

**PENGGABUNGAN KRIPTOGRAFI *SHAMIR SECRET SHARING* DAN
STEGANOGRAFI CITRA RGB *LEAST SIGNIFICANT BIT*
DENGAN *QR CODE***

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar
Sarjana Matematika



Oleh:

Dwi Putri Pebriani

2004317

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

PENGGABUNGAN KRIPTOGRAFI *SHAMIR SECRET SHARING* DAN STEGANOGRAFI CITRA RGB *LEAST SIGNIFICANT BIT* DENGAN *QR CODE*

Oleh
Dwi Putri Pebriani

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

© Dwi Putri Pebriani 2024
Universitas Pendidikan Indonesia
Juli 2024

Hak Cipta dilindungi undang-undang.
Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,
dengan dicetak ulang, difoto kopi, atau cara lainnya tanpa ijin dari penulis.

LEMBAR PENGESAHAN

DWI PUTRI PEBRIANI

PENGGABUNGAN KRIPTOGRAFI *SHAMIR SECRET SHARING* DAN
STEGANOGRAFI CITRA RGB *LEAST SIGNIFICANT BIT* DENGAN *QR CODE*

Disetujui dan disahkan,
Pembimbing I



Dra. Hj. Rini Marwati, M.S.

NIP. 196606251990012001

Pembimbing II



Hj. Dewi Rachmatin, S.Si., M.Si.

NIP. 196909291994122001

Mengetahui,
Ketua Program Studi Matematika



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

NIP. 198207282005012001

ABSTRAK

Keamanan informasi sangat penting di era teknologi yang terus berkembang. Penggabungan teknik kriptografi dan steganografi bertujuan untuk meningkatkan keamanan informasi pada aspek kerahasiaan. Pada penelitian ini dikaji tentang penggabungan kriptografi *Shamir Secret Sharing* (SSS) dan steganografi *Least Significant Bit* (LSB). LSB menggunakan *Pseudo Random Number Generator* (PRNG) untuk membangkitkan bilangan acak sebagai penentu tempat penyisipan bit pesan ke dalam bit *cover object*. Dalam implelementasi penggabungan tersebut, dihasilkan program aplikasi menggunakan Python 3.11.2 dengan Skema (t,w) di mana $2 \leq t \leq w \leq 10$ dan citra RGB sebagai *cover object*. Program dapat melakukan konstruksi *share* maupun rekonstruksi *secret* (pesan). Pesan rahasia yang dapat diproses tidak hanya berupa digit angka, melainkan dapat berupa kombinasi angka, huruf, dan simbol dengan ketentuan maksimal 8 karakter yang terdapat pada karakter ASCII 32 sampai 126. *Share* yang dibagikan kepada partisipan berupa *QR Code* yang merujuk kepada *stego image*. *Stego image* yang dihasilkan tidak terlihat berbeda dengan *cover image*, sehingga sulit untuk diketahui keberadaan informasi yang disisipkan.

Kata Kunci: Kriptografi, *Least Significant Bit*, PRNG, *QR Code*, *Shamir Secret Sharing*, Steganografi Citra.

ABSTRACT

Information security is very important in the era of evolving technology. Combining cryptography and steganography techniques aims to improve information security in the aspect of confidentiality. In this research, the combination of Shamir Secret Sharing (SSS) cryptography and Least Significant Bit (LSB) steganography is studied. LSB uses a Pseudo Random Number Generator (PRNG) to generate a random number to determine where to insert the message bits into the cover object bits. In the implementation of the combining, an application program using Python 3.11.2 with Scheme (t,w) where $2 \leq t \leq w \leq 10$ and RGB image as cover object is produced. The program can perform both share construction and secret (message) reconstruction. The secret message that can be processed is not only in the form of digit numbers, but can be a combination of numbers, letters, and symbols with a maximum of 8 characters contained in ASCII characters 32 to 126. Share that is shared with participants in the form of a QR Code that refers to the stego image. The resulting stego image does not look different from the cover image, making it difficult to know the existence of the inserted information.

