BAB I
PENDAHULUAN

Bab I menyajikan tentang latar belakang penelitian, rumusan penelitian, tujuan penelitian, batasan penelitian, dan sistematika penulisan penelitian mengenai *Data Hiding* pada Video Digital menggunakan teknik DCT.

1.1 Latar Belakang Penelitian

Kehidupan manusia saat ini sangat berkaitan erat dengan pertukaran data. Manusia menggunakan berbagai media seperti media cetak, media elektronik, dan media digital untuk saling bertukar data. Berkas media digital yang dipertukarkan dapat berupa dokumen, audio, citra, serta video. Dalam perkembangan teknologi informasi, pertukaran data melalui media digital semakin meningkat. Hal ini ditandai dengan keanekaragaman data yang dipertukarkan melalui internet.

Data yang dipertukarkan melalui internet bisa saja mengandung informasi biasa atau informasi yang bersifat rahasia, sehingga muncul permasalahan pada saat pertukaran data terkait dengan keamanan data. Untuk itulah muncul pemikiran bagaimana data dapat dipertukarkan secara aman tanpa diketahui orang lain dan menyulitkan bagi yang tidak berkepentingan untuk mengaksesnya.

Untuk menjaga kerahasiaan data, dapat menggunakan metode kriptografi. Metode kriptografi bekerja dengan cara mengubah data asli (*plaintext*) menjadi data acak (*chipertext*) sehingga data tersebut tidak lagi bermakna (Munir, 2006). Proses mengubah data tersebut menggunakan sebuah algoritma khusus yang telah disepakati oleh pihak yang bertukar data. Langkah selanjutnya untuk mendapat data asli yaitu dengan menggunakan kebalikan (inversi) dari algoritma yang sama ketika data sudah diterima. Jika pihak yang tidak mengetahui jenis algoritma apa yang dipakai untuk mengubah isi data tersebut, maka pihak tersebut hanya akan mendapatkan data yang tidak bermakna.

Namun metode kriptografi memiliki kelemahan, yaitu data yang diacak dapat menimbulkan kecurigaan oleh pihak lain. Karena data tersebut tidak berfungsi dengan normal dan seperti tidak mengandung makna apa pun, sehingga data tersebut bisa dirusak agar pihak penerima yang asli juga tidak bisa membuka data

tersebut. Maka dari itu, diperlukan sebuah metode lain yang dapat menyembunyikan data rahasia (*data hiding*) tanpa menimbulkan kecurigaan pihak yang tidak berkepentingan. Metode ini disebut dengan metode steganografi.

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indra manusia (Munir, 2004). Steganografi bekerja dengan cara menyisipkan data ke dalam media penampung (*cover-file*). Media penampung yang telah disisipkan data (*stego-file*) kemudian dipertukarkan melalui jaringan lokal maupun jaringan internet. Berkas yang dipertukarkan melalui jaringan tidak akan menimbulkan kecurigaan, karena bila *cover-file* dibandingkan dengan *stego-file* tidak terlalu menunjukkan perbedaan yang berarti dan dapat berfungsi dengan normal.

Steganografi dapat diimplementasikan pada berbagai media digital seperti dokumen, citra, audio, dan video. Pada penelitian ini berkas media yang digunakan adalah berkas video. Steganografi pada video bisa dilakukan terhadap beberapa format, seperti AVI, MPEG, atau MKV. Selain format video, hal lain yang harus diperhatikan yaitu jenis kodek video. Kodek yang digunakan adalah kodek MJPEG. Kodek MJPEG dipilih karena semua *frame* hanya terdiri dari I-*frame*, tidak seperti H.264 dan H-265 yang memiliki B-*frame* dan P-*frame* (Madenda, 2015). Dengan begitu, apabila salah satu *frame* pada videonya rusak, data yang tersisip pada *frame* lainnya tetap dapat diungkap (ekstrak) tanpa kendala.

