

BAB V PENUTUP

5.1 Kesimpulan

Berdasarkan serangkaian tahapan penelitian yang meliputi studi literatur, Perancangan Algoritma dan Arsitektur Sistem., implementasi kode program, hingga pengujian dan analisis hasil terhadap sistem *invisible watermarking* berbasis *Edge Detection* dan *Arnold Cat Map*, maka dapat ditarik beberapa kesimpulan mendalam yang menjawab rumusan masalah penelitian, yaitu:

1. **Keberhasilan Implementasi Algoritma Hibrida pada Platform Web** Penelitian ini telah berhasil merancang dan membangun sebuah perangkat lunak *watermarking* yang mengintegrasikan tiga metode berbeda: *Least Significant Bit (LSB)* sebagai metode penyisipan, *Canny Edge Detection* sebagai penentu lokasi penyisipan, dan *Arnold Cat Map (ACM)* sebagai algoritma keamanan. Sistem ini diimplementasikan menggunakan bahasa pemrograman Python dengan kerangka kerja (*framework*) Flask, yang memungkinkan pengguna untuk melakukan proses enkripsi dan dekripsi melalui antarmuka berbasis web yang interaktif. Berdasarkan pengujian fungsionalitas (*Black Box Testing*), seluruh fitur utama mulai dari *upload* citra, pengaturan parameter kunci enkripsi (P , Q , N), proses penyisipan pada area tepi, hingga ekstraksi Kembali telah berjalan 100% valid sesuai dengan rancangan sistem tanpa adanya *error* pada saat eksekusi.
2. **Kualitas Visual (Imperceptibility) yang Superior Berkat Deteksi Tepi** Salah satu temuan utama dalam penelitian ini adalah efektivitas penggunaan metode *Canny Edge Detection* dalam meningkatkan aspek *imperceptibility* (ketidaktampakan). Metode *LSB* konvensional cenderung menyisipkan bit secara merata ke seluruh piksel, yang

seringkali menimbulkan noise visual pada area halus (smooth region) seperti langit atau kulit wajah.

Sebaliknya, sistem yang dibangun dalam penelitian ini secara cerdas hanya menyisipkan bit watermark pada piksel-piksel yang teridentifikasi sebagai tepi (*edge*). Hal ini memanfaatkan kelemahan Sistem Visual Manusia (*Human Visual System* - HVS) yang kurang sensitif terhadap perubahan kontras pada area bertekstur rumit. Bukti empiris dari keberhasilan ini terlihat pada hasil perhitungan *Peak Signal-to-Noise Ratio* (PSNR) terhadap tiga citra uji standar yang menunjukkan angka rata-rata yang sangat tinggi, yaitu:

- Citra Lena: Menghasilkan PSNR sebesar 69.08 dB.
- Citra Baboon: Menghasilkan PSNR sebesar 69.74 dB.
- Citra Peppers: Menghasilkan PSNR sebesar 69.17 dB. Nilai-nilai tersebut berada jauh di atas ambang batas standar kualitas citra yang baik (40 dB), yang mengindikasikan bahwa citra stego yang dihasilkan hampir identik secara sempurna dengan citra aslinya secara kasat mata.

3. Tingkat Keamanan Data (*Security*) yang Terjamin melalui Enkripsi ACM Penelitian ini juga berhasil menjawab masalah keamanan yang sering menjadi kelemahan metode LSB murni. Penerapan algoritma Arnold Cat Map (ACM) terbukti mampu memberikan lapisan perlindungan yang kuat (*robustness against visual attack*). Sebelum disisipkan, struktur citra watermark diacak posisinya (*scrambling*) berdasarkan kombinasi kunci rahasia (P , Q) dan jumlah iterasi (N).

Berdasarkan hasil pengujian keamanan, ditemukan bahwa proses ekstraksi hanya akan berhasil memunculkan logo watermark jika dan hanya jika kunci yang dimasukkan sama persis dengan kunci penyisipan. Kesalahan input pada satu parameter saja (misalnya nilai P

bergeser 1 angka) akan menyebabkan kegagalan dekripsi total, di mana hasil yang ditampilkan hanyalah citra noise acak yang tidak bermakna. Hal ini membuktikan bahwa sistem memiliki tingkat kerahasiaan (confidentiality) yang tinggi dan memenuhi syarat sebagai sistem pengamanan hak cipta digital.

