BAB I
PENDAHULUAN

A. Latar Belakang

Pertukaran informasi melalui aplikasi pesan instan telah menjadi tulang punggung komunikasi digital masyarakat modern di tahun 2026. Namun, seiring dengan ketergantungan yang tinggi terhadap platform *mobile*, ancaman terhadap privasi data pengguna juga meningkat secara signifikan. Berbagai kasus kebocoran data (*data breach*) yang melanda aplikasi pesan populer menunjukkan bahwa enkripsi standar yang disediakan penyedia layanan sering memiliki celah, terutama ketika data disimpan di server pihak ketiga atau saat terjadi intersepsi pada jalur komunikasi yang tidak aman. Salah satu temuan krusial menunjukkan bahwa jutaan data nomor ponsel pengguna WhatsApp terbukti sangat rentan diekstraksi secara masif melalui celah *contact discovery* [1]. Risiko ini diperburuk oleh insiden besar seperti kebocoran data Canva yang mengekspos informasi pribadi 139 juta pengguna, serta pembobolan tiket dukungan Discord pada tahun 2023 yang mengakibatkan seluruh isi percakapan dan lampiran sensitif milik pengguna terpapar ke pihak luar. Terungkap bahwa 11 dari 21 aplikasi pesan populer, termasuk platform besar seperti Telegram dan WeChat, secara tidak sadar membocorkan metadata sensitif ke layanan pihak ketiga [2]. Meskipun enkripsi telah menjadi standar, celah pada kebijakan privasi dan konfigurasi pihak ketiga tetap menjadi vektor utama kebocoran data di era *mobile* [3].

Di Indonesia, perlindungan terhadap kerahasiaan komunikasi telah dijamin secara hukum melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Kehadiran UU PDP menjadi instrumen penting untuk menstandardisasi keamanan komunikasi elektronik di Indonesia agar setara dengan standar internasional seperti GDPR. Namun, fakta di lapangan menunjukkan bahwa kebocoran pesan digital masih terus terjadi, yang seringkali berujung pada penyalahgunaan informasi sensitif, pemerasan, hingga pencurian identitas digital. Hal ini memicu kebutuhan akan sistem komunikasi mandiri yang memungkinkan pengguna untuk melindungi pesan mereka secara *end-to-end* dengan kendali kunci enkripsi sepenuhnya di tangan pengguna (*User-Controlled Encryption*) [4].

Dalam dunia kriptografi, algoritma *ChaCha20-Poly1305* menunjukkan latensi yang lebih rendah dan konsumsi daya CPU yang lebih kecil dibandingkan AES-GCM pada perangkat dengan sumber daya terbatas, menjadikannya ideal untuk komunikasi nirkabel modern. Pada perangkat *mobile* dengan spesifikasi beragam, penggunaan AES dapat mengonsumsi daya baterai yang signifikan dan rentan terhadap serangan *cache-timing* jika tidak diimplementasikan dengan sempurna. Kondisi ini membuat para peneliti mulai beralih pada algoritma yang lebih ramah terhadap arsitektur prosesor *mobile* (ARM), yaitu *ChaCha20* [5].

Algoritma *ChaCha20*, yang dipadukan dengan *Poly1305* sebagai *Message Authentication Code* (MAC), menawarkan tingkat keamanan yang setara dengan AES namun dengan efisiensi yang jauh lebih tinggi pada platform *mobile*. *ChaCha20-Poly1305* dirancang untuk menjadi algoritma *Authenticated Encryption with Associated Data* (AEAD) yang sangat cepat dan aman dari serangan berbasis waktu karena strukturnya yang sederhana namun kuat. Penggunaan *Poly1305* dalam sistem ini sangat krusial karena berfungsi sebagai segel digital yang memastikan bahwa pesan digital yang dikirimkan tidak mengalami modifikasi atau manipulasi sekecil apa pun oleh pihak ketiga selama proses transmisi. Kombinasi *ChaCha20-Poly1305* merupakan pilihan paling efisien untuk platform *mobile* berbasis ARM karena mampu menjaga integritas data tanpa mengorbankan performa komputasi atau meningkatkan suhu operasional perangkat dengan signifikan [6].

Selain aspek enkripsi, aspek ketersembunyian (*imperceptibility*) juga menjadi faktor penting dalam pertukaran informasi rahasia guna menghindari kecurigaan pihak luar. Penggunaan metode Steganografi *Least Significant Bit* (LSB) memungkinkan pesan yang telah dienkripsi oleh *ChaCha20-Poly1305* disisipkan ke dalam *bit* terendah piksel sebuah gambar tanpa merusak kualitas visualnya secara kasat mata. Hal ini diperkuat oleh penelitian terbaru yang menunjukkan bahwa penggabungan enkripsi terautentikasi *ChaCha20-Poly1305* dengan skema penyisipan LSB yang diacak mampu menciptakan perlindungan berlapis yang sangat efektif untuk data sensitif dengan beban komputasi yang tetap ringan. Keunggulan utama LSB terletak pada beban komputasinya yang ringan serta kemampuannya menjaga integritas citra sehingga keberadaan pesan digital

seolah-olah tidak pernah ada di dalam file tersebut. Integrasi ini memastikan bahwa jika terjadi intersepsi pada jalur komunikasi, pihak yang tidak berwenang tidak akan menyadari adanya data sensitif yang tersembunyi di balik *file* gambar yang terlihat normal [7].

