

28/S/TEKKOM-KCBR/PK.03.08/16/AGUSTUS/2024

**PENGEMBANGAN APLIKASI KEAMANAN GAMBAR BERBASIS
WEBSITE MENGGUNAKAN ALGORITMA KRIPTOGRAFI DAN
STEGANOGRAFI PADA METADATA GAMBAR**

SKRIPSI

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



oleh
Muhamad Fajar
NIM 2008728

**PROGRAM STUDI TEKNIK KOMPUTER
KAMPUS UPI DI CIBIRU
UNIVERSITAS PENDIDIKAN INDONESIA
2024**

HALAMAN HAK CIPTA

PENGEMBANGAN APLIKASI KEAMANAN GAMBAR BERBASIS WEBSITE MENGGUNAKAN ALGORITMA KRIPTOGRAFI DAN STEGANOGRAFI PADA METADATA GAMBAR

oleh
Muhamad Fajar

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

© Muhamad Fajar
Universitas Pendidikan Indonesia
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

HALAMAN PENGESAHAN SKRIPSI

MUHAMAD FAJAR

**PENGEMBANGAN APLIKASI KEAMANAN GAMBAR BERBASIS
WEBSITE MENGGUNAKAN ALGORITMA KRIPTOGRAFI DAN
STEGANOGRAFI PADA METADATA GAMBAR**

Disetujui dan disahkan oleh pembimbing:

Pembimbing I



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

NIP. 920200419890816101

Pembimbing II

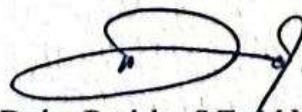


Devi Aprianti Rimadhani Agustini, S.Si., M.Si.

NIP. 920200819890421201

Mengetahui,

Ketua Program Studi Teknik Komputer



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

NIP. 920200419890816101

HALAMAN PERNYATAAN KEASLIAN SKRIPSI DAN BEBAS PLAGIARISME

Dengan ini saya menyatakan bahwa skripsi dengan judul “Pengembangan Aplikasi Keamanan Gambar Berbasis Website Menggunakan Algoritma Kriptografi Dan Steganografi Pada Metadata Gambar” ini beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung resiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Kab. Bandung, 15 Agustus 2024

Penulis,



Muhamad Fajar

NIM. 2008728



HALAMAN UCAPAN TERIMA KASIH

Penulis mengucapkan puji syukur kepada Allah SWT atas rahmat, hidayah, dan karunia-Nya yang memungkinkan penulis untuk menyelesaikan skripsi berjudul "Pengembangan Aplikasi Keamanan Gambar Berbasis Website Menggunakan Algoritma Kriptografi dan Steganografi pada Metadata Gambar" tepat pada waktunya. Penulis juga menyampaikan penghargaan dan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan selama proses penulisan skripsi ini. Dengan penuh hormat, penulis ingin menyampaikan terima kasih kepada:

1. Kedua orang tua, adik, dan keluarga besar yang selalu memberikan dukungan baik secara moral maupun material, serta senantiasa mendoakan saya setiap hari hingga saya dapat menyelesaikan tugas akhir skripsi ini. Kasih sayang yang telah mereka berikan tidak akan pernah terbalas, semoga Allah SWT senantiasa memberikan kesehatan kepada mereka.
2. Bapak Deden Pradeka, S.T., M.Kom., Ketua Program Studi Teknik Komputer sekaligus dosen pembimbing pertama, terima kasih atas bimbingan, dukungan, dan ilmu yang telah Bapak berikan. Tanpa arahan dan saran Bapak, penelitian ini tidak akan terselesaikan dengan baik.
3. Ibu Devi Aprianti Rimadhani Agustini, S.Si., M.Si., dosen pembimbing kedua, terima kasih atas bimbingan dan dukungan yang Ibu berikan. Pandangan Ibu sangat berarti dalam membantu saya menyelesaikan tugas akhir ini dengan sukses.
4. Bapak Wirmanto Suteddy, S.T., M.T., dosen pembimbing akademik, terima kasih atas bimbingan dan dukungan yang Bapak berikan selama masa studi saya. Arahan Bapak sangat membantu dalam kelancaran Ketika menjalani masa perkuliahan.
5. Seluruh Dosen dan Staf Program Studi Teknik Komputer, terima kasih atas ilmu dan wawasan yang bermanfaat selama masa perkuliahan, serta informasi penting yang selalu diberikan kepada saya.
6. Seseorang yang telah menjadi *support system* terbaik penulis. Dukungan, kesabaran, dan semangatnya menjadi salah satu sumber kekuatan utama