Untuk menyisipkan pesan rahasia ke dalam sebuah video terdapat berbagai jenis teknik, seperti teknik *Discrete Wavelet Transform* (DWT) yaitu teknik yang bekerja dengan cara mentransformasi dan menyisipkan data rahasia bentuk citra ke komponen frekuensi, *Bit-Plane Complexity Segmentation* (BPCS) bekerja dengan cara menyisipkan data rahasia pada setiap *bit-plane*, dan DCT yang bekerja dengan cara menyubstitusikan nilai data dengan nilai koefisien transformasi *direct current* (DC) yang kemudian melekat pada sebagian atau seluruh koefisien yang ditransformasi (Shanthakumari & Malliga, 2014). Pada penelitian ini digunakan teknik DCT karena algoritmanya sesuai dengan kodek MJPEG.

Kualifikasi metode Steganografi yang baik dapat dinilai dari beberapa faktor meliputi faktor *fidelity* yaitu mutu citra penampung tidak jauh berubah setelah penambahan data rahasia, *robustness* yaitu data yang disembunyikan harus tahan

terhadap manipulasi yang dilakukan pada citra penampung (seperti pengubahan kontras, penajaman, pemadatan, rotasi, pembesaran gambar, pemotongan, enkripsi, dan sebagainya), dan *recovery* yaitu data yang disembunyikan harus dapat diungkapkan kembali (Munir, 2006).

Dalam penyisipan data, video yang disisipkan pasti akan mengalami perubahan walaupun sangat kecil. Untuk menghitung perubahan tersebut dilakukan perhitungan nilai *Mean Squared Error* (MSE) dan PSNR. Semakin kecil nilai MSE menandakan video yang sudah disisipi data rahasia memiliki tingkat *fidelity* semakin baik, sedangkan nilai PSNR semakin besar semakin baik.

Penelitian yang dilakukan oleh (Deshmukh & Rahangdale, 2014) menunjukkan bahwa metode steganografi dapat menyembunyikan data pada video digital secara aman dengan nilai MSE rendah dan PSNR tinggi. Hasil penelitian yang dilakukan oleh (Priya & Amritha, 2016) juga menunjukkan bahwa metode steganografi dapat digunakan untuk menyembunyikan data pada berbagai jenis kodek video digital seperti H.264, H.265, dan MJPEG.

Berdasarkan paparan di atas maka terlihat bahwa *data hiding* menggunakan metode steganografi teknik DCT dapat diaplikasikan pada berkas video digital. Pada penelitian ini, dibuat aplikasi steganografi yang akan digunakan untuk menyembunyikan data pada berkas video digital MJPEG. Aplikasi ini sangat diperlukan oleh berbagai kalangan yang memerlukan data pribadinya tidak bisa diakses oleh sembarang orang.

1.2 Rumusan Masalah

Rumusan masalah dari penelitian ini adalah:

1. Bagaimanakah data rahasia pada berkas video digital menggunakan teknik DCT diamankan?
2. Bagaimanakah proses penyisipan dan pengungkapan data rahasia?
3. Bagaimanakah hasil pengujian kriteria steganografi dari implementasi teknik DCT terhadap berkas video digital yang telah disisipkan data rahasia?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Membuktikan implementasi *data hiding* pada berkas video digital menggunakan teknik DCT.
2. Mengimplementasikan proses penyisipan dan ekstraksi menggunakan teknik DCT.
3. Menganalisis hasil uji kualitas *data hiding* terhadap berkas video digital dengan faktor *fidelity*, *robustness*, dan *recovery*.

1.4 Batasan Masalah

Dalam penelitian ini dilakukan pembatasan masalah sebagai berikut:

1. Data rahasia yang disembunyikan pada video digital berupa teks.
2. Video digital kodek MJPEG.

1.5 Struktur Organisasi Skripsi

Sistematika penulisan skripsi disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan, meliputi:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, penelitian relevan, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi penjelasan tentang teori-teori & konsep, algoritma yang digunakan dalam penelitian, serta alur penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan langkah-langkah yang dilakukan dalam penelitian.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisi uraian tentang hasil penelitian dan pembahasan terhadap hasil penelitian.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil penelitian, serta saran dari penulis untuk kegiatan penelitian selanjutnya terkait dengan topik yang sedang dibahas.