

BAB I

PENDAHULUAN

1.1. Latar Belakang

Di era pertukaran informasi digital yang berkembang pesat, keamanan Informasi menjadi sangat penting (Musri et al., 2020). Steganografi merupakan suatu metode yang efektif untuk menyembunyikan informasi rahasia tanpa menarik perhatian pihak yang tidak berhak (Syahril & Jaya, 2019). Penerapan steganografi pada file steganografi multimedia seperti audio, video, gambar dan dokumen. memberikan keunggulan dalam memanfaatkan media visual untuk menyembunyikan data. *Low Bit Coding* menjadi salah satu metode yang menarik karena dapat menyisipkan informasi pada bit yang kurang signifikan, mengoptimalkan kapasitas penyisipan tanpa mengorbankan kualitas file steganografi multimedia secara signifikan. Dengan meningkatnya frekuensi dan kecerdasan serangan *siber*, kebutuhan akan metode keamanan yang kuat semakin mendesak (Chaharlang et al, 2020).

Steganografi muncul sebagai solusi untuk menyembunyikan data sensitif dari pihak yang tidak berhak dalam industri kreatif, penggunaan steganografi file steganografi memungkinkan pelacakannya untuk melindungi hak cipta pada karya seni, foto, audio atau video dokumen. Sehingga harus adanya keamanan dengan perlunya enkripsi aes. Kombinasi steganografi file steganografi dengan *Low Bit Coding* pada file steganografi multimedia bertujuan untuk mengoptimalkan kapasitas penyisipan informasi (Darwis & Dedi 2019).

Metode steganografi yang paling umum pada tipe berkas audio dan gambar adalah low bit coding atau *least significant bit*. Teknik *low bit coding* adalah cara yang digunakan untuk menyimpan data kedalam file steganografi multimedia seperti gambar, audio, video dan dokumen yang implementasikan dengan mengganti bit-bit yang paling akhir atau *low significant bit* metode ini berasal dari angka yang paling kurang signifikan dari jumlah bit dalam 1byte pada setiap titik sampling dengan string berkode biner (coded binary string), dapat menyisipkan sejumlah besar data ke dalam suara digital (Ramadani, 2019). Dengan memilih bit

yang kurang signifikan, diharapkan kualitas file steganografi multimedia semakin lebih baik. (Mulyono et al, 2019)

Metode *Low Bit Coding* ini memberikan kapasitas penyisipan yang lebih tinggi dibandingkan dengan beberapa metode steganografi lainnya ketahanan terhadap deteksi penerapan pada bit yang kurang signifikan membuat informasi rahasia lebih sulit dideteksi, terutama oleh algoritma deteksi yang mengandalkan perubahan visual yang signifikan. Efisiensi dan Kinerja yang Baik *Low Bit Coding* dapat diimplementasikan dengan biaya komputasi yang rendah, memberikan efisiensi dan kinerja yang baik (Ilham et al, 2023).

Pada penelitian ini menggunakan media digital yang digunakan sebagai wadah penampungan suara (audio), dan citra (image), video dan dokumen. Dengan beberapa file multimedia penelitian ini mendapatkan hasil yang lebih maksimal dan pengujian terhadap file steganografi multimedia.

Pemilihan media pembawa pesan ini di dasari dari hasil keluaran akhir dengan tingkat akurasi dan kualitas file steganografi multimedia. dari hasil steganografi memiliki persepsi yang sama dengan aslinya, tentunya persepsi disini sebatas kemampuan indra manusia, tetapi tidak oleh komputer atau pengolah digital lainnya. Maka dari itu diperlukan pengujian terhadap mutu (fidelity) steganografi dengan mengukur Mean Square Error (MSE) atau nilai kedekatan antara estimator dengan nilai yang di estimasi dan Peak Signal to Noise Ratio (PSNR) atau perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau berpengaruh pada sinyal tersebut, keduanya merupakan nilai yang memiliki satuan Db (desibels). Semakin rendah nilai MSE maka kualitas citra semakin baik begitupun sebaliknya. Sementara itu, mutu stego-image dikatakan baik jika nilai PSNR 40 dB atau lebih dan jika nilai PSNR rendah maka semakin turun kualitas citra (Pamungkas et al, 2020).