dalam menyelesaikan skripsi ini. Penulis merasa sangat beruntung telah melewati suka dan duka perkuliahan bersama.

7. Rekan-rekan mahasiswa Teknik Komputer angkatan 2020, khususnya grup Trio Sekawan Pencari Gelar, grup Pangandaran, grup Pangandaran part 2, terima kasih telah menjadi teman dan keluarga selama masa studi ini. Dukungan, persahabatan, dan kenangan yang kita bagikan sangat berarti. Perjalanan ini tidak akan sama tanpa kalian. Semoga keakraban kita terus terjaga dan kita semua mencapai kesuksesan di masa depan. Terima kasih atas segala hal yang telah kita lalui bersama.
8. Para staf kependidikan dan seluruh sivitas akademika Universitas Pendidikan Indonesia yang telah memberikan berbagai kebaikan dan kontribusi selama masa studi saya.

Ucapan terima kasih ini penulis persembahkan kepada semua pihak yang membantu penulis dalam menyelesaikan penelitian ini hingga selesai. Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat berbagai kekurangan, untuk itu penulis mengharapkan kritik dan saran yang membangun demi perbaikan di masa yang akan datang. Akhir kata, semoga skripsi ini dapat bermanfaat bagi penulis khususnya dan pembaca pada umumnya.

Kab. Bandung, 15 Agustus 2024

Penulis,



Muhamad Fajar

NIM.2008728

PENGEMBANGAN APLIKASI KEAMANAN GAMBAR BERBASIS WEBSITE MENGGUNAKAN ALGORITMA KRIPTOGRAFI DAN STEGANOGRAFI PADA METADATA GAMBAR

Muhamad Fajar

2008728

ABSTRAK

Dalam era digital, keamanan gambar digital menjadi isu yang sangat penting mengingat risiko modifikasi dan akses tidak sah selama transmisi data. Penelitian ini bertujuan untuk mengembangkan aplikasi keamanan gambar berbasis web dengan mengintegrasikan algoritma kriptografi DES dan AES serta teknik steganografi pada metadata gambar. Algoritma DES digunakan untuk permutasi kunci, sedangkan AES digunakan untuk enkripsi data gambar, sehingga menghasilkan *ciphertext* yang akan disisipkan ke dalam metadata gambar menggunakan teknik steganografi. Penelitian ini dilakukan dengan pendekatan metode *Design and Development*. Untuk aplikasi web dikembangkan menggunakan metode *Agile* dan fungsionalitasnya diuji dengan metode *black box*. Hasil pengujian menunjukkan bahwa aplikasi web dapat berfungsi sesuai dengan yang diharapkan. Sementara itu, Hasil pengujian sistem menunjukkan bahwa algoritma pembangkitan kunci DES mampu menghasilkan kunci yang kompleks, yang merupakan salah satu strategi efektif dalam mencegah peretasan kunci. Adapun algoritma AES berhasil mengenkripsi gambar menjadi *ciphertext* yang disisipkan ke dalam metadata tanpa mengubah visual gambar asli. Pengujian lebih lanjut menunjukkan bahwa nilai *Mean Squared Error* (MSE) antara *cover image* dan *stego image* adalah 0, dengan nilai *Peak Signal-to-Noise Ratio* (PSNR) mencapai tak terhingga, menunjukkan tidak ada perbedaan visual. Namun, terdapat kekurangan berupa perubahan ukuran file yang signifikan setelah penyisipan informasi. Pengujian ketahanan (*robustness*) juga mengungkap bahwa pesan yang disisipkan dapat dipertahankan setelah pengeditan menggunakan Microsoft Paint.