Keywords: *Cryptography, Least Significant Bit, PRNG, QR Code, Shamir Secret Sharing, Steganography Image.*

DAFTAR ISI

LEMBAR HAK CIPTA	i
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
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian.....	4
1.4 Batasan Masalah.....	4
1.5 Manfaat Penelitian.....	4
BAB II LANDASAN TEORI	6
2.1 Teori Dasar Matematika.....	6
2.1.1 Keterbagian	6
2.1.2 Faktor Persekutuan Terbesar (FPB).....	6
2.1.3 Bilangan Prima.....	6
2.1.4 Relatif Prima	6
2.1.5 Kekongruenan	6
2.1.6 Bilangan Bulat Modulo n	7
2.1.7 Invers Modulo	7
2.1.8 Interpolasi Polinom	7
2.1.9 Polinom Lagrange	7
2.2 Kriptografi	8
2.2.1 Terminologi dalam Kriptografi.....	8

2.2.2	Kriptosistem	9
2.2.3	Tujuan Kriptografi	9
2.2.4	<i>Secret Sharing</i>	9
2.3	Steganografi.....	14
2.3.1	Terminologi dalam Steganografi.....	14
2.3.2	<i>Least Significant Bit (LSB)</i>	15
2.4	<i>QR Code</i>	16
2.5	Bit	16
2.6	<i>Pseudo Random Number Generator (PRNG)</i>	17
2.7	Citra Digital	19
2.8	<i>Peak Signal to Noise Ratio (PSNR)</i>	20
2.9	ASCII.....	22
2.10	Bahasa Pemrograman Python	23
BAB III METODE PENELITIAN.....		24
3.1	Identifikasi Masalah	24
3.2	Model Dasar	24
3.2.1	Skema <i>Shamir Secret Sharing</i>	24
3.2.2	Skema Steganografi <i>Least Significant Bit</i>	25
3.3	Pengembangan Model	26
3.4	Konstruksi Program Aplikasi	27
3.4.1	Algoritma Deskriptif	28
3.4.2	Desain Tampilan	28
3.4.3	<i>Library</i>	33
3.5	Proses Validasi	34
3.6	Pengambilan Kesimpulan.....	34
BAB IV HASIL DAN PEMBAHASAN		36
4.1	Skema Kriptografi <i>Shamir Secret Sharing</i> dan Steganografi Citra RGB <i>Least Significant Bit</i> dengan <i>QR Code</i>	36
4.2	Algoritma <i>Pseudocode</i> Kriptografi <i>Shamir Secret Sharing</i> dan Steganografi Citra RGB <i>Least Significant Bit</i> dengan <i>QR Code</i>	39

4.2.1	<i>Pseudocode</i> Algoritma Konstruksi <i>Share</i>	39
4.2.2	<i>Pseudocode</i> Algoritma Rekonstruksi <i>Secret</i>	45
4.3	Program Aplikasi Penggabungan Kriptografi <i>Shamir Secret Sharing</i> dan Steganografi Citra RGB <i>Least Significant Bit</i> dengan <i>QR Code</i>	49
4.4	Validasi Program Kriptografi <i>Shamir Secret Sharing</i> dan Steganografi Citra RGB <i>Least Significant Bit</i> dengan <i>QR Code</i>	56
BAB V KESIMPULAN DAN SARAN.....		72
5.1.	Kesimpulan.....	72
5.2.	Saran	73
DAFTAR PUSTAKA		74
LAMPIRAN		77