Berdasarkan penelitian sebelumnya yang dilakukan oleh Rika Humayrah, Andi Marwan Elhanafi, dkk mengenai pengujian terhadap dua buah citra berdasarkan penelitian tersebut pada setiap cover citra memiliki nilai MSE, dan PSNR yang berbeda. Dari Analisa pengujian diketahui bahwa jika cover citra yang digunakan sama, dengan jumlah karakter teks yang sama dan kunci yang sama,

maka nilai MSE dan PSNR sama. Jika cover citra yang digunakan sama dengan jumlah karakter teks yang sama namun kunci berbeda, maka hasil nilai MSE dan PSNR berbeda. Jika cover citra yang digunakan sama namun jumlah karakter teks berbeda dengan kunci yang sama, maka nilai MSE dan PSNR yang dihasilkan berbeda. Dapat disimpulkan bahwa jika salah satu dari bahan uji coba ada yang berbeda maka hasil MSE dan PSNR yang dihasilkan akan berbeda, hanya bahan uji coba yang memiliki semua kesamaan yang memiliki nilai MSE dan PSNR yang sama. Diketahui bahwa semakin rendah nilai MSE maka semakin baik kualitas dari stego citra, dan semakin tinggi nilai PSNR maka semakin baik pula kualitas hasil stego citra yang diencoding. Dari Analisa pengujian di atas dapat dilihat bahwa yang memiliki nilai MSE terendah dan PSNR tertinggi merupakan cover citra format. Jpg dengan nilai MSE 0.00251 dan PSNR 74.12625 decibel dan yang memiliki nilai MSE tertinggi dan PSNR terendah merupakan cover citra format.png yaitu nilai MSE 0.18888 dan PSNR 55.36899 decibel. Dapat disimpulkan bahwa dari ketiga cover citra yang memiliki kualitas citra paling baik yaitu cover citra yang berformat .jpg dan kualitas citra kurang baik yaitu cover citra yang berformat png (Humayrah et al, 2022).

Adapun berdasarkan penelitian yang dilakukan oleh Ibnu Utomo Wahyu Mulyono, dkk dari hasil penelitian 50 citra dan audio berdurasi 2 – 4 menit didapatkan hasil bahwa proses stegonografi telah berhasil dilakukan dan mendapatkan hasil yang baik, dimana kapasitas audio berkisar antara 195bit sampai 32550 bit pesan. Setelah dilakukan penyisipan, stego audio memiliki MSE 0 dan PSNR tidak terhingga atau diatas 40dB, yang berarti audio tidak berubah setelah disisipi pesan maka dapat dikatakan akurasi dan kualitas dari hasil stegono itu baik. (Mulyono et al, 2019).

Berdasarkan penelitian oleh Dufan J. P. Manajang, Sherwin R.U.A dkk tahun 2020 dengan judul Implementasi tensorflow object detention dalam mengklasifikasi jenis kendaraan bermotor. Hasil pengujian tingkat akurasi deteksi objek yang dilakukan pada kelima file video yang digunakan sebagai video uji coba dapat dilihat pada tabel VI. Rata-rata tingkat akurasi deteksi objek pada pengujian kelima file video uji coba adalah 90.8%. Nilai overall accuracy yang

tinggi belum menjamin ketepatan dari algoritma deteksi objek yang digunakan dalam melakukan deteksi dan klasifikasi, hal ini dapat dilihat dari nilai precision dan nilai recall setiap class. Misalkan, meskipun nilai overall accuracy yang ada pada file video4.mp4 adalah 100%, namun file video4.mp4 memiliki nilai recall yang rendah pada masing-masing class dikarenakan ada beberapa objek yang tidak dapat terdeteksi oleh algoritma deteksi objek. Berdasarkan perhitungan sebelumnya mengenai jumlah kendaraan pada masing-masing class menyatakan bahwa algoritma deteksi objek sulit untuk mendeteksi objek yang ada pada video yang memiliki kualitas rendah atau yang memiliki tingkat kecahayaan yang kurang. (Dufan et al, 2020)

