

**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

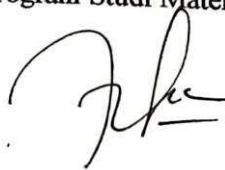


Dra. Rini Marwati, M.S.

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 menyembunyikan *share* ke dalam *file* audio *wav* berdasarkan *pseudorandom Hitzl-Zele* sebagai pemilihan lokasi penyematkan 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

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN.....	iii
KATA PENGANTAR	iv
UCAPAN TERIMA KASIH.....	v
ABSTRAK.....	vii
ABSTRACT.....	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Tujuan Penelitian	4
1.4 Batasan Masalah.....	5
1.5 Manfaat Penelitian	5
BAB II KAJIAN PUSTAKA.....	6
2.1 Teori Dasar Matematika.....	6
2.1.1 Bilangan Pembagi Terbesar	6
2.1.2 Relatif Prima	6
2.1.3 Kongruen Modulo	6
2.1.4 Invers Perkalian pada Modulo	6
2.1.5 Interpolasi Lagrange.....	7
2.2 Teori <i>Coding</i>	7
2.2.1 Bit.....	7
2.2.2 <i>ASCII</i>	8
2.2.3 Operasi XOR.....	8
2.3 Teori Dasar Kriptografi.....	9
2.3.1 Terminologi Istilah dalam Kriptografi.....	10
2.3.2 Kriptosistem	10

2.4 Skema Pembagian Rahasia (<i>Secret Sharing Scheme</i>).....	11
2.4.1 <i>Threshold Schemes</i>	11
2.4.2 Kriptosistem <i>Shamir (t, w)-Threshold Schemes</i>	11
2.5 File Audio Waveform Audio Format.....	13
2.6 Steganografi	14
2.6.1 Terminologi Istilah dalam Steganografi.....	14
2.6.2 Steganografi Audio.....	15
2.6.3 Least Significant Bit (LSB) Audio.....	16
2.6.4 Peak Signal-to-Noise Ratio (PSNR)	17
2.7 Pseudorandom Hitzl-Zele	18
2.8 Bahasa Pemrograman Python	20
BAB III METODE PENELITIAN.....	21
3.1 Identifikasi Masalah.....	21
3.2 Model Dasar	22
3.2.1 Skema (<i>t, w</i>).....	22
3.2.2 Pseudorandom Bit Generator Hitzl-Zele.....	23
3.2.3 Embedding Share pada File Audio Wav dengan Least Significant Bit	23
3.2.4 Extracting Share dari File Audio Wav dengan Least Significant Bit ..	24
3.2.5 Konstruksi <i>Plaintext</i>	25
3.3 Pengembangan Model.....	25
3.4 Konstruksi Program Aplikasi.....	26
3.4.1 Algoritma Deskriptif.....	27
3.4.2 Rancangan Desain Tampilan.....	30
3.4.3 <i>Library</i> Program.....	32
3.5 Proses Validasi	33
3.6 Pengambilan Kesimpulan.....	34
BAB IV HASIL DAN PEMBAHASAN	35
4.1 Skema (<i>t, w</i>)- <i>Threshold Scheme and LSB Hitzl-Zele</i>	35
4.2 Program Aplikasi (<i>t, w</i>)- <i>Threshold Scheme and LSB Hitzl-Zele</i>	41

4.2.1 Algoritma Program Aplikasi (t, w) -Threshold Scheme and LSB Hitzl-Zele.....	41
4.2.2 Tampilan Program Aplikasi (t, w) -Threshold Scheme and LSB Hitzl-Zele dan Petunjuk Penggunaannya.....	52
4.3 Validasi Program Aplikasi (t, w) -Threshold Scheme and LSB Hitzl-Zele	58
4.3.1 Validasi Program Aplikasi dengan Menggunakan Perhitungan Manual	59
4.3.2 Validasi Perumuman Program Aplikasi.....	75
4.3.3 Validasi dengan Tes <i>PSNR</i>	79
BAB V KESIMPULAN DAN SARAN.....	81
5.1 Kesimpulan	81
5.2 Saran.....	82
DAFTAR PUSTAKA	83
LAMPIRAN	85

