

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES DAN
NOISELESS STEGANOGRAFI AUDIO UNTUK PENGAMANAN
DATA TEKS BERBASIS APLIKASI WEB**



SKRIPSI

diajukan untuk memenuhi sebagian syarat
untuk memperoleh gelar Sarjana Teknik Program Studi Teknik Komputer

Oleh
Raoul Khakim Annur
2101553

**PROGRAM STUDI TEKNIK KOMPUTER
KAMPUS UPI DI CIBIRU
UNIVERSITAS PENDIDIKAN INDONESIA
2025**

HALAMAN HAK CIPTA

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES DAN NOISELESS
STEGANOGRAFI AUDIO UNTUK PENGAMANAN DATA TEKS BERBASIS
APLIKASI WEB**

oleh
Raoul Khakim Annur
NIM 2101553

Sebuah Skripsi yang Diajukan untuk Memenuhi Salah Satu Syarat Memperoleh Gelar
Sarjana Teknik pada Program Studi S1 Teknik Komputer

© Raoul Khakim Annur
Universitas Pendidikan Indonesia
2025

Hak Cipta Dilindungi Undang-Undang
Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian, dengan dicetak
ulang, difoto kopi, atau cara lainnya tanpa izin penulis

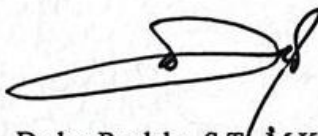
HALAMAN PENGESAHAN SKRIPSI

RAOUL KHAKIM ANNUR

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES DAN NOISELESS
STEGANOGRAFI AUDIO UNTUK PENGAMANAN DATA TEKS
BERBASIS APLIKASI WEB**

Disetujui dan disahkan oleh:

Pembimbing 1



Deden Pradeka, S.T., M.Kom.

NIP. 920200419890816101

Pembimbing 2

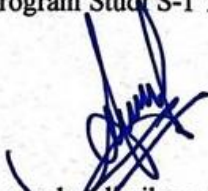


Muhammad Taufik, S.Tr.Kom, M.T.I

NIP. 920200819940117101

Mengetahui

Ketua Program Studi S-1 Teknik Komputer



Anugrah Adiwilaga, S.ST., M.T.

NIP. 920200819880813101

PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Raoul Khakim Annur

NIM : 2101553

Program Studi : Teknik Komputer

Judul Karya : Implementasi Algoritma Kriptografi AES dan Noiseless Steganografi
Audio Untuk Pengamanan Data Teks Berbasis Aplikasi Web

Dengan ini saya menyatakan bahwa karya tulis ini merupakan hasil kerja saya sendiri. Saya menjamin bahwa seluruh isi karya ini baik, baik sebagian maupun keseluruhan, bukan merupakan plagiarisme dari karya orang lain, kecuali pada bagian yang telah dinyatakan dan disebutkan sumbernya dengan jelas.

Jika di kemudian hari ditemukan pelanggaran terhadap etika akademi atau unsur plagiarisme, saya bersedia menerima sanksi sesuai peraturan yang berlaku di
Universitas Pendidikan Indonesia

Kabupaten Bandung, 30 Agustus 2025



Raoul Khakim Annur

KATA PENGANTAR

Terima kasih kepada Allah SWT atas rahmat, hidayah, dan karunia-Nya, yang memungkinkan penulis menyelesaikan skripsi berjudul "Implementasi Algoritma Kriptografi AES dan Noiseless Steganografi Audio Untuk Pengamanan Data Teks Berbasis Aplikasi Web" tepat waktu. Penulis juga mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu selama proses penulisan skripsi ini, di antaranya:

1. Orang tua dan keluarga yang terus memberikan dukungan moral, material, dan doa yang tak pernah berhenti. Dukungan dan kasih sayang mereka sangat berarti dan tidak akan pernah terbalas. Semoga Allah SWT senantiasa melimpahkan kesehatan bagi mereka.
2. Bapak Deden Pradeka, S.T., M.Kom., selaku dosen pembimbing pertama, atas bimbingan, arahan, dan ilmunya yang sangat berharga. Tanpa bantuan beliau, penelitian ini tidak akan dapat diselesaikan.
3. Bapak Muhammad Taufik, S.Tr.Kom, M.T.I, selaku dosen pembimbing kedua, atas bimbingan dan masukannya yang sangat membantu dalam menyelesaikan tugas akhir ini.
4. Seluruh dosen dan staf Program Studi Teknik Komputer, atas ilmu dan wawasan yang telah diberikan selama masa perkuliahan.

