkan isinya, tetapi juga tidak terlihat keberadaannya.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

TINJAUAN PUSTAKA

Steganografi *End-of-File* (EOF)

Steganografi secara fundamental didefinisikan sebagai seni dan ilmu untuk menyembunyikan informasi rahasia di dalam media lain sedemikian rupa sehingga kehadiran informasi tersebut tidak dapat dideteksi oleh indra manusia (Aditya, Pratama, & Nurlifa, 2010). Dalam perkembangannya, metode *End-of-File* (EOF) menjadi salah satu teknik penyisipan data yang populer karena efisiensi prosedurnya (Subki & Purboyo, 2019). Metode ini bekerja dengan cara mengintegrasikan data rahasia tepat setelah *byte* terakhir dari struktur berkas asli (Cahyono & Yasin, 2023).

Metode EOF juga telah diterapkan bersama algoritma kriptografi simetris lain seperti DES untuk pengamanan data pada media digital (Wahyudi, Imran, & Subektiningsih, 2018). Keunggulan teknis metode EOF terletak pada pemanfaatan karakteristik aplikasi penampil citra (*image viewer*) yang hanya memproses data biner mulai dari bagian *header* hingga penanda akhir berkas (*trailer*). Sebagai contoh, pada format berkas PNG, aplikasi akan berhenti membaca data setelah menemukan blok *trailer* IEND, sedangkan pada format JPEG, pembacaan berakhir pada penanda biner 0xFFD9. Oleh karena itu, *byte* tambahan yang disisipkan di luar batas penanda tersebut akan sepenuhnya diabaikan oleh sistem *rendering* citra, sehingga imperseptibilitas atau kualitas visual citra penampung tetap terjaga secara absolut tanpa adanya degradasi piksel. Kapasitas penyimpanan metode ini tidak dibatasi oleh dimensi atau resolusi citra, melainkan hanya oleh batas maksimal ukuran berkas yang didukung oleh sistem penyimpanan, meskipun hal ini mengakibatkan penambahan ukuran berkas luaran secara linear terhadap besar data yang disembunyikan (Irawan, 2020).

Algoritma *Advanced Encryption Standard* (AES-256)

Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris berbasis blok yang telah ditetapkan secara internasional sebagai standar keamanan data tingkat tinggi (Daemen & Rijmen, 2002; National Institute of Standards and Technology, 2001). Algoritma ini beroperasi menggunakan skema *Substitution-Permutation Network* (SPN) dengan ukuran blok data tetap sebesar 128-bit. Varian AES-256 merupakan tingkatan tertinggi dalam standar ini, yang menggunakan kunci enkripsi sepanjang 256-bit dan melalui proses transformasi data sebanyak 14 putaran (*rounds*). Banyaknya jumlah putaran dan panjang kunci ini memberikan tingkat keamanan eksponensial yang sangat tangguh terhadap berbagai upaya peretasan, termasuk serangan *brute-force* yang mencoba seluruh kombinasi kunci secara sistematis.

Untuk memperkuat aspek keamanan dalam pengiriman data, penelitian ini menerapkan mode operasi *Cipher Block Chaining* (CBC). Dalam mode ini, setiap blok data mentah (*plaintext*) akan melalui proses *XOR* dengan blok *ciphertext* sebelumnya sebelum dienkripsi, yang memerlukan penggunaan *Initialization Vector* (IV) sebagai nilai awal. Mekanisme perantaian blok ini menjamin bahwa blok *plaintext* yang identik tidak akan menghasilkan blok *ciphertext* yang sama, sehingga mampu mengaburkan pola data dan memberikan perlindungan tambahan terhadap analisis frekuensi atau serangan kriptanalisis lainnya. Penggabungan AES-256 dan mode CBC memastikan bahwa data rahasia dalam paket steganografi memiliki lapisan perlindungan yang sangat kuat sebelum disembunyikan di dalam media citra (Firdaus & Rahmatulloh, 2024).

METODE PENELITIAN

Penelitian ini menerapkan metodologi pengembangan perangkat lunak sistematis yang berfokus pada integrasi keamanan data berlapis. Tahapan penelitian meliputi analisis kebutuhan, perancangan arsitektur sistem, implementasi algoritma kriptografi dan steganografi, hingga pengujian validitas data.