DAFTAR GAMBAR

Gambar 2.1 Contoh <i>QR Code</i>	16
Gambar 2.2 Contoh Jenis-Jenis Citra Digital.....	20
Gambar 2.3 Daftar Kode ASCII.....	22
Gambar 3.1 Skema (t, w)	25
Gambar 3.2 Skema Steganografi LSB	25
Gambar 3.3 Skema Pengembangan Model	27
Gambar 3.4 Desain Tampilan Utama Program	29
Gambar 3.5 Desain Tampilan Konstruksi <i>Share</i> (1).....	29
Gambar 3. 6 Desain Tampilan Konstruksi <i>Share</i> (2).....	30
Gambar 3.7 Desain Tampilan Konstruksi <i>Share</i> (3).....	31
Gambar 3.8 Desain Tampilan Konstruksi <i>Share</i> (4).....	31
Gambar 3.9 Desain Tampilan Rekonstruksi <i>Secret</i> (1).....	32
Gambar 3.10 Desain Tampilan Rekonstruksi <i>Secret</i> (2).....	32
Gambar 4.1 Skema Konstruksi <i>Share</i> pada Penggabungan SSS dan LSB dengan <i>QR Code</i>	36
Gambar 4.2 Skema Rekonstruksi <i>Secret</i> pada Penggabungan SSS dan LSB dengan <i>QR Code</i>	38
Gambar 4.3 Tampilan Menu Utama Program Aplikasi	49
Gambar 4.4 Tampilan Halaman Pertama Konstruksi <i>Share</i>	51
Gambar 4.5 Tampilan Halaman Kedua Konstruksi <i>Share</i>	51
Gambar 4.6 Tampilan Halaman Ketiga Konstruksi <i>Share</i>	52
Gambar 4.7 Jendela <i>File Explorer</i> Penyimpanan <i>Stego Image</i>	52
Gambar 4.8 Tampilan Halaman Terakhir Konstruksi <i>Share</i>	53
Gambar 4.9 Tampilan Halaman Pertama Rekonstruksi <i>Secret</i>	54
Gambar 4.10 Jendela <i>File Explorer</i> Membuka <i>QR Code</i>	55
Gambar 4.11 Tampilan Halaman Terakhir Rekonstruksi <i>Secret</i>	56
Gambar 4. 12 Proses <i>Sharing</i> Validasi Skema (3,5) pada Program (1).....	57
Gambar 4.13 Proses <i>Sharing</i> Validasi Skema (3,5) pada Program (2).....	58
Gambar 4.14 Proses <i>Sharing</i> Validasi Skema (2,2) pada Microsoft Excel	58

Gambar 4.15 <i>Cover Image</i>	59
Gambar 4.16 <i>Share Stego</i> Validasi Skema (2,2).....	59
Gambar 4.17 <i>Code</i> Python Program PSNR	59
Gambar 4.18 <i>File</i> Informasi.txt pada Validasi Skema (2,2)	60
Gambar 4.19 Rekonstruksi <i>Secret</i> Validasi Skema (2,2) pada Program (1)	61
Gambar 4.20 Rekonstruksi <i>Secret</i> Validasi Skema (2,2) pada Program (2).....	61
Gambar 4.21 Proses <i>Sharing</i> Validasi Skema (3,5) pada Program.....	62
Gambar 4.22 Proses <i>Sharing</i> Validasi Skema (3,5) pada Microsoft Excel	63
Gambar 4.23 <i>Share Stego</i> Validasi Skema (3,5).....	63
Gambar 4.24 <i>File</i> Informasi.txt pada Validasi Skema (3,5)	64
Gambar 4.25 Rekonstruksi <i>Secret</i> Validasi Skema (3,5) pada Program (1)	65
Gambar 4.26 Rekontruksi <i>Secret</i> Validasi Skema (3,5) pada Program (2)	65
Gambar 4.27 Proses <i>Sharing</i> Validasi Skema (10,10) pada Microsoft Excel	66
Gambar 4.28 Proses <i>Sharing</i> Validasi Skema (10,10) pada Program	67
Gambar 4.29 <i>Share Stego</i> Validasi Skema (10,10).....	68
Gambar 4.30 <i>File</i> Informasi.txt pada Validasi Skema (10,10)	69
Gambar 4.31 Rekonstruksi <i>Secret</i> Validasi Skema (10,10) pada Program (1).....	70
Gambar 4.32 Rekontruksi <i>Secret</i> Validasi Skema (10,10) pada Program (2)	70

