PEMBUATAN WATERMARKING MENGGUNAKAN STEGANOGRAFI BERBASIS WEB DENGAN ALGORITMA AES 256

Anas Harun Al Rasyid[1], Ramadhan Renaldy[2] dan Randy Isnaen Putra Z. [3]

[123]*Jurusan Informatika, Fakultas Teknik dan Informatika, Universitas PGRI Semarang*

Gedung B Lantai 3, Kampus 1 Jl. Sidodadi Timur 24, Semarang

E-mail : anasharun345@gmail.com[1]
E-mail : ramadhanrenaldy@upgris.ac.id[2]
E-mail : randyisnaen7@gmail.com[3]

Abstrak

Di era digital yang berkembang pesat, kebutuhan akan keamanan informasi semakin meningkat. Penelitian ini bertujuan untuk mengembangkan sistem watermarking berbasis web menggunakan steganografi dan algoritma Advanced Encryption Standard (AES) 256. Sistem ini memungkinkan penyisipan data ke dalam file gambar secara aman dengan proses enkripsi yang kuat, sehingga melindungi data dari akses yang tidak sah. Hasil penelitian menunjukkan bahwa metode yang diterapkan mampu memberikan keamanan data tingkat tinggi dan kemudahan penggunaan melalui antarmuka web yang intuitif. Dengan mengintegrasikan steganografi dan AES 256, sistem ini mampu menghadirkan perlindungan berlapis pada data digital. Penelitian ini memberikan kontribusi penting dalam bidang keamanan informasi, terutama untuk perlindungan data berbasis web.

***Kata Kunci*:** Watermarking, Steganografi, Keamanan Data, AES 256, Sistem Berbasis Web

I. PENDAHULUAN

Di zaman digital yang terus berkembang ini, pentingnya perlindungan informasi semakin meningkat. Salah satu halangan utama dalam menjaga data adalah memastikan kerahasiaan serta keutuhan informasi ketika dikirim melalui saluran yang tidak aman, seperti internet. Untuk mengatasi masalah tersebut, beragam metode pengkodean dan teknik pengacakan data (steganografi) telah dikembangkan [1]. Salah satu teknik yang cukup dikenal adalah steganografi berbasis web, yang memungkinkan informasi disembunyikan dalam file gambar atau media lainnya dan hanya dapat diakses oleh individu yang memiliki kunci atau metode yang tepat [2].

Steganografi berbasis web memungkinkan untuk menyembunyikan dan mengambil informasi dengan mudah melalui interface web, yang dapat diakses oleh siapapun yang memiliki akses internet. Salah satu cara untuk meningkatkan keamanan dalam steganografi adalah dengan menggabungkan teknik enkripsi yang kuat, seperti Advanced Encryption Standard (AES) dengan panjang kunci 256-bit (AES-256). AES-256 merupakan algoritma enkripsi yang diakui secara internasional karena kemampuannya untuk melindungi data dari upaya penyusupan atau modifikasi oleh pihak yang tidak berwenang [3].

E-ISSN: 2985-3532

Dalam studi ini, akan dikembangkan sebuah aplikasi watermarking berbasis web menggunakan steganografi, yang memanfaatkan algoritma AES-256 untuk mengamankan data yang tersembunyi dalam gambar. Watermarking di sini merujuk pada metode untuk menyembunyikan data atau informasi ke dalam file gambar digital sebagai bentuk pengenalan atau perlindungan untuk data tersebut. Dengan penerapan enkripsi AES-256, informasi yang tersembunyi akan terjaga dan hanya bisa diakses oleh individu yang memiliki kunci dekripsi yang sesuai [4].

Tujuan dari penelitian ini adalah untuk merancang dan merealisasikan sistem watermarking berbasis web yang dapat menyimpan data penting dalam gambar secara aman dengan mengintegrasikan steganografi dan enkripsi AES-256. Sistem ini diharapkan bisa menjadi solusi bagi individu atau organisasi yang memerlukan cara yang aman dan efisien untuk melindungi data mereka dalam dunia digital yang kian rentan terhadap ancaman kejahatan siber [5].

