JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i3.9536

KEAMANAN DOKUMEN MULTI-LAYER MENGGUNAKAN STEGANOGRAFI DAN HONEY ENCRYPTION

Gabriel Nathanael Purba[1], Kadek Yota Ernanda Aryanto[2], I Ketut Resika Arthana[3]
[1,2,3]Fakultas Teknik dan Kejuruan, Universitas Pendidikan Ganesha

Keywords:
Honey Encryption;
AES-CBC;
LSB Steganography;
Multi-Layer Security.

Corespondent Email:
gabriel@student.undiksha.ac.id

Abstrak. Transformasi digital meningkatkan penggunaan dokumen digital yang rentan terhadap serangan siber seperti brute-force dan steganalisis. Enkripsi konvensional menjaga kerahasiaan data, namun memberikan indikator kegagalan saat kunci tidak sesuai sehingga dapat dimanfaatkan untuk memvalidasi percobaan kunci. Penelitian sebelumnya mengkaji Honey Encryption dan steganografi LSB secara terpisah: implementasi Honey Encryption umumnya terbatas pada pengamanan kredensial berbasis teks, sementara kombinasi LSB dengan kriptografi masih menggunakan enkripsi konvensional yang mengekspos indikator kegagalan dekripsi. Penelitian ini mengusulkan sistem keamanan dokumen multi-layer yang mengintegrasikan Honey Encryption dan steganografi Least Significant Bit (LSB) dengan algoritma AES-CBC, sebagai pendekatan baru yang menyatukan mekanisme deception-based cryptography dengan penyembunyian ciphertext pada media citra. Dokumen PDF dipetakan menjadi seed melalui Distribution Transforming Encoder yang disederhanakan, dienkripsi, lalu disisipkan ke citra PNG menggunakan metode LSB. Evaluasi dilakukan melalui pengujian fungsional, simulasi brute-force, pengukuran waktu proses, analisis kualitas visual menggunakan Peak Signal-to-Noise Ratio (PSNR) dan Mean Square Error (MSE), serta steganalisis menggunakan StegExpose. Hasil menunjukkan sistem menghasilkan dokumen umpan yang valid secara struktural saat kunci salah digunakan tanpa indikator kegagalan dekripsi bagi pengguna. Nilai PSNR tinggi dan MSE rendah, yang merupakan konsekuensi dari desain payload berukuran kecil dan konstan, menunjukkan distorsi visual minimal, sementara hasil steganalisis berada dalam ambang deteksi yang dapat diterima.

Abstract. *Digital transformation has increased use of digital documents vulnerable to cyber threats such as brute-force attacks and steganalysis. Conventional encryption ensures data confidentiality but provides explicit failure indicators when incorrect keys are used, potentially aiding attackers. Prior studies examined Honey Encryption and LSB steganography separately: Honey Encryption has largely focused on credential or text-based data, while LSB with cryptography has relied on conventional encryption that still exposes decryption failure indicators. This study proposes a multi-layer document security system integrating Honey Encryption and Least Significant Bit (LSB) steganography with AES-CBC, representing a novel integration of deception-based cryptography and covert data embedding within a unified framework. PDF documents are mapped into seeds using a simplified Distribution Transforming Encoder, then encrypted and embedded into PNG images using LSB. The system is evaluated through functional testing, brute-force simulation, processing time measurement, visual quality analysis using Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE), and steganalysis using StegExpose. Results show the system generates structurally valid decoy documents when incorrect keys are applied, without exposing failure indicators to the user. High PSNR and low MSE values, a consequence of the small constant-size payload, indicate minimal visual distortion, while steganalysis results remain within acceptable detection thresholds.*

1. PENDAHULUAN

Transformasi digital telah meningkatkan penggunaan dokumen dalam format elektronik pada berbagai sektor, yang secara langsung meningkatkan risiko ancaman keamanan siber terhadap data sensitif [1], [2]. Dokumen digital yang dipertukarkan melalui jaringan terbuka rentan terhadap pencurian, manipulasi, serta akses tidak sah. Oleh karena itu, mekanisme perlindungan data yang efektif menjadi kebutuhan utama dalam sistem informasi modern.

Salah satu metode yang umum digunakan untuk menjaga kerahasiaan data adalah kriptografi, khususnya algoritma Advanced Encryption Standard (AES) karena efisiensi dan tingkat keamanannya yang tinggi [3], [4]. Namun, meskipun AES dirancang untuk tahan terhadap berbagai serangan kriptanalisis, proses dekripsi dengan kunci yang salah umumnya menghasilkan keluaran yang tidak valid atau pesan kesalahan yang dapat digunakan sebagai indikator keberhasilan atau kegagalan percobaan kunci [5]. Kondisi ini berpotensi dimanfaatkan dalam skenario serangan brute-force atau dictionary attack untuk memvalidasi tebakan kunci secara sistematis [6].

Untuk mengatasi keterbatasan tersebut, Honey Encryption diperkenalkan sebagai pendekatan kriptografi yang menghasilkan keluaran yang tampak valid meskipun proses dekripsi dilakukan dengan kunci yang salah [7]. Dengan memanfaatkan Distribution Transforming Encoder (DTE), sistem dapat menghasilkan dokumen umpan (decoy) yang secara struktural tetap konsisten, sehingga tidak memberikan indikator eksplisit kepada penyerang mengenai keberhasilan dekripsi [8].

Selain kriptografi, steganografi juga digunakan untuk meningkatkan lapisan keamanan dengan menyembunyikan keberadaan informasi rahasia di dalam media digital. Metode Least Significant Bit (LSB) merupakan teknik yang banyak digunakan karena implementasinya sederhana dan memiliki distorsi visual yang relatif rendah [9], [10]. Namun, teknik ini tetap memiliki risiko terdeteksi melalui analisis statistik apabila tidak dikonfigurasi dengan parameter yang tepat [11].