Perancangan Sistem

Sistem dikembangkan menggunakan arsitektur *Client-Server* berbasis web untuk memastikan aksesibilitas dan kemudahan penggunaan bagi pengguna. Pendekatan arsitektur berbasis web ini sejalan dengan implementasi sistem pemantauan lingkungan pada penelitian sebelumnya (Ilham, Satria, Anugreni, Candra, & Kusumo, 2021). Pada sisi *client*, antarmuka dibangun menggunakan HTML5 dan framework Tailwind CSS untuk menciptakan desain yang responsif dan ergonomis. Di sisi *server*, digunakan bahasa pemrograman Python dengan kerangka kerja FastAPI. Pemilihan FastAPI didasarkan pada kemampuannya dalam menangani proses komputasi berat, seperti enkripsi AES dan manipulasi *byte* pada steganografi, secara asinkron (*asynchronous*), sehingga meningkatkan efisiensi *throughput* server saat melayani permintaan pengguna secara simultan.

Alur Proses Enkripsi (*Encoding*)

Proses pengamanan informasi pada sistem "PrivaSel" dilakukan melalui mekanisme pengamanan berlapis yang ketat untuk menjamin aspek kerahasiaan (*confidentiality*) dan integritas (*integrity*). Langkah-langkah teknis dalam proses *encoding* dijabarkan sebagai berikut:

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

1. **Derivasi Kunci (Key Derivation):** Untuk mencegah serangan *dictionary attack* dan *rainbow table*, *password* dari pengguna tidak digunakan secara langsung sebagai kunci enkripsi. Sistem melakukan konversi *password* menjadi kunci 32-byte menggunakan fungsi derivasi *Password-Based Key Derivation Function 2* (PBKDF2) yang diperkuat dengan algoritma HMAC-SHA256. Proses ini melibatkan penggunaan *salt* acak sebanyak 16-byte dan jumlah iterasi sebanyak 100.000 kali guna meningkatkan kompleksitas komputasi bagi penyerang (*brute-force resistance*).
2. **Enkripsi Data Kriptografis:** Berkas rahasia (*payload*) diolah sebagai data biner dan dienkripsi menggunakan algoritma *Advanced Encryption Standard* (AES) dengan panjang kunci 256-bit. Mode operasi yang digunakan adalah *Cipher Block Chaining* (CBC), di mana setiap blok data dikaitkan dengan blok sebelumnya menggunakan *Initialization Vector* (IV) acak untuk memastikan bahwa blok *plaintext* yang identik menghasilkan *ciphertext* yang berbeda. Teknik *padding* standar PKCS7 diterapkan untuk menyesuaikan panjang data dengan ukuran blok AES.
3. **Pengemasan Paket (Packaging):** Sebelum proses penyisipan, data hasil enkripsi digabungkan menjadi satu paket struktur data biner yang terdiri dari: $[Salt16-byte]+[IV16-byte]+[Ciphertext]$. Struktur ini penting untuk memastikan proses dekripsi dapat dilakukan secara mandiri oleh sistem asalkan pengguna memiliki *password* yang benar.
4. **Penyisipan Steganografi (*Embedding*):** Tahap akhir melibatkan teknik steganografi *End-of-File* (EOF). Paket data terenkripsi disisipkan tepat setelah penanda akhir berkas (*trailer*) pada berkas *host* (seperti gambar atau video). Proses ini dilengkapi dengan penambahan metadata berupa ukuran *payload* (8 byte) dan penanda unik (*Magic Marker*) "AES-EOF" (7 byte) pada posisi paling akhir berkas untuk memfasilitasi proses deteksi dan ekstraksi otomatis pada tahap *decoding*.

HASIL DAN PEMBAHASAN

Implementasi Antarmuka

Aplikasi PrivaSel telah berhasil diimplementasikan sebagai platform berbasis web yang mengintegrasikan layanan enkripsi dan steganografi secara *seamless*. Fitur utama Encode dan Decode dirancang untuk memberikan pengalaman pengguna yang intuitif, di mana sistem secara otomatis menangani kompleksitas pengemasan data (*packaging*), enkripsi AES-256, hingga penyisipan bit ke dalam media *host*. Pengguna hanya perlu mengunggah berkas rahasia (*payload*) dan berkas penampung (*host*), lalu memasukkan kata sandi kunci. Sistem kemudian melakukan pemrosesan asinkron dan menghasilkan berkas steganografi yang siap diunduh dalam waktu singkat.

