

ABSTRACT

The *End of File* (EOF) steganography method is a data hiding technique that appends messages to the end of a cover object. While advantageous in preserving the visual quality of the original image, this method suffers from a fundamental drawback: a linear increase in file size relative to the embedded message size, which can arouse suspicion. This study aims to optimize storage efficiency and time performance in EOF steganography by implementing and comparing four compression algorithms: Zstandard, Brotli, LZMA, and Huffman Encoding. The testing methodology utilized PNG images as cover objects and five types of secret file formats (.json, .wav, .txt, .csv, and .bmp). Performance validation was conducted through two rigorous testing stages: first, testing across file size variations of 1MB, 10MB, and 100MB to measure algorithm consistency and scalability; second, iterative testing performed 10 times on standard 10MB samples to ensure data reliability and accuracy. Measured performance parameters included compression ratio, processing duration (embedding and extraction), and memory usage. The results indicate significant differences in performance characteristics among the algorithms. The LZMA algorithm proved superior in space efficiency, consistently yielding the highest compression ratios (reaching 92.59% on audio files and 95.70% on JSON files) along with the lowest memory usage. Conversely, the Zstandard algorithm dominated in speed and scalability, achieving the fastest average embedding time (86.71 ms on 10MB) and remaining stable under 1 second during 100MB load testing. Meanwhile, Brotli experienced extreme time performance degradation on large files, and Huffman Encoding demonstrated ineffective compression ratios on multimedia files. In conclusion, LZMA is recommended for systems prioritizing maximum storage savings, whereas Zstandard is recommended for environments requiring real-time responsiveness..

Keywords: Brotli, Data Compression, EOF, Huffman Encoding, LZMA, Steganography, ZStandard

ABSTRAK

Steganografi metode *End of File* (EOF) merupakan teknik penyembunyian data yang menyisipkan pesan di akhir *file* penampung (*cover object*). Meskipun memiliki keunggulan dalam menjaga kualitas visual citra asli, metode ini memiliki kelemahan mendasar yaitu peningkatan ukuran *file* yang linear terhadap besarnya pesan yang disisipkan, yang dapat memicu kecurigaan pihak ketiga. Penelitian ini bertujuan untuk mengoptimalkan efisiensi penyimpanan dan kinerja waktu pada steganografi EOF dengan mengimplementasikan dan membandingkan empat algoritma kompresi yaitu *Zstandard*, *Brotli*, LZMA, dan *Huffman Encoding*. Metodologi pengujian menggunakan citra PNG sebagai *cover object* dan lima jenis format *file* rahasia (.json, .wav, .txt, .csv, dan .bmp). Validasi kinerja dilakukan melalui dua tahap pengujian ketat. Pertama, pengujian pada variasi ukuran *file* 1MB, 10MB, dan 100MB untuk mengukur konsistensi dan skalabilitas algoritma. Kedua, pengujian iteratif sebanyak 10 kali pada sampel standar 10MB untuk menjamin reliabilitas dan akurasi data rata-rata. Parameter kinerja yang diukur meliputi rasio kompresi, durasi pemrosesan (*embedding* dan *extraction*), serta penggunaan memori. Hasil penelitian menunjukkan bahwa karakteristik kinerja setiap algoritma berbeda secara signifikan. Algoritma LZMA terbukti paling unggul dalam efisiensi ruang, secara konsisten menghasilkan rasio kompresi tertinggi (mencapai 92,59% pada *file* audio dan 95,70% pada file JSON) serta penggunaan memori terendah. Sebaliknya, algoritma *Zstandard* mendominasi aspek kecepatan dan skalabilitas, mencatatkan waktu penyisipan rata-rata tercepat (86,71 ms pada 10MB) dan tetap stabil di bawah 1 detik pada pengujian beban 100MB. Sementara itu, *Brotli* mengalami degradasi performa waktu yang ekstrem pada *file* berukuran besar, dan *Huffman Encoding* menunjukkan kinerja rasio yang tidak efektif pada *file* multimedia. Kesimpulannya, LZMA direkomendasikan untuk prioritas penghematan penyimpanan maksimal, sedangkan *Zstandard* direkomendasikan untuk sistem yang membutuhkan responsivitas waktu real-time.

Kata kunci – *Brotli*, EOF, *Huffman Encoding*, Kompresi Data, LZMA, Steganografi, *ZStandard*