IMPLEMENTASI KRIPTOGRAFI *ELLIPTIC CURVE CRYPTOGRAPHY* (ECC) DAN STEGANOGRAFI *SPREAD SPECTRUM* PADA PENGAMANAN PESAN KE DALAM GAMBAR

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar

Sarjana Matematika

Oleh**:**

Muhammad Daud

NIM: 1904812

PROGRAM STUDI MATEMATIKA

DEPARTEMEN PENDIDIKAN MATEMATIKA

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2023

IMPLEMENTASI KRIPTOGRAFI *ELLIPTIC CURVE CRYPTOGRAPHY* (ECC) DAN STEGANOGRAFI *SPREAD SPRECTRUM* PADA PENGAMANAN PESAN KE DALAM GAMBAR

Oleh:
Muhammad Daud
NIM 1904812

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Matematika pada

Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia

Agustus 2023

LEMBAR PENGESAHAN

MUHAMMAD DAUD

IMPLEMENTASI KRIPTOGRAFI *ELLIPTIC CURVE CRYPTOGRAPHY* (ECC) DAN STEGANOGRAFI *SPREAD SPRECTRUM* PADA PENGAMANAN PESAN KE DALAM GAMBAR

Disetujui dan disahkan oleh pembimbing:

Pembimbing I

Dra. Hj. Rini Marwati, M.Si.

NIP. 196606251990012001

Pembimbing II

Dr. Sumanang Muhtar Gozali, M.Si.

NIP. 197411242005011001

Mengetahui

Ketua Program Studi Matematika

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

NIP. 198207282005012001

SURAT PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul "Implementasi Kriptografi *Elliptic Curve Cryptography* (ECC) dan Steganografi *Spread Spectrum* pada Pengamanan Pesan ke dalam Gambar" 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, 29 Juli 2023

Yang membuat pernyataan,

Muhammad Daud

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT, karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan skripsi yang berjudul "Implementasi Kriptografi *Elliptic Curve Cryptography* (ECC) dan Steganografi *Spread Spectrum* pada Pengamanan Pesan ke dalam Gambar" sebagai salah satu syarat memperoleh gelar Sarjana Matematika di Universitas Pendidikan Indonesia (UPI).

Penulis menyadari bahwa masih terdapat kekurangan di penulisan skripsi ini. Oleh karena itu kritik dan saran yang membangun sangat diperlukan guna menyempurnakan dan mengembangkan skripsi ini. Penulis berharap skripsi ini dapat bermanfaat bagi pembaca, khususnya yang sedang mendalami kriptografi ECC dan steganografi *Spread Spectrum*.

Bandung, 29 Juli 2023

Penulis

UCAPAN TERIMAKASIH

Penulis menyadari bahwa selama penulisan skripsi terdapat pihak yang secara langsung maupun tidak langsung telah memberikan bantuan, doa, dan semangat. Oleh karena itu, penulis ingin menyampaikan terimakasih kepada:

1. Ibu Dra. Hj. Rini Marwati, M.Si. selaku dosen Pembimbing I yang telah mengajarkan penulis dengan penuh kesabaran mengenai topik yang penulis bahas dalam skripsi ini.
2. Bapak Dr. Sumanang Muhtar Gozali, M.Si. selaku dosen Pembimbing II yang telah memberikan arahan dan bimbingan dari awal hingga akhir penulisan skripsi ini.
3. Ibu Hj. Entit Puspita, S.Pd., M.Si. selaku dosen pembimbing akademik yang telah membina penulis selama menjalani perkuliahan di UPI.
4. Kedua orang tua yang telah mendoakan dan mendukung agar skripsi ini dapat diselesaikan tepat waktu.
5. Rekan-rekan mahasiswa Matematika UPI 2019 yang juga telah memberikan motivasi dan dukungannya, serta menemani penulis belajar selama masa perkuliahan.
6. Pihak lainnya yang tidak bisa disebutkan satu persatu yang telah membantu penulis dalam perkuliahan maupun penyelesaian skripsi ini.

Penulis

ABSTRAK

Kemajuan teknologi membuat seseorang menjadi lebih mudah untuk berkomunikasi. Namun seringkali pesan yang dikirim diretas oleh pihak yang tidak berhak. Oleh karena itu dibutuhkan suatu sistem keamanan yang dapat mencegah peretasan tersebut oleh pihak yang tidak berhak. Media komunikasi yang digunakan saat ini ada berbagai jenis, antara lain berbentuk *file* teks dan juga *file* gambar. Cara untuk mengamankan data antara lain dapat menggunakan kriptografi dan juga steganografi. Penelitian ini mengimplementasikan dan mengonstruksi program aplikasi untuk penyamaran pesan menggunakan kriptografi *Elliptic Curve Cryptography* (ECC) dan steganografi *Spread Spectrum*. Pesan yang telah dienkripsi menggunakan kriptografi ECC disembunyikan ke dalam gambar menggunakan steganografi *Spread Spectrum*. Program aplikasi kriptografi ECC dan steganografi Spread Spectrum pada pengamanan pesan ke dalam gambar akan dikonstruksi menggunakan bahasa pemrograman *Python*. Hasil penyisipan pesan yang telah dienkripsi ke dalam gambar tidak menimbulkan perubahan yang signifikan pada gambar sehingga pesan dapat disembunyikan dengan baik tanpa menimbulkan kecurigaan.