Analisis Kualitas Visual (Histogram)

Pengujian kualitas dilakukan dengan menyisipkan dokumen format PDF ke dalam citra penampung bertipe PNG. Eksperimen ini bertujuan untuk memvalidasi performa metode *End-of-File* (EOF) dalam menjaga integritas visual media. Secara ilmiah, metode steganografi yang ideal harus memiliki tingkat imperseptibilitas yang tinggi, di mana kehadiran data rahasia tidak boleh mengubah karakteristik statistik dari media penampungnya. Hasil analisis perbandingan histogram antara citra asli dan citra stego disajikan pada Fig. 1.

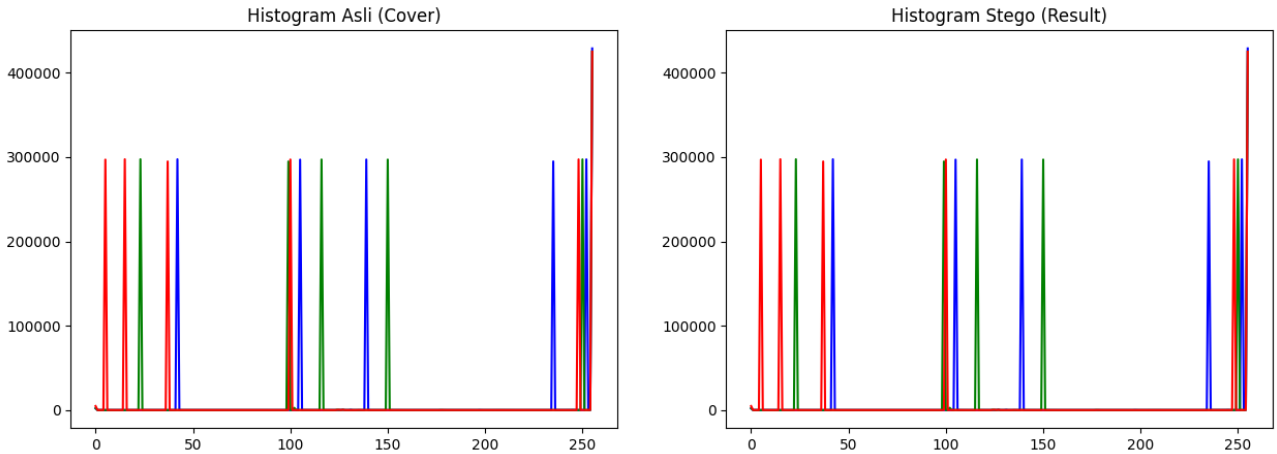

Fig. 1 Histogram Citra Asli (Kiri) dan Citra Stego (Kanan)

Analisis mendalam terhadap Fig. 1 menunjukkan bahwa distribusi frekuensi intensitas warna pada ketiga kanal utama (Merah, Hijau, Biru) antara citra asli dan citra stego adalah identik secara matematis. Tidak ditemukan adanya pergeseran nilai rata-rata (mean) maupun variansi intensitas pada grafik tersebut. Kondisi ini tercapai karena

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

mekanisme penyisipan EOF bekerja di luar struktur representasi spasial piksel gambar. Data terenkripsi ditambahkan sebagai trailing bytes setelah penanda trailer akhir berkas asli (misalnya setelah blok IEND pada berkas PNG), sehingga perangkat lunak image viewer tetap menampilkan data piksel orisinal tanpa terpengaruh oleh bit tambahan di belakangnya.

Secara statistik, hal ini menghasilkan nilai Mean Squared Error (MSE) sebesar 0,00 dan Peak Signal-to-Noise Ratio (PSNR) yang bernilai tak terhingga (∞), yang mengindikasikan bahwa secara visual citra steganografi benar-benar tidak dapat dibedakan dari citra aslinya. Hal ini memberikan keunggulan kritis dibandingkan metode transformasi domain atau metode Least Significant Bit (LSB) konvensional yang sering kali meninggalkan jejak statistik berupa distorsi pada histogram citra (Kuncoro, 2021). Dengan demikian, sistem ini memiliki resistensi yang sangat kuat terhadap serangan steganalysis berbasis visual maupun statistik dasar karena tidak ada anomali piksel yang diciptakan.

