BAB I
PENDAHULUAN

1.1 Latar Belakang

Dorongan dalam inovasi data dan komunikasi yang canggih telah membuat banyak celah yang tidak terpakai, sekaligus menimbulkan bahaya yang belum pernah terjadi pada keamanan data. Dengan meluasnya transmisi informasi sensitif bahaya serangan siber, termasuk penyadapan, peretasan, pembobolan informasi, dan pelanggaran perlindungan, juga semakin meluas[1]. Dalam kondisi ini, keamanan informasi gambar digital menjadi sangat penting untuk menjaga privasi dan penilaian data. Strategi seperti kriptografi dan steganografi dengan cepat berkembang sebagai pengaturan yang berhasil untuk mengatasi bahaya ini[2].

Pendekatan yang menarik untuk mengamankan informasi adalah melalui kriptografi, yang dapat menjadi metode untuk mengamankan data dengan mengubahnya menjadi bentuk yang tidak jelas tanpa kunci tertentu. Salah satu perhitungan kriptografi yang digunakan secara luas saat ini adalah ChaCha20, sebuah stream cipher yang dikenal karena kecepatan dan keamanannya[3]. Dibandingkan dengan Advanced Encryption Standard (AES), ChaCha20 lebih efisien pada perangkat lunak, terutama di perangkat mobile dan IoT, sementara AES lebih optimal pada perangkat keras[4]. Sementara itu, jika dibandingkan dengan stream cipher lain seperti Salsa20, ChaCha20 menawarkan tingkat keamanan dan produktivitas yang lebih tinggi. Dengan putaran bit yang lebih kompleks, ChaCha20 memperbaiki kekurangan Salsa20[5].

Dalam konteks keamanan data, muncul teknologi baru bernama steganografi yang memungkinkan data disembunyikan atau disisipkan ke dalam file gambar digital [6]. Dalam hal ini, steganografi dapat digunakan untuk menyembunyikan data di dalam file gambar digital. Beberapa teknik seperti Adaptive Least Significant Bit (LSB) dan Pixel Value Differencing (PVD), ini umum digunakan dan disesuaikan dengan berbagai karakteristik gambar. Steganografi berbasis LSB adaptif merupakan penyisipan data berdasarkan

kombinasi yang bergantung pada intensitas warna masing-masing komponen R, G, dan B[7], [8]. Sedangkan metode Pixel Value Differencing menawarkan kapasitas penyimpanan pesan yang lebih besar dan kualitas gambar yang lebih baik dibandingkan dengan metode lain[6]. Pendekatan adaptif ini lebih efisien dan sulit dideteksi, mengatasi keterbatasan, seperti Kerentanan terhadap serangan atau deteksi [9].

Dengan menggabungkan enkripsi dan steganografi dapat meningkatkan keamanan data. Namun saat menggunakan cara ini, harus mempertimbangkan kualitas gambar dan ketahanan terhadap berbagai jenis serangan [10]. Pendekatan hybrid ini melindungi data melalui enkripsi sekaligus menyamarkan keberadaannya, sehingga sulit dideteksi oleh pihak yang tidak berkepentingan. Penelitian ini mengusulkan kombinasi enkripsi ChaCha20 dan steganografi hybrid berbasis adaptif LSB dan PVD untuk melindungi data sensitif yang tertanam dalam gambar digital. Pendekatan ini diharapkan dapat mengatasi tantangan kualitas gambar dan ketahanan terhadap serangan.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, permasalahan dirumuskan adalah Bagaimana mengukur efektivitas dan ketahanan gambar digital yang menggunakan enkripsi ChaCha20 dan metode steganografi hybrid Adaptive LSB dan PVD terhadap serangan atau deteksi?

1.3 Batasan Masalah

Penelitian ini difokuskan pada:

1. Implementasi algoritma kriptografi ChaCha20 untuk mengenkripsi data sebelum disisipkan ke dalam gambar.
2. Penggunaan metode steganografi hybrid berbasis Adaptive LSB dan PVD untuk penyisipan data yang telah dienkripsi.
3. Penelitian menggunakan 5 gambar yang berbeda dengan resolusi yang berbeda.
4. Penelitian menggunakan panjang pesan yang berbeda untuk penyisipan

pesan rahasia.

