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

Universitas Pendidikan Indonesia
Juli 2024

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 impelementasi 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

DAFTAR GAMBAR

DAFTAR TABEL

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/10.1 7509/ 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_seventbook4y ou.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). Stegnografi 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

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/10.2 8932/jutisi.v6i3.2817