PENYISIPAN PESAN RAHASIA PADA GAMBAR DENGAN MENGGUNAKAN *AFFINE CIPHER* DAN *LEAST SIGNIFICANT BIT-2* (LSB-2)

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh
gelar Sarjana Matematika

Oleh:
Firda Kurniasih
1902724

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

2023

LEMBAR HAK CIPTA

PENYISIPAN PESAN RAHASIA PADA GAMBAR DENGAN MENGGUNAKAN *AFFINE CIPHER* DAN *LEAST SIGNIFICANT BIT-2* (LSB-2)

Disusun oleh:
Firda Kurniasih
NIM 1902724

Diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

LEMBAR PENGESAHAN

FIRDA KURNIASIH

PENYISIPAN PESAN RAHASIA PADA GAMBAR DENGAN MENGGUNAKAN *AFFINE CIPHER* DAN *LEAST SIGNIFICANT BIT-2* (LSB-2)

disetujui dan disahkan oleh pembimbing:

Pembimbing I

Dra. H. Rini Marwati, M.S.

NIP. 196606251990012001

Pembimbing II

Ririn Sispiyati, S.Si., M.Si.

NIP. 198106282005012001

Mengetahui

Ketua Program Studi Matematika

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

NIP. 198207282005012001

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul "Penyisipan Pesan Rahasia pada Gambar dengan Menggunakan *Affine Cipher* dan *Least Significant Bit-2* (LSB-2)" ini beserta seluruh isinya adalah benar-benar karya saya sendiri, kecuali kutipan-kutipan dari ringkasan yang semuanya telah saya jelaskan sumbernya. Apabila dikemudian hari ditemukan adanya pelanggaran, saya bersedia menanggung resiko atau sanksi yang dijatuhkan kepada saya.

Bandung, Agustus 2023

Yang membuat pernyataan,

Firda Kurniasih

NIM. 1902724

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji serta syukur penulis panjatkan kehadirat *Allah Subhanahu Wa Ta'ala* yang telah memberikan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Penyisipan Pesan Rahasia pada Gambar dengan Menggunakan *Affine Cipher* dan *Least Significant Bit-2* (LSB-2)". Skripsi ini diajukan untuk memenuhi salah satu syarat untuk memperoleh gelar Sarjana Matematika di Universitas Pendidikan Indonesia.

Pada kesempatan ini, penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan semangat dan motivasi dalam menyelesaikan skripsi ini. Skripsi ini harapannya dapat memberikan ilmu pengetahuan mengenai penelitian yang dilakukan oleh penulis. Penulis menyadari masih terdapat kekurangan dalam penulisan skripsi ini yang disebabkan oleh keterbatasan pengetahuan dan pengalaman yang dimiliki penulis. Oleh karena itu, penulis menerima saran dan kritik yang dapat membangun penelitian ini. Penulis berharap skripsi ini dapat bermanfaat untuk berbagai pihak, baik penulis sendiri maupun para pembaca.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Bandung, Agustus 2023

Penulis,

Firda Kurniasih

UCAPAN TERIMAKASIH

Penulis menyadari bahwa penulisan skripsi ini tidak luput dari bantuan, bimbingan, arahan, dukungan, motivasi dan doa dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan rasa hormat dan terimakasih kepada:

1. Ibu Dra. Hj. Rini Marwati, M.S. selaku dosen Pembimbing I yang telah bersedia memberikan bimbingan, kritik, saran, serta mengawasi kemajuan proses penyusunan skripsi ini.
2. Ibu Ririn Sispiyati, S.Si., M.Si. selaku dosen Pembimbing II yang juga telah memberikan arahan dan bimbingan dalam penulisan skripsi ini.
3. Ibu Dr. Kartika Yulianti, S.Pd., M.Si. selaku Ketua Program Studi Matematika, Universitas Pendidikan Indonesia.
4. Bapak Dr. H. Cece Kustiawan, M.Si. selaku dosen pembimbing akademik yang telah membina dan membantu penulis selama menjalani perkuliahan.
5. Seluruh dosen dan civitas akademika di lingkungan Program Studi Matematika, Universitas Pendidikan Indonesia.
6. Kedua orang tua saya Bapak Jiman A.Md. dan Ibu Wasilah yang senantiasa mendoakan, mencurahkan kasih sayang, perhatian, motivasi, nasihat serta dukungan baik secara moril maupun materil.
7. Kakak saya Langgeng Setyo Pambudi yang telah mendo'akan, mendukung dan memberikan bantuan untuk penulis agar segera menyelesaikan skripsi..
8. Kepada Iyan Sufiansyah S.Psi. sebagai *partner* yang selalu setia membersamai dalam suka dan duka, memberikan banyak dukungan, bantuan, do'a dan semangat kepada penulis.
9. Sahabat pena saya Salsa A. Oktariana dan Widya Catur Utami yang senantiasa menemani dan membantu dalam penyusunan skripsi.
10. Rekan-rekan KEMENPORA BEM REMA UPI 2021 khususnya Muhammad Adam Hawari, Anggia Lyana Julieta, Ilham Syahiidul Amiin, Nurul Zahra Zahirah,

Rahmah Qonitin, Rahmi Maitsa dan Ramadhan Gunawan yang telah memberikan dukungan, bantuan dan kebersamaan selama menjalani perkuliahan S1.