5. Pengujian sistem menggunakan gambar digital dalam format PNG dan BMP dan mengevaluasinya berdasarkan parameter kualitas gambar (PSNR), dan ketahanan terhadap serangan deteksi atau keamanan.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitiannya adalah mengukur efektivitas dan ketahanan gambar digital yang mengenkripsi data dengan ChaCha20 serta menyisipkan data menggunakan steganografi hybrid Adaptive LSB dan PVD terhadap serangan atau deteksi.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Menambah wawasan dalam pengembangan sistem keamanan data berbasis kombinasi kriptografi dan steganografi.
2. Menyediakan solusi untuk melindungi data sensitif dalam gambar digital, terutama untuk komunikasi dan penyimpanan yang aman.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN, perkembangan teknologi komunikasi dan data menimbulkan risiko keamanan yang tinggi, terutama pada informasi gambar digital, untuk menjaga privasi, kriptografi dan steganografi berkembang sebagai solusi. ChaCha20 adalah algoritma kriptografi yang cepat dan aman, lebih efisien di perangkat lunak dibanding AES dan lebih unggul dibanding Salsa20, steganografi memungkinkan penyembunyian data dalam gambar dengan teknik Adaptive LSB dan PVD yang menyesuaikan penyisipan berdasarkan karakteristik gambar, menawarkan kapasitas dan kualitas lebih baik serta sulit dideteksi, kombinasi enkripsi ChaCha20 dan steganografi hybrid Adaptive LSB-PVD diusulkan untuk melindungi data sensitif sekaligus menjaga kualitas gambar dan ketahanan terhadap serangan, rumusan masalah penelitian ini adalah bagaimana mengukur efektivitas dan ketahanan gambar digital yang menggunakan enkripsi ChaCha20 dan steganografi hybrid Adaptive LSB-PVD terhadap serangan atau

deteksi, penelitian difokuskan pada implementasi ChaCha20 untuk enkripsi data, metode steganografi hybrid Adaptive LSB dan PVD untuk penyisipan data terenkripsi, serta pengujian pada gambar PNG dan BMP dengan evaluasi kualitas gambar (PSNR) dan ketahanan keamanan, tujuan penelitian adalah mengukur efektivitas dan ketahanan gambar digital yang mengombinasikan enkripsi ChaCha20 dan steganografi hybrid Adaptive LSB-PVD terhadap serangan atau deteksi, manfaat penelitian diharapkan menambah wawasan dalam pengembangan keamanan data berbasis kriptografi dan steganografi, serta menyediakan solusi untuk melindungi data sensitif dalam komunikasi dan penyimpanan gambar digital.

BAB II TINJAUAN PUSTAKA, Perlindungan data digital saat pengiriman melalui jaringan terbuka menjadi semakin penting seiring dengan perkembangan teknologi dan meningkatnya ancaman keamanan. Kombinasi steganografi dan kriptografi telah menjadi metode populer untuk memberikan pengamanan berlapis, di mana steganografi berfungsi menyembunyikan data dalam media seperti gambar, sementara kriptografi mengenkripsi data agar tidak dapat dipahami oleh pihak yang tidak berwenang. Berbagai penelitian sebelumnya telah menggunakan algoritma enkripsi dan teknik steganografi yang beragam. Misalnya, algoritma Affine Cipher digabungkan dengan metode Pixel Value Differencing (PVD) untuk menyisipkan pesan dalam gambar, walaupun memiliki keterbatasan dalam kompleksitas enkripsi. Algoritma RC4+ dengan teknik Spread Spectrum juga digunakan untuk meningkatkan keamanan, namun kurang kuat jika dibandingkan dengan ChaCha20. Selain itu, kombinasi enkripsi ElGamal dan metode Least Significant Bit (LSB) berhasil menjaga kualitas gambar, meskipun rentan terhadap serangan. Metode lain menggunakan RSA dengan LSB yang efektif menjaga kualitas gambar, tetapi memiliki keterbatasan performa pada data berukuran besar. Sementara itu, enkripsi Vigenère cipher dengan LSB meningkatkan keamanan, namun tidak sekuat algoritma enkripsi modern. Penelitian juga menunjukkan penggunaan AES dengan LSB dapat melindungi pesan secara efektif, meskipun membutuhkan sumber daya komputasi yang lebih besar dan tidak memiliki mekanisme adaptif seperti PVD. Oleh karena itu, penelitian ini berfokus pada pengembangan metode yang mengatasi kelemahan dari pendekatan-pendekatan sebelumnya dengan

