

**KRIPTOGRAFI GAMBAR MENGGUNAKAN MODE OPERASI
COUNTER RAES YANG DIMODIFIKASI**

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana
Matematika



Oleh:

Fawwaz Muhammad Tsani

NIM 2004811

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

LEMBAR HAK CIPTA

**KRIPTOGRAFI GAMBAR MENGGUNAKAN MODE OPERASI
COUNTER RAES YANG DIMODIFIKASI**

Oleh:

Fawwaz Muhammad Tsani

2004811

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

© Fawwaz Muhammad Tsani 2024

Universitas Pendidikan Indonesia

April 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

FAWWAZ MUHAMMAD TSANI

KRIPTOGRAFI GAMBAR MENGGUNAKAN MODE OPERASI *COUNTER*
RAES YANG DIMODIFIKASI


Disetujui dan disahkan,

Pembimbing I

 22/4/2024

Dra. Hj. Rini Marwati, M.S.
NIP. 196606251990012001

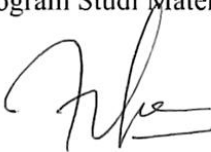
Pembimbing II

 22/4/2024

Dr. Sumanang Muhtar Gozali, M.Si.
NIP. 197411242005011001

Mengetahui,

Ketua Program Studi Matematika



Dr. Kartika Yulianti, S.Pd., M.Si.
NIP. 198207282005012001

ABSTRAK

Keamanan data digital sangat penting mengingat kini banyak terjadi kasus kebocoran data berupa gambar seperti Kartu Tanda Penduduk dan Kartu Keluarga. Gambar tersebut dapat disalahgunakan oleh pihak yang tidak bertanggungjawab sehingga perlu diamankan dengan cara menyamarkan pesan pada gambar menggunakan kriptografi. Pada penelitian ini, kriptografi yang digunakan dikembangkan menggunakan studi literatur, pengembangan model kriptosistem, dan pengujian model menggunakan program aplikasi. Kriptografi diterapkan pada gambar menggunakan RAES yang dimodifikasi dalam mode operasi *Counter*. RAES adalah algoritma kriptografi *block-cipher* hasil kombinasi antara AES dan *rail-fence cipher*. Modifikasi pada RAES dilakukan dengan menggunakan algoritma *rail-fence cipher* yang telah dioptimalkan dan mengelola kunci *rail-fence cipher* yang digunakan. *Counter* pada mode operasi *Counter* dibangkitkan dengan memanfaatkan konsep $GF(2^8)$ dan fungsi penambahan standar. Implementasi ini dilakukan menggunakan program aplikasi. Selain itu, program aplikasi digunakan untuk melakukan validasi bahwa gambar yang telah tersamarkan dapat dikembalikan menjadi seperti semula. Hasil dari penelitian ini menunjukkan bahwa algoritma kriptografi dapat diterapkan pada gambar, pesan pada gambar dapat disamarkan dengan baik, dan validasi berhasil dilakukan.

Kata Kunci: Kriptografi, Kriptografi Gambar, RAES yang Dimodifikasi, Mode Operasi *Counter*, *Counter*

ABSTRACT

Digital data security is fundamental, considering that there are now many cases of data leakage in the form of images, such as Identity Cards and Family Cards. Irresponsible parties can misuse the image, so it needs to be secured by disguising the message in the image using cryptography. In this research, the cryptography used is developed using literature studies, cryptosystem model development, and model testing using application programs. Cryptography is applied to images using modified RAES in Counter mode of operation. RAES is a block-cipher cryptographic algorithm that combines AES and rail-fence cipher. The modification to RAES is done by using an optimized rail-fence cipher algorithm and managing the rail-fence cipher keys used. Counters in the Counter mode of operation are generated by utilizing the concept of $GF(2^8)$ and standard addition function. This implementation is done using an application program. In addition, the application program is used to validate that the hidden image can be restored to its original state. This research shows that the cryptographic algorithm can be applied to the image, the message on the image can be well disguised, and the validation is successfully performed.

Keywords: *Cryptography, Image Cryptography, Modified RAES, Counter Mode of Operation, Counter*

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN	iii
KATA PENGANTAR.....	iv
UCAPAN TERIMA KASIH	v
ABSTRAK.....	vi
ABSTRACT.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xiii
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian	3
BAB II KAJIAN PUSTAKA	4
2.1 Teori Dasar Matematika	4
2.1.1 Bilangan Biner, Bilangan Desimal, dan Bilangan Heksadesimal	4
2.1.2 Grup, Ring, dan Lapangan	5
2.1.3 Lapangan Galois 28	6
2.1.4 XOR	7
2.2 Teori Dasar Kriptografi	8
2.2.1 Terminologi Istilah	8
2.2.2 Kriptosistem	8
2.2.3 Kriptografi Gambar	9
2.2.4 Bit dan <i>Byte</i>	10
2.2.5 <i>Substitution Cipher</i> dan <i>Transposition Cipher</i>	10
2.2.6 <i>Stream Cipher</i> dan <i>Block Cipher</i>	11
2.2.7 <i>Rail-fence Cipher</i>	12
2.2.8 <i>Advanced Encryption Standard (AES)</i>	13

