BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan pesat teknologi informasi dan komunikasi mendorong peningkatan aktivitas daring, termasuk transaksi keuangan, penyimpanan dokumen pribadi, dan pertukaran data sensitif, sehingga keamanan informasi menjadi krusial untuk mencegah penyalahgunaan. Di Indonesia, perlindungan data pribadi telah diatur melalui UU PDP dan penguatan hak atas perlindungan diri serta data pribadi sebagaimana termuat dalam Pasal 28G ayat (1). Meskipun regulasi tersebut telah berlaku sejak 2022, insiden kebocoran data pribadi masih terjadi, salah satunya kebocoran data pengguna Tokopedia yang dilaporkan mencapai 91.000.000 data pengguna [1], [2].

Salah satu bentuk media yang banyak digunakan untuk bertukar informasi saat ini adalah gambar digital (foto). Gambar tidak hanya berfungsi sebagai media visual, tetapi juga dapat dimanfaatkan untuk menyembunyikan pesan rahasia melalui teknik *steganografi*. *Steganografi* memungkinkan penyisipan data ke dalam media (misalnya citra) sedemikian rupa sehingga keberadaan pesan tersembunyi sulit terdeteksi oleh pihak luar. Salah satu teknik *steganografi* citra yang populer adalah *Least Significant Bit* (LSB), yaitu metode yang memodifikasi *bit* paling tidak signifikan pada *piksel* gambar untuk memuat pesan rahasia dengan perubahan visual yang minimal. Selain itu, keamanan sistem dapat diperkuat dengan penerapan autentikasi biometrik, karena penggunaan biometrik membuat proses pemalsuan atau manipulasi menjadi lebih sulit [3].

Namun demikian, penerapan steganografi saja tidak cukup untuk menjamin bahwa hanya penerima yang tepat yang dapat mengakses pesan tersebut. Pada situasi ketika penyalahgunaan data identitas sangat potensial misalnya penggunaan *selfie* bersama KTP tanpa izin diperlukan mekanisme autentikasi tambahan agar hanya penerima yang sah yang dapat membuka pesan, yaitu autentikasi biometrik. Penerapan autentikasi biometrik juga dapat mempercepat proses identifikasi dan konfirmasi identitas individu yang bersifat unik, universal, dan relatif permanen [4].

Penggabungan *steganografi* dengan autentikasi biometrik mulai mendapat perhatian sebagai cara untuk meningkatkan keamanan pada sistem komunikasi rahasia. Salah satu pendekatan yang dikaji adalah perlindungan citra sidik jari dengan cara menyisipkannya ke dalam media pembawa, sehingga data biometrik tidak mudah

diidentifikasi maupun diekstraksi secara langsung. Dengan adanya lapisan penyamaran tersebut, mekanisme perlindungan menjadi berlapis dan sejalan dengan konsep *defense-in-depth*, sehingga berpotensi memperkuat keamanan pada proses pengiriman maupun penyimpanan data biometrik yang bersifat sensitif. Pendekatan lain juga menunjukkan bahwa data biometrik dapat dienkripsi terlebih dahulu sebelum disisipkan ke dalam media sebagai lapisan keamanan tambahan. Namun dalam literatur yang ditinjau pada penelitian ini, tidak dijumpai aplikasi *steganografi* citra di platform mobile yang menyertakan autentikasi biometrik sidik jari sebagai syarat untuk membuka pesan [5], [6].

Seiring berkembangnya teknologi *steganografi* dan autentikasi biometrik, pesan tersembunyi tetap berisiko diekstraksi dan disalahgunakan apabila tidak dilindungi dengan pengelolaan kunci dan mekanisme enkripsi yang memadai. Sebagai contoh, penggunaan kunci simetris yang tidak ditangani secara aman dapat menyebabkan kegagalan perlindungan, karena kebocoran kunci akan membuka seluruh isi pesan rahasia. Selain itu, penerapan *AES-GCM* juga memiliki batasan penting, terutama terkait penggunaan *nonce* yang berulang serta pembatasan jumlah data atau pesan yang dapat dienkripsi dengan satu kunci; jika aspek ini tidak diantisipasi, dapat muncul celah serangan kriptografi [7].

Kombinasi autentikasi sidik jari dan enkripsi *AES-GCM* pada sistem layanan kritikal dilaporkan dapat meningkatkan integritas dan kerahasiaan data secara signifikan. Namun, penerapannya pada penelitian terdahulu masih berfokus pada skenario *e-voting* dan *watermarking*, sehingga belum secara spesifik membahas kebutuhan *steganografi* citra pada *platform mobile* yang memerlukan mekanisme distribusi kunci asimetris untuk pengelolaan kunci yang lebih aman [8].