menggabungkan algoritma ChaCha20 yang lebih efisien dan aman, serta metode steganografi hybrid adaptif LSB-PVD untuk menyisipkan pesan ke dalam citra digital. Kombinasi ini diharapkan mampu memberikan tingkat keamanan yang lebih tinggi serta ketahanan terhadap berbagai jenis serangan, Citra digital merupakan representasi visual diskrit dari gambar, dibentuk oleh susunan piksel yang masing-masing memiliki intensitas warna tertentu. Piksel-piksel ini memiliki koordinat (x, y) dan nilai warna f(x, y) yang merepresentasikan warna spesifik. Format bitmap seperti .bmp, .jpg, dan .png adalah contoh format umum citra digital, dengan kualitas tergantung pada kerapatan piksel. Ketika diperbesar, citra bitmap dapat terlihat pecah karena keterbatasan resolusi. Dalam konteks keamanan informasi, citra digital digunakan sebagai media pembawa untuk menyisipkan data secara tersembunyi. Dengan mengubah data asli menjadi bentuk terenkripsi yang hanya dapat dipahami oleh pihak berwenang, kriptografi adalah alat penting untuk menjaga kerahasiaan data. ChaCha20, yang dikenal sebagai stream cipher, adalah salah satu algoritma kriptografi modern yang paling banyak digunakan. Dinilai lebih efisien dan ringan dibandingkan AES, terutama dalam penggunaan perangkat lunak. ChaCha20 juga unggul dalam ketahanannya terhadap serangan kriptografi, yang membuatnya pilihan yang baik untuk sistem keamanan data digital saat ini. ChaCha20, yang merupakan evolusi dari Salsa20, menggunakan prinsip ARX (Tambahan, Rotasi, XOR) untuk proses pembangkitan keystream. Salah satu fungsi utama algoritma ini adalah Fungsi Quarter Round, yang memproses blok 512-bit dalam dua puluh putaran enkripsi. Dengan desain yang memungkinkan akses acak dan komputasi paralel, ChaCha20 cocok untuk mengenkripsi data secara efisien dan aman. Saat enkripsi, keystream yang dihasilkan digunakan dengan plaintext dan saat dekripsi, dengan ciphertext. Steganografi, di sisi lain, adalah metode untuk menyembunyikan informasi dalam media seperti gambar, di mana informasi tidak dapat dilihat secara kasat mata. LSB (Least Significant Bit) dan PVD (Pixel Value Differencing) adalah dua teknik yang paling umum digunakan. LSB mengganti bit terakhir dari piksel untuk menyisipkan data, sedangkan PVD mengubah jumlah bit yang disisipkan berdasarkan perbedaan intensitas piksel. Kedua memiliki kapasitas dan ketahanan yang lebih baik terhadap deteksi. Metode LSB efektif dan mudah