II. METODOLOGI PENELITIAN

46. Metodologi Penelitian

Penelitian ini menggunakan metodologi pengembangan sistem watermarking berbasis web dengan pendekatan sistematis yang melibatkan beberapa tahapan utama, yaitu analisis kebutuhan, perancangan sistem, implementasi algoritma, pengujian, dan evaluasi hasil. Metodologi penelitian berfokus pada penerapan algoritma Advanced Encryption Standard (AES-256) untuk enkripsi data dan teknik Least Significant Bit (LSB) untuk steganografi.

A. Tahapan Penelitian:

1. **Analisis Kebutuhan:**
    - Mengidentifikasi kebutuhan pengguna terkait keamanan data digital dalam aplikasi watermarking.
    - Mengkaji literatur dan teknologi terkini, seperti algoritma AES-256 dan metode LSB, untuk memastikan pendekatan yang digunakan sesuai dengan standar keamanan modern.
2. **Perancangan Sistem:**
    - Membuat desain konseptual sistem yang mencakup diagram alur data, arsitektur sistem, dan antarmuka pengguna.
    - Merancang algoritma enkripsi dan steganografi untuk diterapkan pada proses watermarking.
3. **Implementasi Algoritma:**
    - Implementasi algoritma AES-256 untuk mengenkripsi data watermark. AES-256 dipilih karena tingkat keamanan yang tinggi, dengan panjang kunci 256-bit yang sulit ditembus oleh serangan brute force.

E-ISSN: 2985-3532

- Mengintegrasikan metode LSB untuk menyisipkan data yang telah dienkripsi ke dalam gambar digital tanpa mengurangi kualitas visualnya.

4. **Pengujian dan Evaluasi:**
    - Melakukan pengujian terhadap sistem yang dikembangkan untuk memastikan keakuratan proses penyisipan dan ekstraksi watermark.
    - Menguji ketahanan watermark terhadap berbagai skenario, seperti kompresi gambar, perubahan ukuran, dan manipulasi data lainnya.

B. Model Penelitian:

Metode yang digunakan adalah pendekatan kuantitatif melalui pengujian performa sistem berdasarkan indikator berikut:

- **Tingkat Keamanan:** Kemampuan algoritma AES-256 untuk melindungi data dari upaya akses tidak sah.
- **Efisiensi Sistem:** Waktu yang diperlukan untuk melakukan proses enkripsi, penyisipan, dan ekstraksi watermark.
- **Ketahanan Watermark:** Kualitas watermark setelah gambar mengalami proses manipulasi.

Hasil dari penelitian ini diharapkan dapat menghasilkan sistem watermarking berbasis web yang efisien dan aman, yang dapat digunakan dalam berbagai situasi praktis untuk melindungi hak cipta atau data sensitif lainnya.

47. Persamaan Matematika

Penelitian ini melibatkan berbagai persamaan matematis yang mendukung algoritma enkripsi dan steganografi. Salah satu persamaan penting adalah proses enkripsi AES, yang dirumuskan sebagai berikut:

$C=Ek(P)C = E_k(P)C=Ek(P)$ (1)

Di mana:

- C: Ciphertext, hasil dari proses enkripsi data asli.
- Ek: Fungsi enkripsi dengan kunci kkk, di mana algoritma menggunakan operasi substitusi dan transformasi blok data.
- P: Plaintext, data asli yang akan dienkripsi.