Meskipun Honey Encryption dan steganografi LSB telah diteliti secara terpisah, integrasi keduanya dalam satu sistem keamanan dokumen yang saling melengkapi masih belum banyak dieksplorasi. Penelitian sebelumnya yang menggunakan Honey Encryption umumnya berfokus pada pengamanan kredensial atau data berbasis teks, tanpa mempertimbangkan penyembunyian keberadaan ciphertext itu sendiri [7], [8], [12], [13]. Di sisi lain, penelitian steganografi LSB yang dikombinasikan dengan kriptografi umumnya menggunakan enkripsi konvensional yang tetap mengekspos indikator kegagalan dekripsi [14], [15]. Kesenjangan ini menunjukkan perlunya pendekatan yang mengintegrasikan mekanisme deception-based cryptography dengan penyembunyian data pada media citra, sehingga sistem tidak hanya mengamankan konten dokumen tetapi juga menyembunyikan keberadaan data terenkripsi sekaligus mengeliminasi umpan balik yang dapat dieksploitasi penyerang.

Berdasarkan latar belakang tersebut, penelitian ini mengusulkan sistem keamanan dokumen multi-layer yang mengintegrasikan Honey Encryption berbasis AES-CBC dengan steganografi LSB pada citra PNG. Kontribusi utama penelitian ini adalah mengintegrasikan kedua teknik tersebut dalam satu sistem yang saling melengkapi: Honey Encryption menyediakan mekanisme penipu kriptografis yang menyembunyikan indikator kegagalan dekripsi dari pengguna, sementara steganografi LSB menyembunyikan keberadaan ciphertext itu sendiri di dalam media citra. Kombinasi ini belum dieksplorasi pada studi sebelumnya yang mengkaji kedua teknik secara terpisah. Sistem dirancang untuk menghasilkan dokumen umpan ketika kunci yang salah digunakan serta menyembunyikan ciphertext ke dalam media citra guna mengurangi kemungkinan deteksi melalui steganalisis. Evaluasi dilakukan melalui pengujian fungsional, simulasi brute-force, pengukuran waktu proses, analisis kualitas citra menggunakan Peak Signal-to-Noise Ratio (PSNR) dan Mean Square Error (MSE), serta pengujian deteksi menggunakan StegExpose.

2. TINJAUAN PUSTAKA

2.1 Honey Encryption dan Distribution Transforming Encoder

Honey Encryption (HE) merupakan pendekatan kriptografi yang dirancang untuk mengatasi kelemahan enkripsi konvensional

terhadap serangan brute-force dengan menghasilkan keluaran yang tampak valid meskipun kunci yang digunakan salah [7] [8]. Berbeda dengan enkripsi tradisional yang menghasilkan keluaran acak atau pesan kesalahan ketika kunci tidak sesuai, HE memanfaatkan mekanisme Distribution Transforming Encoder (DTE) untuk memetakan pesan ke dalam ruang distribusi tertentu sehingga setiap kunci menghasilkan plaintext yang secara struktural valid [8].

Beberapa penelitian telah mengembangkan pendekatan HE dalam berbagai skenario implementasi, termasuk integrasi dengan skema hybrid encryption untuk meningkatkan fleksibilitas distribusi pesan [12], serta penerapan dalam lingkungan komputasi awan guna meningkatkan perlindungan data terhadap serangan offline [13]. Pendekatan tersebut menunjukkan bahwa HE efektif dalam memberikan lapisan perlindungan tambahan melalui mekanisme deception-based cryptography.

2.2 Steganografi Metode Least Significant Bit (LSB)

Steganografi merupakan teknik penyembunyian informasi dengan menyisipkan data rahasia ke dalam media digital seperti citra, audio, atau video [9], [1]. Metode Least Significant Bit (LSB) merupakan salah satu teknik yang paling banyak digunakan karena implementasinya sederhana dan memiliki dampak visual yang relatif rendah terhadap citra penampung [10].

Penggunaan citra berformat PNG sering dipilih dalam implementasi LSB karena tidak menggunakan kompresi lossy sehingga perubahan bit pada level piksel tidak menyebabkan degradasi kualitas yang signifikan [14]. Beberapa penelitian juga mengombinasikan teknik LSB dengan algoritma kriptografi untuk meningkatkan keamanan sistem secara keseluruhan [15]. Sebagai contoh, Firdaus dan Rahmatulloh mengimplementasikan LSB dengan enkripsi AES-256 dan teknik embedding pseudorandom pada citra PNG, yang terbukti berhasil menyisipkan dan mengekstraksi pesan dengan tetap mempertahankan kualitas visual citra penampung [16].

Meskipun demikian, teknik LSB tetap memiliki risiko terdeteksi melalui metode steganalisis berbasis statistik apabila kapasitas penyisipan terlalu besar [9].

2.3 Evaluasi Kualitas Citra dan Deteksi Steganalisis

Kualitas citra hasil penyisipan umumnya dievaluasi menggunakan parameter kuantitatif seperti Mean Square Error (MSE) dan Peak Signal-to-Noise Ratio (PSNR). Nilai PSNR yang tinggi dan MSE yang rendah menunjukkan bahwa perubahan visual akibat proses penyisipan relatif kecil [17].

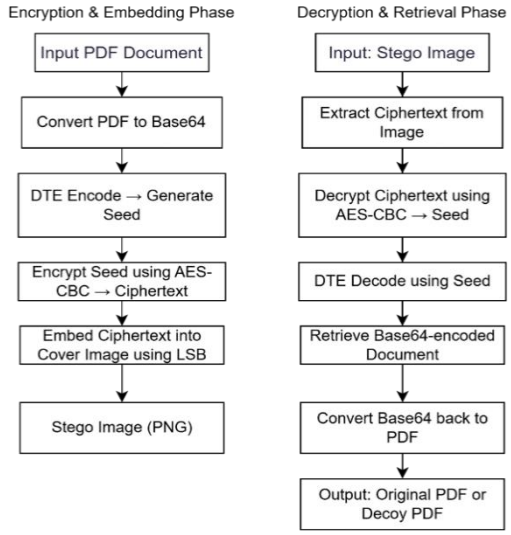
Selain itu, deteksi keberadaan pesan tersembunyi dapat dilakukan menggunakan alat analisis seperti StegExpose yang mengombinasikan beberapa metode deteksi statistik untuk mengidentifikasi kemungkinan adanya steganografi dalam citra digital [18]. Pengujian ini penting untuk memastikan bahwa sistem tidak hanya mampu menyembunyikan data, tetapi juga memiliki tingkat resistensi terhadap proses steganalisis.