DAFTAR TABEL

Tabel 2.1 Nilai n dan X_n untuk $m = 32, a = 17, b = 23$	18
Tabel 2.2 Nilai RGB pada Beberapa Warna	20
Tabel 2.3 Kriteria Kualitas Citra berdasarkan PSNR	21
Tabel 3.1 <i>Input</i> dan <i>Ouput</i> Rancangan Program.....	27
Tabel 4.1 Hasil PSNR dari <i>Share Stego</i> Validasi Skema (2,2)	60
Tabel 4.2 Hasil PSNR dari <i>Share Stego</i> Validasi Skema (3,5).....	64
Tabel 4.3 Hasil PSNR dari <i>Share Stego</i> Validasi Skema (10,10).....	69

DAFTAR PUSTAKA

- Andono, P. N., & Sutojo, T. (2018). *Pengolahan Citra Digital*. Yogyakarta: Penerbit ANDI. [Online]. Diakses dari <https://books.google.com/books?hl=id&lr=&id=zUJRDwAAQBAJ>.
- Az-Zahra, F., Marwati, R., & Sispiyati, R. (2023). Implementasi QR Code dengan Algoritma SHA-256 dan RSA yang Ditingkatkan untuk Autentikasi Dokumen Digital. *Jurnal EurekaMatika*, 12(1), 11-22. doi: <https://doi.org/10.17509/jem.v12i1.67161>
- Burton, David M. (2011). *Elementary Number Theory (7th Edition)*. McGraw-Hill. [Online]. Diakses dari https://undergraduatemaths.wordpress.com/wpcontent/uploads/2017/12/david_m_burton_elementary_number_theory_seventbook4you.pdf
- Crisman, K. D. (2024). *Number Theory: In Context and Interactive (6th Edition)*. Gordon College, Wenham: Independently Published. [Online]. Diakses dari <https://math.gordon.edu/ntic/ntic.pdf>
- Chuang, J. C., Hu, Y. C., & Ko, H. J. (2010). A Novel Secret Sharing Technique Using QR Code. *International Journal Of Image Processing*, 4(5), 468-475. [Online]. Diakses dari https://www.researchgate.net/publication/49603949_A_Novel_Secret_Sharing_Technique_Using_QR_Code.
- Daniel. (2017). *Konstruksi Skema Pembagian Data Rahasia Menggunakan Algoritma Karnin-Greene-Hellman dan Skema Shamir*. (Skripsi). Fakultas Matematika Dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta, Jakarta. [Online]. Diakses dari <http://repository.unj.ac.id/id/eprint/25268>.
- Djuwitaningrum, E. R., & Apriyani, M. (2017). Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit dan Algoritma Linear Congruential Generator. *JUITA: Jurnal Informatika*, 4(2), 79-85. doi: 10.30595/juita.v0i0.1333.
- Fahrizal, M., & Solichin, A. (2020). Pengamanan M-Commerce Menggunakan One Time Password Metode Pseudo Random Number Generator (PRNG). *Rabit:*

