BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Pada tahun 2020, dengan total penduduk dunia yang berjumlah 7,75 milyar ada sekitar 7,95 milyar koneksi dari ponsel dan belum termasuk koneksi IOT, 4,54 milyar pengguna internet, dan 3,80 milyar pengguna sosial media yang aktif. Sedangkan di Indonesia dengan total penduduk yang berjumlah 272,1 juta jiwa ada sekitar 338,2 juta koneksi ponsel unik yang berarti ada orang-orang yang memiliki lebih dari satu ponsel, 175,4 juta pengguna internet, dan 160 juta pengguna sosial media yang aktif [1].

Era digital membawa tantangan baru dalam kehidupan manusia. Salah satunya adalah cyber crime atau tindak kejahatan siber yang melibatkan komputer atau smartphone sebagai alat dan target, dan *computer-related crime* yang merupakan segala jenis bentuk kriminal dengan komputer atau smartphone sebagai barang bukti [2].

Menurut data statistik laporan masyarakat melalui portal patrolisiber.id maraknya tindak kejahatan siber melonjak tajam sejak tahun 2015 dan tingkat paling tinggi ada pada tahun 2019 yaitu 4586 laporan, dan 2284 kasus terselesaikan [3]. Dalam merespons insiden serangan siber, diperlukan investigasi untuk menentukan apakah telah terjadi tindakan ilegal.

Digital forensik adalah cabang ilmu forensik yang mempelajari tentang bagaimana mendeteksi dan mengamati kondisi abnormal pada suatu aplikasi, file,

dan perangkat digital untuk dijadikan barang bukti kuat di mata hukum [4]. Barang bukti elektronik adalah bukti yang memiliki wujud fisik seperti perangkat komputer, sedangkan barang bukti digital adalah bukti yang merupakan hasil keluaran dari barang bukti elektronik yang berbentuk *file* [5]. Indonesia memiliki standar operasional prosedur bersertifikasi Standar Nasional Indonesia yang bernama SNI ISO/IEC 27037:2014 yang diadopsi dari dokumen ISO/IEC 27037:2012 yang merupakan pedoman dalam proses identifikasi, pengumpulan, akuisisi, sampai dengan preservasi atau penyajian bukti digital. Dalam proses tersebut ada kemungkinan barang bukti dapat menjadi tidak bisa diidentifikasi yang diakibatkan oleh anti-forensik.

Menurut [6] anti-forensik itu adalah sebuah tindakan yang dilakukan untuk membuat pemeriksaan terhadap barang bukti tersebut menjadi sulit bahkan hingga tidak mungkin untuk dilakukan. Sayangnya [7] menunjukkan kurangnya penelitian akademis terhadap anti-forensik, dibandingkan dengan penelitian tentang forensik digital, dan hanya 2% dari 500 makalah penelitian forensik digital yang berfokus pada anti-forensik. Salah satu contoh dari anti-forensik adalah steganografi.

Steganografi adalah ilmu menyematkan rahasia pada media digital seperti file gambar, audio, dan video menjadi tidak terlihat [8]. Sebagai metode ilmiah tidak ada penelitian yang menyatakan seberapa berbahayanya steganografi secara langsung. Namun steganografi bisa menjadi sangat berbahaya ketika digunakan oleh kelompok kriminal atau teroris dalam berkomunikasi [9]. Berdasarkan [10] pengelompokan teknik steganografi yang relatif baru adalah teknik steganografi adaptif karena memanfaatkan *machine learning* dan *artificial intelligence*.

Algoritma genetika merupakan algoritma *machine learning* yang diciptakan terinspirasi dari seleksi alam dan teori evolusi [11]. Algoritma ini dipilih sebagai upaya optimasi karena dapat melakukan optimasi masalah dengan masalah yang kompleks dan ruang pencarian yang sangat luas serta hasil kromosom algoritma genetika sangat fleksibel dapat digunakan untuk memodifikasi teknik steganografi.

Pembaharuan penelitian ini terletak pada pemanfaatan hasil kromosom algoritma genetika yang akan menjadi representasi dari parameter yang digunakan untuk memperlakukan proses steganografi yang bertujuan untuk menemukan tempat penyematan yang paling baik untuk bit rahasia. Algoritma genetika bertugas sangat penting untuk mencari nilai yang paling optimal dari parameter-parameter tersebut. Serta pada penelitian ini, metode yang diusulkan tidak hanya mampu menyematkan citra digital kedalam citra digital lainnya saja namun juga termasuk file audio, text, malware, dan juga virus. Penelitian ini memiliki manfaat sebagai gambaran perkembangan anti-forensik dengan memanfaatkan *machine learning* dan *artificial intelligence*, serta sebagai solusi keamanan data dari dampak era digital yang membuat ranah privasi orang seolah-olah hilang. Tulisan ini juga dapat menjadi masukan bagaimana prosedur digital forensik harus dikembangkan lagi untuk dapat mencegah teknik anti-forensik yang semakin berkembang.