3. METODE PENELITIAN

3.1 Rancangan Sistem

Penelitian ini menggunakan pendekatan kuantitatif eksperimental untuk merancang dan mengevaluasi sistem keamanan dokumen yang mengintegrasikan Honey Encryption dan steganografi LSB dalam dua fase utama: fase enkripsi dan penyisipan, serta fase dekripsi dan pengambilan kembali, sebagaimana ditunjukkan pada Gambar 1.

Pada fase enkripsi, dokumen PDF dikonversi ke Base64, dipetakan ke seed acak melalui mekanisme Honey Encryption, kemudian seed dienkripsi menggunakan AES-CBC dan disisipkan ke dalam citra PNG menggunakan LSB, menghasilkan stego image sebagai keluaran. Pada fase dekripsi, ciphertext diekstraksi dari stego image, didekripsi untuk memperoleh seed, lalu dicocokkan dengan tabel pemetaan dokumen. Kunci yang benar menghasilkan dokumen PDF asli, sedangkan kunci yang salah menghasilkan dokumen umpan (decoy) yang secara struktural valid namun tidak mengandung informasi asli.



Gambar 1. System Flow Diagram: Encryption & Embedding Phase dan Decryption & Retrieval Phase

3.2 Implementasi Honey Encryption

Honey Encryption diimplementasikan melalui mekanisme pemetaan dokumen ke seed menggunakan pendekatan Distribution Transforming Encoder (DTE). Setiap dokumen PDF terlebih dahulu dikonversi ke format Base64, kemudian sistem menghasilkan seed acak sepanjang 10 karakter alfanumerik yang unik untuk setiap dokumen. Pasangan seed dan representasi dokumen disimpan dalam struktur JSON sebagai tabel pencarian (lookup table).

DTE berfungsi sebagai lapisan transformasi yang memetakan ruang pesan (dokumen) ke ruang seed secara deterministik dan dapat dibalik. Perlu dicatat bahwa implementasi DTE dalam penelitian ini merupakan pendekatan yang disederhanakan: struktur DTE diadopsi tanpa pemodelan probabilistik yang kompleks sebagaimana pada konstruksi Honey Encryption formal, namun tujuan utamanya tetap sama, yaitu memastikan bahwa setiap keluaran dekripsi bersifat valid secara struktural, baik untuk dokumen asli maupun dokumen umpan [7][8]. Dalam implementasi ini, DTE dioperasikan melalui dua tabel pemetaan JSON yang terpisah: satu untuk dokumen asli dan satu untuk dokumen umpan. Pemisahan ini memungkinkan sistem untuk secara konsisten mengembalikan keluaran yang tampak valid untuk semua kunci, baik benar maupun salah, tanpa mengekspos struktur internal sistem kepada penyerang. Panjang seed ditetapkan 10 karakter alfanumerik (menggunakan set karakter A–Z, a–z, 0–9, sehingga 62 karakter) yang menghasilkan ruang kemungkinan sebesar $62^{10} \approx 8{,}39 \times 10^{17}$ kombinasi unik. Ukuran ini dipilih sebagai keseimbangan antara ruang kemungkinan yang cukup besar untuk mencegah tumbukan seed (collision) antar dokumen, sekaligus mempertahankan efisiensi proses karena seed hanya perlu dicocokkan dalam tabel JSON tanpa operasi kriptografis tambahan.

Sebanyak 100 dokumen umpan disiapkan dalam tahap awal dan disimpan dalam pemetaan dokumen umpan. Dokumen umpan dirancang menyerupai dokumen resmi nyata dalam hal format dan konten, mencakup berbagai template seperti laporan evaluasi, audit keuangan, pernyataan resmi, dan proposal proyek, yang masing-masing diisi dengan data acak yang kontekstual.

Pada tahap enkripsi, hanya seed dari dokumen asli yang dienkripsi menggunakan AES-CBC. Pada tahap dekripsi, seed hasil dekripsi dicocokkan dengan pemetaan dokumen asli. Apabila seed ditemukan, dokumen asli dikembalikan. Apabila tidak ditemukan, sistem secara otomatis mengakses pemetaan dokumen umpan dan mengembalikan salah satu dokumen umpan sebagai keluaran tanpa memberikan indikator kesalahan kepada pengguna. Mekanisme ini memastikan bahwa setiap percobaan dekripsi, baik dengan kunci benar maupun salah, selalu menghasilkan keluaran yang tampak valid.

3.3 Implementasi LSB Steganography

Metode steganografi yang diterapkan adalah Least Significant Bit (LSB) pada tingkat bit piksel citra digital. Citra berformat PNG dipilih sebagai media penampung karena menggunakan kompresi lossless sehingga data yang disisipkan tidak mengalami kerusakan. Untuk setiap piksel RGB dalam citra, sistem memodifikasi satu bit paling tidak signifikan pada masing-masing kanal warna (R, G, dan B), sehingga setiap piksel mampu menampung tiga bit data.

Payload yang disisipkan ke dalam citra tidak langsung berupa dokumen PDF, melainkan berupa seed terenkripsi beserta initialization vector (IV) yang dihasilkan oleh proses AES-CBC. Ukuran payload yang kecil dan hampir konstan ini memungkinkan

perubahan bit pada piksel tetap minimal dan tidak menimbulkan distorsi visual yang terdeteksi. Sebelum data utama disisipkan, sistem terlebih dahulu menyisipkan informasi mengenai ukuran payload sehingga proses ekstraksi dapat menentukan batas data yang perlu diambil dari citra secara akurat.