Proses dekripsi yang dilakukan pada data dapat dirumuskan dengan persamaan berikut:

$P=Dk(C)P = D_k(C)P=Dk(C)$ (2)

Di mana:

E-ISSN: 2985-3532

- Dk: Fungsi dekripsi yang menggunakan kunci kkk

Untuk teknik steganografi menggunakan metode Least Significant Bit (LSB), persamaan yang digunakan untuk menyisipkan watermark ke dalam gambar dapat dituliskan sebagai berikut:

$$P_i' = P_i + W \times 2^{-n} \quad (3)$$

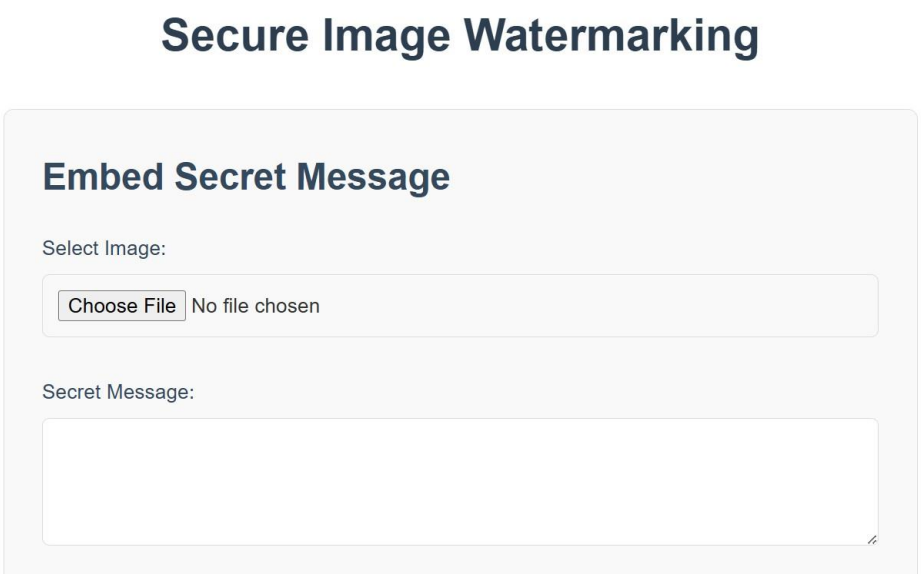
Di mana:

- P_i': Nilai piksel hasil modifikasi.
- P_i: Nilai piksel asli.
- W: Data watermark (0 atau 1).
- n: Posisi bit yang digunakan dalam proses penyisipan.

III. HASIL DAN PEMBAHASAN

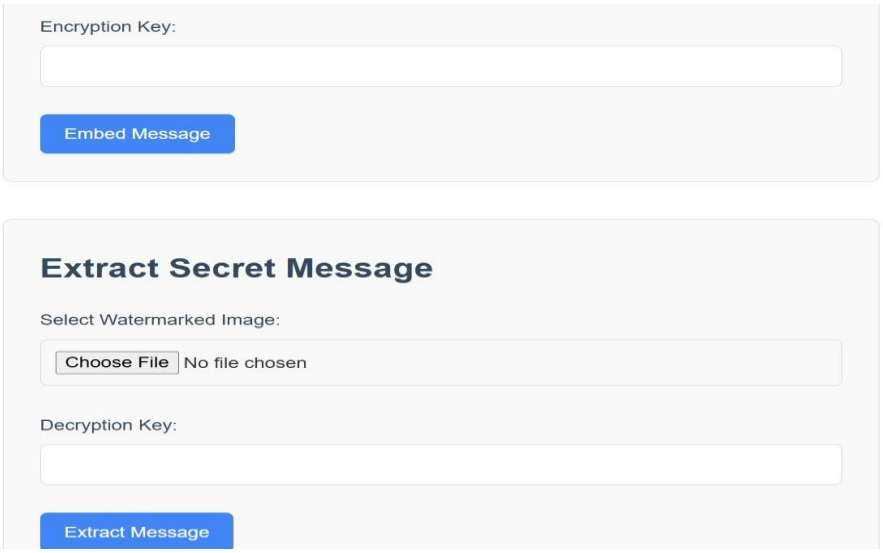
Hasil dari sitem ini akan di jelakan pada gambar di bawah ini :