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES DAN NOISELESS STEGANOGRAFI AUDIO UNTUK PENGAMANAN DATA TEKS BERBASIS APLIKASI WEB

Raoul Khakim Annur
2101553

ABSTRAK

Ancaman keamanan siber dan kebocoran data di era digital modern, khususnya yang menargetkan data teks, telah menjadi isu krusial di Indonesia. Serangan ini menyoroti perlunya metode perlindungan data yang kuat. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sebuah aplikasi web yang menggabungkan dua metode keamanan, yaitu kriptografi AES dan *Noiseless Steganography*, untuk menciptakan lapisan perlindungan ganda pada data teks. Metode yang digunakan dalam penelitian ini adalah pendekatan *Design and Development* (D&D) dengan pendekatan *Agile*. Dalam implementasinya, algoritma AES digunakan untuk mengenkripsi *plaintext* menjadi *ciphertext*. Selanjutnya, *ciphertext* biner ini direkonstruksi ke dalam sebuah file audio berformat WAV menggunakan teknik *Noiseless Steganography* (NoStega) dan menyisipkan password AES yang sudah dilakukan *hash* MD5 pada *metadata* file WAV, di mana biner tersebut dipetakan ke dalam pola melodi lagu "Mary Had a Little Lamb". Pengujian *Black Box* dilakukan untuk memastikan bahwa semua fitur aplikasi beroperasi sesuai dengan ekspektasi. Uji korelasi Pearson membuktikan hubungan yang sangat lemah antara *plaintext* dan *ciphertext*, dimana rata-rata korelasi biner sekitar 0.02, yang mengonfirmasi algoritma enkripsi AES dalam melakukan pengacakan data. Pengujian juga dilakukan untuk menentukan batasan kapasitas pesan, di mana sistem berhasil mengubah *plaintext* dengan ukuran minimal 1 karakter dan maksimal 5.386 karakter. Selain itu, kuesioner yang diisi oleh 30 responden dengan skala Likert menunjukkan presentase 94,57% terhadap kualitas audio yang dihasilkan, tanpa menimbulkan kecurigaan atau adanya *noise*. Secara keseluruhan, penelitian ini membuktikan bahwa kombinasi AES dan NoStega adalah solusi yang efektif dan inovatif untuk mengurangi tingkat kemungkinan untuk muncul rasa kecurigaan pada khalayak umum terhadap file stego audio.

Kata Kunci: Kriptografi AES, *Noiseless Steganography*, Keamanan Data, Aplikasi Web, Audio Steganografi.

IMPLEMENTATION OF AES CRYPTOGRAPHIC ALGORITHM AND NOISELESS AUDIO STEGANOGRAPHY FOR TEXT DATA SECURITY IN A WEB-BASED APPLICATION