Kata Kunci: Keamanan Gambar Digital;DES;AES;Steganografi;Metadata Gambar;Aplikasi Web

**DEVELOPMENT OF WEB-BASED IMAGE SECURITY APPLICATIONS
USING CRYPTOGRAPHY ALGORITHMS AND STEGANOGRAPHY ON
IMAGE METADATA**

Muhamad Fajar

2008728

ABSTRACT

In the digital era, digital image security becomes a very important issue considering the risk of modification and unauthorized access during data transmission. This research aims to develop a web-based image security application by integrating DES and AES cryptographic algorithms and steganography techniques on image metadata. The DES algorithm is used for key permutation, while AES is used for image data encryption, resulting in a ciphertext that will be inserted into the image metadata using steganography techniques. This research was conducted using the Design and Development method approach. The web application was developed using the Agile method and its functionality was tested using the black box method. The test results show that the web application can function as expected. Meanwhile, the system test results show that the DES key generation algorithm is able to generate complex keys, which is one of the effective strategies in preventing key hacking. As for the AES algorithm, it successfully encrypts the image into ciphertext that is inserted into the metadata without changing the visuals of the original image. Further testing shows that the Mean Squared Error (MSE) value between the cover image and the stego image is 0, with the Peak Signal-to-Noise Ratio (PSNR) value reaching infinity, indicating no visual difference. However, there is a drawback in the form of a significant change in file size after information insertion. Robustness testing also revealed that the inserted message can be preserved after editing using Microsoft Paint.

Keywords: *Digital Image Security;DES;AES;Steganography;Image Metadata;Web Applications;*

DAFTAR ISI

HALAMAN HAK CIPTA	i
HALAMAN PENGESAHAN SKRIPSI.....	ii
HALAMAN PERNYATAAN	iii
HALAMAN UCAPAN TERIMA KASIH	iv
ABSTRAK.....	vi
<i>ABSTRACT</i>	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	viii
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN.....	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Penelitian	1
1.2 Rumusan Masalah Penelitian	4
1.3 Tujuan Penelitian	4
1.4 Batasan Penelitian	5
1.5 Manfaat Penelitian	5
1.5.1 Manfaat Teoritis	5
1.5.2 Manfaat Praktis.....	6
1.6 Struktur Organisasi Skripsi	6
BAB II KAJIAN PUSTAKA.....	8
2.1 Kriptografi.....	8
2.1.1 Kriptografi Simetris.....	9
2.1.2 Kriptografi Asimetris	9
2.2 Data Encryption Standard (DES).....	10
2.2.1 Proses Pembangkitan Kunci.....	11
2.3 Advanced Encryption Standard (AES)	15
2.3.1 Proses Transformasi pada Algoritma AES.....	20
2.3.1.1 Transformasi <i>SubBytes</i>	20
2.3.1.2 Transformasi <i>ShiftRows</i>	22
2.3.1.3 Transformasi <i>MixColumns</i>	23
2.3.1.4 Transformasi <i>AddRoundKey</i>	24