Integrasi algoritma enkripsi simetris dan asimetris dalam skema *hybrid encryption* dapat menjadi solusi atas dua kebutuhan utama dalam komunikasi aman, yaitu efisiensi enkripsi untuk data berukuran besar dan keamanan distribusi kunci enkripsi. Pendekatan ini menunjukkan bahwa pesan dapat dienkripsi menggunakan algoritma simetris untuk menjaga performa, sementara kunci simetrisnya diamankan menggunakan algoritma asimetris agar proses pertukaran kunci lebih terlindungi. Berdasarkan hal tersebut, masih terdapat ruang pengembangan pada implementasi *steganografi* citra, khususnya untuk menambahkan lapisan keamanan pada *payload* yang disisipkan melalui penerapan *hybrid encryption* dengan algoritma kriptografi

modern seperti *AES-GCM* untuk enkripsi payload dan *RSA-OAEP* untuk pengamanan kunci sesi [9].

Dengan demikian, urgensi penelitian ini semakin tinggi: tidak hanya bagaimana menyembunyikan pesan, tetapi bagaimana memastikan bahwa pesan tersebut tetap terlindungi setelah disisipkan, dan hanya dapat diakses oleh penerima yang sah melalui autentikasi biometrik sidik jari. Penelitian ini berupaya mengisi gap tersebut dengan mengembangkan aplikasi *mobile* yang mengintegrasikan *steganografi LSB*, *hybrid encryption (AES-GCM + RSA-OAEP)*, dan autentikasi sidik jari, sehingga menawarkan kontribusi baru baik dari sisi teori maupun implementasi.

B. Rumusan Masalah

Berdasarkan pemaparan latar belakang di atas, rumusan masalah dalam penelitian ini adalah, " Bagaimana performa metode *hybrid encryption* (*RSA-OAEP* dan *AES-GCM*) serta penyisipan pesan menggunakan *Least Significant Bit* (*LSB*) dalam menjaga keamanan, kualitas citra, dan keberhasilan ekstraksi pesan pada aplikasi *steganografi* berbasis *mobile* dengan autentikasi biometrik sidik jari?"

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. Penelitian ini hanya membahas penerapan metode *Least Significant Bit (LSB)* pada steganografi citra untuk penyisipan pesan rahasia, tanpa melakukan perbandingan dengan metode steganografi lain.
2 Autentikasi biometrik yang digunakan dalam penelitian ini terbatas pada sidik jari *(fingerprint)* yang tersedia secara default di perangkat *mobile* berbasis *Android*, dan tidak mencakup jenis biometrik lain seperti wajah *(face recognition)* atau suara.
3 Setiap akun (*username)* hanya dapat digunakan pada satu perangkat (*device)*.
4 Penelitian ini berfokus pada aplikasi *mobile* berbasis *Android*, sehingga tidak mencakup implementasi pada platform lain seperti *IOS* atau *desktop.*
5 Jenis citra yang digunakan dalam penelitian ini terbatas pada citra digital berformat PNG. Format gambar lain seperti JPEG atau BMP tidak menjadi fokus penelitian.

6 Pengiriman *stego-image* tidak diatur oleh sistem dan dilakukan melalui media eksternal apa pun (misalnya *Whatsapp*, *Email*, atau platform lain). Mekanisme distribusi file tidak menjadi fokus pada penelitian ini.

7 Pesan yang disisipkan berupa teks rahasia sederhana *(plaintext),* tidak termasuk file kompleks seperti audio, video, atau dokumen.

8 Pesan yang dapat disisipkan maksimal 250 KB, menyesuaikan dengan kapasitas metode LSB pada citra PNG

9 Sistem tidak menyediakan mekanisme pemulihan akun (*account recovery)* atau pemindahan akun ke perangkat lain.

D. Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menganalisis dan mengevaluasi performa metode *hybrid encryption (RSA-OAEP* dan *AES-GCM)* serta penyisipan pesan menggunakan metode *Least Significant Bit (LSB)* pada aplikasi *steganografi* berbasis *mobile* dengan autentikasi biometrik sidik jari.

E. Manfaat Penelitian

Adapaun manfaat yang dapat diperoleh dari penelitian ini, antara lain:

1. Bagi penulis, penelitian ini memberikan pengalaman dan pemahaman mendalam mengenai implementasi *steganografi* citra menggunakan metode *LSB*, mekanisme *hybrid encryption* (*RSA-OAEP* dan *AES-GCM*), serta autentikasi biometrik sidik jari pada aplikasi *mobile*. Penelitian ini juga memberikan kesempatan untuk menguji keamanan, fungsionalitas, dan efektivitas integrasi ketiga teknik tersebut dalam satu sistem.
2. Bagi peneliti dan akademisi, penelitian ini memberikan kontribusi pada pengembangan bidang keamanan informasi, khususnya terkait penerapan *steganografi* yang dikombinasikan dengan teknik kriptografi modern dan autentikasi biometrik. Hasil penelitian ini dapat menjadi referensi bagi penelitian lanjutan terkait pengamanan data pada platform *mobile* maupun pengembangan metode *steganografi* yang lebih aman.

Bagi pembaca dan masyarakat umum, penelitian ini dapat meningkatkan kesadaran mengenai pentingnya perlindungan data pribadi dan keamanan pesan digital. Selain itu, penelitian ini memberikan solusi alternatif berbasis aplikasi *mobile*

yang dapat digunakan untuk menjaga kerahasiaan informasi melalui penyisipan pesan terenkripsi yang hanya dapat diakses oleh penerima yang sah.