Raoul Khakim Annur
2101553

ABSTRACT

The threat of cyberattacks and data breaches in the modern digital era, especially those targeting text data, has become a crucial issue in Indonesia. These attacks highlight the need for a strong and undetectable data protection method. This research aims to design and implement a web application that combines two security methods, namely AES cryptography and Noiseless Steganography, to create a double layer of protection for text data. The method used in this study is the Design and Development (D&D) approach with an Agile methodology. In its implementation, the AES algorithm is used to encrypt plaintext into ciphertext. Subsequently, this binary ciphertext is reconstructed into a WAV audio file using the Noiseless Steganography (NoStega) technique and the AES password, which has been hashed with MD5, is embedded in the WAV file's metadata, where the binary data is mapped to the melody pattern of the song "Mary Had a Little Lamb". Black Box testing was conducted to ensure that all application features operated as expected. The Pearson correlation test proved a very weak relationship between plaintext and ciphertext, with an average binary correlation of approximately 0.02, which confirms the AES encryption algorithm's effectiveness in data randomization. Testing was also performed to determine the message capacity limit, where the system successfully embedded plaintext with a minimum size of 1 character and a maximum of 5,386 characters. Furthermore, a questionnaire filled out by 30 respondents using a Likert scale showed a 94.57% acceptance rate for the quality of the generated audio, without raising suspicion or containing any noise. Overall, this research proves that the combination of AES and NoStega is an effective and innovative solution for enhancing the security of web-based text data.

Keywords: AES Cryptography, Noiseless Steganography, Data Security, Web Application, Audio Steganography.

DAFTAR ISI

HALAMAN HAK CIPTA	i
HALAMAN PENGESAHAN SKRIPSI.....	ii
PERNYATAAN BEBAS PLAGIARISME	iii
KATA PENGANTAR.....	iv
ABSTRAK	v
<i>ABSTRACT</i>	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xi
DAFTAR PERSAMAAN.....	xii
DAFTAR LAMPIRAN	xiii
BAB I.....	1
PENDAHULUAN.....	1
1.1. Latar Belakang Penelitian	1
1.2. Rumusan Masalah Penelitian	4
1.3. Tujuan Penelitian	4
1.4. Manfaat Penelitian	5
1.4.1. Manfaat Teoritis	5
1.4.2. Manfaat Praktis	5
1.5. Ruang Lingkup Penelitian.....	5
BAB II	7
TINJAUAN PUSTAKA	7
2.1. Kriptografi.....	7
2.1.1. Kriptografi Simetris	7
2.1.1.1. <i>Advanced Encryption Standard</i> (AES)	8
2.1.2. Kriptografi Asimetris	10
2.1.3. <i>Hash</i>	11
2.1.3.1. <i>Message Digest 5</i> (MD5)	11
2.2. Steganografi	13
2.2.1. <i>Noiseless Steganography</i> (NoStega).....	14
2.3. <i>File Audio</i>	15

2.3.1. Waveform Audio.....	16
2.4. Aplikasi	16
2.4.1. Aplikasi Berbasis <i>Website</i>	17
2.5. Python	17
2.5.1. Flask	18
2.6. Korelasi Pearson.....	18
2.7. Kerangka Pemikiran.....	20
2.8. Hipotesis.....	22
2.9. Penelitian Terkait	23
BAB III.....	28
METODE PENELITIAN	28
3.1. Metode Penelitian.....	28
3.2. Analisis.....	29
3.3. Perancangan Sistem	29
3.3.1. Diagram Arsitektur Sistem.....	30
3.3.2. <i>Flowchart</i> Sistem	30
3.3.3. Diagram <i>Use Case</i>	37
3.3.4. Desain <i>Website</i>	39
3.4. Pengembangan	44
3.4.1. Alat Penelitian.....	45
3.4.2. Metode Pengembangan Aplikasi.....	45
3.5. Pengujian dan Evaluasi	48
3.6. Pelaporan.....	54
BAB IV.....	55
HASIL DAN PEMBAHASAN	55
4.1. Hasil Pengembangan Aplikasi	55
4.1.1. Hasil Antarmuka Aplikasi.....	55
4.1.2. Hasil Pengujian <i>Black Box</i>	60
4.2. Hasil Pengujian Korelasi Pearson	65
4.3. Hasil Pengujian <i>Plaintext</i> Minimal dan Maksimal pada Aplikasi	70
4.4. Hasil Pengujian Sampel dengan Kuesioner	77
BAB V.....	83

SIMPULAN DAN SARAN.....	83
5.1. Simpulan	83
5.2. Saran.....	84
DAFTAR PUSTAKA	85
LAMPIRAN.....	89