11. Teman-teman mahasiswa Matematika UPI 2019 yang berjuang bersama-sama penulis dan telah memberikan motivasi serta dukungannya.
12. Semua pihak lainnya yang telah membantu penulis dalam perkuliahan maupun dalam penyelesaian skripsi ini.

Penulis berharap semoga kebaikan yang diberikan kepada penulis dari berbagai pihak akan dibalas dan dilipat gandakan oleh *Allah Subhanahu Wa Ta'ala*.

ABSTRAK

Seiring dengan perkembangan teknologi, pesan atau infromasi yang bersifat rahasia semakin rentan diretas oleh pihak yang tidak berwenang Oleh karena itu, keamanan terhadap pesan perlu ditingkatkan. Penggabungan antara kriptografi dan steganografi adalah salah satu cara untuk meningkatkan keamanan pesan. Pada penelitian ini penulis mengkaji tentang penggabungan kriptografi *Affine Cipher* dan steganografi *Least Significant Bit-2* (LSB-2). Dalam penggabungan tersebut, dilakukan peningkatan keamanan dengan menyamarkan isi pesan terlebih dahulu menggunakan kriptografi *Affine Cipher* kemudian hasil penyamaran pesan tersebut disembuyikan pada sebuah gambar dengan menggunakan *Least Significant Bit-2*. *Least Significant Bit-2* merupakan modifikasi dari metode *Least Significant Bit* (LSB) yang umumnya digunakan untuk menyembunyikan pesan rahasia pada media lain. *Least Significant Bit-2* bekerja dengan konsep menukarkan bit ke 8-2 (bit ke 6) dari setiap elemen warna *pixel* gambar dengan bit pesan rahasia. *Least Significant Bit-2* yang digunakan merupakan *Least Significant Bit-2* secara acak. Bilangan acak yang dibangkitkan menggunakan *Pseudo Random Number Generator* (PRNG). Selain itu, hasil penelitian diimplementasikan menjadi suatu program aplikasi komputer menggunakan bahasa pemrograman Python versi 3.11.

Kata Kunci: kriptografi, *affine Cipher*, steganografi, LSB-2, keamanan pesan

ABSTRACT

Along with the development of technology, messages or information that are confidential are increasingly vulnerable to being hacked by unauthorized parties Therefore, the security of messages needs to be improved. The combination of cryptography and steganography is one way to increase message security. In this study, the author will examine the combination of Affine Cipher cryptography and Least Significant Bit-2 (LSB-2) steganography. In the merger, security is increased by disguising the contents of the message first using Affine Cipher cryptography then the results of the disguised message are hidden in an image using Least Significant Bit-2. Least Significant Bit-2 is a modification of the Least Significant Bit (LSB) method which is commonly used to hide secret messages on other media. Least Significant Bit-2 works by exchanging the 8-2 bits (6th bit) of each pixel color element of the image with a secret message bit. The Least Significant Bit-2 used is the Least Significant Bit-2 randomly. Random numbers generated using a Pseudo Random Number Generator (PRNG). In addition, the results of the research were implemented into a computer application program using Python programming language version 3.11.

Keywords: *cryptography, affine cipher, steganography, LSB-2, message security*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Anwar, N. (2018). Perancangan Steganografi Hidden Message Dengan Metode Least Significant Bit (LSB) Berbasis Matlab. *Jurnal Algoritma, Logika Dan Komputasi*, *1*(1). doi: http://dx.doi.org/10.30813/j-alu.v1i1.1107

Budi, D. A. (2021). Perancangan Sistem Login Pada Aplikasi Berbasis GUI Menggunakan QTDesigner Python. *Jurnal SIMADA (Sistem Informasi dan Manajemen Basis Data)*, *4*(2), 92-100.

Djoko, R. (2014). *Modifikasi Affine Cipher Menggunakan Fungsi Gamma dan Fungsi Hiperbolik*. (Thesis). Program Studi Teknik Informatika, Universitas Kristen Satya Wacana.

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

Enterprise, J. (2019). *Python untuk Programmer Pemula*. Jakarta: Elex Media Komputindo.

Fadlan, M., & Hadriansa, H. (2017). Rekayasa Aplikasi Kriptografi dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman dan Affine Cipher. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, 4(4), 268-274. doi: http://dx.doi.org/10.25126/jtiik.201744468

Fithri, D. L. (2016). Analisa Kriptografi Untuk Keamanan Dalam Manajemen Sistem Terdistribusi Perusahaan. *Jurnal Disprotek*, *7*(1). doi: https://doi.org/10.34001/jdpt.v7i1.357

Hafiz, A. (2019). Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB). *Jurnal Cendikia*, *17*(1), 194-198.

