IMPLEMENTASI KRIPTOGRAFI *SECRET SHARING SCHEME* DAN STEGANOGRAFI AUDIO *LEAST SIGNIFICANT BIT* MENGGUNAKAN *PSEUDORANDOM HITZL-ZELE*

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar
Sarjana Matematika

Oleh:
Miftah Fadillah Sopian
NIM 2008079

PROGRAM STUDI MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA
2024

Implementasi Kriptografi *Secret Sharing Scheme* dan Steganografi Audio *Least Significant Bit* Menggunakan *Pseudorandom Hitzl-Zele*

Oleh:
Miftah Fadillah Sopian
NIM. 2008079

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam Universitas Pendidikan Indonesia

© Miftah Fadillah Sopian 2024
Universitas Pendidikan Indonesia
Agustus 2024

Hak cipta dilindungi undang-undang.
Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,
dengan dicetak ulang, difotokopi, atau cara lainnya tanpa izin dari penulis.

LEMBAR PENGESAHAN

MIFTAH FADILLAH SOPIAN

IMPLEMENTASI KRIPTOGRAFI *SECRET SHARING SCHEME* DAN STEGANOGRAFI AUDIO *LEAST SIGNIFICANT BIT* MENGGUNAKAN *PSEUDORANDOM HITZL-ZELE*

Disetujui dan disahkan oleh pembimbing:

Pembimbing I

Prof. Siti Fatimah, S.Pd., M.Si., Ph.D.

NIP. 196808231994032002

Pembimbing II

Dra. Rini Marwati, M.S.

NIP. 196606251990012001

Mengetahui,

Ketua Program Studi Matematika

Dr. Kartika Yulianti, M.Si.

NIP. 198207282005012001

ABSTRAK

Pertukaran informasi semakin mudah dan cepat dengan berbagai media yang berakibat pertukaran informasi sulit dikendalikan keamanannya. Dalam rangka menghindari kebocoran informasi dan ancaman keamanan informasi lainnya, dilakukan penggabungan kriptografi dan steganografi. Kriptografi *secret sharing scheme* (skema (t, w)) memungkinkan pemilik informasi untuk membagikan informasi rahasia menjadi beberapa bagian, disebut sebagai *share* yang diberikan kepada sejumlah pemegang kunci, sehingga tidak ada pemegang kunci tunggal. Steganografi audio *Least Significant Bit* (*LSB*) digunakan untuk meyembunyikan *share* ke dalam *file* audio *wav* berdasarkan *pseudorandom Hitzl-Zele* sebagai pemilihan lokasi penyematan pada data *file* audio. Penggabungan kriptografi *secret sharing scheme* dan steganografi audio *LSB* menggunakan *pseudorandom Hitzl-Zele* diimplementasikan menjadi sebuah program aplikasi yang dikonstruksi menggunakan bahasa pemrograman Python 3.12 dan diberi nama "*(t, w)-Threshold Scheme and LSB Hitzl-Zele*". Program aplikasi tersebut menunjukkan performa yang lebih baik dalam menampung informasi rahasia dengan nilai *PSNR* diperoleh 112,43 dB. Nilai *PSNR* tersebut sedikit lebih tinggi dibandingkan penelitian terkait, yaitu diperoleh 109,35 dB. Perbandingan tersebut berdasarkan nilai *PSNR* dari persentase panjang data bit yang disematkan dan panjang data audio sebanyak 10% dan pada *file* audio dengan *bit depth* 16-bit.

Kata Kunci: Kriptografi, Skema (t, w), Steganografi Audio, *Least Significant Bit*, *Pseudorandom Hitzl-Zele*.

ABSTRACT

The exchange of information has become easier and faster with various media, resulting in the difficulty of controlling information security. To prevent information leakage and other security threats, a combination of cryptographic and steganographic methods is used. Secret sharing scheme cryptography ((t,w)-threshold scheme) allows the owner of the information to split the secret information into several parts, called shares, which are given to multiple key holders, ensuring no single key holder has the complete information. Audio steganography Least Significant Bit (LSB) technique is used to hide the shares in a wav audio file, based on the Hitzl-Zele pseudorandom algorithm for determining the embedding locations in the audio file data. The combination of the secret sharing scheme cryptography and audio steganography LSB using the Hitzl-Zele pseudorandom algorithm was implemented as an application program constructed using Python 3.12 and named "(t,w)-Threshold Scheme and LSB Hitzl-Zele." This application program demonstrated better performance in holding secret information with a PSNR value of 112.43 dB. This PSNR value is slightly higher compared to related research, which obtained 109.35 dB. The comparison is based on the PSNR value from the percentage of the bit length of the embedded data and the length of the audio data, which is 10% in a 16-bit depth audio file.

