BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan teknologi dan penggunaan internet yang berkembang pesat saat ini memudahkan setiap orang untuk mendapatkan dan membagikan informasi dalam bentuk media digital. Berbagai data seperti gambar dan suara dapat dengan mudah disebarluaskan dan diakses oleh berbagai kalangan. Hal tersebut menjadikan hak kepemilikan suatu informasi atau yang biasa disebut dengan hak cipta tidak lagi terjamin. Maka diperlukan sebuah metode untuk verifikasi dan autentifikasi data digital untuk melindungi hak cipta. Pada kasus ini *watermarking* dapat menjadi solusi permasalahan.

Watermarking adalah salah satu cabang dari ilmu steganografi. Steganografi sendiri merupakan ilmu yang mempelajari metode untuk menyembunyikan suatu informasi yang bersifat rahasia ke dalam media informasi lainnya. *Watermarking* merupakan proses penyisipan watermark dalam suatu *host file* sebagai informasi kepemilikan tanpa merubah file aslinya yang bertujuan untuk melindungi orisinalitas dari sebuah karya . *Watermarking* tediri dari dua tahap utama, yaitu proses penyisipan dan proses ekstraksi. Dimana pada proses penyisipan watermark disisipkan ke dalam *host file*, sedangkan dalam proses ekstraksi *watermark* yang telah disisipkan akan dideteksi. *Watermark* harus memiliki sifat tidak boleh tampak, tidak terdeteksi serta tahan terhadap serangan. Ketiga sifat tersebut biasa disebut *imperceptibility, security,* dan *robustness*. Pada penelitian ini akan digunakan metode berbasis *Multi-bit Spread Spectrum* (*Multi-bit* SS) dan *Convolutional Neural Network* (CNN). Pada proses penyisipan, digunakan *Pseudo Noise Code* (PN *Code*) untuk penyebaran data agar *attacker* yang melakukan penyerangan terhadap *watermark* sulit mengidentifikasi posisi *watermark*, sehingga data tidak dapat diekstraksi tanpa mengetahui PN *code* nya [1]. *Convolutional Neural Network* (CNN) bisa dilatih menggunakan data *training*, sehingga CNN dapat digunakan sebagai pendeteksi *watermark* yang tidak sempurna akibat serangan agar bisa dikembalikan menjadi *watermark* sebelum terkena serangan.

Perancangan sistem *audio watermarking* dapat dilakukan dengan menggunakan berbagai metode. Pada penelitian [2] menggunakan metode Spread Spectrum (SS) dan *Discrete Cosine Transform* (DCT). Metode SS digunakan untuk meningkatkan ketahanan terhadap serangan dan DCT memiliki fungsi untuk mengubah sinyal dari domain waktu ke domain frekuensi. Penelitian ini menggunakan *detection rate* (DR) untuk mengukur *robustness* dari metode yang digunakan. Hasil dari penelitian [2] ini memiliki nilai DR yang tinggi sehingga metode yang digunakan kuat terhadap serangan yang berbeda. Pada penelitian [3] menjelaskan bahwa *Discrete Wavelet Transform* (DWT) dan *Direct Sequence Spread Spectrum (DSSS)* digunakan agar *watermark* dapat disisipkan di frekuensi rendah yang kurang terdengar. Hasil penelitian [3] ini memperoleh nilai SNR (22.64), ODG (-0.22), dan Payload (83.00).

Pada penelitian [4], menjelaskan *data hiding* menggunakan metode *Compressive Sampling* (CS) dengan *Multi-bit* SS untuk mengambil sampel sinyal audio dan menyisipkan *watermark* pada saat yang sama sehingga ukuran sinyal sampel nya lebih kecil. Hasil penelitian [4] ini memiliki *imperceptibility* yang tinggi dengan nilai *payload* (729-5292) bps, *Compression Ratio* (CR) (1.47-4.84). Sedangkan untuk nilai ODG nya berada di rentang (-0.94 -0.74) dan nilai BER tertingginya 13%.

Pada penelitian [5], menjelaskan *Convolutional Neural Network* (CNN) untuk mendeteksi beberapa jenis serangan pada *image watermarking*. Model dari CNN yang digunakan berupa beberapa layer yang berisi *Input, Convolutional layer, Pooling layer, Fully connected layer,* dan *Softmax classifier*. Parameter dari model CNN tersebut menggunakan fungsi aktivasi *Rectified Linear Unit* (ReLU), *optimizer* Adam, 20 epoch, dan 50 *batch size.* Untuk pengukuran performa menggunakan PSNR, NC, dan SSIM. Hasil dari penelitian [5] mendapatkan performa yang baik akurasi 98% untuk mendeteksi beberapa jenis serangan pada *watermark* yang sudah di ekstraksi.

Pada penelitian [6], menjelaskan *Deep Learning-based audio-in-image watermarking* dengan menggunakan *Similarity Network* yang digunakan untuk mendeteksi *watermark* yang terganggu. Untuk 100 epoch, nilai akurasi yang

didapatkan dari *Similarity Network* setelah di training adalah 99.44%. Nilai rata-rata *Root Mean Square Error* (RMSE) adalah 0.009452 berdasarkan lebih dari 5.800 *audio watermark* yang berbeda.