Perbedaan penelitian saat ini dengan penelitian sebelumnya terletak pada hasil kromosom pada algoritma genetika yang akan menjadi representasi dari parameter yang akan digunakan untuk memperlakukan gambar cover dan data rahasia yang akan disematkan, serta pengujian menggunakan *steganalysis* untuk menguji keandalan teknik steganografi yang diusulkan.

1.2 Rumusan Masalah

Steganografi sebagai salah satu teknik anti-forensik yang merupakan sebuah metode ilmiah, yang menurut [10], [12] masalah utamanya adalah tidak mudah dideteksi, keamanan data, kapasitas penyimpanan data yang besar, dan ketahanan terhadap berbagai pemrosesan gambar. Banyak penelitian yang menyimpulkan bahwa metode penyematan LSB adalah metode yang paling baik [13]–[15], namun memiliki masalah di keamanan karena mudah dideteksi oleh beberapa program *steganalysis* [16], [17]. Berdasarkan paparan tersebut maka dirumuskan permasalahan penelitian ini sebagai berikut :

1. Bagaimana menerapkan algoritma genetika pada teknik steganografi untuk rasio penyematan yang besar.
2. Bagaimana algoritma genetika dapat bertahan terhadap pemrosesan gambar sehingga kualitas gambar stego yang mengandung pesan rahasia tetap tinggi.
3. Bagaimana keamanan data yang tinggi dapat dihasilkan dari teknik steganografi yang menggunakan algoritma genetika.
4. Bagaimana algoritma genetika dapat membuat teknik steganografi sebagai metode anti-forensik tidak mudah dideteksi pada saat investigasi menggunakan teknik *steganalysis*.

1.3 Batasan Masalah

1. File berformat BMP, atau disebut juga dengan DIB (*Device Independent Bitmap*), dimana didalam gambar ini tersusun dari kumpulan *pixel* yang tersusun membentuk gambar pada monitor. BMP digunakan karena merupakan format file gambar yang tidak terkompresi dan pada steganografi yang menyematkan data rahasianya pada nilai spektrum warna tidak boleh ada kompresi yang terjadi pada nilai nilai piksel pada gambar.
2. Terdapat uji perbandingan metode LSB biasa dengan metode yang diusulkan.
3. Terdapat uji forensik steganografi/ *steganalysis* menggunakan teknik *chi-squared* dan RS-*Analysis*
4. Menggunakan bahasa pemrograman Python dalam mengaplikasikan konsep ini.
5. Memanfaatkan framework *Distributed Evolutionary Algorithms in Python* (DEAP)

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah mendapatkan metode yang bisa membuat sebuah proses membuat pemeriksaan terhadap barang bukti digital dalam hal ini citra digital, menjadi sulit bahkan hingga tidak mungkin untuk dilakukan menggunakan teknik steganografi. Serta menjadi gambaran sampai sejauh mana

steganografi sebagai teknik anti-forensik bisa berkembang dengan memanfaatkan *machine learning* dan *artificial intelligence*.

1.5 Sistematika Penulisan

Pada bagian akan dijabarkan sistematika penulisan skripsi yang memuat uraian secara garis besar isi untuk tiap–tiap bab.

Bab I Pendahuluan, berisi: latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

Bab II Landasan Teori, berisi: hasil penelitian sejenis yang sudah pernah dilakukan sebelumnya, teori penunjang, dan referensi berupa buku, dan jurnal..

Bab III Metodologi Penelitian, berisi: penjelasan mengenai metode penelitian yang digunakan untuk memahami dan mengeksplorasi objek penelitian, hasil observasi / pengumpulan data, masalah yang terdapat pada objek, dan gambaran umum proyek atau objek penelitian, hingga Rencana Alur Penelitian.

Bab IV Pembahasan, berisi: rancangan proyek, implementasi *coding*. Selanjutnya alur pengerjaan proyek, metode testing, hingga hasil akhir penelitian dan pembahasan analisis hasil akhir penelitian, termasuk pembahasan hasil-hasil uji coba (testing), serta perbandingan dengan metode sebelumnya. Data hasil akhir pengujian dapat berupa grafik, tabel.

Bab V Penutup, berisi kesimpulan dari hasil akhir penilaian proyek, dan saran.