2.3.2	Ekspansi Kunci.....	24
2.4	Steganografi	26
2.5	Metadata.....	29
2.6	Gambar digital.....	30
2.7	Aplikasi	31
2.8	Aplikasi Berbasis <i>Website</i>	31
2.9	<i>Bootstrap</i>	32
2.10	<i>Spring Boot</i>	32
2.11	MSE dan PSNR.....	33
2.12	Penelitian Terkait	34
BAB III METODE PENELITIAN.....		37
3.1	Desain Penelitian.....	37
3.2	Analisis.....	37
3.3	Desain atau Perancangan Sistem.....	38
3.3.1	Desain Arsitektur Sistem.....	38
3.3.2	Diagram Alir Sistem.....	39
3.3.3	Diagram Alir Aplikasi	42
3.3.4	Diagram <i>Use Case</i>	44
3.3.5	Diagram Aktivitas	45
3.4	Pengembangan	47
3.4.1	Alat dan Bahan	47
3.4.2	Metode Pengembangan Aplikasi.....	48
3.5	Pengujian dan Evaluasi	50
3.6	Pelaporan.....	52
BAB IV TEMUAN DAN PEMBAHASAN		53
4.1	Hasil Pengembangan Aplikasi	53
4.1.1	Hasil Antarmuka Aplikasi	53
4.1.2	Hasil Pengujian <i>Black box</i>	56
4.2	Hasil Implementasi Algoritma DES dan AES serta Steganografi	58
4.2.1	Hasil Implementasi Permutasi Kunci DES	59
4.2.2	Hasil Implementasi Enkripsi dan Dekripsi AES	60
4.2.3	Hasil Implementasi Steganografi Metadata.....	62

4.3	Hasil Evaluasi Enkripsi AES dan Teknik Steganografi.....	67
4.3.1	Pengukuran Waktu Enkripsi dan Dekripsi	67
4.3.2	Pengukuran MSE dan PSNR	70
4.3.3	Pengujian Ketahanan (<i>Robustness</i>)	73
BAB V SIMPULAN, IMPLIKASI, DAN REKOMENDASI		77
5.1	Simpulan	77
5.2	Implikasi.....	78
5.3	Rekomendasi	78
DAFTAR PUSTAKA		80
LAMPIRAN.....		84

DAFTAR TABEL

Tabel 2.1 Jumlah pergeseran bit pada setiap putaran.....	13
Tabel 2.2 Beberapa Versi Algoritma AES.....	16
Tabel 2.3 S-box (Stallings, 2009)	21
Tabel 2.4 S-box <i>Inverse</i> (Stallings, 2009).....	22
Tabel 2.5 Penelitian Terkait	36
Tabel 4.1 Hasil Pengujian Black Box	56
Tabel 4.2 Tabel Hasil Permutasi Kunci DES.....	59
Tabel 4.3 Pengukuran Rata-rata Waktu Enkripsi dan Dekripsi	68
Tabel 4.4 Perbandingan Berapa Lama Waktu Yang Diperlukan untuk Serangan <i>Bruteforce</i>	70
Tabel 4.5 Hasil Pengujian MSE dan PSNR	71
Tabel 4.6 Hasil Pengujian <i>Crop</i>	74
Tabel 4.7 Hasil Pengujian <i>Rotate</i>	75
Tabel 4.8 Hasil Pengujian <i>Flip</i>	75

