IMPLEMENTASI KRIPTOGRAFI CHACHA20 DAN STEGANOGRAFI HYBRID BERBASIS ADAPTIF LSB DAN PVD UNTUK KEAMANAN DATA PADA GAMBAR DIGITAL

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

MUHAMMAD ADITYA FEBRIANSYAH TANJUNG

21.83.0685

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

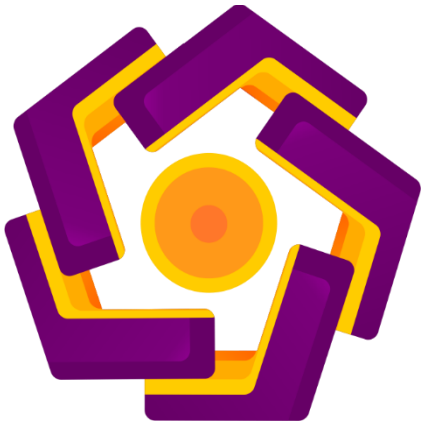
2025

IMPLEMENTASI KRIPTOGRAFI CHACHA20 DAN STEGANOGRAFI HYBRID BERBASIS ADAPTIF LSB DAN PVD UNTUK KEAMANAN DATA PADA GAMBAR DIGITAL

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



disusun oleh

MUHAMMAD ADITYA FEBRIANSYAH TANJUNG

21.83.0685

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

IMPLEMENTASI KRIPTOGRAFI CHACHA20 DAN STEGANOGRAFI HYBRID BERBASIS ADAPTIF LSB DAN PVD UNTUK KEAMANAN DATA PADA GAMBAR DIGITAL

yang disusun dan diajukan oleh

MUHAMMAD ADITYA FEBRIANSYAH TANJUNG

21.83.0685

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 28 Juli 2025

Dosen Pembimbing,

Dr. Dony Ariyus, S.S., M.Kom.
NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

IMPLEMENTASI KRIPTOGRAFI CHACHA20 DAN STEGANOGRAFI HYBRID BERBASIS ADAPTIF LSB DAN PVD UNTUK KEAMANAN DATA PADA GAMBAR DIGITAL

yang disusun dan diajukan oleh

MUHAMMAD ADITYA FEBRIANSYAH TANJUNG

21.83.0685

Telah dipertahankan di depan Dewan Penguji
pada tanggal 28 Juli 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Jeki Kuswanto, S.Kom., M.Kom. **NIK. 190302456**	
Rina Pramitasari, S.Si., M.Cs. **NIK. 190302335**	
Dr. Dony Ariyus, S.S., M.Kom. **NIK. 190302128**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 28 Juli 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : MUHAMMAD ADITYA FEBRIANSYAH TANJUNG
NIM : 21.83.0685

Menyatakan bahwa Skripsi dengan judul berikut:

IMPLEMENTASI KRIPTOGRAFI CHACHA20 DAN STEGANOGRAFI HYBRID BERBASIS ADAPTIF LSB DAN PVD UNTUK KEAMANAN DATA PADA GAMBAR DIGITAL

Dosen Pembimbing : Dr. Dony Ariyus, S.S., M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 28 Juli 2025

Yang Menyatakan,

Muhammad Aditya Febriansyah Tanjung

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur dan hormat, karya skripsi ini saya persembahkan kepada:

- Allah SWT, atas rahmat dan karunia-Nya yang tak terhingga.
- Kedua orang tua tercinta, yang selalu memberikan doa, kasih sayang, dan semangat tiada henti.
- Seluruh keluarga besar dan sahabat yang selalu memberikan semangat dan motivasi.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Implementasi Kriptografi ChaCha20 dan Steganografi Hybrid Adaptif LSB dan PVD pada Citra Digital" ini dengan baik.

Skripsi ini disusun untuk memenuhi salah satu syarat dalam memperoleh gelar Sarjana Komputer pada Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.

Penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

- Dr. Dony Ariyus, S.S., M.Kom., selaku dosen pembimbing, atas bimbingan dan arahannya selama proses penyusunan skripsi ini.
- Seluruh dosen dan staf di Fakultas Ilmu Komputer Universitas Amikom Yogyakarta atas ilmu dan bantuan yang telah diberikan.
- Orang tua tercinta yang selalu mendoakan dan mendukung penulis dengan penuh kasih sayang.
- Teman-teman seperjuangan yang turut memberikan semangat, bantuan, dan kebersamaan selama masa studi.

Semoga skripsi ini dapat memberikan manfaat bagi semua pihak yang membutuhkan. Penulis menyadari masih banyak kekurangan dalam penulisan ini. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan.

Yogyakarta, 06 Juli 2025

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG DAN SINGKATAN

PSNR	Peak Signal-to-Noise Ratio
LSB	Least Significant Bit
PVD	Pixel Value Differencing
GUI	Graphical User Interface
RGB	Red, Green, Blue (komponen warna pada citra digital)
AES	Advanced Encryption Standard
OPAP	Optimal Pixel Adjustment Process
LBP	Local Binary Pattern
MSB	Most Significant Bit
XOR	Exclusive-OR (operator logika pada kriptografi)
ARX	Add-Rotate-XOR (struktur pada ChaCha20)
QRF	Quarter Round Function (fungsi utama dalam ChaCha20)
CTR	Counter Mode (mode operasi kriptografi)
ECB	Electronic Code Book (mode operasi AES)
CBC	Cipher Block Chaining (mode operasi AES)
CFB	Cipher Feedback (mode operasi AES)
OFB	Output Feedback (mode operasi AES)
PNG	Portable Network Graphics (format citra)
BMP	Bitmap Image File (format citra)
SHA-256	Secure Hash Algorithm 256-bit
Nonce	Number used once (nilai acak dalam enkripsi stream)
RAM	Random Access Memory
IoT	Internet of Things
AES-NI	Advanced Encryption Standard - New Instructions
ASCII	American Standard Code for Information Interchange
MSE	Mean Square Error
PDF	Portable Document Format
zlib	Library Python untuk kompresi data
PIL	Python Imaging Library

cv2	OpenCV (Computer Vision Library)
NumPy	Numerical Python (library numerik)
bpp	Bits Per Pixel

DAFTAR ISTILAH

Ciphertext	Hasil dari proses enkripsi; data yang sudah disandikan dan tidak bisa dibaca tanpa dekripsi.
Plaintext	Data asli sebelum dienkripsi.
Keystream	Deretan bit acak semu yang dihasilkan oleh algoritma stream cipher untuk proses enkripsi dan dekripsi.
Nonce	Bilangan acak yang hanya digunakan satu kali dalam proses enkripsi untuk meningkatkan keamanan.
Least Significant Bit	Bit paling kanan dalam representasi biner; digunakan dalam steganografi untuk menyisipkan data karena pengaruhnya terhadap nilai piksel sangat kecil.
Most Significant Bit	Bit paling kiri dalam representasi biner; mengandung informasi terbesar dari suatu byte.
Adaptive LSB	Teknik steganografi LSB yang menyesuaikan jumlah bit yang disisipkan berdasarkan kompleksitas area gambar.
PVD (Pixel Value Differencing)	Metode steganografi yang menyisipkan data berdasarkan perbedaan nilai intensitas antara dua piksel bersebelahan.
PSNR (Peak Signal-to-Noise Ratio)	Ukuran kuantitatif untuk mengevaluasi kualitas visual citra hasil steganografi; semakin tinggi PSNR, semakin kecil distorsi.
Steganografi	Teknik menyembunyikan informasi di dalam media digital seperti gambar atau audio agar tidak terlihat secara kasat mata.
Kriptografi	Ilmu yang mempelajari metode pengamanan data melalui proses enkripsi dan dekripsi.
ChaCha20	Algoritma stream cipher yang digunakan untuk enkripsi, terkenal karena kecepatan dan keamanannya.

