UJI KERENTANAN ANTIVIRUS TERHADAP MALWARE YANG DISEMATKAN KE DALAM CITRA PNG DENGAN METODE STEGANOGRAFI LSB

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika

Disusun oleh

RAFIF PUTERA HARDIANSYAH

18.11.2387

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

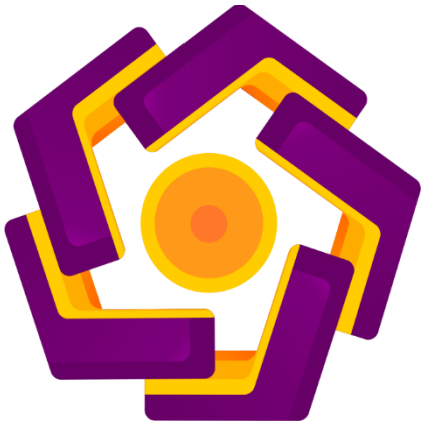
2025

UJI KERENTANAN ANTIVIRUS TERHADAP MALWARE YANG DISEMATKAN KE DALAM CITRA PNG DENGAN METODE STEGANOGRAFI LSB

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika



Disusun oleh

RAFIF PUTERA HARDIANSYAH

18.11.2387

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

UJI KERENTANAN ANTIVIRUS TERHADAP MALWARE YANG DISEMATKAN KE DALAM CITRA PNG DENGAN METODE STEGANOGRAFI LSB

Yang disusun dan diajukan oleh

Rafif Putera Hardiansyah

18.11.2387

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 Mei 2025

Dosen Pembimbing,

Ahlihi Masruro, S.Kom., M.Kom.
NIK. 190302148

HALAMAN PENGESAHAN

SKRIPSI

UJI KERENTANAN ANTIVIRUS TERHADAP MALWARE YANG DISEMATKAN KE DALAM CITRA PNG DENGAN METODE STEGANOGRAFI LSB

Yang disusun dan diajukan oleh

Rafif Putera Hardiansyah

18.11.2387

Telah dipertahankan di depan Dewan Penguji
pada tanggal 18 Juni 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Uyock Anggoro Saputro, S.Kom., M.Kom. **NIK. 190302419**	
Subektiningsih, S.Kom., M.Kom. **NIK. 190302413**	
Ahlihi Masruro, S.Kom., M.Kom. **NIK. 190302148**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
pada tanggal 18 Juni 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Rafif Putera Hardiansyah
NIM : 18.11.2387

Menyatakan bahwa Skripsi dengan judul berikut:

Uji Kerentanan Antivirus Terhadap Malware Yang Disematkan Ke Dalam Citra PNG Dengan Metode Steganografi LSB

Dosen Pembimbing : Ahlihi Masruro, S.Kom., M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 18 Juni 2025

Yang Menyatakan,

Rafif Putera Hardiansyah

HALAMAN PERSEMBAHAN

Dengan segala kerendahan hati, skripsi ini saya persembahkan kepada:

Ayah dan Ibu tercinta, terima kasih atas setiap tetes doa, kasih sayang, dukungan tanpa batas, serta pengorbanan yang tak terhingga. Kalian adalah inspirasi terbesar dan alasan di balik setiap langkah penulis.

Teman-teman seperjuangan Angkatan 2018, terima kasih atas tawa, cerita, dukungan, dan kenangan indah selama masa perkuliahan. Kebersamaan kita adalah salah satu bagian terbaik dari perjalanan ini.

Saudara kandung, terima kasih atas pengertian, semangat, dan selalu menjadi pendengar setia. Anda adalah anggota keluarga yang tak tergantikan.

Semoga karya sederhana ini dapat menjadi permulaan dari kontribusi yang lebih besar di masa depan.

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan judul **"Uji Kerentanan Antivirus Terhadap Malware Yang Disematkan Ke Dalam Citra PNG Dengan Metode Steganografi LSB"** sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer di Universitas Amikom Yogyakarta.