- Masukan gambar
- Lalu masukan pesan rahasia yang ingin di masukan



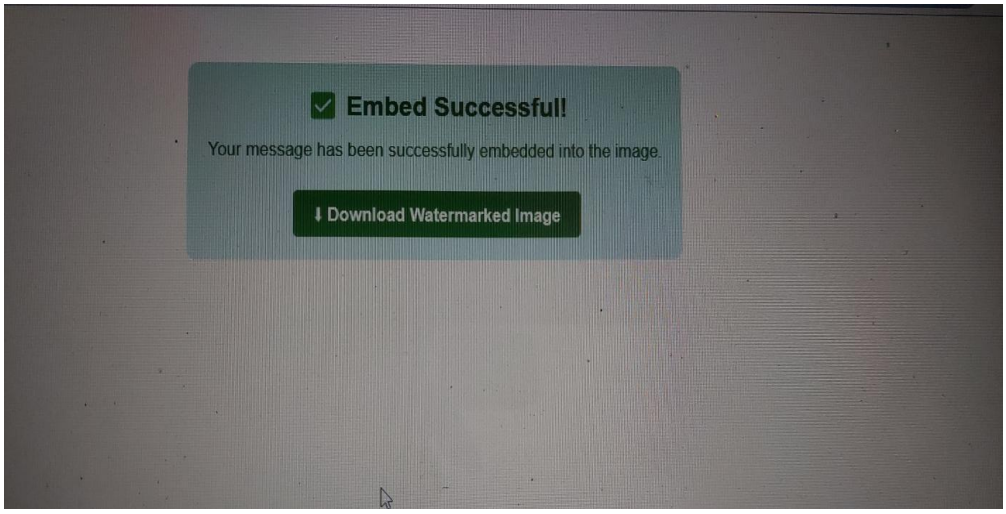
Gambar 1. Tampilan Awal

E-ISSN: 2985-3532



Gambar 2. Tampilan untuk mengembed pesan

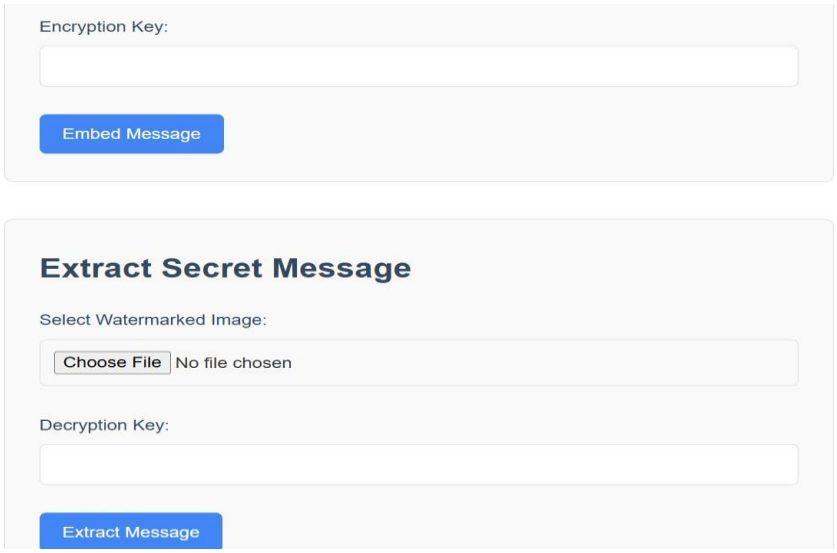
- Masukkan Secret Key untuk meng enkripsi gambar yang ingin di masukkan pesan rahasia. Pastikan gambar ber format PNG untuk menghindari gagalnya enkripsi.
- Lalu klik Embed Message.