4. Karakteristik Ketahanan (Robustness) Sistem Meskipun unggul dalam kualitas visual dan keamanan, harus diakui bahwa metode penyisipan pada domain spasial (LSB pada area tepi) memiliki karakteristik fragile atau rapuh. Berdasarkan pengujian serangan (attack simulation), sistem terbukti sangat sensitif terhadap manipulasi geometri dan kompresi. Serangan berupa cropping, resizing, atau kompresi JPEG dapat merusak struktur bit LSB pada area tepi, yang mengakibatkan kegagalan proses ekstraksi. Oleh karena itu, sistem ini disimpulkan lebih cocok diterapkan untuk kebutuhan autentikasi keaslian data (tamper detection) pada media penyimpanan lossless (seperti PNG/BMP), dibandingkan untuk perlindungan hak cipta pada media sosial yang menerapkan kompresi otomatis.

5.2 Saran

Penelitian ini merupakan langkah awal dalam pengembangan sistem watermarking cerdas. Demi penyempurnaan sistem dan pengembangan ilmu pengetahuan di masa mendatang, penulis mengajukan beberapa saran konstruktif yang dapat dijadikan rujukan bagi peneliti selanjutnya:

1. Transformasi ke Domain Frekuensi untuk Meningkatkan Ketahanan Mengingat sifat metode LSB yang rapuh (fragile) terhadap kompresi dan manipulasi citra, peneliti selanjutnya sangat disarankan untuk mengembangkan metode ini dengan beralih dari domain spasial ke domain frekuensi. Penggabungan metode Edge Detection dengan transformasi frekuensi seperti Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), atau Singular Value Decomposition (SVD) diyakini

dapat meningkatkan ketahanan (robustness) watermark terhadap serangan kompresi JPEG tanpa mengorbankan kualitas visual secara signifikan.

2. Implementasi pada Citra Berwarna (RGB Imagery) Sistem yang dibangun saat ini masih terbatas pada pengolahan citra berskala keabuan (grayscale). Mengingat mayoritas media digital saat ini berupa citra berwarna, pengembangan selanjutnya diharapkan dapat mendukung citra format RGB. Peneliti dapat mengeksplorasi teknik penyisipan pada kanal warna tertentu (misalnya kanal Biru atau Blue Channel) karena mata manusia diketahui paling kurang sensitif terhadap perubahan pada warna biru, sehingga kapasitas penyisipan dapat ditingkatkan tanpa merusak estetika gambar.
3. Penggunaan Metode Adaptif untuk Optimalisasi Kapasitas Kapasitas penyisipan data pada sistem ini sangat bergantung pada jumlah tepi yang terdeteksi oleh algoritma Canny. Citra yang memiliki tekstur halus (sedikit tepi) akan memiliki kapasitas tampung (payload) yang sangat kecil. Untuk mengatasi hal ini, disarankan menggunakan metode Adaptive Thresholding atau Region of Interest (ROI) yang dinamis. Algoritma dapat dirancang untuk secara otomatis menurunkan ambang batas deteksi tepi jika kapasitas dirasa kurang, sehingga sistem dapat menyeimbangkan antara kebutuhan kapasitas data dan kualitas visual secara otomatis.
4. Peningkatan Algoritma Keamanan Kriptografi Meskipun Arnold Cat Map sudah cukup baik dalam mengacak posisi piksel, keamanan sistem dapat ditingkatkan lagi dengan mengombinasikannya dengan algoritma kriptografi modern. Peneliti selanjutnya dapat menyandikan bit watermark menggunakan algoritma AES (Advanced Encryption Standard) atau RSA sebelum dilakukan pengacakan posisi dengan ACM. Hal ini akan memberikan keamanan berlapis (double layer security), di mana penyerang harus memecahkan dua algoritma sekaligus untuk mendapatkan citra watermark yang asli.

5. Pengembangan Platform Menjadi Aplikasi Mobile Guna memperluas jangkauan penggunaan, sistem ini dapat dikembangkan lebih lanjut menjadi aplikasi berbasis mobile (Android atau iOS). Dengan demikian, pengguna dapat melakukan perlindungan hak cipta pada foto hasil jepretan kamera smartphone secara real-time sebelum mengunggahnya ke internet. Integrasi dengan layanan cloud storage juga dapat dipertimbangkan untuk penyimpanan kunci rahasia yang lebih aman dan termanajemen.