Kata Kunci: Kriptografi, *Elliptic Curve Cryptography*, Steganografi, *Spread Spectrum*

ABSTRACT

Advances in technology make it easier for people to communicating. But often the messages sent are hacked by unauthorized parties. Therefore, there is a need for a security system that can prevent the message from being hacked by unauthorized parties. There are various types of communication media used today, including text files and image files. Ways to secure data include cryptography and steganography. This research implements and constructs an application program to secure messages using Elliptic Curve Cryptography (ECC) and Spread Spectrum steganography. Messages that have been encrypted using ECC cryptography are hidden into images using Spread Spectrum steganography. The application program of ECC cryptography and Spread Spectrum steganography on securing messages into images will be constructed using the Python programming language. The results of inserting a message that has been encrypted into the image do not cause significant changes in the image so the message can be hidden properly without causing suspicion.

***Keywords**: Cryptography, Elliptic Curve Cryptography, Steganography, Spread Spectrum*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

Cahyani, A. D. (2022). Penyamaran Teks dengan Skema *Hybrid* Menggunakan Algoritma Enigma dan Algoritma Elgamal. Skripsi Sarjana. Universitas Pendidikan Indonesia.

Handoyo, A. E., dkk. (2018). Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA. Jurnal Teknologi dan Sistem Komputer, 6(1).

Herstein, I. N. (1975). *Topics in Algebra.* John Wiley and Sons Inc.

Hikmah, A. N. (2020). Penyandian Pesan dengan Menggunakan Kriptografi *Hybrid Autokey Vigenere Cipher* dan Algoritma *Elgamal*. Skripsi Sarjana. Universitas Pendidikan Indonesia.

Gunawan, I., & Sumarmo. (2018). Penggunaan Algoritma Kriptografi Steganografi *Least Significant Bit* Untuk Pengamanan Pesan Teks dan Data Video 64. Jurnal Sains Komputer & Informatika, Vol.2, No.1, Maret 2018.

Jaya, I. M. (2017). Implementasi Kriptografi Pengamanan Pesan Email Dengan Kombinasi Algoritma *Caesar Cipher* Dan *Vigenere Cipher*.

Munir, R. (2019). Kriptografi Edisi 2. Bandung: Institut Teknologi Bandung.

Naufal, M. F. (2021). Kriptografi Audio Menggunakan Transposisi dan *Affine Cipher* yang Dikembangkan dengan Algoritma *Blum Blum Shub*. Skripsi Sarjana. Universitas Pendidikan Indonesia.

Noercholis, A., & Nugraha, Y. (2016). Pengamanan Data Teks Menggunakan Teknik Steganografi *Spread Spectrum* Berbasis Android. Jurnal Antivirus, 10(1), 1 Mei 2016.

Pakereng, I. M. A. (2010). Perbandingan Steganografi Metode *Spread Spectrum* dan *Least* Sign*ificant Bit* (LSB) Antara Waktu Proses dan Ukuran File Gambar. Jurnal Informatika, Vol 6, No 2, 2010.

Putranto, A. (2009). Steganografi Melalui Media Gambar dengan Metode *Spread Spectrum*. Program Studi Teknik Informatika. Institut Teknologi Bandung.

Ridho, A. (2022). Implementasi Enkripsi *Vigenere Cipher* dan *Reverse Cipher* Menggunakan Bahasa Pemrograman *Python*. Jurnal Teknologi Informasi, Vol 1, No 1. Mei 2022.

Scheiner, B. (1996). *Applied Cryptography 2nd*. John Wiley and Sons.

Septayuda, A., Hidayat, B., & Nuha, H. H. (2014). Analisis Steganografi Citra Digital Menggunakan Metode *Spread Spectrum* Berbasis Android. E-Proceding of Engineering : Vol.1, No.1 Desember 2014.

Sinaga, M. (2020). Implementasi Steganografi Menggunakan Metode *Spread Spectrum* dalam Pengamanan Data Teks pada Citra Digital. Skripsi Sarjana. Universitas Islam Negeri Sumatera Utara.

Stinson, D. R. (2006). *Cryptography Theory and Practice 3rd Edition*. Chapman and Hall/CRC.

Vembrina, Y. G. (2006). Spread Spectrum Steganografi. Program Studi Teknik Informatika. Institut Teknologi Bandung.

Yusuf, R. N., Furqan, M., & Sinaga, M. S. (2020). Implementasi Steganografi Menggunakan Metode *Spread Spectrum* Dalam Pengamanan Data Teks Pada Citra Digital. Jurnal Sains Komputer & Informatika, Vol.4, No.2, September 2020.

Zahra, D. A. (2020). Kriptografi Visual pada Gambar Berwarna (RGB) Menggunakan Algoritma *Elliptic Curve Cryptography*. Skripsi Sarjana. Universitas Pendidikan Indonesia.