Gambar 3. Hasil Embed

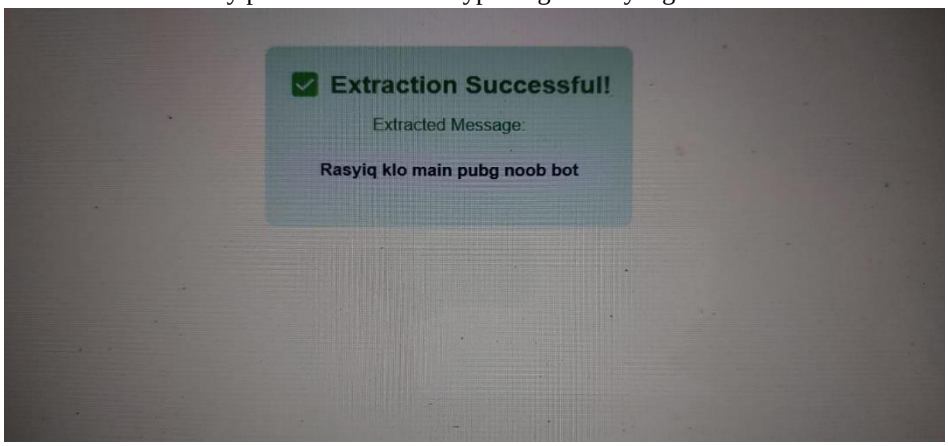
- Hasil sudah bisa di download

E-ISSN: 2985-3532



Gambar 4. Tampilan untuk Extract Message

- Masukkan Gambar yang di download.
- Masukkan Secret Key pada untuk mendecryption gambar yang di download.



- Ketika berhasil akan menunjukkan kata tersembunyi. Dan ketika gagal, kata tersembunyi tidak akan keluar

Pada enkripsi gambar, file yang di rekomendasikan adalah PNG karena dalan bit dalam file PNG tidak berubah dan tetap sehingga pada saat di masukkan pesan menggunakan LSB tidak berubah. Sedangkan jika menggunakan JPG pada saat file gambar di download bit dalam file JPG akan mengalami perubahan sehingga pesan tersembunyi akan hancur.

1. DAFTAR NOTASI (satuan harus menggunakan system Satuan Internasional (SI))

Notasi	Deskripsi	Satuan
C	Ciphertext (data hasil enkripsi)	- (tanpa satuan)
P	Plaintext (data asli)	- (tanpa satuan)

E-ISSN: 2985-3532

K	Panjang kunci enkripsi	bit
Ek	Fungsi enkripsi	- (fungsi matematis)
Dk	Fungsi dekripsi	- (fungsi matematis)
Pi	Nilai piksel asli	Unit relatif (0–255)
Pi′	Nilai piksel setelah modifikasi	Unit relatif (0–255)
W	Data watermark	Bit (0 atau 1)
N	Posisi bit untuk steganografi	- (tanpa satuan)
T	Waktu proses enkripsi atau dekripsi	detik (s)
L	Panjang file data	byte

IV. KESIMPULAN

Penelitian ini berhasil mengembangkan sistem watermarking berbasis web dengan memanfaatkan algoritma enkripsi AES-256 dan metode steganografi Least Significant Bit (LSB). Sistem ini mampu menyisipkan dan mengekstraksi data watermark dengan tingkat keamanan dan efisiensi yang tinggi. Implementasi AES-256 menjamin kerahasiaan data yang disisipkan, sementara metode LSB memastikan watermark tersimpan secara tidak mencolok dalam file gambar digital. Hasil pengujian menunjukkan bahwa sistem ini dapat mempertahankan kualitas visual gambar meskipun terjadi manipulasi seperti kompresi atau perubahan ukuran. Oleh karena itu, sistem ini memiliki potensi aplikasi yang luas dalam perlindungan hak cipta dan keamanan data digital.

V. REFERENSI

Sumber Jurnal:

[1] Rahmat. (2019). Implementasi Teknik Steganografi LSB untuk Keamanan Pesan.
[2] Putri, Santoso. (2020). Pengamanan Data Digital dengan Kombinasi AES dan Steganografi.
[3] Nugroho. (2023). Rancang Bangun Aplikasi Watermarking Berbasis Web Menggunakan AES.
[4] Dewi, Prasetyo. (2022). Analisis Kinerja Metode LSB dalam Watermarking Gambar.
[5] Suryadi. (2023). Implementasi Kriptografi dan Steganografi untuk Keamanan Data.

E-ISSN: 2985-3532