2.2.9	Mode Operasi <i>Block Cipher</i>	21
2.2.10	Mode Operasi <i>Counter (CTR)</i>	22
2.3	<i>Block Rail-fence Cipher</i>	24
2.4	RAES	26
2.5	Python	27
BAB III METODE PENELITIAN		28
3.1	Identifikasi Masalah	28
3.2	Model Dasar	28
3.3	Pengembangan Model Dasar	28
3.4	Konstruksi Program Aplikasi	30
3.4.1	Masukan dan Keluaran	30
3.4.2	Algoritma Deskriptif	31
3.4.3	Rancangan Tampilan	31
3.4.4	Library	31
3.5	Proses Validasi	32
3.6	Penarikan Kesimpulan	32
BAB IV HASIL DAN PEMBAHASAN		33
4.1	Skema Kriptografi Gambar Menggunakan Mode Operasi Counter RAES yang Dimodifikasi	33
4.2	Algoritma Program Aplikasi Kriptografi Gambar Menggunakan Mode Operasi Counter RAES yang Dimodifikasi	37
4.2.1	Pseudocode Algoritma Enkripsi Rail-fence Cipher yang Telah Dioptimalkan	38
4.2.2	Pseudocode Algoritma KEYEXPANSION()	38
4.2.3	Pseudocode Algoritma Enkripsi RAES yang Dimodifikasi	40
4.2.4	Pseudocode Algoritma Pembangkitan Counter	43
4.2.5	Pseudocode Algoritma Enkripsi dan Dekripsi Gambar RGB Menggunakan Mode Operasi Counter RAES yang Dimodifikasi	44
4.3	Program Aplikasi Kriptografi Gambar Menggunakan Mode Operasi Counter RAES yang Dimodifikasi	46
4.4	Validasi	48
BAB V KESIMPULAN DAN SARAN		53

5.1	Kesimpulan	53
5.2	Saran.....	53
	DAFTAR PUSTAKA.....	55
	LAMPIRAN.....	58

DAFTAR GAMBAR

Gambar 2.1 Gambar RGB 8-bit berukuran 2×2 piksel	10
Gambar 2.2 Contoh <i>stream cipher</i> pada <i>plaintext</i> berupa teks	11
Gambar 2.3 Contoh <i>block cipher</i> pada <i>plaintext</i> berupa teks	12
Gambar 2.4 Enkripsi dan Dekripsi AES	13
Gambar 2.5 Larik <i>state input</i> dan <i>output</i> (NIST, 2023)	15
Gambar 2.6 Ilustrasi SUBBYTES() pada <i>state</i>	18
Gambar 2.7 Ilustrasi SHIFTRROWS() pada <i>state</i>	19
Gambar 2.8 Ilustrasi MIXCOLUMNS() pada <i>state</i>	19
Gambar 2.9 Ilustrasi ADDROUNDKEY() pada <i>state</i>	21
Gambar 2.10 Mode operasi <i>Counter</i>	22
Gambar 2.11 Ilustrasi enkripsi <i>block rail-fence cipher</i>	26
Gambar 2.12 Enkripsi dan Dekripsi RAES	26
Gambar 3.1 Enkripsi dan Dekripsi Gambar dengan RAES-CTR.....	29
Gambar 3.2 Enkripsi dan Dekripsi dengan RAES-CTR.....	29
Gambar 3.3 Modifikasi enkripsi <i>rail-fence cipher</i> pada RAES	30
Gambar 3.4 Rancangan Tampilan Program Aplikasi.....	31
Gambar 4.1 Skema enkripsi mode operasi <i>counter</i> RAES yang dimodifikasi	33
Gambar 4.2 Struktur berkas Program Aplikasi Kriptografi Gambar Menggunakan Mode Operasi <i>Counter</i> RAES yang Dimodifikasi.....	46
Gambar 4.3 Halaman utama program aplikasi Kriptografi Gambar Menggunakan Mode Operasi <i>Counter</i> RAES yang Dimodifikasi.....	46
Gambar 4.4 Halaman Tentang program aplikasi Kriptografi Gambar Menggunakan Mode Operasi <i>Counter</i> RAES yang Dimodifikasi.....	48
Gambar 4.5 <i>Plain image</i> RGB berukuran 251×251 piksel dengan latar berwarna sama (Sumber: Unsplash)	49
Gambar 4.6 Hasil enkripsi Gambar 4.7 dengan RAES-CTR-128	49
Gambar 4.7 Hasil enkripsi Gambar 4.7 dengan RAES-CTR-192	49
Gambar 4.8 Hasil enkripsi Gambar 4.7 dengan RAES-CTR-256	49
Gambar 4.9 Hasil dekripsi Gambar 4.6 dengan RAES-CTR-128	49
Gambar 4.10 Hasil dekripsi Gambar 4.7 dengan RAES-CTR-192	49
Gambar 4.11 Hasil dekripsi Gambar 4.8 dengan RAES-CTR-256.....	49