Hidayat, E. Y., & Hastuti, K. (2013). Analisis Steganografi Metode Least Significant Bit (LSB) dengan Penyisipan Sekuensial dan Acak Secara Kuantitatif dan Visual. *Techno. Com*, *12*(3), 157-167. doi:

https://doi.org/10.33633/tc.v12i3.797

Humaira, A. F., Marwati, R., & Yulianti, K. (2023). Implementasi Kriptografi Secret Sharing Scheme dan Steganografi Audio Least Significant Bit (LSB). *JMT: Jurnal Matematika dan Terapan*, *5*(1), 1-11. doi: https://doi.org/10.21009/jmt.5.1.1

Irfan. (2013). Penyembunyian Informasi (*steganography*) Gambar Menggunakan Metode LSB (*Least Significant Bit*). *Rekayasa Teknologi*: *3*(1), 1-6.

Leleury, Z. A. (2022). *Teori Bilangan: Dilengkapi Pembahasan Soal-Soal Olimpiade Matematika*. Yogyakarta: CV. Bintang Semesta Media.

Marisman, A. F., & Hidayati, A. (2015). Pembangunan Aplikasi Pembanding Kriptografi Dengan Caesar Cipher dan Advance Encryption Standard (Aes) Untuk File Teks. *Jurnal Penelitian Komunikasi dan Opini Publik*, *19*(3). doi: https://doi.org/10.33299/jpkop.19.3.348

Maryanti, S., Rakhman, A. & Suroso. (2018). Perancangan Aplikasi Kerahasiaan Pesan dengan Algoritma Hill Cipher. *Prosiding Seniati*, *4*(2), 70-74. doi: https://doi.org/10.36040/seniati.v4i1.326

Munir, R. (2019). *Kriptografi* (Edisi Kedua). Bandung: Informatika.

Munir, R. (2004). *Teori Bilangan (Number Theory)*. Departemen Teknik Informatika, Institut Teknologi Bandung.

Putri, A. E., Kartikadewi, A., & Rosyid, L. A. (2021). Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang. *Applied Information Systems and Management*, *3*(2), 69-78.

Riski, A., Purwantoro, H., & Kamsyakawuni, A. (2018). Penyembunyian Ciphertext Algoritma Gost pada Citra ke dalam Audio dengan Metode Least Significant Bit. *Jurnal Ilmiah Matematika dan Pendidikan Matematika*, *10*(2), 49-62. doi: https://doi.org/10.20884/1.jmp.2018.10.2.2844

Rosen, K. H. (1986). *Elementary Number Theory and lts Application*. Addison Wesley.

Ruing, M. (2020). Penerapan Kombinasi Algoritma Kriptografi (Caesar, Vigenere, Zig-Zag) dan Metode Steganografi LSB Untuk Mengamankan Pesan ke Dalam Citra Digital. (*Disertasi*). Universitas Teknologi Yogyakarta, Yogyakarta.

Soetarmono, A. N. (2012). Studi Mengenai Aplikasi Steganografi Camouflage. *Teknika, 1*(1), 55-65. doi: https://doi.org/10.34148/teknika.v1i1.7

Stinson, D. R. dan Paterson, M. B. (2018). *Cryptography Theory and Practice* (Edisi Keempat). Boca Raton : CRC Press, Taylor & Francis.

Tantoni, A., & Zaen, M. T. A. (2018). Implementasi Double Caesar Cipher Menggunakan Ascii. *Jurnal Informatika dan Rekayasa Elektronik, 1*(2), 24-32.

Triana, F. (2020). Implementasi Caesar Cipher Cryptography dan Least Significant Bit-2 (LSB-2) Steganography Untuk Keamanan Data Berbasis Android. (*Skrips*i). Politeknik Negeri Sriwijaya, Palembang.

Togiana, E. (2018). Aplikasi Pembelajaran Algoritma Affine Cipher Dan Vigenere Cipher Menggunakan Metode Computer Assisted Instruction. *Media Informasi Analisa dan Sistem*, *3*(1), 42-48.

Ulva, A. F. (2019). Analisis Kinerja Kombinasi Algoritma Affine Cipher, Hill Cipher dan Algoritma El Gamal dalam Pengamanan Data. *Sisfo: Jurnal Ilmiah Sistem Informasi*, *3*(1), 65-66. doi: https://doi.org/10.29103/sisfo.v3i1.6306

Zebua, T. (2015). Penerapan Metode LSB-2 untuk Menyembunyikan Ciphertext pada Citra Digital. Pelita Informatika: Informasi dan Informatika, 10(3), 135-137.