

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dan analisis yang telah dilakukan mengenai uji kerentanan antivirus terhadap malware yang disematkan ke dalam citra PNG dengan metode steganografi LSB, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Metode steganografi LSB berhasil diimplementasikan untuk melakukan proses penyematan malware ke dalam citra sampul, baik untuk citra abu-abu maupun citra berwarna menggunakan Python di Google Colaboratory.
2. Penyematan malware dengan metode LSB menghasilkan citra stego dengan kualitas visual yang sangat tinggi. Hal ini dibuktikan dengan:
 - a. Nilai MSE yang sangat rendah (rata-rata 0.16 untuk citra abu-abu dan 0.05 untuk citra berwarna), menunjukkan perbedaan minimal antara citra sampul dan citra stego.
 - b. Nilai PSNR yang sangat tinggi (rata-rata 56.08 dB untuk citra abu-abu dan 60.87 dB untuk citra berwarna), mengindikasikan distorsi yang hampir tidak kasat mata.
 - c. Nilai SSIM yang mendekati sempurna (rata-rata 0.999 untuk kedua jenis citra), menunjukkan kesamaan struktural yang tinggi antara citra sampul dan citra stego.
 - d. Citra berwarna menunjukkan metrik kualitas yang sedikit lebih baik (MSE lebih rendah, PSNR lebih tinggi) dibandingkan citra abu-abu karena kapasitas penyembunyian data yang lebih besar.
3. Mesin antivirus yang diuji melalui layanan VirusTotal (sebanyak 61 mesin) sepenuhnya gagal mendeteksi keberadaan malware yang telah disematkan ke dalam keenam citra stego (baik abu-abu maupun berwarna).
4. Penelitian ini menunjukkan bahwa metode steganografi LSB merupakan teknik yang efektif untuk menyisipkan malware di dalam citra PNG tanpa terdeteksi oleh sebagian besar mesin antivirus saat ini, sekaligus

mempertahankan kualitas citra yang tinggi sehingga tidak menimbulkan kecurigaan visual. Hal ini mengindikasikan adanya potensi celah keamanan yang dapat dieksploitasi untuk penyebaran malware.

5.2 Saran

Berisi hal-hal yang masih dapat dikerjakan dengan lebih baik dan dapat dikembangkan lebih lanjut.

1. Untuk Pengembang Antivirus dan Keamanan Siber:

- a. Pengembang antivirus disarankan untuk mengintegrasikan modul steganalisis ringan yang secara proaktif melakukan analisis statistik pada file citra, terutama format lossless seperti PNG. Analisis ini bisa mencakup *chi-square attack* atau analisis histogram untuk mendeteksi anomali distribusi nilai piksel yang sering menjadi penanda adanya penyematan LSB.

2. Untuk Penelitian Selanjutnya:

- a. Penelitian selanjutnya dapat membandingkan kerentanan antivirus terhadap metode steganografi di domain transformasi (seperti DCT atau DWT) yang lebih tahan terhadap kompresi citra.
- b. Melakukan pengujian dengan jenis malware yang berbeda dan ukuran payload yang bervariasi untuk menganalisis dampaknya terhadap kualitas citra dan kemungkinan deteksi.
- c. Menggunakan variasi format citra yang lebih luas (seperti JPEG atau BMP) sebagai media penampung.
- d. Menganalisis dampak penyematan pada citra dengan resolusi dan kedalaman warna yang berbeda.