Gambar 4.12 <i>Plain image</i> dan <i>cipher image</i> hasil enkripsi seadanya menggunakan AES-128 tanpa mode operasi seperti mode operasi <i>Counter</i>	50
Gambar 4.13 Gambar RGB berukuran 256×256 piksel dengan latar tidak berwarna sama (Sumber: Unsplash).....	50
Gambar 4.14 Hasil enkripsi Gambar 4.14 dengan RAES-CTR-128	51
Gambar 4.15 Hasil enkripsi Gambar 4.14 dengan RAES-CTR-192	51
Gambar 4.16 Hasil enkripsi Gambar 4.14 dengan RAES-CTR-256	51
Gambar 4.17 Hasil dekripsi Gambar 4.15 dengan RAES-CTR-128	51
Gambar 4.18 Hasil dekripsi Gambar 4.16 dengan RAES-CTR-192	51
Gambar 4.19 Hasil dekripsi Gambar 4.17 dengan RAES-CTR-256	51

DAFTAR TABEL

Tabel 2.1 Nilai Kunci, Blok, dan Round	15
Tabel 2.2 Nilai Rconj dalam heksadesimal	16
Tabel 2.3 Tabel SBOX(): nilai substitusi untuk byte XY (dalam heksadesimal)	18
Tabel 4.1 Tabel Substitusi SGF(): nilai substitusi untuk byte XY (dalam heksadesimal)	35
Tabel 4.2 Tabel Substitusi SKEYRF(): nilai substitusi untuk byte XY (dalam heksadesimal).....	36

DAFTAR LAMPIRAN

Lampiran 1. Kode Python Enkripsi Rail-fence Cipher Yang Telah Dioptimalkan	58
Lampiran 2. Kode Python KEYEXPANSION() dan Enkripsi RAES yang Dimodifikasi.....	58
Lampiran 3. Kode Python Pembangkitan <i>Counter</i>	61
Lampiran 4. Kode Python Enkripsi dan Dekripsi Gambar RGB Menggunakan Mode Operasi <i>Counter</i> RAES yang Dimodifikasi.....	62
Lampiran 5. Tabel $GF(2^8)$ dengan Polinomial <i>Irreducible</i> $m(x) = x^8 + x^4 + x^3 + x + 1$ dan $GF(2^8)$ dengan Polinomial <i>Irreducible</i> $m^*(x) = x^8 + x^7 + x^5 + x^4 + 1$ Menggunakan <i>Library</i> Galois 0.3.8 dalam Representasi Polinomial <i>Generator</i> , Polinomial, dan Desimal	64

DAFTAR PUSTAKA

- Blazhevski, D. dkk. (2013). "Modes of operation of the AES algorithm". Dalam I. Mishovski & S. Ristov (Penyunting), *The 10th Conference for Informatics and Information Technology (CIIT 2013)* (hlm. 212-216). Skopje: Faculty of Computer Science and Engineering Ss Cyril and Methodius University. Diakses dari <https://ciit.finki.ukim.mk/data/papers/10CiIT/10CiIT-46.pdf>.
- CNN Indonesia. (2022, 14 September). "102 Juta Data KTP Bocor di Forum Hacker, Diduga dari Kemensos". *CNN Indonesia*. Diakses dari <https://www.cnnindonesia.com/teknologi/20220914130145-192-847677/102-juta-data-ktp-bocor-di-forum-hacker-diduga-dari-kemensos>.
- Dworkin, M. (2001). NIST SP 800-38a 2001 edition, recommendation for block cipher modes of operation: methods and techniques. *NIST Special Publication, 800, 38A*. doi: <https://doi.org/10.6028/NIST.SP.800-38A>.
- Gao, H., & Wang, X. (2021). Chaotic image encryption algorithm based on zigzag transform with bidirectional crossover from random position. *IEEE Access, 9*, 105627-105640. doi: <https://doi.org/10.1109/ACCESS.2021.3099214>.
- Godara, S., Kundu, S., & Kaler, R. (2018). An Improved Algorithmic Implementation of Rail Fence Cipher. *International Journal of Future Generation Communication and Networking, 11(2)*, 23-32. doi: <http://dx.doi.org/10.14257/ijfgcn.2018.11.2.03>.
- Gonzalez, R. C. & Woods, R. E. (2018). *Digital Image Processing, Global Edition, Fourth Edition*. Harlow: Pearson Education. Diakses dari <https://www.pearson.com/en-gb/subject-catalog/p/digital-image-processing-global-edition/P200000004313/9781292223070>.
- Graham, R. D. (2019). *ECB Penguin Demonstration*. [Daring]. Diakses dari <https://github.com/robertdavidgraham/ecb-penguin>.
- Hassan, M. U. dkk. (2023). A Novel RGB Image Obfuscation Technique Using Dynamically Generated All Order-4 Magic Squares. *IEEE Access, 11*, 46382-46398. doi: <https://doi.org/10.1109/ACCESS.2023.3275019>.
- Herstein, I. R. (1999). *Abstract Algebra, Third Edition*. New York: John Wiley & Sons. Diakses dari <https://www.wiley.com/en-ca/Abstract+Algebra,+3rd+Edition-p-9780471368793>.