Pengujian dilakukan menggunakan tiga variasi ukuran dokumen PDF (kecil: 100–200 KB, sedang: 500–600 KB, besar: 800–1000 KB) dan tiga variasi resolusi citra penampung (256×256, 512×512, dan 1024×1024 piksel). Evaluasi mencakup pengujian fungsional dan simulasi brute-force, analisis kualitas visual menggunakan PSNR dan MSE, pengujian steganalisis menggunakan StegExpose, serta perbandingan perilaku dekripsi antara sistem Honey Encryption dan AES-CBC konvensional. Implementasi sistem dibangun menggunakan Python 3.13 dengan pustaka PyCryptodome untuk enkripsi AES-CBC, Pillow untuk manipulasi citra, NumPy untuk operasi bit-level dan perhitungan PSNR/MSE, serta fpdf untuk pembuatan dokumen umpan.

4. HASIL DAN PEMBAHASAN

4.1 Pengujian Fungsional dan Simulasi Brute-Force

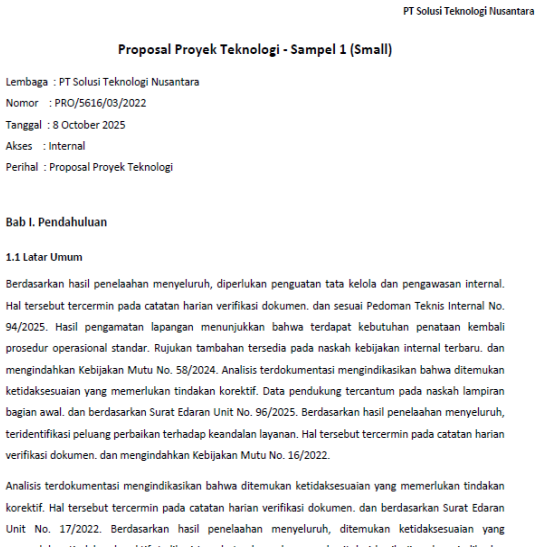
Pengujian fungsional dilakukan untuk memverifikasi alur kerja sistem secara menyeluruh, mencakup proses enkripsi, penyisipan, ekstraksi, dan dekripsi. Pengujian dilakukan menggunakan sampel dokumen PDF dengan variasi ukuran (kecil, sedang, besar) dan citra penampung dengan resolusi 256×256, 512×512, dan 1024×1024 piksel.

Hasil pengujian fungsional menunjukkan bahwa seluruh proses inti sistem berjalan sesuai rancangan. Ketika kunci yang benar dimasukkan, sistem berhasil memulihkan dokumen PDF asli yang dapat dibuka menggunakan PDF reader standar. Dokumen yang dipulihkan memiliki struktur dan konten yang identik dengan dokumen sumber, dibuktikan dengan kecocokan SHA-256 checksum. Ketika kunci yang salah dimasukkan, sistem tidak menghasilkan keluaran acak atau pesan error, melainkan menghasilkan dokumen umpan dalam format PDF yang valid dan dapat dibuka secara normal.

Simulasi brute-force dilakukan dengan melakukan 200 percobaan dekripsi menggunakan stego image yang sama, terdiri dari 100 percobaan menggunakan kunci benar dan 100 percobaan menggunakan kunci yang berbeda-beda. Setiap keluaran disimpan dalam format PDF dan diverifikasi menggunakan SHA-256 checksum untuk memastikan keidentikan byte dengan dokumen sumber. Hasil pengujian disajikan pada Tabel 1.

Tabel 1. Ringkasan Hasil Simulasi Brute-Force

Metrik	Kunci Benar	Kunci Salah
Total percobaan ekstraksi	100	100
Kecocokan dengan dokumen asli	100	0



PT Solusi Teknologi Nusantara

Proposal Proyek Teknologi - Sampel 1 (Small)

Lembaga : PT Solusi Teknologi Nusantara
Nomor : PRO/5616/03/2022
Tanggal : 8 October 2025
Akses : Internal
Perihal : Proposal Proyek Teknologi

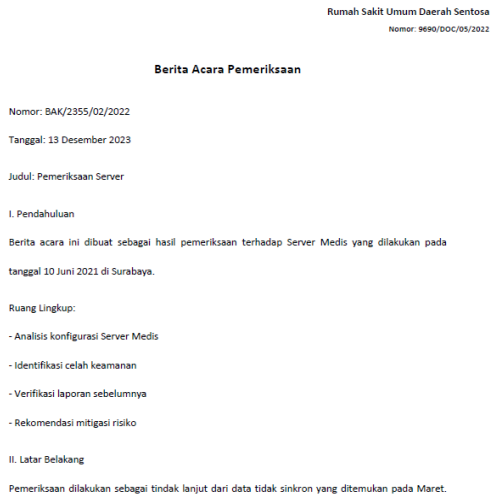
Bab I. Pendahuluan

1.1 Latar Umum

Berdasarkan hasil penelaahan menyeluruh, diperlukan penguatan tata kelola dan pengawasan internal. Hal tersebut tercermin pada catatan harian verifikasi dokumen. dan sesuai Pedoman Teknis Internal No. 94/2025. Hasil pengamatan lapangan menunjukkan bahwa terdapat kebutuhan penataan kembali prosedur operasional standar. Rujukan tambahan tersedia pada naskah kebijakan internal terbaru. dan mengindahkan Kebijakan Mutu No. 58/2024. Analisis terdokumentasi mengindikasikan bahwa ditemukan ketidaksesuaian yang memerlukan tindakan korektif. Data pendukung tercantum pada naskah lampiran bagian awal. dan berdasarkan Surat Edaran Unit No. 96/2025. Berdasarkan hasil penelaahan menyeluruh, teridentifikasi peluang perbaikan terhadap keandalan layanan. Hal tersebut tercermin pada catatan harian verifikasi dokumen. dan mengindahkan Kebijakan Mutu No. 16/2022.

Analisis terdokumentasi mengindikasikan bahwa ditemukan ketidaksesuaian yang memerlukan tindakan korektif. Hal tersebut tercermin pada catatan harian verifikasi dokumen. dan berdasarkan Surat Edaran Unit No. 17/2022. Berdasarkan hasil penelaahan menyeluruh, ditemukan ketidaksesuaian yang

(a)



Rumah Sakit Umum Daerah Sentosa
Nomor: 9690/DOC/05/2022

Berita Acara Pemeriksaan

Nomor: BAK/2355/02/2022

Tanggal: 13 Desember 2023

Judul: Pemeriksaan Server

I. Pendahuluan

Berita acara ini dibuat sebagai hasil pemeriksaan terhadap Server Medis yang dilakukan pada tanggal 10 Juni 2021 di Surabaya.