DAFTAR GAMBAR

Gambar 1.1 Trafik Anomali Serangan Siber di Indonesia (BSSN, 2024)	2
Gambar 2.1 Kriptografi Simetris.....	9
Gambar 2.2 Kriptografi Asimetris	10
Gambar 2.3 Skema Global Algoritma DES (Munir, 2004b)	11
Gambar 2.4 Matriks Masukan (a) dan Matriks Permutasi PC-1 (b) (Nugraha, 2023)	12
Gambar 2.5 Matriks Permutasi PC-2 (Nugraha, 2023).....	14
Gambar 2.6 Proses Pembangkitan Kunci DES	15
Gambar 2.7 Proses Konversi Gambar Menjadi <i>plaintext</i>	17
Gambar 2.8 Alur Proses Enkripsi dan Dekripsi Algoritma AES	18
Gambar 2.9 <i>Array State</i> (Munir, 2004a)	19
Gambar 2.10 Menyalin Data Masukan ke <i>Array State</i> (Munir, 2004a).....	19
Gambar 2.11 Elemen <i>State</i> dan Kunci dalam HEX (Munir, 2004a).....	20
Gambar 2.12 Alur Transformasi <i>Substitute Byte</i> (Stallings, 2009).....	21
Gambar 2.13 Transformasi <i>SubBytes</i> (Stallings, 2009)	22
Gambar 2.14 Transformasi <i>ShiftRows</i> (Stallings, 2009).....	23
Gambar 2.15 Transformasi <i>MixCollumns</i> (Stallings, 2009)	23
Gambar 2.16 Contoh Transformasi <i>MixCollumns</i> (Stallings, 2009).....	23
Gambar 2.17 Trasformasi <i>Inverse</i> (Stallings, 2009)	24
Gambar 2.18 Transformasi <i>AddRoundKey</i> (Stallings, 2009).....	24
Gambar 2.19 Ekspansi Kunci AES (Stallings, 2009)	25
Gambar 2.20 Model Sistem Steganografi (Hafiz, 2019).....	27
Gambar 2.21 Proses <i>Embedding</i> dan <i>Extraction</i> Steganografi Metadata	29
Gambar 2.22 Contoh Metadata File Gambar	30
Gambar 3.1 Desain Penelitian.....	37
Gambar 3.2 Desain Arsitektur Sistem.....	39
Gambar 3.3 Diagram Alir Sistem Enkripsi	40
Gambar 3.4 Diagram Alir Sistem Dekripsi	41
Gambar 3.5 Diagram Alir Aplikasi Enkripsi	42
Gambar 3.6 Diagram Alir Aplikasi Dekripsi	43
Gambar 3.7 Diagram <i>Use Case</i>	45
Gambar 3.8 Diagram Aktivitas Enkripsi.....	46
Gambar 3.9 Diagram Aktivitas Dekripsi	47
Gambar 3.10 Metode Pengembangan Sistem <i>Agile</i>	48
Gambar 3.11 Cara Kerja Metode Pengujian <i>Black Box</i>	51
Gambar 4.1 Tampilan Menu Utama.....	53
Gambar 4.2 Tampilan Menu <i>Encryption</i>	54
Gambar 4.3 Tampilan Hasil Enkripsi.....	55
Gambar 4.4 Tampilan Menu <i>Decryption</i>	55
Gambar 4.5 Tampilan Hasil Dekripsi	56
Gambar 4.7 Pesan Yang Dienkripsi	61
Gambar 4.8 <i>Ciphertext</i> Hasil Enkripsi	61
Gambar 4.9 Pesan Hasil Dekripsi	62

Gambar 4.10 Sampul Steganografi	63
Gambar 4.11 Metadata Gambar Sebelum Penyisipan <i>Ciphertext</i>	64
Gambar 4.12 Metadata Gambar Setelah Penyisipan <i>Ciphertext</i>	65
Gambar 4.13 Sampul Steganografi Setelah Disisipkan <i>Ciphertext</i>	66
Gambar 4.14 Gambar Hasil Ekstraksi dan Dekripsi	66
Gambar 4.15 Grafik Distribusi Waktu Enkripsi dan Dekripsi.....	69
Gambar 4.16 Histogram Perbandingan <i>Channel</i> Warna Gambar 1.....	72
Gambar 4.17 Histogram Perbandingan <i>Channel</i> Warna Gambar 2.....	73

DAFTAR LAMPIRAN

Lampiran 1. Jadwal Penelitian	84
Lampiran 2. <i>Repository</i> Github untuk <i>Source Code</i> Aplikasi.....	85
Lampiran 3. Code MATLAB Perhitungan MSE dan PSNR	85
Lampiran 4. Code MATLAB Perbandingan Histogram	86
Lampiran 5. Dokumentasi Pengujian Enkripsi	86
Lampiran 6. Dokumentasi Pengujian Perhitungan MSE dan PSNR.....	87
Lampiran 7. Hasil Pengujian Waktu Proses Enkripsi dan Dekripsi	87
Lampiran 8. Hasil Pengujian dengan Gambar Pesan Ukuran 2048x2048	93

