ABSTRAK

MUHAMMAD NOVAL**.** Pengamanan pesan rahasia berbasis *mobile* menggunakan *Steganografi LSB, RSA-OAEP, AES-GCM,* dan Autentikasi Biometrik Sidik Jari. Dibimbing oleh Nurul Hayaty dan Rifaldi Herikson.

Pertukaran data sensitif melalui layanan daring meningkatkan risiko kebocoran, sementara gambar digital sering digunakan sebagai media berbagi sehingga berpotensi dimanfaatkan untuk penyisipan pesan. Penelitian ini mengembangkan aplikasi mobile *GoSnap* yang menerapkan *steganografi Least Significant Bit (LSB)* pada citra *PNG*, dengan *payload* terlebih dahulu diamankan menggunakan *hybrid encryption: AES-256-GCM* untuk mengenkripsi pesan dan *RSA-OAEP* untuk mengenkripsi kunci *AES*. Kunci privat *RSA* disimpan di *Android Keystore* dan akses dekripsi dibatasi melalui autentikasi biometrik sidik jari.

Evaluasi dilakukan melalui pengujian kualitas citra (*MSE/PSNR*), akurasi ekstraksi (*MAR*), analisis statistik (*entropy* dan korelasi), performa, serta uji keamanan (modifikasi *payload*, percobaan akses tidak sah, *cropping*, dan kompresi). Hasil menunjukkan *stego-image* tetap berkualitas tinggi (*PSNR* 89,540 *dB*; *MSE* 0,000072 pada resolusi 3000×3000) dan pesan dapat diekstraksi identik (*MAR* 100%). Sistem menolak modifikasi *payload* dan membatasi percobaan biometrik melalui mekanisme lockout, namun tidak tahan terhadap perubahan *lossy* atau *spasial* seperti *JPEG* dan *cropping* ≥10%. Temuan ini menegaskan efektivitas *defense-in-depth* pada pengiriman pesan rahasia berbasis citra selama *file* dipertahankan dalam format *PNG* tanpa pengeditan.

Kata kunci: *AES-GCM*, autentikasi biometrik, *LSB, RSA-OAEP, steganografi*.

ABSTRACT

MUHAMMAD NOVAL. *Securing mobile-based secret messages using LSB steganography, RSA-OAEP, AES-GCM, and fingerprint biometric authentication.* Supervised by Nurul Hayaty and Rifaldi Herikson.

Sharing sensitive information online increases the risk of interception, while digital images are widely exchanged and can be abused to hide messages. This research develops a mobile application, GoSnap, that embeds an encrypted payload into PNG images using Least Significant Bit (LSB) steganography. The payload is protected with hybrid encryption: AES-256-GCM encrypts the message and RSA-OAEP encrypts the AES session key. The RSA private key is stored in the Android Keystore and decryption is gated by fingerprint biometric authentication.

The system is evaluated using image quality metrics (MSE/PSNR), message extraction accuracy (MAR), statistical analysis (entropy and pixel correlation), performance, and security tests (payload modification, unauthorized access attempts, cropping, and compression). Results show high stego-image quality (PSNR 89.540 dB; MSE 0.000072 at 3000×3000) and perfect extraction fidelity (MAR 100%). Payload tampering is rejected and repeated biometric failures trigger OS-level lockout, but the method is fragile to lossy or spatial edits such as JPEG compression and cropping ≥10%. These findings indicate that a defense-in-depth approach can secure image-based secret messaging as long as the PNG file is not modified.

Keywords: AES-GCM, biometric authentication, LSB, RSA-OAEP, steganography.