Ruang Lingkup:

- Analisis konfigurasi Server Medis
- Identifikasi celah keamanan
- Verifikasi laporan sebelumnya
- Rekomendasi mitigasi risiko

II. Latar Belakang

Pemeriksaan dilakukan sebagai tindak lanjut dari data tidak sinkron yang ditemukan pada Maret.

(b)

Gambar 2. Tampilan PDF hasil dekripsi dengan kunci benar (a) dan kunci salah/decoy (b)

Hasil verifikasi menunjukkan bahwa seluruh 100 percobaan dengan kunci benar menghasilkan file dengan checksum yang identik dengan dokumen asli. Sebaliknya, seluruh 100 percobaan dengan kunci yang salah menghasilkan checksum yang berbeda, mengonfirmasi bahwa setiap keluaran merupakan dokumen umpan. Secara teoritis, sifat desain Honey Encryption yang menghasilkan keluaran valid untuk setiap kunci dapat diformulasikan sebagai minimisasi mutual information antara kunci dan keluaran dekripsi, $I(Key;Output) \approx 0$, sehingga percobaan brute-force tidak memperoleh umpan balik yang dapat membedakan kunci benar dari kunci salah. Probabilitas keberhasilan serangan tetap terikat pada peluang acak sebesar n/K, di mana n adalah jumlah percobaan dan K adalah ukuran ruang kunci. Hasil eksperimen yang diperoleh konsisten dengan ekspektasi teoritis tersebut.

Untuk mengkuantifikasi ketahanan sistem terhadap serangan brute-force secara lebih konkret, dilakukan analisis terhadap ruang kunci (key space) yang berlaku pada sistem yang diusulkan. Kunci enkripsi AES-CBC yang digunakan dalam sistem ini memiliki panjang 256 bit, sehingga ruang kunci mencapai $2^{256} \approx 1{,}16 \times 10^{77}$ kemungkinan nilai yang berbeda. Entropi kunci $H(K) = \log_2 K = 256$ bit menunjukkan bahwa penyerang harus meresolusi 256 bit ketidakpastian untuk menemukan kunci yang benar. Dengan asumsi serangan dapat mencoba 10^{12} kunci per detik menggunakan perangkat keras khusus, waktu yang dibutuhkan untuk menghabiskan seluruh ruang kunci setara dengan $10^{75} \times$ usia alam semesta, sehingga serangan brute-force terhadap kunci AES-256 dianggap tidak layak secara komputasional.

Dalam konteks Honey Encryption, ketahanan terhadap brute-force tidak hanya bergantung pada ukuran ruang kunci AES-256, tetapi juga pada ketidakmampuan penyerang untuk memvalidasi kebenaran kunci dari keluaran dekripsi. Pada enkripsi konvensional, penyerang dapat mereduksi ruang pencarian secara efektif dengan mengeliminasi kunci yang menghasilkan keluaran tidak valid. Mekanisme ini tidak berlaku pada sistem yang diusulkan karena setiap kunci selalu menghasilkan dokumen PDF yang tampak valid, sehingga $I(Key;Output) \approx 0$ mempertahankan entropi penuh ruang kunci selama proses serangan. Kondisi ini memaksa penyerang untuk tetap beroperasi dalam ruang pencarian penuh sebesar 2^{256}, tanpa keuntungan informasi dari setiap percobaan kunci yang gagal.

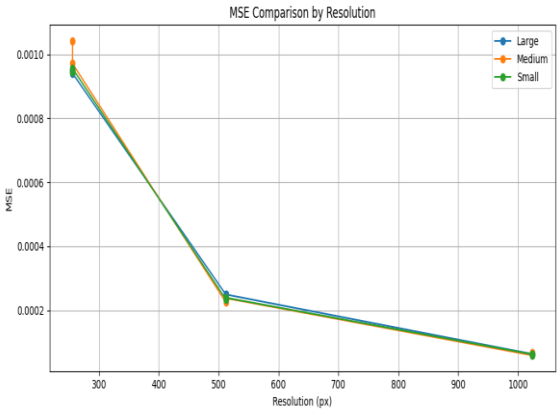
4.2 Pengujian Kualitas Visual (PSNR dan MSE)

Pengujian kualitas visual dilakukan untuk mengevaluasi sejauh mana proses penyisipan data mempengaruhi tampilan citra penampung. Dua metrik kuantitatif yang digunakan adalah Mean Square Error (MSE) dan Peak Signal-to-Noise Ratio (PSNR). MSE mengukur rata-rata kuadrat selisih intensitas piksel antara citra penampung asli dan stego image, sedangkan PSNR menyatakan rasio antara kekuatan sinyal maksimum citra terhadap noise yang diakibatkan oleh proses penyisipan, dinyatakan dalam satuan desibel (dB).

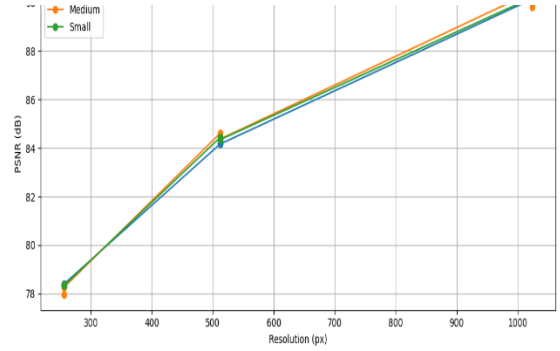
Perlu dicatat bahwa payload yang disisipkan ke dalam citra bukan dokumen PDF itu sendiri, melainkan seed terenkripsi beserta initialization vector (IV) yang berukuran kecil dan hampir konstan. Oleh karena itu, ukuran dokumen tidak berpengaruh langsung terhadap kualitas visual. Faktor utama yang menentukan kualitas visual adalah resolusi citra penampung, yang

menentukan jumlah piksel yang tersedia untuk mendistribusikan bit yang disisipkan.