DAFTAR GAMBAR

Gambar 1.1 Jumlah serangan <i>cyber</i> di Indonesia selama semester 1 2024 (AwanPintar.id, 2024).....	1
Gambar 2.1 Alur Kriptografi Simetris (Geta Putri dkk., 2015).....	8
Gambar 2.2 Alur proses AES (Dunkelman dkk., 2010).	9
Gambar 2.3 Alur Kriptografi Asimetris (Geta Putri dkk., 2015).....	11
Gambar 2.4 Alur proses enkripsi dan dekripsi steganografi	14
Gambar 2.5 Kerangka Pemikiran.....	22
Gambar 3.1 Tahapan Penelitian Metode <i>Design and Development</i>	28
Gambar 3.2 Diagram Arsitektur Sistem.....	30
Gambar 3.3 Kode program definisi melodi dan panjang tiap chord	32
Gambar 3.4 Kode program mendefinisikan unit ke durasi satuan detik	33
Gambar 3.5 <i>Flowchart</i> sistem enkripsi	35
Gambar 3.6 <i>Flowchart</i> sistem dekripsi	37
Gambar 3.7 Diagram <i>Use Case</i>	39
Gambar 3.8 Desain Menu Utama.....	39
Gambar 3.9 Desain Menu Enkripsi	40
Gambar 3.10 Desain Menu Hasil Enkripsi	41
Gambar 3.11 Desain Menu Dekripsi.....	42
Gambar 3.12 Desain Menu Hasil Dekripsi	43
Gambar 3.13 Desain Menu Tentang	44
Gambar 3.14 Tahapan Metode Agile (Badiwibowo Atim & Korespondensi, 2024)..	46
Gambar 3.15 Pengujian Black Box.....	48
Gambar 4.1 Tampilan Menu Utama.....	56
Gambar 4.2 Tampilan Menu Enkripsi.....	56
Gambar 4.3 Tampilan Menu hasil Enkripsi	57
Gambar 4.4 Tampilan Menu Dekripsi	58
Gambar 4.5 Tampilan Menu hasil Dekripsi.....	59
Gambar 4.6 Tampilan Menu Tentang	60
Gambar 4.7 <i>Pie Chart</i> Jawaban Responden Pengguna Aplikasi <i>Editing Audio</i>	79

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait	23
Tabel 3.1 Skenario uji coba <i>Black Box</i> Aplikasi Web.....	49
Tabel 3.2 Instrumen Penerimaan Responden Terhadap Stego Audio.....	52
Tabel 3.3 Interpretasi Persentase Besar dari Kuesioner (Sugiyono, 2019).....	53
Tabel 4.1 Hasil Pengujian <i>Black Box</i>	61
Tabel 4.2 Hasil Pengujian Korelasi Pearson <i>plaintext</i> dan <i>ciphertext</i> dalam bentuk biner.....	66
Tabel 4.3 Hasil Pengujian <i>Plaintext</i> Minimal dan Maksimal pada Aplikasi	71
Tabel 4.4 Distribusi semua jawaban Responden per Pertanyaan.....	77
Tabel 4.5 Distribusi Jawaban Responden Berpengalaman (N=5)	80

DAFTAR PERSAMAAN

Persamaan Korelasi Pearson (1)	19
Persamaan Skala Likert (2)	53

DAFTAR LAMPIRAN

Lampiran 1 Jadwal Penelitian	89
Lampiran 2 Enkripsi AES dan Konversi ke Biner	89
Lampiran 3 Pemetaan Biner ke Pola Lagu dan <i>Generate</i> Audio	90
Lampiran 4 Dekripsi AES	93
Lampiran 5 Ekstraksi Metadata dan Biner dari <i>File</i> Audio	94
Lampiran 6 Skrip Pengujian Korelasi Pearson	96
Lampiran 7 Hasil Pengujian <i>Blackbox</i>	99
Lampiran 8 Hasil Pengujian Korelasi Pearson <i>plaintext</i> dan <i>ciphertext</i> dalam bentuk biner.....	102
Lampiran 9 Pengujian Minimal dan Maksimal Pada Aplikasi	107
Lampiran 10 Kuesioner Google Form	113
Lampiran 11 Distribusi Semua Jawaban Responden per Pertanyaan	115
Lampiran 12 Hasil Kuesioner	117
Lampiran 13 Hasil Cek Turnitin	123
Lampiran 14 Hasil Cek AI Detector	123