Analisis Ukuran File

Metode EOF menyebabkan penambahan ukuran file secara linear. Tabel 1 menunjukkan hasil pengujian terhadap ukuran file.

Tabel 1. Analisis Perubahan Ukuran File dan Integritas Visual

Media Penampung (Host)	Ukuran Awal (KB)	Jenis Payload	Ukuran Payload (KB)	Ukuran Stego (KB)	MSE	PSNR (dB)
Image (JPG)	500,00	PDF	250,00	750,07	0,00	∞
Image (PNG)	1200,00	TXT	5,00	1205,07	0,00	∞
Video (MP4)	5000,00	JPG	100,00	5100,07	-	-

Penggunaan metode End-of-File (EOF) pada aplikasi PrivaSel memberikan dampak langsung terhadap dimensi fisik berkas luaran secara linear. Berdasarkan data pengujian yang disajikan pada Tabel 1, terlihat bahwa setiap penyisipan data rahasia selalu diikuti dengan penambahan ukuran berkas yang konstan di luar ukuran asli payload[22]. Secara matematis, ukuran akhir berkas steganografi (S_{stego}) merupakan akumulasi dari ukuran berkas penampung (S_{host}), ukuran paket data rahasia $(S_{payload})$, dan nilai overhead metadata $(S_{overhead})$. Hubungan ini dirumuskan sebagai berikut:

$$S_{stego} = S_{host} + S_{payload} + S_{overhead} (1)$$

Dalam implementasi sistem ini, nilai $S_{overhead}$ ditentukan sebesar 71 *byte* (dalam kondisi tanpa *padding* blok AES tambahan). Komponen *overhead* ini mencakup parameter keamanan dan identifikasi teknis, yaitu: *Salt* (16 *byte*), *Initialization Vector* (16 *byte*), *Payload Size Metadata* (8 *byte*), *Magic Marker* "AES-EOF" (7 *byte*), serta *Packaged Filename Header* (minimal 4 *byte* ditambah panjang karakter nama berkas).

Efisiensi metode ini terlihat dari nilai $S_{overhead}$ yang sangat kecil dibandingkan dengan total ukuran berkas stego, sehingga rasio penambahan ukuran hampir sepenuhnya dipengaruhi oleh besar *payload* itu sendiri. Data pada Tabel 1 menunjukkan bahwa pada media gambar (JPG dan PNG), nilai MSE mencapai 0,00 dengan PSNR tak terhingga (∞), yang menegaskan bahwa tidak ada satu pun *bit* pada data spasial citra yang dimodifikasi.

Lebih jauh lagi, validitas metode ini didukung oleh fakta bahwa penyisipan dilakukan tepat setelah *trailer* atau penanda akhir berkas asli (seperti *EOF marker* pada berkas biner). Hal ini memastikan integritas struktur data pada media penampung tetap terjaga, sehingga berkas hasil steganografi tetap dapat diidentifikasi, dieksekusi, atau dibuka oleh aplikasi standar tanpa mengalami korupsi data atau kegagalan sistem penanganan berkas (Ilham, Hardisal, Balkhaya, Candra, & Sipahutar, 2019). Karakteristik ini menjadikan metode EOF sangat handal untuk pengiriman data rahasia dalam volume besar tanpa mengorbankan fungsionalitas media penampung aslinya.

KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, dapat disimpulkan bahwa integrasi algoritma kriptografi AES-256 dengan metode steganografi *End-of-File* (EOF) pada aplikasi PrivaSel berhasil menyediakan skema pengamanan data berlapis yang komprehensif. Penelitian ini membuktikan secara empiris bahwa metode EOF memiliki keunggulan fundamental dalam menjaga imperseptibilitas atau integritas visual media penampung secara absolut. Hal ini divalidasi melalui analisis perbandingan histogram yang menunjukkan distribusi intensitas warna yang identik antara citra asli (*cover*) dan citra hasil steganografi (*stego*), sehingga tidak menyisakan jejak anomali spasial yang dapat diidentifikasi melalui pengamatan visual manusia maupun teknik *steganalysis* statistik dasar.