Pengujian dilakukan pada tiga resolusi citra (256×256, 512×512, dan 1024×1024 piksel) dengan tiga kategori ukuran dokumen dan tiga dokumen per kategori, sehingga setiap konfigurasi diuji sebanyak tiga kali untuk memastikan konsistensi hasil. Nilai MSE dan PSNR dihitung melalui perbandingan piksel per piksel antara stego image dan citra penampung asli.



Gambar 3. Grafik MSE berdasarkan resolusi citra



Gambar 4. Grafik PSNR berdasarkan resolusi citra

Hasil pengujian menunjukkan tren yang konsisten: nilai MSE menurun seiring meningkatnya resolusi citra penampung. Pada resolusi 256×256 piksel, nilai MSE berkisar antara 0,00095 hingga 0,0010. Nilai tersebut turun signifikan ke kisaran 0,00022–0,00025 pada resolusi 512×512 piksel, dan mencapai nilai terendah sekitar 0,00006 pada resolusi 1024×1024 piksel. Sejalan dengan penurunan MSE, nilai PSNR meningkat dari kisaran 78–79 dB pada resolusi 256×256 piksel, menjadi 84–85 dB pada resolusi 512×512 piksel, dan mencapai 90–91 dB pada resolusi 1024×1024 piksel.

Nilai PSNR yang jauh melampaui ambang 40 dB (yang umumnya dianggap sebagai batas kualitas baik dalam analisis citra digital) mengindikasikan bahwa proses penyisipan tidak menimbulkan distorsi visual yang dapat dipersepsi oleh mata manusia. Tingginya nilai PSNR dan rendahnya nilai MSE pada seluruh konfigurasi pengujian membuktikan bahwa metode LSB yang diterapkan mempertahankan tingkat imperceptibility yang tinggi terlepas dari ukuran dokumen yang diamankan. Perlu ditekankan bahwa performa visual yang sangat baik ini merupakan konsekuensi langsung dari desain sistem di mana payload yang disisipkan hanya berupa seed terenkripsi dan IV dengan ukuran kecil dan hampir konstan, bukan dokumen PDF itu sendiri. Oleh karena itu, hasil PSNR dan MSE ini tidak dapat digeneralisasi untuk skenario steganografi dengan payload berukuran besar.

4.3 Pengujian Steganalisis (StegExpose)

Pengujian steganalisis dilakukan menggunakan StegExpose untuk mengevaluasi kemampuan sistem dalam menyembunyikan data tanpa terdeteksi oleh alat analisis forensik digital. StegExpose menggabungkan empat metode deteksi statistik, yaitu Sample Pair Analysis (SPA), RS Analysis, Chi-Square Attack, dan Primary Sets, kemudian menghitung fusion score sebagai rata-rata hasil keempat metode tersebut. Nilai fusion mendekati 0 mengindikasikan citra bersih tanpa pesan tersembunyi yang terdeteksi, sedangkan nilai mendekati 1 mengindikasikan kemungkinan tinggi adanya data tersembunyi.

Pengujian dilakukan pada stego image yang dihasilkan dari setiap kombinasi kategori dokumen (kecil, sedang, besar) dan resolusi citra (256, 512, 1024 piksel). Hasil pengujian disajikan pada Tabel 2.

Tabel 2. Hasil Deteksi Steganalisis Menggunakan StegExpose

Kategori	256 px	512 px	1024 px	Status
Kecil	0.0304	0.0287	0.0151	CLEAN
Sedang	0.0303	0.0288	0.0152	CLEAN
Besar	0.0304	0.0287	0.0151	CLEAN

Seluruh stego image yang diuji diklasifikasikan sebagai CLEAN dengan nilai fusion berada di bawah ambang 0,2, berkisar antara 0,015 hingga 0,031. Nilai ini konsisten di seluruh resolusi dan kategori ukuran dokumen. Efektivitas ini dapat dikaitkan dengan ukuran payload yang kecil (hanya seed terenkripsi dan IV) sehingga perubahan distribusi bit pada kanal warna citra tidak signifikan untuk dideteksi oleh algoritma StegExpose.

Tren penurunan nilai fusion seiring meningkatnya resolusi citra penampung juga memperkuat temuan pada pengujian PSNR dan MSE: semakin tinggi resolusi citra, semakin terdistribusi data yang disisipkan, sehingga semakin sulit bagi metode steganalisis untuk mendeteksi anomali statistik. Untuk mendalami hubungan ini, dilakukan analisis korelasi Pearson antara nilai PSNR/MSE dan fusion score StegExpose, dengan hasil yang disajikan pada Tabel 3.

Tabel 3. Hasil Analisis Korelasi PSNR/MSE dengan Fusion Score StegExpose

Hubungan	r	p-value	Kategori
PSNR vs Fusion	–0.90	< 0.001	Sangat tinggi
MSE vs Fusion	+0.72	< 0.001	Tinggi

Hubungan antara PSNR dan fusion score menghasilkan koefisien korelasi $r = -0{,}90$ ($p < 0{,}001$), yang dikategorikan sebagai korelasi sangat tinggi dengan arah negatif. Artinya, peningkatan PSNR yang merepresentasikan kualitas visual lebih tinggi berkorelasi dengan penurunan nilai fusion, sehingga stego image berkualitas lebih tinggi lebih sulit dideteksi oleh StegExpose. Hubungan antara MSE dan fusion score menghasilkan koefisien $r = +0{,}72$ ($p < 0{,}001$), yang dikategorikan sebagai korelasi tinggi dengan arah positif, mengonfirmasi bahwa distorsi piksel yang lebih besar meningkatkan kemungkinan deteksi. Temuan ini menunjukkan bahwa kualitas visual dan ketidakterdeteksian statistik merupakan dua dimensi yang saling berkaitan dan keduanya dapat dioptimalkan dengan memilih resolusi citra penampung yang lebih tinggi.

4.4 Perbandingan Perilaku Dekripsi Honey Encryption dan AES-CBC

Pengujian perbandingan dilakukan untuk menunjukkan perbedaan fundamental antara perilaku sistem Honey Encryption yang diusulkan dan sistem AES-CBC konvensional ketika proses dekripsi dijalankan menggunakan kunci yang benar maupun kunci yang salah. Verifikasi byte-level dilakukan menggunakan algoritma SHA-256 untuk memastikan keakuratan hasil pada kedua sistem. Perbandingan lengkap disajikan pada Tabel 4.