DAFTAR PUSTAKA

- Abdala, P., Budiman, M. A., & Herryance, H. (2017). Implementasi Algoritma Kriptografi Vernam Cipher dan DES (Data Encryption Standard) pada Aplikasi Chatting berbasis Android. *Jurnal Ilmiah Core IT: Community Research Information Technology*, 5(1).
- Afriyantari, D., & Putri, P. (2019). Rancang Bangun Media Pembelajaran Bahasa Arab untuk Anak Usia Dini Berbasis Android. Dalam *Technologia* (Vol. 10, Nomor 3).
- Alexander, I., & Khairani, M. (2024). Penerapan Metode Interpolasi Linear dan Geometric Mean Filter Pada Citra Resolusi Rendah Hasil Resampling Application of Linear Interpolation and Geometric Mean Filter Methods to Resampling Low Resolution Images. *Januari*, 2024(1), 72–86. <https://jurnal.unity-academy.sch.id/index.php/jirsi/index72>
- Azanuddin, Yakub, S., & Prayudha, J. (2022). *Implementasi Keamanan Citra Menggunakan Algoritma AES-128 Dengan Aplikasi Client-Server*. 7, 51–61. <https://tunasbangsa.ac.id/ejurnal/index.php/jurasik>
- Tampubolon, N. B., Isnanto, R. R., & Sinuraya, E. W. (2016). Implementasi Dan Analisis Algoritma Advanced Encryption Standard (Aes) Pada Tiga Variasi Panjang Kunci Untuk Berkas Multimedia. *Transient: Jurnal Ilmiah Teknik Elektro*, 4(4), 1008-10112.
- 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>
- Fernando, Y., Darwis, D., Mehta, A. R., Wamiliana, W., & Wantoro, A. (2024). A New Approach of Steganography on Image Metadata. *JOIV: International Journal on Informatics Visualization*, 8(2), 968-976.
- Hafiz, A. (2019). Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB). *Jurnal Cendikia*, 17(1), 194-198.

- Haris, M., Lydia, M. S., & Sutarman, S. (2023). Pengamanan Pada Citra Digital dengan Menggunakan Modifikasi Blok Data Algoritma AES - Rijndael. *Jurnal Media Informatika Budidarma*, 7(1), 444. <https://doi.org/10.30865/mib.v7i1.5458>
- Hendri, H. (2014). Kompresi Citra dari Format BMP ke Format PNG. *Jurnal TIMES*, 3(1).
- Irawan, C., & Winarno, A. (2020). Kombinasi Algoritma Kriptografi Aes Dan Des Untuk Enkripsi File Dokumen Proposal. *Sendiu*, pp. 2–8.
- Kaunang, V. V. R., Djamen, A. C., & Kaende, Q. C. (2024). Implementasi Steganografi Pada Citra Digital Menggunakan Metode Least Significant Bit Dengan Kriptografi Super Enkripsi. *Journal Of Informatics, Business, Education And Innovation Technology*, 5(4), 102-115.
- Kaur, M., Singh, S., & Kaur, M. (2021). Computational image encryption techniques: a comprehensive review. *Mathematical Problems in Engineering*, 2021(1), 5012496.
- Mandang, C., Wuisan, D., & Mandagi, J. (2020). Penerapan Metode RAD dalam Merancang Aplikasi Web Proyek PLN UIP Sulbagut. *JOINTER: Journal Of Informatics Engineering*, 1(02), 49-53.
- Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook Of Applied Cryptography*. Boca Raton: CRC Press.
- Munir, R. (2004a). Advanced Encryption Standard (AES). *Institut Teknologi Bandung*. Diakses pada 14 Mei 2024. Dari <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2020-2021/Review-beberapa-block-cipher-AES.pdf>
- Munir, R. (2004b). Data Encryption Standard (DES). *Institut Teknologi Bandung*. Diakses pada 14 Mei 2024. Dari <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/7%20-%20Review-beberapa-block-cipher%20-%20DES.pdf>