Berdasarkan penelitian oleh Jayakanth Kunhoth & Nandhini Subramanian tahun 2022, dengan judul Video steganography recent advances and challenges. Untuk permasalahannya yaitu mengenai, satu piksel dalam bingkai video sampel memiliki 8 hingga 24 bit berdasarkan formatnya video. Bingkai skala abu-abu memiliki 8 bit sedangkan bingkai warna memiliki 24 bit. Bingkai warna terdiri dari 3 saluran (RGB) dan setiap saluran terdiri dari 8 bit per piksel. Demikian pula dengan RGB bingkai rahasia video terdiri dari 8 bit per piksel untuk ketiga saluran. Bagian paling kecil dari bingkai penutup diganti dengan bagian paling signifikan dari bingkai rahasia. Selama ekstraksi, bit LSB dari stego diambil dan 0 diisi untuk mendapatkan perkiraan informasi rahasia yang dimaksud. Seiring dengan media rahasia yang berbeda, tingkatannya berbeda kapasitas persembunyian dipertimbangkan, dan nilai MSE, PSNR, dan SSIM dari kombinasi berbeda diberikan dalam Tabel. (Jayakanth & Nandhini, 2022).

Berdasarkan penelitian oleh Susan Siti Nurhaliza & Lussiana tahun 2022, dengan judul Pengenalan karakter dokumen secara otomatis menggunakan metode optical character recognition (OCR). Berdasarkan penghitungan akurasi, karakter yang berhasil dikenali menunjukkan kinerja yang baik. Kegagalan dalam mengenali beberapa karakter bisa disebabkan oleh kualitas citra yang diolah. Pada citra 1, hasil cropping menunjukkan bahwa karakter "/" yang tidak dikenali dengan benar tampak kurang tajam atau sedikit buram. Karakter tersebut berdekatan dengan karakter "V" yang dikenali sebagai "N". Karakter lain yang dikenali secara keliru adalah "2" yang

dikenali sebagai "Z" (lihat citra pada Tabel 2; lingkaran kuning menunjukkan karakter yang diuji dan lingkaran merah menunjukkan karakter yang dikenali). Mengenai waktu proses sistem dalam mengenali karakter, waktu yang dibutuhkan jauh lebih cepat dibandingkan dengan pembacaan langsung yang saat ini memakan waktu sekitar 5 menit untuk memeriksa dan menulis dokumen secara manual, sedangkan sistem OCR yang diterapkan dapat mengenali karakter dalam waktu 1,29 detik. Dari pengujian lima citra yang mengandung 316 karakter, metode OCR berhasil mengenali 312 karakter, sehingga tingkat akurasi pengujian mencapai 98,78%. Rata-rata waktu proses yang dibutuhkan untuk mengenali karakter adalah 1,29 detik. Dengan demikian, dapat disimpulkan bahwa metode OCR dapat diterapkan untuk membantu pengenalan dokumen yang berisi berbagai karakter. Namun, masih diperlukan pengembangan lebih lanjut untuk meningkatkan akurasi pengenalan karakter. (Nurhaliza & Lussiana, 2022).