DAFTAR TABEL

Tabel 2.1 Operasi XOR pada dua rangkaian bit	9
Tabel 3.1 Rancangan masukan dan keluaran program <i>dealer</i> : enkripsi-embedding	27
Tabel 3. 2 Rancangan masukan dan keluaran program <i>participant</i> : <i>extracting</i> -dekripsi.....	28
Tabel 4.1 Properti <i>file</i> audio yang digunakan pada proses <i>embedding</i> (Sumber <i>file</i> audio: mmsp.ece.mcgill.ca/Documents/AudioFormats/WAVE/Samples.html)...	55
Tabel 4.2 Properti <i>file</i> audio hasil proses <i>embedding</i>	56
Tabel 4.3 Properti <i>file</i> audio yang digunakan pada proses <i>extracting</i>	58
Tabel 4.4 Uraian nilai variabel masukan pada Gambar 4.4	59
Tabel 4.5 Hasil <i>share</i> yang dibangun menggunakan program aplikasi dan perhitungan manual.....	61
Tabel 4.6 Hasil proses penyesuaian dan konversi <i>share</i> menjadi <i>bitshare</i>	61
Tabel 4.7 Hasil perhitungan rangkaian bit 1 pada <i>stego-key_1</i>	64
Tabel 4.8 Hasil perhitungan untuk membangun <i>stego-key_1</i>	66
Tabel 4.9 Hasil perhitungan untuk membangun <i>stego-key_2</i>	67
Tabel 4. 10 Hasil perhitungan untuk membangun <i>stego-key_3</i>	67
Tabel 4. 11 Hasil perhitungan untuk membangun <i>stego-key_4</i>	67
Tabel 4. 12 Hasil perhitungan untuk membangun <i>stego-key_5</i>	68
Tabel 4.13 Data <i>file</i> audio pada tabel 4.1 dalam biner.....	68
Tabel 4.14 Uraian proses <i>embedding</i> data audio ke-1	69
Tabel 4.15 Perbandingan data audio hasil program aplikasi dan hasil perhitungan manual	70
Tabel 4.16 Uraian nilai variabel masukan pada Gambar 4.6	70
Tabel 4.17 Hasil 4 buah <i>stego_key</i> yang dibangun untuk proses <i>extracting</i>	71
Tabel 4.18 Uraian proses <i>extracting</i> data audio ke-1.....	71
Tabel 4.19 Rangkuman 100 digit pertama dan 100 digit terakhir <i>bitshare</i> ke-1 ..	72
Tabel 4. 20 Konversi byte pada <i>bitshare</i> ke-1 menjadi karakter berdasarkan sistem <i>ASCII</i>	72
Tabel 4. 21 <i>Share</i> hasil <i>extracting</i>	73
Tabel 4. 22 Persentase panjang <i>bitshare</i> dengan panjang data audio	79

Tabel 4.23 Kualitas <i>Stego-Audio</i>	79
Tabel 4. 24 Kualitas <i>stego-audio</i> dibandingkan dengan penelitian terkait	80

DAFTAR GAMBAR

Gambar 2.1 Sistem ASCII (Sumber: <i>theasciicode.com.ar</i>)	8
Gambar 2.2 Skema kriptografi	11
Gambar 2.3 Skema steganografi	15
Gambar 2.4 Skema steganografi audio	15
Gambar 3.1 Skema pembagian rahasia untuk skema (t, w)	22
Gambar 3.2 Skema <i>pseudorandom bit generator Hitzl-Zele</i>	23
Gambar 3.3 Skema <i>embedding share</i> pada <i>file</i> audio <i>wav</i>	24
Gambar 3.4 Skema <i>extracting share</i> dari <i>file</i> audio <i>wav</i>	24
Gambar 3.5 Skema konstruksi <i>plaintext</i>	25
Gambar 3.6 Skema pengembangan model	26
Gambar 3.7 Rancangan program bagian <i>dealer</i> : enkripsi- <i>embedding</i> subbagian enkripsi	30
Gambar 3.8 Rancangan program bagian <i>dealer</i> : enkripsi- <i>embedding</i> subbagian <i>embedding</i>	31
Gambar 3.9 Rancangan program bagian <i>participant</i> : <i>extracting</i> -dekripsi	32
Gambar 4.1 Skema (t, w) - <i>Threshold Scheme and LSB Hitzl-Zele</i> bagian <i>Dealer</i>	35
Gambar 4.2 Skema (t, w) - <i>Threshold Scheme and LSB Hitzl-Zele</i> bagian <i>Participant</i>	38
Gambar 4.3 Tampilan program aplikasi (t, w) - <i>Threshold Scheme and LSB Hitzl-Zele</i> pada bagian Menu Utama	53
Gambar 4.4 Tampilan program aplikasi (t, w) - <i>Threshold Scheme and LSB Hitzl-Zele</i> pada bagian Dealer subbagian Enkripsi	54
Gambar 4.5 Tampilan program aplikasi (t, w) - <i>Threshold Scheme and LSB Hitzl-Zele</i> pada bagian Dealer subbagian <i>Embedding</i>	55
Gambar 4.6 Tampilan program aplikasi (t, w) - <i>Threshold Scheme and LSB Hitzl-Zele</i> pada bagian Participant	57
Gambar 4.7 Sintaks perhitungan nilai awal fungsi <i>Hitzl-Zele</i>	62
Gambar 4.8 Ilustrasi <i>stego-key</i>	63
Gambar 4.9 Sintaks untuk menampilkan data <i>file</i> audio	68
Gambar 4.10 Tampilan program aplikasi pada bagian <i>Dealer</i> subbagian Enkripsi untuk validasi perumuman	76

Gambar 4.11 Tampilan program aplikasi pada bagian <i>Dealer</i> subbagian <i>Embedding</i> untuk validasi perumuman.....	77
Gambar 4.12 Tampilan program aplikasi pada bagian <i>Participant</i> untuk validasi perumuman.....	78

DAFTAR LAMPIRAN

Lampiran 1: <i>Coding</i> Python untuk Skema (\mathbf{t}, \mathbf{w}).....	85
Lampiran 2: <i>Coding</i> Python untuk <i>Pseudorandom Hitzl-Zele</i>	87
Lampiran 3: <i>Coding</i> Python untuk <i>Least Significant Bit</i>	89
Lampiran 4: <i>Coding</i> untuk tes <i>PSNR</i>	91

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., Ragma, 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>