- Munir, R. (2004c). Steganografi dan Watermarking. *Institut Teknologi Bandung*. Diakses pada 14 Mei 2024. Dari <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Steganografi%20dan%20Watermarking.pdf>
- Murdowo, S. (2014). Mengetahui Proses Perhitungan Enkripsi Menggunakan Algoritma Kriptografi Advance Encryption Standard (Aes) Rijndael. *Jurnal Ilmiah Infokam*, 10(1).
- Ningtyas, D., & Rivai, I. (2024). Rancang Bangun Aplikasi Pembukuan Keuangan UMKM Berbasis Website (Studi Kasus: UMKM Indah Fashion). *Jurnal Teknologi Dan Sistem Informasi Bisnis*, 6(1), 11–19. <https://doi.org/10.47233/jteksis.v6i1.1072>
- Nugraha, A. (2023). Data Encryption Standard (DES). *Universitas Dian Nuswantoro*
- Prasetya, A. W. Y., Suhardjo, B., & Munir, R. (2023). Penggunaan Kombinasi Kriptografi Triple DES dan Teknik Steganografi LSB dalam Mengamankan Pesan Militer. *E-JURNAL JUSITI: Jurnal Sistem Informasi dan Teknologi Informasi*, 12(2), 193-199.
- Purnama, K. E., Rozikin, C., & Ridha, A. A. (2023). Analisis Forensic Citra Digital Menggunakan Teknik Error Level Analysis Dan Metadata Berdasarkan Metode Nist. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 7(2), 1100-1107.
- Ratama, N., & Munawaroh, M. (2022). Implementasi Metode Kriptografi dengan Menggunakan Algoritma RC4 dan Steganografi Least Significant Bit Dalam Mengamankan Data Berbasis Android. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, 6(2), 1272. <https://doi.org/10.30865/mib.v6i2.3902>
- Rohayah, S., Sasmito, G. W., & Somantri, O. (2015). Aplikasi Steganografi Untuk Penyisipan Pesan. *Jurnal Informatika Ahmad Dahlan*, 9(1), 102820.
- Saberikamarposhti, M., Ghorbani, A., & Yadollahi, M. (2024). A comprehensive survey on image encryption: Taxonomy, challenges, and future directions. *Chaos, Solitons & Fractals*, 178, 114361.

- Selent, D. (2010). Advanced encryption standard. *Rivier Academic Journal*, 6(2), 1-14.
- Stallings, W. (2009). *Cryptography And Network Security*. Pearson/Prentice Hall.
- Supriatmaja, G. A., Pratama, I. P. M. Y., Mahendra, K., Widyaputra, K. D. D., Deva, J., & Mahendra, G. S. (2022). Sistem Informasi Perpustakaan Menggunakan Framework Bootstrap Dengan PHP Native dan Database MySQL Berbasis Web Pada SMP Negeri 2 Dawan. *Jurnal Teknologi Ilmu Komputer*, 1(1), 7-15.
- Susanto, J., & Ilhamsyah, T. R. (2016). Aplikasi enkripsi dan dekripsi untuk keamanan dokumen menggunakan triple des dengan memanfaatkan usb flash drive. *Coding Jurnal Komputer dan Aplikasi*, 4(2).
- Syafaat, F. (2019). *Implementasi Kriptografi Aes-128 Pada Unmanned Aerial Vehicle Dan Ground Control System* (Doctoral dissertation, Universitas Komputer Indonesia).
- Tiken, C., & Samli, R. (2022). A comprehensive review about image encryption methods. *Harran Üniversitesi Mühendislik Dergisi*, 7(1), 27-49.
- Yamin, M., Malethi, T. T., & Natali, S. (2023). Evaluasi Risiko Pada Penggunaan Password Yang Lemah: Analisis Kasus Penggunaan Password Umum. *Jurnal Ilmiah Multidisiplin Ilmu Komputer*, 1(1), 41-48.
- Zhao, J. (2019). *Personal Blog Based on Spring Boot*. St. Cloud State University Repository. Diakses pada 15 Juli 2024, dari https://repository.stcloudstate.edu/csit_etds/30/