DAFTAR PUSTAKA

- Adhimah, L. F., Nurhafiyah, I., Muntahar, A. A., Kristiaji, F., & Mustofa, D. (2023). IMPLEMENTASI APLIKASI STEGANOGRAFI BERBASIS WEB MENGGUNAKAN ALGORITMA LSB DAN BPCS. *KOMPUTA: Jurnal Ilmiah Komputer Dan Informatika*, 12(2), 100–108.
- Andriyanto, M. R., & Sukmasetya, P. (2022). Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace. *Journal of Computer System and Informatics (JoSYC)*, 4(1), 179–187. <https://doi.org/10.47065/josyc.v4i1.2451>
- Arif, Z., & Nurokhman, A. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi. *Jurnal Teknologi Sistem Informasi*, 4(2), 394–405. <https://doi.org/10.35957/jtsi.v4i2.6077>
- Ashari, I. F., & Munir, R. (2018). Graph Steganography Based on Multimedia Cover to Improve Security and Capacity. *Proceedings of ICAITI 2018 - 1st International Conference on Applied Information Technology and Innovation: Toward A New Paradigm for the Design of Assistive Technology in Smart Home Care*, 194–201. <https://doi.org/10.1109/ICAITI.2018.8686741>
- AwanPintar.id. (2024). Laporan Ancaman Digital di Indonesia. In *AwanPintar*.
- Badiwibowo Atim, S., & Korespondensi, P. (2024). Sianipar, F. R., & Ropianto, M. Unified Modeling Language, waterfall, database. *Journal of Artificial Intelligence and Technology Information (JAITI)*, 2(1), 14–25. <https://doi.org/10.58602/jaiti.v2i1.104>
- BSSN. (2024). *Lanskap Keamanan Siber Indonesia*. 70, 1–107. <https://www.bssn.go.id/wp-content/uploads/2025/02/LANSKAP-KEAMANAN-SIBER-2024-1.pdf>
- Cahyono, T. (2017). Statistik Uji Korelasi. *Yayasan Sanitarian Banyumas, Pertama*, 1–77.
- Desoky, A. (2008). Nostega: A novel noiseless steganography paradigm. *Journal of Digital Forensic Practice*, 2(3), 132–139. <https://doi.org/10.1080/15567280802558818>
- Desoky, A. (2012). *Noiseless Steganography: The Key to Covert Communications* (1st ed.). Auerbach Publications. <https://doi.org/10.1201/b11575>
- Dunkelman, O., Keller, N., & Shamir, A. (2010). *Improved Single-Key Attacks on 8-Round AES-192 and AES-256*. 158–176.
- Geta Putri, G., Styorini, W., & Dian Rahayani, R. (2015). Analisis Kriptografi Simetris AES dan Kriptografi Asimetris RSA Pada Enkripsi Citra Digital. *Ethos (Jurnal Penelitian Dan Pengabdian Masyarakat)*, 3(8), 197–207.
- Ghane, M. C., Uribarri, M. D., Djemai, R., Dunsin, D., & Araujo, I. I. (2023). A Novel Hybrid Method for Effective Identification and Extraction of Digital Evidence Masked by Steganographic Techniques in WAV and MP3 Files. *Journal of Information Security and Cybercrimes Research*, 6(2), 89–104. <https://doi.org/10.26735/izbk9372>
- Graciela Fausten Novindri, & Ocsa Nugraha Saian, P. (2022). Implementasi Flask Pada

