BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk cara berbagi dan menyimpan data. Citra digital merupakan salah satu bentuk media yang paling sering digunakan dan didistribusikan melalui internet [1]. Format citra seperti PNG banyak dipilih karena kemampuannya menyimpan citra dengan kualitas baik dan mendukung transparansi [2]. Seiring dengan meningkatnya penggunaan citra digital, muncul pula berbagai teknik untuk menyematkan pesan rahasia ke dalamnya, salah satunya adalah steganografi.

Di sisi lain, malware, khususnya yang didistribusikan dalam format APK, terus menunjukkan peningkatan yang eksponensial. Berbagai laporan mengindikasikan bahwa jutaan sampel malware terdeteksi setiap tahun, bahkan mencapai ribuan per hari. Sebagai contoh, data yang lebih baru menunjukkan bahwa sekitar 560.000 ancaman malware terdeteksi setiap hari secara global pada tahun 2025 [3], dan tercatat serangan malware Android mencapai 33.3 juta pada tahun 2024 [4]. Ancaman malware Android tidak bersifat statis, melainkan terus berevolusi baik dalam hal volume maupun tingkat kecanggihannya. Sementara itu, penjahat siber terus mencari metode baru untuk menyebarkan malware dan menghindari deteksi mesin antivirus [5]. Penyematan malware ke dalam media digital menggunakan steganografi menjadi salah satu teknik yang semakin mendapat perhatian [6]. Dengan menyematkan malware ke dalam citra yang tampak normal, penyerang dapat melewati pemeriksaan keamanan tradisional yang mungkin tidak dirancang untuk menganalisis lapisan steganografi.

Antivirus merupakan garda terdepan dalam melindungi sistem komputer dari serangan malware. Namun, efektivitas mesin antivirus dalam mendeteksi malware yang disematkan menggunakan teknik steganografi, khususnya pada citra dengan metode LSB, masih menjadi pertanyaan yang perlu diinvestigasi lebih

lanjut [7]. Kegagalan deteksi dapat berakibat fatal, memungkinkan malware terdistribusi dan menginfeksi sistem tanpa terdeteksi. Kualitas citra setelah proses penyematan juga menjadi faktor penting, karena perubahan signifikan pada citra dapat menimbulkan kecurigaan. Oleh karena itu, analisis kualitas citra menggunakan metrik pengukuran kuantitatif seperti *Mean Squared Error* (MSE), *Peak Signal-to-Noise Ratio* (PSNR), dan *Structural Similarity Index Measure* (SSIM) diperlukan untuk menilai tingkat *imperceptibility* (tidak terdeteksi secara visual) hasil steganografi [8].

Hasil dari penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam bidang keamanan siber, khususnya dalam memahami efektivitas mesin antivirus saat ini dalam menghadapi ancaman distribusi malware dengan metode steganografi sekaligus mendorong pengembangan teknologi antivirus yang lebih canggih dan efektif untuk menghadapi ancaman siber yang terus berkembang.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana implementasi program steganografi LSB menggunakan Python di Google Colaboratory?
2. Bagaimana kualitas citra stego dibandingkan citra sampul berdasarkan metrik pengukuran kuantitatif (MSE, PSNR, SSIM)?
3. Bagaimana efektivitas mesin antivirus yang disediakan oleh VirusTotal dalam mendeteksi keberadaan malware?

1.3 Batasan Masalah

Untuk menjaga fokus penelitian, maka ditetapkan batasan masalah sebagai berikut:

1. Penelitian ini hanya menguji efektivitas deteksi malware yang telah disematkan ke dalam citra (abu-abu dan berwarna) dengan metode steganografi LSB menggunakan mesin antivirus yang disediakan oleh layanan VirusTotal.

2. Malware yang digunakan adalah dalam format APK, tetapi penelitian ini tidak menguji eksekusi malware tersebut, melainkan hanya deteksi keberadaannya di dalam citra.
3. Penelitian ini tidak mencakup pengujian terhadap format citra lain (seperti JPEG atau BMP) dan metode steganografi lain (seperti DCT atau DWT).
4. Bahasa pemrograman yang digunakan adalah Python dan berjalan di lingkungan Google Colaboratory.
5. Penelitian ini tidak membahas metode enkripsi malware sebelum proses penyematan.
6. Penelitian ini tidak mengembangkan metode deteksi baru, tetapi hanya menguji kerentanan mesin antivirus yang sudah ada.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Mengimplementasikan program steganografi LSB menggunakan Python di Google Colaboratory.
2. Mengevaluasi dampak penyematan malware terhadap kualitas citra menggunakan metrik pengukuran kuantitatif (MSE, PSNR, SSIM).
3. Menguji kemampuan mesin antivirus dalam mendeteksi keberadaan malware yang telah disematkan ke dalam citra.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Bagi Dunia Akademik: Memberikan kontribusi dalam bidang keamanan siber dengan mengeksplorasi teknik steganografi dan deteksi malware, serta menjadi referensi untuk penelitian serupa di masa depan.
2. Bagi Pengembang Antivirus: Memberikan wawasan tentang kelemahan sistem deteksi malware saat ini, sehingga dapat mendorong pengembangan algoritma deteksi yang lebih canggih.

3. Bagi Pengguna Umum: Meningkatkan kesadaran tentang potensi ancaman dari citra digital yang tampak tidak berbahaya, sehingga pengguna lebih berhati-hati dalam mengunduh atau membuka file dari sumber yang tidak dikenal.

1.6 Sistematika Penulisan

Skripsi ini disusun dalam lima bab dengan struktur sebagai berikut:

1. BAB I PENDAHULUAN, berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.
2. BAB II TINJAUAN PUSTAKA, membahas teori-teori yang relevan dengan penelitian, termasuk konsep steganografi, metode LSB, citra digital, malware, antivirus, serta metrik pengukuran kuantitatif seperti MSE, PSNR, dan SSIM.
3. BAB III METODE PENELITIAN, menjelaskan alur penelitian, mulai dari pengembangan program steganografi LSB hingga pengujian menggunakan layanan VirusTotal.
4. BAB IV HASIL DAN PEMBAHASAN, menyajikan hasil pengujian, analisis data, dan pembahasan terkait temuan penelitian.
5. BAB V PENUTUP, merangkum kesimpulan dari penelitian dan memberikan saran untuk penelitian mendatang.