Keywords: *Cryptography, (t,w)-Threshold Scheme, Audio Steganography, Least Significant Bit, Hitzl-Zele Pseudorandom.*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

Al-Hooti, M. H. A., Djanali, S., & Ahmad, T. (2016). *Audio data hiding based on sample value modification using modulus function*. Journal of information processing systems, 12(3), 525-537.

Behnia, S., Akhavan, A., Akhshani, A., & Samsudin, A. (2011). *A Novel Dynamic Model of Pseudorandom Number Generator*. Journal of Computational and Applied Mathematics, 235 (12), 3455-3463.

Brookshear, J. G., & Brylow, D. (2015). *Computer Science: An Overview (12th ed.)*. Pearson.

Burton, D. M. (2010). *Elementary Number Theory (7th ed.)*. New York: The McGraw Hill Companies.

Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). *Digital Watermarking and Steganography*. Morgan Kaufmann.

Deshpande, R. G., Ragha, L. L., & Sharma, S. K. (2018). Video quality assessment through PSNR estimation for different compression standards. Indonesian Journal of Electrical Engineering and Computer Science, 11(3), 918-924. https://doi.org/10.11591/ijeecs.v11.i3.pp918-924

Herlinawati, H. (2016). Steganografi Video H263 dengan Metode Discrete Cosine Transform. Electrician: Jurnal Rekayasa dan Teknologi Elektro, 10(1), 11-20. https://doi.org/10.23960/elc.v10n1.189

Hrishikesh Dutta, Rohan Kumar Das, Sukumar Nandi & S. R. Mahadeva Prasanna. (2019). *An Overview of Digital Audio Steganography*. IETE Technical Review. https://doi.org/10.1080/02564602.2019.1699454

Humaira, A. F., Marwati, R., & Yulianti, K. (2023). *Implementasi Kriptografi Secret Sharing Scheme dan Steganografi Audio Least Significant Bit (LSB)*. JMT: Jurnal Matematika dan Terapan, 5(1), 1-11. DOI: https://doi.org/10.21009/jmt.5.1.1

Katadata Insight Center. (2022). *Indonesia Masuk 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak Dunia*. Daring pada https://databoks.katadata.co.id/datapublish/2022/09/13/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia diakses 5 Desember 2023.

Kordov, K. M., & Stoyanov, B. (2017). *Least Significant Bit Steganography using Hitzl-Zele Chaotic*. International Journal of Electronics and Telecommunications; Vol 63, No 4 (2017); 417-422; 2300-1933. http://ijet.pl/index.php/ijet/article/view/10.1515-eletel-2017-0061

Mufadilah, A. T. (2019). *Implementasi Kriptografi Rivest Shamir Adleman (RSA) yang Ditingkatkan dan Steganografi Least Significant Bit (LSB)*. (Skripsi). Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung.

Munir, R. (2019). *Kriptografi* (edisi ke-2). Bandung: Informatika.

Naik, R. B., & Singh, U. (2022). *A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption*. Annals of Data Science, 1-26.

Shamir, A. (1979). *How to Share a Secret*. Communications of the ACM, 22 (11), 612-61.

Stinson, D.R., & Paterson, M. (2017). *Cryptography: Theory and Practice (4th ed.)*. Chapman and Hall/CRC. https://doi.org/10.1201/9781315282497

The ASCII Code. *The complete table of ASCII characters, codes, symbols and signs*. Daring pada https://theasciicode.com.ar diakses 28 Januari 2024.

Ulfah, N. (2020). *Pengamanan Pesan Teks dengan Kriptografi Advanced Encryption Standard (AES) dan Steganografi Least Significant Bit (LSB)*. (Skripsi). Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung.

Yuwono, E. I., & Antonio, T. (2015). *Studi Format Audio dan Teks Untuk Modul Speech to Text*. http://dspace.uc.ac.id/handle/123456789/1059