



ABSTRACT

Steganography has been widely developed with various methods using various types of digital media as cover. In audio steganography, MP3 is one of audio type that widely used as steganography cover. Conventional steganography techniques generally use a single MP3 file as a cover. The use of a single MP3 file as a cover has limitations in terms of capacity where the size of the secret message must be adjusted to the MP3 cover steganography capacity. The use of a single MP3 file also has security limitations in which the secret message is centered on a single cover file, making the secret messages easier to identified.

In this study, multiple MP3 files are used as cover with the aim of increasing steganographic capacity without limiting the number of used files. The homogeneous frame of an MP3 file that is a representation of the silent sound is used as a medium for storing the bits of embedded messages. Before being inserted into an MP3 cover file, the secret message is encrypted with the AES algorithm with the key that has already been processed by the MD5 hash function. Key characters "INFRM" and "forb" are used as password and secret messages identifiers. The use of multiple MP3 files and cryptography is expected to increase the security of secret messages, since secret messages are no longer centered on one MP3 file.

The results of this study indicate that the steganography method of multiple MP3 files can increase the capacity by adding MP3 covers and extracting secret messages using homogenous frame utilization methods without resizing and reducing the quality of used MP3 audio file. However, the use of key characters "INFRM" and "forb" makes the system can only use plural files with the total of max stego at least 84 bytes.

Keywords : steganography, homogeneous frame, max stego, multiple MP3 cover files.



INTISARI

Steganografi telah banyak dikembangkan dengan berbagai metode menggunakan berbagai jenis media digital sebagai *cover*. Pada steganografi audio, MP3 adalah salah satu jenis *cover* yang banyak digunakan. Teknik steganografi konvensional umumnya menggunakan berkas MP3 tunggal sebagai *cover*. Penggunaan berkas MP3 tunggal sebagai *cover* memiliki keterbatasan dari segi kapasitas dimana ukuran pesan rahasia harus disesuaikan dengan kapasitas steganografi MP3 *cover* yang digunakan. Penggunaan berkas MP3 tunggal juga memiliki keterbatasan dari segi keamanan dimana pesan rahasia terpusat pada satu berkas *cover* sehingga memudahkan pihak ketiga mengidentifikasi pesan rahasia.

Pada penelitian ini, berkas MP3 jamak digunakan sebagai media *cover* dengan tujuan peningkatan kapasitas steganografi tanpa membatasi jumlah berkas yang digunakan. Jumlah *cover* disesuaikan dengan ukuran pesan rahasia. *Frame* homogen dari berkas MP3 yang merupakan representasi dari suara diam dimanfaatkan sebagai media penyimpan informasi bit-bit pesan rahasia yang disisipkan. Sebelum disisipkan ke dalam berkas MP3 *cover*, pesan rahasia terlebih dahulu dienkripsi dengan algoritme AES dengan kunci yang sudah dikenai proses MD5 *hash function*. Karakter kunci “INFRM” dan “forb” digunakan sebagai pengenal password dan pesan rahasia. Penggunaan berkas MP3 jamak dan penggunaan kriptografi diharapkan dapat menjaga keamanan pesan rahasia, karena pesan rahasia tidak lagi terpusat pada satu berkas MP3.

Hasil penelitian ini menunjukkan bahwa metode steganografi pada berkas MP3 jamak dapat melakukan penambahan kapasitas dengan cara penambahan *cover* MP3 dan mengekstraksi kembali pesan rahasia dengan menggunakan metode pemanfaatan *frame* homogen tanpa mengubah ukuran dan mengurangi kualitas berkas audio MP3 yang digunakan. Namun penggunaan karakter kunci “INFRM” dan “forb” membuat sistem hanya dapat menggunakan berkas jamak dengan total *max stego* minimal sebesar 84 *byte*.

Kata kunci -- steganografi, *frame* homogen, *max stego*, berkas MP3 jamak.