Tabel 4. Perbandingan Perilaku Dekripsi Honey Encryption dan AES-CBC

Aspek	Honey Encryption (HE)	AES-CBC Konvensional
Keluaran kunci benar	Dokumen asli berhasil dipulihkan (100/100)	Dokumen asli berhasil dipulihkan (100/100)
Keluaran kunci salah	File umpan dalam format PDF valid (0/100 identik)	File rusak atau tidak dapat dibuka (0/100 identik)
Validitas format	Selalu menghasilkan PDF yang dapat dibuka	PDF tidak valid, tidak dapat dibuka
Indikator kegagalan	Tersembunyi, tidak ada pesan error	Eksplisit, error padding/format mudah terdeteksi
Sifat probabilistik	Keluaran plausibel untuk semua kunci, $I(\text{Key};\text{Output}) \approx 0$	Keluaran mengungkap kebenaran kunci, $I(\text{Key};\text{Output}) > 0$

Ketika kunci yang benar digunakan, kedua sistem berhasil memulihkan dokumen asli dengan struktur file yang valid, dibuktikan dengan kehadiran header %PDF dan struktur internal yang sesuai format PDF. Perbedaan mendasar muncul ketika kunci yang salah digunakan.

Pada sistem AES-CBC konvensional, dekripsi dengan kunci salah menghasilkan data acak tanpa struktur yang dapat dikenali. File keluaran tidak memiliki header %PDF dan tidak dapat dibuka oleh aplikasi PDF reader manapun, disertai pesan error yang mengindikasikan kerusakan file. Kondisi ini memberikan umpan balik eksplisit kepada penyerang mengenai ketidakvalidan kunci yang digunakan, sehingga dapat dimanfaatkan untuk memvalidasi tebakan kunci secara sistematis dalam serangan brute-force.

Sebaliknya, pada sistem Honey Encryption yang diusulkan, dekripsi dengan kunci salah tetap menghasilkan file PDF yang valid secara struktural dan dapat dibuka secara normal. File tersebut berisi dokumen umpan dengan konten yang berbeda dari dokumen asli namun tampak seperti dokumen resmi yang autentik. Tidak ada pesan error maupun indikator kegagalan yang ditampilkan kepada pengguna. Mekanisme ini secara efektif menghilangkan umpan balik yang dapat dimanfaatkan penyerang, karena setiap percobaan dekripsi menghasilkan keluaran yang tampak sama validnya. Hal ini sejalan dengan sifat teoritis Honey Encryption yang meminimalkan mutual information antara kunci dan keluaran, $I(\text{Key};\text{Output}) \approx 0$, sehingga probabilitas keberhasilan brute-force tetap terikat pada peluang acak semata.

5. KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem keamanan dokumen multi-layer yang mengintegrasikan Honey Encryption berbasis AES-CBC dan steganografi LSB pada citra PNG. Berdasarkan hasil pengujian yang telah dilakukan, dapat ditarik kesimpulan sebagai berikut.

- Sistem berhasil mengimplementasikan mekanisme Honey Encryption menggunakan pendekatan Distribution Transforming Encoder (DTE) yang memetakan dokumen PDF ke seed acak 10 karakter alfanumerik. Seed tersebut dienkripsi dengan AES-CBC dan disisipkan ke dalam citra PNG melalui metode LSB, menghasilkan stego image yang secara visual tidak berbeda dari citra penampung asli.
- Sistem terbukti mampu menghasilkan dokumen umpan yang valid secara struktural ketika proses dekripsi dilakukan dengan kunci yang salah. Simulasi brute-force dengan 100 percobaan kunci benar dan 100 percobaan kunci salah menunjukkan bahwa seluruh percobaan dengan kunci benar menghasilkan dokumen asli (100/100), sementara seluruh percobaan dengan kunci salah menghasilkan dokumen umpan (0/100 identik dengan asli). Tidak ada indikator kegagalan yang terekspos kepada pengguna, sehingga penyerang tidak dapat membedakan keluaran benar dari keluaran umpan.
- Pengujian kualitas visual menunjukkan nilai PSNR yang sangat tinggi, berkisar antara 78–79 dB pada resolusi 256×256 piksel hingga 90–91 dB pada resolusi 1024×1024 piksel, dengan nilai MSE yang sangat rendah di seluruh konfigurasi. Nilai ini jauh melampaui ambang 40 dB yang umumnya dianggap sebagai indikator kualitas visual yang baik, membuktikan bahwa proses penyisipan tidak menimbulkan distorsi yang dapat dipersepsi secara visual.
- Pengujian steganalisis menggunakan StegExpose menghasilkan fusion score antara 0,015 hingga 0,031 pada seluruh kombinasi resolusi dan ukuran dokumen, jauh di bawah ambang deteksi 0,2. Seluruh stego image diklasifikasikan sebagai CLEAN, mengonfirmasi bahwa data yang disisipkan tidak menimbulkan anomali statistik yang dapat dideteksi. Analisis korelasi Pearson menunjukkan hubungan yang sangat kuat antara kualitas visual dan ketidakterdeteksian: PSNR berkorelasi negatif dengan fusion score ($r = -0{,}90$), sementara MSE berkorelasi positif ($r = +0{,}72$).
- Perbandingan perilaku dekripsi antara sistem Honey Encryption dan AES-CBC konvensional menunjukkan perbedaan yang fundamental. Sistem AES-CBC konvensional menghasilkan keluaran acak yang tidak dapat dibuka ketika kunci salah digunakan, memberikan umpan balik eksplisit kepada penyerang. Sebaliknya, sistem Honey Encryption selalu menghasilkan keluaran berformat PDF yang valid untuk kunci apapun, menghilangkan sinyal yang dapat dimanfaatkan dalam serangan brute-force dan mempertahankan probabilitas keberhasilan serangan pada batas peluang acak n/K.