Meskipun keunggulan *ChaCha20-Poly1305* sudah mulai diadopsi oleh protokol besar seperti TLS 1.3 dan VPN WireGuard, implementasinya pada aplikasi pesan digital berbasis *mobile* yang berdiri sendiri (*standalone*) masih tergolong minim. Sebagian besar penelitian sebelumnya masih terfokus pada pengamanan jalur data di tingkat jaringan (*network layer*), namun belum menyentuh tingkat aplikasi yang praktis dan mudah digunakan oleh masyarakat awam untuk melindungi pesan digital mereka secara langsung. Fokus utama penelitian saat ini masih berkisar pada batas keamanan *multi-user* dalam protokol seperti TLS 1.3, yang seringkali mengabaikan aspek kepraktisan implementasi pada antarmuka aplikasi pesan untuk pengguna umum [8].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengembangkan sebuah sistem pesan digital pada platform *mobile* yang mengimplementasikan algoritma *ChaCha20-Poly1305* dan steganografi LSB. Sistem ini dirancang untuk memberikan perlindungan ganda yaitu menjaga kerahasiaan isi pesan agar tidak dapat diintip dan menjamin integritas data agar pesan tidak dapat diubah. Dengan memanfaatkan *ChaCha20* dan steganografi LSB di perangkat *mobile*, diharapkan pengguna dapat berkomunikasi dengan tingkat keamanan tinggi tanpa mengorbankan performa perangkat, sekaligus memberikan solusi terhadap ancaman kebocoran data pesan yang marak terjadi saat ini.

B. Rumusan Masalah

Berdasarkan pemaparan latar belakang di atas, rumusan masalah dalam penelitian ini adalah, “Bagaimana efektivitas kombinasi algoritma *ChaCha20-Poly1305* dan metode Steganografi *Least Significant Bit* (LSB) dalam menjamin keamanan, integritas, serta ketersembunyian (*imperceptibility*) pesan digital pada aplikasi berbasis *mobile*?”

C. Batasan Penelitian

Agar penelitian lebih terarah dan fokus pada permasalahan utama, serta tidak keluar dari ruang lingkup yang telah ditetapkan, maka batasan penelitian ini adalah sebagai berikut:

1 Keamanan yang dibangun berfokus pada perangkat *mobile* berbasis Android, sehingga hasil penelitian ini tidak diuji pada platform lain seperti iOS, Windows, atau macOS.

2 Sistem ini berfokus pada mekanisme pengolahan pesan digital melalui proses enkripsi *ChaCha20-Poly1305* dan penyisipan steganografi LSB hingga menghasilkan citra penampung (*stego-image*), tanpa membahas infrastruktur pengiriman data (*networking*) atau arsitektur server pihak ketiga.

3 *Input* data yang diproses terbatas pada format teks (*plaintext*), tidak mencakup pengamanan data dalam bentuk *file* multimedia seperti gambar, audio, video, atau dokumen kompleks lainnya.

4 Manajemen kunci enkripsi bersifat mandiri, di mana *secret key* disimpan secara lokal melalui *Secure Storage* yang memanfaatkan mekanisme Android Keystore untuk mengurangi risiko kunci terbaca langsung dari penyimpanan aplikasi.

5 Kapasitas pesan digital yang dapat disisipkan dibatasi oleh dimensi citra penampung (*cover image*), dengan mekanisme rasio penyisipan maksimal sebesar 1 *bit* per komponen warna (RGB) pada setiap piksel untuk menjaga kualitas visual (*imperceptibility*) dan integritas data.

6 *Input* teks difokuskan pada karakter ASCII *standard printable* (sebanyak 95 karakter), yang mencakup huruf (A-Z, a-z), angka (0-9), dan simbol-simbol umum. Sistem tidak menjamin pemrosesan karakter di luar standar tersebut.

D. Tujuan Penelitian

Tujuan penelitian ini adalah untuk menganalisis efektivitas dengan menguji kombinasi algoritma *ChaCha20-Poly1305* dan metode Steganografi *Least Significant Bit* (LSB) dalam menjamin keamanan, integritas, serta ketersembunyian (*imperceptibility*) pesan digital pada aplikasi berbasis *mobile*.

E. Manfaat Penelitian

Manfaat yang dapat diperoleh dari penelitian ini, antara lain:

1. Bagi penulis, penelitian ini menjadi sarana untuk memperdalam pemahaman teknis mengenai implementasi dan efektivitas algoritma *stream cipher* modern *ChaCha20*, mekanisme *Message Authentication Code* (MAC) menggunakan *Poly1305* pada ekosistem *mobile,* dan steganografi LSB. Selain itu, penulis memperoleh pengalaman praktis dalam membangun sistem perlindungan data yang efisien untuk perangkat dengan sumber daya terbatas.
2. Bagi peneliti dan akademisi, penelitian ini diharapkan dapat memberikan kontribusi ilmiah dalam bidang keamanan siber (*cybersecurity*), khususnya mengenai penggunaan algoritma AEAD (*Authenticated Encryption with Associated Data*) sebagai alternatif yang lebih ringan dibandingkan standar AES pada platform *mobile*. Hasil pengujian performa dalam penelitian ini dapat dijadikan referensi atau basis data bagi peneliti selanjutnya yang ingin mengembangkan sistem proteksi data dengan tingkat efisiensi tinggi pada arsitektur ARM.
3. Bagi pembaca dan masyarakat umum, penelitian ini memberikan solusi aplikatif berupa wadah penyimpanan pesan yang aman (*secure vault*) untuk melindungi informasi sensitif secara mandiri. Dengan adanya sistem ini, masyarakat dapat memiliki kontrol penuh terhadap privasi komunikasi tanpa harus khawatir terhadap risiko kebocoran data yang sering terjadi pada server aplikasi pihak ketiga atau penyadapan di jaringan publik.