AES (Advanced Encryption Standard)	Algoritma block cipher yang banyak digunakan untuk enkripsi data secara aman.
ARX (Addition-Rotation-XOR)	Teknik enkripsi yang menggunakan penjumlahan modular, rotasi bit, dan operasi XOR untuk membentuk keystream.
Histogram RGB	Grafik distribusi intensitas warna merah, hijau, dan biru dalam citra digital.
OPAP (Optimal Pixel Adjustment Process)	Teknik optimasi dalam LSB untuk mengurangi distorsi citra setelah proses embedding.
LBP (Local Binary Pattern)	Metode dalam pengolahan citra untuk mendeskripsikan tekstur berdasarkan nilai biner lokal di sekitar piksel pusat.
Checksum SHA-256	Fungsi hash yang digunakan untuk menjamin integritas data; menghasilkan nilai unik dari data asli.
Little-endian	Format penyimpanan data biner di mana byte terkecil disimpan terlebih dahulu.
Payload	Data yang disisipkan ke dalam media (misalnya gambar) dalam proses steganografi.
Stego-image	Gambar hasil dari proses steganografi yang sudah berisi pesan tersembunyi.

INTISARI

Keamanan informasi digital, terutama dalam bentuk citra, semakin penting seiring meningkatnya serangan siber seperti penyadapan dan pembobolan data. Kombinasi antara kriptografi dan steganografi menjadi pendekatan efektif dalam melindungi data. Penelitian ini mengimplementasikan algoritma ChaCha20 sebagai metode kriptografi untuk mengenkripsi pesan, serta menggabungkannya dengan metode steganografi hybrid adaptif Least Significant Bit (LSB) dan Pixel Value Differencing (PVD) dalam menyisipkan pesan ke dalam citra digital. ChaCha20 dipilih karena efisiensinya dalam perangkat lunak dan ketahanannya terhadap serangan kriptografi, sementara metode hybrid LSB-PVD dipilih untuk menjaga kualitas visual citra dan meningkatkan kapasitas penyisipan data secara tersembunyi. Sistem ini diujikan pada citra berformat PNG atau BMP menggunakan aplikasi GUI berbasis Python, dengan hasil yang dievaluasi menggunakan PSNR dan histogram. Hasil pengujian menunjukkan bahwa metode ini mampu menyisipkan pesan secara aman tanpa penurunan kualitas visual yang signifikan, dengan nilai PSNR > 60 dB dan distribusi histogram yang stabil. Pendekatan ini tidak hanya menjaga kerahasiaan melalui enkripsi, tetapi juga menyembunyikan keberadaan pesan dengan efisien, sehingga cocok diterapkan dalam sistem keamanan komunikasi digital masa kini. Penelitian ini juga membuka peluang pengembangan lebih lanjut pada format lain.

Kata kunci: Kriptografi, ChaCha20, Steganografi, LSB Adaptif, PVD

ABSTRACT

The security of digital information, especially in the form of images, is increasingly important as cyberattacks such as eavesdropping and data breaches increase. The combination of cryptography and steganography is an effective approach in protecting data. This research implements the ChaCha20 algorithm as a cryptographic method to encrypt messages, and combines it with the Least Significant Bit (LSB) and Pixel Value Differencing (PVD) adaptive hybrid steganography methods to insert messages into digital images. ChaCha20 was chosen for its software efficiency and resistance to cryptographic attacks, while the hybrid LSB-PVD method was chosen to preserve the visual quality of the image and increase the hidden data insertion capacity. The system was tested on PNG and BMP format images using a Python-based GUI application, with results evaluated using PSNR and histograms. The test results show that the method is able to securely insert messages without significant degradation of visual quality, with PSNR values > 60 dB and stable histogram distribution. This approach not only maintains confidentiality through encryption, but also hides the presence of the message efficiently, making it suitable for implementation in today's digital communication security systems. This research also opens up opportunities for further development in other formats.

Keyword: *Cryptography, ChaCha20, Steganography, Adaptive LSB, PVD*