- Sistem Penentuan Minimal Order Untuk Tiap Item Barang Di Distribution Center Pada Pt Xyz Berbasis Website. *Jurnal Mnemonic*, 5(2), 81–85. <https://doi.org/10.36040/mnemonic.v5i2.4670>
- Handayani, H., Faizah, K. U., Mutiara Ayulya, A., Rozan, M. F., Wulan, D., & Hamzah, M. L. (2023). Perancangan Sistem Informasi Inventory Barang Berbasis Web Menggunakan Metode Agile Software Development Designing a Web-Based Inventory Information System Using the Agile Software Development Method. *Jurnal Testing Dan Implementasi Sistem Informasi*, 1(1), 29–40.
- Hidayat, M., Tahir, M., Sukriyadi, A., Sulton, A., A, C. A. S., & F, S. A. (2023). Penerapan Kriptografi Caesar Chiper Dalam Pengamanan Data. *Jurnal Ilmiah Multidisiplin*, 2(03), 35–41. <https://doi.org/10.56127/jukim.v2i03.619>
- Irmayanti. (2023). Perancangan Sistem Informasi Penyewaan Thermoking di PT. Moderen Prima dengan Flask Python. *Jurnal Sistem Dan Teknologi Informasi Cendekia*, 1(1), 19–28.
- J. Ellis, T., & Levy, Y. (2010). A Guide for Novice Researchers: Design and Development Research Methods. *Proceedings of the 2010 InSITE Conference*, 107–118. <https://doi.org/10.28945/1237>
- Jabnabillah, F., & Margina, N. (2022). Analisis Korelasi Pearson Dalam Menentukan Hubungan Antara Motivasi Belajar Dengan Kemandirian Belajar Pada Pembelajaran Daring. *Jurnal Sintak*, 1(1), 14–18.
- Juhari, J., & Andrean, M. F. (2022). On the Application of Noiseless Steganography and Elliptic Curves Cryptography Digital Signature Algorithm Methods in Securing Text Messages. *CAUCHY: Jurnal Matematika Murni Dan Aplikasi*, 7(3), 483–492. <https://doi.org/10.18860/ca.v7i3.17358>
- Khairani, K., & Siambaton, M. Z. (2023). Pengamanan Data Teks Menggunakan Algoritma Kriptografi Elgamal dan XOR dari Serangan Hacker. *Sudo Jurnal Teknik Informatika*, 2(4), 176–187. <https://doi.org/10.56211/sudo.v2i4.401>
- Khoirudin, N. H., & Windarto, W. (2024). Penerapan Algoritme Advanced Encryption Standard (AES-512) untuk Pengamanan File Berbasis Web. *KRESNA: Jurnal Riset Dan Pengabdian Masyarakat*, 4(1), 62–71. <https://doi.org/10.36080/kresna.v4i1.104>
- Kurnia, R. N., Pradiptha, A. D., Fajar, M., Permana, J., Pradja, A. Di, Afrizal, R., Pradeka, D., & Khaerunnisa, Z. (2025). *Implementation of Least Significant Bit Steganography with Caesar Cipher Layout Dvorak web-based*. 14(1), 105–116.
- Latip, P. N. (2025). IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES DALAM PENGAMANAN FILE TEKS. *Jurnal Riset Sistem Informasi*, 2(3), 01–04. <https://doi.org/https://doi.org/10.69714/k6pr0s45>
- Li, J., Wang, K., & Jia, X. (2023). A Coverless Audio Steganography Based on Generative Adversarial Networks. *Electronics (Switzerland)*, 12(5). <https://doi.org/10.3390/electronics12051253>
- M. Nasution, R. (2022). Implementasi Metode Secure Hash Algorithm (SHA-1) Untuk Mendeteksi Orisinalitas File Audio. *Bulletin of Computer Science Research*, 2(3), 73–84. <https://doi.org/10.47065/bulletincsr.v2i3.140>
- Manurung, J., Sihombing, A. P. E., & Pandiangan, B. (2023). Sosialisasi Dan Edukasi