digunakan karena hanya mengubah bagian yang paling kecil tanpa mengganggu kualitas visual. Misalnya, jika Anda ingin memasukkan huruf "A" ke dalam tiga piksel RGB, bit-bit terakhir dari warna merah, hijau, atau biru akan diubah. Namun, metode ini bersifat statis, menyisipkan jumlah bit yang sama ke setiap piksel tanpa memperhatikan konteks visual, sehingga rawan terhadap artefak dan analisis statistik jika terlalu banyak data dimasukkan. Metode LSB adaptif datang sebagai pengembangan untuk mengatasi kelemahan metode LSB konvensional. Metode ini menyisipkan bit yang didasarkan pada kompleksitas lokal piksel, seperti area tepi atau bertekstur tinggi yang lebih toleran terhadap perubahan. Dengan demikian, metode adaptif dapat menyisipkan lebih banyak bit pada area tertentu sambil mempertahankan kualitas visual. Untuk mengoptimalkan nilai piksel tanpa merusak data, berbagai metode telah dikembangkan, seperti representasi LBP dan OPAP. Dengan menggunakan perbedaan intensitas antara dua piksel berdekatan, teknik PVD memperkuat strategi penyisipan. Jumlah bit yang dapat disisipkan sebanding dengan perbedaan intensitas. PVD dapat digunakan secara selektif pada kanal warna Red, Green, atau Blue dengan pengaturan khusus agar perubahan warna tidak terdeteksi secara kasat mata saat diterapkan pada gambar berwarna. Kombinasi metode ini meningkatkan kapasitas penyimpanan sambil mempertahankan distribusi statistik gambar. Ada juga metode hybrid LSB-PVD, yang menggabungkan keunggulan LSB dan PVD. Metode hybrid ini menyisipkan data menggunakan LSB pada area dengan perbedaan piksel kecil dan PVD pada area dengan perbedaan piksel yang besar. Sistem adaptif seperti OPVD melakukan embedding berdasarkan arah perbedaan dan nilai selisih. Selain itu, proses ekstraksi tetap konsisten diawasi. Hasil eksperimen menunjukkan bahwa metode hybrid menawarkan kualitas visual dan kapasitas yang lebih besar daripada metode tunggal. Dalam skema multi-kanal pada gambar berwarna, metode hybrid LSB-PVD dapat diterapkan untuk aplikasi tambahan. Misalnya, kanal G digunakan untuk PVD yang lebih stabil secara visual, sementara kanal R dan B digunakan untuk LSB adaptif. Metode ini meningkatkan efisiensi penyisipan dan membuat pola penyisipan lebih tersebar dan tidak mudah diidentifikasi oleh metode deteksi seperti analisis histogram atau RS. Distribusi adaptif ini juga memperkuat

perlindungan data dalam berbagai skenario serangan steganografi. Terakhir, metrik seperti Peak Signal-to-Noise Ratio (PSNR) dan ketahanan terhadap deteksi digunakan untuk mengevaluasi efektivitas penyisipan data. PSNR tinggi menunjukkan bahwa perubahan visual yang disebabkan oleh penyisipan data sangat kecil dan sulit dideteksi oleh mata manusia. Sebaliknya, ketahanan terhadap deteksi mengukur seberapa baik sistem penyisipan dapat menghindari pengenalan melalui analisis statistik. Komunikasi rahasia yang aman dan tidak terdeteksi dapat dilakukan dengan kombinasi metode hybrid LSB-PVD untuk steganografi dan ChaCha20 sebagai enkripsi.

BAB III METODE PENELITIAN, Penelitian ini menggunakan gambar digital berformat PNG dan BMP sebagai objek karena kedua format tersebut menghasilkan kualitas gambar tinggi dan menyimpan data tanpa kompresi yang merusak, sehingga cocok untuk penyisipan pesan rahasia, dimana pesan tersebut dienkripsi menggunakan algoritma ChaCha20 guna menjamin kerahasiaannya, kemudian disisipkan ke dalam gambar dengan metode steganografi hybrid adaptif yang menggabungkan teknik Least Significant Bit (LSB) dan Pixel Value Differencing (PVD), analisis masalah difokuskan pada bagaimana mengamankan pesan secara efektif serta menjaga kualitas visual gambar stego setelah penyisipan, solusi yang ditawarkan adalah penerapan ChaCha20 untuk enkripsi cepat dan aman serta metode hybrid LSB-PVD untuk meningkatkan kapasitas penyisipan sekaligus mempertahankan kualitas gambar, rancangan sistem meliputi tahap pemilihan gambar dan pesan, enkripsi pesan, penyisipan pesan terenkripsi ke dalam gambar, dan pengujian kualitas serta keamanan gambar stego, tahapan pelaksanaan terdiri dari identifikasi dan perumusan masalah, studi literatur, perancangan dan implementasi sistem menggunakan Python dan library pendukung, serta pengujian dengan evaluasi PSNR dan uji ketahanan data melalui ekstraksi dan dekripsi pesan, perangkat yang digunakan adalah laptop dengan prosesor AMD Ryzen 7, RAM 16 GB, dan software Python dengan lingkungan pengembangan Visual Studio Code.