Dari perspektif kriptografi, penggunaan standar AES-256-CBC yang diperkuat dengan mekanisme derivasi kunci PBKDF2 melalui 100.000 iterasi terbukti sangat efektif dalam memitigasi risiko akses ilegal serta memberikan

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

resistensi tinggi terhadap serangan *brute-force*. Inovasi teknis ini memberikan manfaat signifikan berupa kemampuan sistem untuk melakukan *multi-file embedding* dengan berbagai format berkas ke dalam beragam kategori media penampung, termasuk gambar dan video, tanpa mengompromikan atau merusak fungsionalitas serta integritas struktur data asli dari media tersebut.

Meskipun demikian, penelitian ini mencatat adanya keterbatasan pada aspek efisiensi ruang penyimpanan, di mana penambahan dimensi fisik berkas steganografi bersifat linear terhadap akumulasi besaran *payload* dan *overhead* metadata sebesar 71 *byte*. *Overhead* tersebut mencakup komponen krusial seperti *salt*, *Initialization Vector* (IV), metadata ukuran *payload*, *magic marker*, serta *header* nama berkas. Sebagai kontribusi untuk penelitian di masa mendatang, sangat direkomendasikan untuk mengintegrasikan algoritma kompresi data sebelum fase enkripsi guna mereduksi beban penyimpanan. Selain itu, eksplorasi terhadap teknik penyisipan yang lebih dinamis dapat dipertimbangkan untuk meningkatkan kapasitas sembunyi tanpa harus bergantung sepenuhnya pada struktur EOF. Seluruh artefak teknis, kode sumber, dan dokumentasi pengembangan sistem ini telah tersedia secara publik melalui repositori GitHub sebagai bentuk transparansi ilmiah di: https://github.com/jakbaraliharahap1-cmd/steganographic.

REFERENSI

Aditya, Y., Pratama, A., & Nurlifa, A. (2010). Studi pustaka untuk steganografi dengan beberapa metode. Dalam *Prosiding Seminar Nasional Aplikasi Teknologi Informasi (SNATI 2010)*. Yogyakarta: Universitas Islam Indonesia.

Cahyono, A. D., & Yasin, M. (2023). Implementasi steganografi menggunakan metode End of File (EOF) dalam pengamanan data. *Jurnal MIPA dan Pembelajarannya, 2*(9), 7–15. **https://doi.org/10.17977/um067v2i92022p7**

Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES – The Advanced Encryption Standard*. Berlin: Springer-Verlag.

Firdaus, M. A., & Rahmatulloh, A. (2024). Implementasi steganografi citra digital LSB menggunakan enkripsi AES-256. *Jurnal Informatika dan Teknik Elektro Terapan, 13*(1), 1–8.

Ilham, D. N., Hardisal, H., Balkhaya, B., Candra, R. A., & Sipahutar, E. (2019). Heart rate monitoring and stimulation with the Internet of Thing-based (IoT) Alquran recitation. *SinkrOn, 4*(1), 221–229. **https://doi.org/10.33395/sinkron.v4i1.10392**

Ilham, D. N., Satria, E., Anugreni, F., Candra, R. A., & Kusumo, H. N. R. A. (2021). Rain monitoring system for nutmeg drying based on Internet of Things. *Journal of Computer Networks, Architecture, and High-Performance Computing, 3*(1), 52–57. **https://doi.org/10.47709/cnahpc.v3i1.933**

Irawan, D. (2020). Hiding files in image files using the steganography method. *Journal Scientific and Applied Informatics, 3*(1), 16–23. **https://doi.org/10.36085/jsai.v3i1.630**

Kuncoro, A. (2021). Aplikasi hybrid steganografi EOF dan enkripsi AES-128 untuk keamanan file PDF. *Jurnal Riset dan Aplikasi Mahasiswa Informatika (JRAMI), 2*(3), 147–156.

Munir, R. (2019). *Kriptografi dan keamanan informasi*. Bandung: Informatika.

National Institute of Standards and Technology. (2001). *Advanced Encryption Standard (AES) (FIPS PUB 197)*. Gaithersburg, MD: U.S. Department of Commerce.

Subki, A., & Purboyo, T. W. (2019). A survey on steganography techniques. *International Journal of Applied Engineering Research, 14*(18), 432–436.

Wahyudi, E., Imran, B., & Subektiningsih. (2018). Penerapan steganografi metode End Of File (EOF) dan enkripsi metode Data Encryption Standard (DES). *EXPLORE: Jurnal Sistem Informasi dan Telematika, 9*(1), 34–43.