Berdasarkan penelitian oleh irvan maulana yusuf, carudin dkk tahun 2020, dengan judul Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen. pengembangan perangkat lunak dengan menggunakan metode Waterfall, Prototyping, Rational Unified Process (RUP), dan bahasa pemrograman Java. Juga mencakup pengamanan dokumen menggunakan algoritma steganografi dan analisis webometrics pada repositori perguruan tinggi Islam negeri. File yang bersifat rahasia atau penting yang hanya ingin diketahui oleh pihak tertentu dapat diamankan menggunakan perangkat lunak berbasis bahasa pemrograman Java yang menerapkan algoritma Caesar Cipher dan algoritma Least Significant Bit (LSB). File dokumen yang dienkripsi dengan algoritma Caesar Cipher dilakukan dengan menggeser huruf-huruf sesuai jumlah geser yang ditentukan oleh kunci yang dimasukkan. File yang disisipkan ke dalam gambar menggunakan algoritma LSB dilakukan dengan mengubah bit paling kanan atau paling belakang pada file penampung dengan bit dari file dokumen. Dalam proses enkripsi, semua file dokumen dapat dienkripsi, tetapi dalam proses penyisipan hanya 2 dari 5 file dokumen yang dapat disisipkan. File dokumen yang akan disisipkan hanya bisa memuat maksimal 31 karakter, karena ukuran piksel file penampung dalam perangkat lunak ini adalah 250x250. Semua file dokumen yang

dienkripsi, dari total 5 file, dapat didekripsi dengan baik. Dan dari 2 file yang bisa disisipkan, kedua file tersebut dapat dikembalikan saat proses ekstraksi. (Irvan & Carudin, 2020).

Berdasarkan penelitian tersebut diketahui bahwa pengukuran akurasi dan kualitas file steganografi multimedia hasil stegono diperlukan dengan melakukan pengukuran melalui pendekatan nilai MSE dan PSNR untuk menilai kualitas file multimedia.

Maka dari itu urgensi pada penelitian ini dilakukan memfokuskan pada bidang digital forensik dan multimedia dengan pengimplementasian dari penggunaan steganografi dengan metode algoritma *low bit coding* menggunakan file multimedia sebagai data untuk mengukur tingkat akurasi dan kualitas file multimedia seperti audio, gambar, video dan dokumen dengan menggunakan Parameter Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) dan Structural Similarity Index Measure (SSIM) sebagai hasil akhir pengujian dalam file steganografi.

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas maka dapat di rumuskan masalah dalam penelitiannya di antaranya:

1. Bagaimana mengukur tingkat akurasi dan kualitas file steganografi menggunakan algoritma *low bit coding*?
2. Bagaimana cara melakukan pengujian dengan menggunakan parameter MSE, PSNR dan SSIM untuk menghitung nilai akurasi dan kualitas file steganografi?

1.3. Batasan Masalah

Ada pula beberapa batasan masalah yang di gunakan untuk penelitian ini agar dapat di jalankan secara spesifik di antaranya:

1. Jenis file citra digital yang digunakan adalah format JPEG dan PNG.
2. Ukuran file Image maksimal 10mb
3. Ukuran file audio Maksimal 8mb.
4. Ukuran file video maksimal 1080p.
5. Ukuran file dokumen maksimal 1mb.

1.4. Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah maka, tujuan penelitian ini sebagai berikut:

1. Untuk mengukur tingkat akurasi dan kualitas file steganografi dengan algoritma *low bit coding* dengan pendekatan Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) dan Structural Similarity Index Measure (SSIM) Menganalisis hasil pengukuran dengan Mean Square Error (MSE), Peak Signal to Noise (PSNR) dan Structural Similarity Index Measure (SSIM) untuk membandingkan kualitas tiap file steganografi seperti audio, video, image dan dokumen.

1.5. Manfaat Penelitian

Berdasarkan latar belakang yang telah di uraikan maka di peroleh manfaat dari penelitian ini di antaranya:

1. Untuk memanfaatkan steganografi pengukuran tingkat akurasi dan kualitas file Steganografi.
2. Penerapan steganografi pada konteks multimedia suara, gambar, dokumen dan video.