BAB IV HASIL DAN PEMBAHASAN, Penulis melakukan simulasi lengkap alur kerja aplikasi untuk memasukkan dan mengekstrak pesan rahasia dari gambar

digital pada tahap pengujian dan penerapan sistem. Melalui tombol "Pilih Gambar" di antarmuka aplikasi, pengguna memulai proses dengan memilih gambar sebagai media penampung, seperti sponge.png. Setelah gambar dimuat dan ditampilkan dalam area pratinjau berukuran 300 x 300 piksel, pengguna mengklik tombol "Sisipkan Pesan" dan memasukkan pesan rahasia, seperti "Rahasia 123" dan password enkripsi "kunciSandi". Algoritma ChaCha20 mengenkripsi pesan dengan nonce 12 byte, dan untuk menjamin integritas data, checksum SHA-256 ditambahkan. Metode Hybrid Adaptive LSB+PVD menambahkan payload yang terdiri dari nonce dan hasil enkripsi ke dalam citra. Metode ini menggunakan pasangan piksel adaptif untuk menyebarkan bit payload ke dalam ketiga kanal warna (R, G, dan B). Setelah proses embedding selesai, gambar stego ditampilkan di antarmuka dan disimpan otomatis dengan nama unik berdasarkan tanggal, seperti sponge_stego_20250531_143210.png. Sistem juga secara otomatis menghasilkan histogram kanal RGB dari gambar asli dan stego (original_hist_20250531_143210.png dan stego_hist_20250531_143210.png), menghitung nilai PSNR (misalnya 76,62 dB) sebagai pengukur kualitas visual, dan menghasilkan laporan. Untuk menguji proses ekstraksi, pengguna memuat kembali gambar stego yang telah dibuat sebelumnya. Kemudian, klik tombol "Ekstrak Pesan" dan masukkan kata sandi yang sama "kunciSandi". Fungsi hybrid_extract_rgb_balanced diaktifkan oleh sistem. Fungsi ini mengambil bit tersembunyi dari ketiga kanal warna berdasarkan perbedaan nilai antara pasangan piksel. Kemudian, ia menggabungkannya ke bytes_data. Empat byte pertama dihitung sebagai panjang payload, misalnya 32 byte. Kemudian sistem membedakan bagian nonce (12 byte) dan enkripsi data. Algoritma ChaCha20 kemudian menggunakan nonce dan kunci yang dibuat dari hash password untuk mendekripsi pesan. Setelah itu, verifikasi checksum SHA-256 dilakukan. Setelah validasi berhasil, hasil dekripsi didekompresi dengan zlib.decompress untuk mendapatkan kembali pesan asli, yang disebut sebagai "Rahasia 123", kepada pengguna.

BAB V PENUTUP, Berdasarkan evaluasi kuantitatif dan visual, metode steganografi hybrid Adaptive LSB–PVD yang digabungkan dengan enkripsi

ChaCha20 terbukti sangat efektif dalam menyembunyikan pesan pada kanal RGB citra digital tanpa menurunkan kualitas visual, dengan semua nilai PSNR di atas 60 dB jauh melampaui ambang 40 dB yang tak terlihat oleh mata manusia dengan nilai tertinggi 76,17 dB untuk 26 karakter pada citra 256×256 dan nilai terendah 63,33 dB untuk 237 karakter, serta pada citra beresolusi lebih tinggi (512×512 dan 1366×768) penyisipan hingga 446 karakter masih menghasilkan PSNR ≥ 68,79 dB yang menunjukkan skalabilitas metode, pertumbuhan ukuran file stego terutama disebabkan oleh format penyimpanan (PNG/BMP) bukan degradasi visual, dan distribusi histogram RGB yang stabil menegaskan bahwa data tersembunyi tidak menciptakan pola mencolok, sehingga pendekatan ini adaptif terhadap sensitivitas bit dan perbedaan intensitas piksel, mempertahankan kualitas tinggi, serta dapat diterapkan pada beragam resolusi dengan keamanan dan ketidakdeteksian yang baik, **saran pengembangan lebih lanjut** meliputi pengujian pada format gambar lain seperti grayscale, RGBA, atau JPEG untuk memahami pengaruh kompresi, penerapan algoritma kompresi lossless pasca-embedding guna mengendalikan pertumbuhan ukuran file, dan ekspansi metode ke media video dengan penyisipan data pada frame-frame tertentu guna memperbesar kapasitas dan memperkuat keamanan penyembunyian.