- Huffman, W. C. & Pless, V. (2003). *Fundamentals of Error-Correcting Codes*. Cambridge: Cambridge University Press. Diakses dari <https://www.cambridge.org/core/books/fundamentals-of-errorcorrecting-codes/BF3AFDFB539C3C023BBD9DCBA4CDA761>.
- Kahate, A. (2013). *Cryptography and Network Security Third Edition*. New Delhi: McGraw Hill Education. Diakses dari <https://www.vitalsource.com/products/cryptography-and-network-security-atul-kahate-v9789332900929>.
- Kamal, S. T. dkk. (2021). A new image encryption algorithm for grey and color medical images. *IEEE Access*, 9, 37855-37865. doi: <https://doi.org/10.1109/ACCESS.2021.3063237>.
- Kneusel, R. T. (2017). *Numbers and Computers*. Switzerland: Springer. Diakses dari <https://link.springer.com/book/10.1007/978-3-319-50508-4>.
- Matthes, E. (2023). *Python Crash Course, 3rd Edition*. San Francisco: No Starch Press. Diakses dari <https://nostarch.com/python-crash-course-3rd-edition>.
- Nahar, K. & Chakraborty, C. (2020). Improved Approach of Rail Fence for Enhancing Security. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 9(9), 583-585. doi: <http://doi.org/10.35940/ijitee.I7637.079920>.
- NIST. (2023). Federal information processing standards publication (FIPS) 197 advanced encryption standard (AES). doi: <https://doi.org/10.6028/NIST.FIPS.197-upd1>.
- Pless, V. (1998). *Introduction to the theory of error-correcting codes*, third edition. John Wiley & Sons. doi: <https://doi.org/10.1002/9781118032749>.
- Rosen, K. H. (2010). *Elementary number theory and its applications, 6th edition*. Boston: Pearson. Diakses dari <https://www.pearson.com/en-us/subject-catalog/p/elementary-number-theory/P200000006332/9780134310053>.
- Rosen, K. H. (2019). *Discrete Mathematics and Its Applications, Eighth Edition*. New York: McGraw-Hill Education. Diakses dari <https://www.mheducation.com/highered/product/discrete-mathematics-applications-rosen/M9781259676512.html>.

- Schneier, B. (1995). *Applied cryptography: protocols, algorithms, and source code in C, second edition*. New York: John Wiley & Sons. Diakses dari <https://www.wiley.com/en-us/Applied+Cryptography%3A+Protocols%2C+Algorithms%2C+and+Source+Code+in+C%2C+2nd+Edition-p-9781119183471>.
- Shah, T., Haq, T. U., & Farooq, G. (2020). Improved SERPENT algorithm: design to RGB image encryption implementation. *IEEE Access*, 8, 52609-52621. doi: <https://doi.org/10.1109/ACCESS.2020.2978083>.
- Shaker, H. dkk. (2022). A Hybrid Approach for a Secured Information Security Using Modified Encryption Technique. *International Journal for Multidisciplinary Research (IJFMR)*, 4(6). doi: <https://doi.org/10.36948/ijfmr.2022.v04i06.1124>.
- Stallings, W. (2023). *Cryptography And Network Security Principles and Practice Eighth Edition Global Edition*. Harlow: Pearson. Diakses dari <https://www.pearson.com/en-gb/subject-catalog/p/cryptography-and-network-security-principles-and-practice-global-edition/P200000007245/9781292437477>.
- Stinson, D. R. & Paterson, M. B. (2018). *Cryptography Theory and Practice Fourth Edition*. Boca Raton: CRC Press. Diakses dari <https://www.routledge.com/Cryptography-Theory-and-Practice/Stinson-Paterson/p/book/9781032476049>.