- Tentang Keamanan Data Dan Privasi Di Era Digital Untuk Meningkatkan Kesadaran Dan Perlindungan Masyarakat. *Jurnal Pengabdian Masyarakat Nauli*, 2(1), 1–7.
<https://ejournal.marqchainstitute.or.id/index.php/Nauli/article/view/103>
- Nuryadi, Astuti, T. D., Utami, E. S., & Budiantara, M. (2017). Buku Ajar Dasar-dasar Statistik Penelitian. In *Sibuku Media*.
- Permana, A. A. (2020). Implementasi Steganography pada Audio Menggunakan Algoritma End of File (EOF). *FORMAT: Jurnal Ilmiah Teknik Informatika*, 9(1), 91–98.
- Prasetyo, B., Gernowo, R., & Noranita, B. (2015). Kombinasi Steganografi Berbasis Bit Matching dan Kriptografi DES untuk Pengamanan Data. *Scientific Journal of Informatics*, 1(1), 79–93. <https://doi.org/10.15294/sji.v1i1.3643>
- Prastowo, W. D., Danianti, D., & Pramuntadi, A. (2023). Analisis Risiko Pada Pengembangan Perangkat Lunak Menggunakan Metode Agile Dan Rad (Rapid Application Development). *Citizen : Jurnal Ilmiah Multidisiplin Indonesia*, 3(3), 169–174. <https://doi.org/10.53866/jimi.v3i3.388>
- Rizal Pradana, Abd. Hallim, F. (2025). Steganography for Data Hiding in Digital Audio Data Using Combined Least Significant Bit and Blowfish Method. *JSE Journal of Science and Engineering*, 3(2), 90–95.
<https://doi.org/https://doi.org/10.30650/jse.v3i2.3924>
- Santoso, M. H., Girsang, N. D., Siagian, H., Wahyudi, A., & Sitorus, B. A. (2019). Perbandingan Algoritma Kriptografi Hash MD5 dan SHA-1. *Seminar Nasional Teknologi Informatika*, 2(1), 54–59.
- Sari, S. R., Resmawan, Yahya, N. I., & Yahya4, L. (2024). Implementasi Kriptografi dengan Algoritma RSA (Rivest-Shamir-Adleman) dalam Penyandian Pesan Teks dan Dokumen. *JOSTECH Journal of Science and Technology*, 4(1), 97–107.
- Saripa, S. (2023). Implementasi Sistem Keamanan File Menggunakan Algoritma AES untuk Mengamankan File Pribadi. *Progressive Information, Security, Computer, and Embedded System*, 1(2), 138–148.
- Setiyani, L. (2018). Rekayasa Perangkat Lunak [Software Engineering]. In *Jatayu Catra Internusa*.
- Simanjuntak, R. (2021). Noiseless Steganography Pada Motion Objek Dalam Gambar Animasi. In *Rake Sarasin*. Institut Teknologi Sumatera.
- Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice 7th Global Edition*.
- Sugiyono. (2019). *Metode Penelitian Kuantitatif Kualitatif dan R&D*. Penerbit Alfabeta.
- Umam, C., & Muslih, M. (2023). Enkripsi Data Teks Dengan AES dan Steganografi DWT. *InComTech : Jurnal Telekomunikasi Dan Komputer*, 13(1), 28.
<https://doi.org/10.22441/incomtech.v13i1.15059>
- Wachid Hidayatulloh, N., Tahir, M., Amalia, H., Afdlolul Basyar, N., Faizal Prianggara, A., & Yasin, M. (2023). Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data. *Digital Transformation Technology (Digitech)*, Vol.03(No.1), 1–10.

- Wiguna, M. R. (2024). *PENERAPAN TEKNIK STEGANOGRAFI DENGAN METODE GRAPHSTEGA DAN KRIPTOGRAFI AES BERBASIS APLIKASI WEB*. Universitas Pendidikan Indonesia.
- Yanti, F., & Budayawan, K. (2023). Implementasi Steganografi Menggunakan Metode Least Significant Bit (LSB) dalam Pengamanan Informasi pada Citra Digital. *Voteteknika (Vocational Teknik Elektronika Dan Informatika)*, 11(1), 63. <https://doi.org/10.24036/voteteknika.v11i1.121968>