Secara keseluruhan, penelitian ini menunjukkan bahwa integrasi Honey Encryption dan steganografi LSB dapat memberikan perlindungan dokumen digital yang lebih kuat melalui kombinasi mekanisme penyamaran kriptografis dan penyembunyian data. Namun demikian, terdapat beberapa

keterbatasan yang perlu diperhatikan. Pertama, karena setiap percobaan dekripsi selalu menghasilkan keluaran yang tampak valid, pengguna yang sah yang memasukkan kunci salah akibat kesalahan ketik tidak akan menerima indikator kegagalan yang jelas. Kedua, mekanisme pemulihan dokumen asli sepenuhnya bergantung pada ketersediaan tabel pemetaan JSON eksternal; apabila file tersebut hilang atau dikompromikan, dokumen asli tidak dapat dipulihkan meskipun kunci enkripsi diketahui. Ketiga, implementasi DTE dalam penelitian ini merupakan pendekatan yang disederhanakan tanpa pemodelan probabilistik formal, sehingga jaminan keamanan teoretis penuh dari konstruksi Honey Encryption formal belum sepenuhnya terpenuhi. Keempat, sistem menggunakan AES-CBC tanpa mekanisme autentikasi ciphertext seperti MAC atau authenticated encryption, sehingga integritas ciphertext tidak dapat diverifikasi sebelum proses dekripsi. Kelima, perbandingan baseline dalam penelitian ini terbatas pada AES-CBC konvensional; perbandingan dengan konfigurasi lain seperti steganografi dengan payload penuh atau metode HE berbasis distribusi yang lebih kompleks belum dilakukan. Keterbatasan-keterbatasan ini dapat menjadi arah pengembangan pada penelitian selanjutnya.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada I Ketut Purnamawan, S.Kom., M.Kom. dan Ir. Ketut Agus Seputra, S.ST., M.T. selaku penguji, atas masukan dan saran konstruktif yang diberikan sehingga penelitian ini dapat berkembang menjadi lebih baik.

DAFTAR PUSTAKA

[1] S. Saeed and others, “Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations,” *Sensors*, vol. 23, no. 15, 2023, doi: 10.3390/s23156666.

[2] W. S. Admass and others, “Cyber security: State of the art, challenges and future directions,” *Cyber Security and Applications*, vol. 2, no. 2, p. 100031, 2024, doi: 10.1016/j.csa.2023.100031.

[3] S. Fatima and others, “Comparative analysis of AES and RSA algorithms for data security in cloud computing,” in *Proc. IEEC*, 2022. doi: 10.3390/engproc2022020014.

[4] S. Oktaviani and others, “Analisis keamanan data dengan menggunakan kriptografi modern algoritma Advance Encryption Standard (AES),” *Jurnal Media Informatika*, vol. 4, no. 2, pp. 97–101, 2023, doi: 10.55338/jumin.v4i2.435.

[5] H. Zodpe and A. Shaikh, “A survey on various cryptanalytic attacks on the AES algorithm,” *International Journal of Next-Generation Computing*, vol. 12, no. 2, pp. 115–123, 2021, doi: 10.47164/ijngc.v12i2.756.

[6] I. Alkhwaja and others, “Password cracking with brute force algorithm and dictionary attack using parallel programming,” *Applied Sciences*, vol. 13, no. 10, p. 5979, 2023, doi: 10.3390/app13105979.

[7] A. Majeed and A. S. Noori, “Honey encryption security techniques: A review paper,” *AL-Rafidain Journal of Computer Sciences and Mathematics*, vol. 16, no. 1, pp. 1–14, 2022, doi: 10.33899/csmj.2022.174390.

[8] K. Ravindranadh and others, “Data migration in cloud computing using honey encryption,” *International Journal of Engineering and Technology*, vol. 7, no. 2.8, p. 230, 2018, doi: 10.14419/ijet.v7i2.8.10415.

[9] W. Luo and others, “A comprehensive survey of digital image steganography and steganalysis,” *APSIPA Trans. Signal Inf. Process.*, vol. 13, no. 1, 2024, doi: 10.1561/116.20240038.

[10] S. Rustad and others, “Inverted LSB image steganography using adaptive pattern to improve imperceptibility,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 3559–3568, 2022, doi: 10.1016/j.jksuci.2020.12.017.

[11] M. Dalal and M. Juneja, “Steganography and steganalysis (in digital forensics): A cybersecurity guide,” *Multimed. Tools Appl.*, vol. 80, 2020, doi: 10.1007/s11042-020-09929-9.

[12] S. Jain and others, “Honey2Fish—A hybrid encryption approach for improved password and message security,” in *IEEE BigDataSecurity / HPSC / IDS*, 2023, pp. 198–203. doi: 10.1109/bigdatasecurity-hpsc-ids58521.2023.00042.

[13] N. Mehta and M. V Naiyer, “An approach of security on cloud computing using honey encryption technique,” *International*

Journal of Current Science, vol. 14, no. 2, pp. 2250–2270, 2024.

[14] M. Alanzy and others, "Image steganography using LSB and hybrid encryption algorithms," *Applied Sciences*, vol. 13, no. 21, p. 11771, 2023, doi: 10.3390/app132111771.

[15] E. G. Jacinto and others, "Enhanced security: Implementation of hybrid image steganography technique using low-contrast LSB and AES-CBC cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, 2022, doi: 10.14569/ijacsa.2022.01308104.

[16] M. A. Firdaus and A. Rahmatulloh, "Implementasi steganografi citra digital LSB menggunakan enkripsi AES-256 dan embedding pseudorandom," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 1, 2025, doi: 10.23960/jitet.v13i1.5620.

[17] A. M. Ramadhani and T. Hasanuddin, "Modifikasi least significant bits pada gambar sebagai data hiding steganography," *Indonesian Journal of Data Science*, vol. 2, no. 2, pp. 91–102, 2021, doi: 10.56705/ijodas.v2i3.48.

[18] S. Fadel and others, "Analisis keamanan steganografi teks dengan metode LSB (Least Significant Bit) pada citra digital," *Journal of Computer Science and Information Technology*, vol. 5, no. 1, pp. 36–41, 2024, doi: 10.37859/coscitech.v5i1.6759.