Pada penelitian [7], menjelaskan *digital image watermarking* meggunakan *Convolutional Neural Network* (CNN). Network pada proses penyisipan menggunakan CNN dengan mempertahankan resolusi untuk menampilkan gambar yang diberi *watermark*. Network pada proses ekstraksi juga menggunakan CNN dengan mengurangi resolusi untuk menampilkan informasi *watermark*. Nilai rata-rata PSNR yang didapat adalah 40.58 dB. Untuk ketahanan terhadap serangan, ketika diberi serangan yang merubah nilai piksel didapatkan nilai BER yang baik yaitu kurang dari 10%.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Bagaimana hasil dari perancangan dan simulasi sistem *audio watermarking* yang menggunakan metode *Multi-bit Spread Spectrum* (*Multi-bit* SS) dan *Convolutional Neural Network*?
2. Bagaimana *Convolutional Neural Network* dapat mendeteksi *watermark* yang tidak sempurna akibat serangan?
3. Bagaimana ketahanan sistem *audio watermarking* terhadap serangan yang diberikan?

1.3 Tujuan dan Manfaat

Tujuan dan manfaat dari penelitian ini adalah sebagai berikut:

1. Membuat sistem *audio watermarking* berbasis *Multi-bit* SS.
2. Mendeteksi *watermark* yang tidak sempurna akibat serangan dengan *Convolutional Neural Network.*
3. Menganalisis kinerja skema *audio watermarking* berdasarkan nilai *Bit Error Rate* (BER), *Objective Differece Grade* (ODG) dan *Signal to Noise Ratio* (SNR).

Manfaat dari penelitian ini adalah memberikan perlindungan hak cipta pada *file* audio.

1.4 Batasan Masalah

Adapun batasan masalah pada penelitian ini adalah sebagai berikut:

1. *Host file* yang akan disisipi oleh *watermark* berupa *audio file* atau suara.
2. Format *file* audio yang digunakan adalah **.wav.*
3. Metode *watermarking* yang digunakan adalah *Multi-bit* SS dengan *watermark* berupa huruf A, R, dan Y yang digabungkan dan dikonversi menjadi gambar.
4. Jumlah *audio host* berjumlah 3 buah file, masing-masing dengan frekuensi *sampling* 44100 Hz.
5. Metode *Machine Learning* yang digunakan adalah *Convolutional Neural Network* (CNN).
6. Serangan yang dilakukan pada *watermarked audio* adalah *Low Pass Filter* (LPF), *Band Pass Filter* (BPF), *noise*, *resampling*, *Time Scale Modification* (TSM), *Linear Speed Change*, *pitch shifting*, *equalizer*, *echo*, *kompresi* MP3.
7. Parameter yang digunakan sebagai analisis adalah BER, ODG, SNR dan C.

1.5 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Studi Literatur

   Mempelajari konsep serta dasar teori terkait *audio watermarking, Multi-bit* SS*,* dan *Convolutional Neural Network.* Sumber yang digunakan berasal dari jurnal, paper, dan literatur lainnya baik yang diakses secara online maupun offline.
2. Analisis Masalah

Penemuan solusi dapat menggunakan referensi penelitian sebelumnya denga berdiskusi dengan pembimbing kemudian disesuaikan dengan masalah serta parameter yang ingin dikaji dan diperbaiki.

3. Desain Perancangan Sistem

   Merancang model sistem *audio watermarking* yang digunakan sebagai pemecahan masalah. Dilakukan pemodelan sistem, diagram alir, dan cara kerja sistem.

4. Pengujian Model

   Sistem *audio watermarking* yang sudah dirancang kemudian dilakukan pengujian dengan parameter yang sudah ditentukan.

5. Pengumpulan dan Analisis Data

   Pengujian model akan menghasilkan data yang kemudian dapat dianalisis untuk mengetahui performa sistem yang telah diuji.

6. Penarikan Kesimpulan

   Penarikan kesimpulan berdasarkan pengujian dan analisis data.

1.6 Sistematika Penulisan

Sistematika Penulisan pada penelitian ini adalah sebagai berikut:

1. BAB I PENDAHULUAN

   Pada bab ini berisi penjelasan mengenai latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah, dan metode penelitian yang menjadi dasar dalam pengerjaan tugas akhir ini.

2. BAB II KONSEP DASAR

   Pada bab ini berisi penjelasan mengenai konsep dasar dari *audio watermarking*, *Machine Learning*, *Multi-bit SS,* berbagai serangan yang digunakan, dan parameter kinerja dari sebuah sistem *audio watermarking.*

3. BAB III MODEL SISTEM DAN PERANCANGAN

   Pada bab ini berisi penjelasan mengenai desain sistem dan simulasi yang dilakukan dalam penelitian yang berisi desain sistem proses penyisipan dan desain sistem proses ekstraksi.

4. BAB IV HASIL DAN PEMBAHASAN

Pada bab ini dijelaskan mengenai hasil simulasi yang telah dilakukan dengan analisis yang sesuai sehingga dapat dihubungkan dengan konsep dasar dan tujuan penelitian.

5. BAB V KESIMPULAN DAN SARAN

   Bab ini merupakan bagian penutup dari penelitian yang berisi kesimpulan dari penelitian yang telah dilakukan dan saran untuk penelitian yang akan datang.