- Jurnal Teknologi dan Sistem Informasi Univrab*, 5(2), 108-116. doi: <https://doi.org/10.36341/rabit.v5i2.1363>.
- Febrianto, E. R., & Sarwoko, E. A. (2018). Kriptografi Citra Digital Menggunakan Algoritma Hill Cipher Dan Affine Cipher Berbasis Android. *Jurnal Masyarakat Informatika*, 10(2). doi: <https://doi.org/10.14710/jmasif.10.2.31495>.
- Humaira, A. F., Marwati, R., & Yulianti, K. (2023). Implementasi Kriptografi *Secret Sharing Scheme* dan Steganografi *Audio Least Significant Bit (LSB)*. *JMT (Jurnal Matematika Terapan)*, 5(1). <https://doi.org/10.21009/jmt.5.1.1>.
- Ispandi, I., Fauzi, A., & Sugiono, S. (2019). Steganografi Menggunakan Metode *Least Significant Bit* dan *Quick Response Code (QR-Code)*. *JURIKOM (Jurnal Riset Komputer)*, 6(5). doi: <http://dx.doi.org/10.30865/jurikom.v6i5.1205>.
- Kurniasih, F., Marwati, R., & Sispiyati, R. (2023). Penyisipan Pesan Rahasia pada Gambar dengan Menggunakan *Affine Cipher* dan *Least Significant Bit-2 (LSB-2)*. *JEM (Jurnal Eureka Matika)*, 11(2). doi: <https://doi.org/10.17509/jem.v11i2>.
- Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of Applied Cryptography*. CRC Press. [Online]. Diakses dari <https://books.google.co.id/books?hl=id&lr=&id=YyCyDwAAQBAJ>.
- 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. [Online]. Diakses dari <https://repository.upi.edu/34949/>.
- Muhamad, M. (2014). *Analisis Dan Implementasi Pembagian Rahasia Menggunakan Skema Ambang Shamir*. (Skripsi). Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor, Bogor. Diakses dari <https://repository.unugha.ac.id/363/1/26.pdf>.
- Munir. (2015). *Metode Numerik*. Bandung: Informatika. [Online]. Diakses dari <https://online.flipbuilder.com/unindrapustaka/kzlw/>

- Munir, Rinaldi. (2019). *Kriptografi*. Program Studi Informatika, Institut Teknologi Bandung. [Online]. Diakses dari [https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2018-2019/Pengantar-Kriptografi-\(2019\).pdf](https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2018-2019/Pengantar-Kriptografi-(2019).pdf)
- Munir, Rinaldi. (2020). *Bahan Kuliah Steganografi*. Program Studi Informatika, Institut Teknologi Bandung. [Online]. Diakses dari <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Steganografi-Bagian1-2020.pdf>
- Nugraha, M. P., & Munir, R. (2011). Pengembangan Aplikasi *QR Code Generator* dan *QR Code Reader* dari Data Berbentuk *Image*. *Konferensi Nasional Informatika*. [Online]. Diakses dari <https://informatika.stei.itb.ac.id/~rinaldi.munir/Penelitian/Makalah-KNIF-2011-05.pdf>
- Nurfitri, K., & Suyanto, M. (2017). Penilaian Kualitas Pemampatan Citra pada Aplikasi-Aplikasi *Instant Messenger*. *MULTITEK INDONESIA*, 10(2). doi: <http://dx.doi.org/10.24269/mtkind.v10i2.346>.
- Sadikin R. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: Penerbit ANDI. [Online]. Diakses dari: <https://elibrary.bsi.ac.id/readbook/205264/kriptografi-untuk-keamanan-jaringan>.
- Stinson, D R. & Maura B. P. (2018). *Cryptography: Theory and Practice 4th Edition*. Boca Raton: CRC Press of Taylor & Francis Group. [Online]. Diakses dari <https://www.ic.unicamp.br>.
- Ulfah, N. (2020). *Pengamanan Pesan Teks Dengan Kriptografi Advanced Encryption Standard (AES) dan Steganografi Least Significant Bit (LSB)*. Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung. [Online]. Diakses dari <http://repository.upi.edu/48423/>.
- Yusup, I. M., Carudin, C., & Purnamasari, I. (2020). Implementasi Algoritma Caesar Cipher dan Steganografi *Least Significant Bit* Untuk File Dokumen. *Jurnal Teknik Informatika dan Sistem Informasi*, 6(3). doi: <https://doi.org/10.28932/jutisi.v6i3.2817>