Penyusunan skripsi ini tidak lepas dari bimbingan, arahan, dan dukungan dari berbagai pihak. Oleh karena itu, izinkan penulis menyampaikan rasa terima kasih yang setulus-tulusnya kepada:

1. Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta, atas kesempatan yang telah diberikan untuk menuntut ilmu di lingkungan kampus yang inspiratif.
2. Prof. Dr. Kusrini, M.Kom. selaku Dekan Fakultas Ilmu Komputer, atas segala fasilitas dan dukungan yang telah diberikan selama masa studi.
3. Ibu Eli Pujastuti, M.Kom. selaku Ketua Program Studi Informatika, atas bimbingan dan arahan dalam proses pendidikan.
4. Bapak Ahlihi Masruro, M.Kom. selaku Dosen Pembimbing, atas kesabaran, waktu, bimbingan, serta masukan yang sangat berharga dalam penyusunan skripsi ini dari awal hingga akhir.
5. Ibu Rakhma Shafrida Kurnia, M.Kom. selaku Dosen Wali, atas perhatian dan motivasinya selama masa perkuliahan.

Penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi perbaikan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat bagi perkembangan ilmu pengetahuan, khususnya di bidang keamanan siber.

Yogyakarta,
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

Perkembangan teknologi digital telah membawa kemudahan dalam berbagai aspek kehidupan, namun juga membuka celah bagi ancaman siber baru. Salah satu media yang sering dimanfaatkan untuk penyebaran *malware* (perangkat lunak berbahaya) adalah citra digital karena sifatnya yang umum digunakan dan seringkali tidak dicurigai. Penelitian ini berfokus pada analisis kerentanan mesin antivirus terhadap malware dalam format APK (*Android Package Kit*) yang disematkan ke dalam citra berformat PNG (*Portable Network Graphics*) dengan metode steganografi LSB (*Least Significant Bit*). Metode LSB dipilih karena kesederhanaannya dalam menyisipkan pesan rahasia (*payload*) ke dalam bit paling tidak signifikan dari piksel citra sehingga perubahan visual pada citra *stego* (citra yang telah disisipi pesan rahasia) minimal dan sulit dideteksi oleh mata manusia. Tujuan dari penelitian ini adalah untuk menguji sejauh mana mesin antivirus saat ini dalam mendeteksi keberadaan malware yang disematkan ke dalam citra dengan metode tersebut. Proses pengujian dilakukan dengan menyematkan sampel malware ke dalam beberapa citra (abu-abu dan berwarna). Selanjutnya, citra stego diunggah ke layanan VirusTotal untuk dianalisis oleh berbagai mesin antivirus. Hasil pengujian menunjukkan bahwa dari 61 mesin antivirus yang tersedia di VirusTotal, tidak ada satupun (0 dari 61) yang berhasil mendeteksi keberadaan malware di dalam citra. Temuan ini mengindikasikan adanya kerentanan yang signifikan pada mesin antivirus saat ini yang berpotensi menjadi ancaman serius dalam distribusi malware.

Kata kunci: Steganografi, LSB, Citra, Malware, Antivirus

ABSTRACT

The development of digital technology has brought convenience to many aspects of life, but it has also opened the door to new cyber threats. One of the media that is often utilized for the spread of malware (malicious software) is digital images because of their commonly used and often unsuspected nature. This research focuses on analyzing the vulnerability of antivirus engines to malware in APK (Android Package Kit) format embedded into PNG (Portable Network Graphics) format images with the LSB (Least Significant Bit) steganography method. The LSB method was chosen because of its simplicity in inserting the secret message (payload) into the least significant bit of the image pixel so that the visual changes in the stego image (image that has been inserted with a secret message) are minimal and difficult to detect by the human eye. The purpose of this research is to test the extent to which current antivirus engines can detect the presence of malware embedded into images using this method. The testing process is done by embedding malware samples into several images (gray and color). Subsequently, the stego images were uploaded to the VirusTotal service to be analyzed by various antivirus engines. The test results showed that out of 61 antivirus engines available on VirusTotal, none (0 out of 61) successfully detected the presence of malware in the images. This finding indicates a significant vulnerability in current antivirus engines that could potentially pose a serious threat to malware distribution.

Keyword**:** *Steganography, LSB, Image, Malware, Antivirus*