

ABSTRAK

JANUMELAH. Keamanan Pesan Digital Berbasis *Mobile* Menggunakan *ChaCha20-Poly1305* dan Steganografi *Least Significant Bit (LSB)*. Dibimbing oleh Nurul Hayaty, S.T., M.Cs. dan Feri Irawan, S.Kom., M.Kom.

Pertukaran pesan digital melalui perangkat *mobile* memiliki risiko kebocoran data, penyadapan, dan manipulasi pesan, sehingga diperlukan mekanisme pengamanan yang mampu menjaga keamanan, integritas, dan ketersembunyian data. Penelitian ini bertujuan untuk menguji efektivitas kombinasi algoritma *ChaCha20-Poly1305* dan metode steganografi *Least Significant Bit (LSB)* dalam mengamankan pesan digital pada aplikasi Android. Sistem yang dikembangkan diberi nama *Cryptixel*, yaitu aplikasi yang mengenkripsi pesan menggunakan *ChaCha20-Poly1305*, menyimpan kunci secara lokal melalui *Secure Storage* yang memanfaatkan Android Keystore, serta menyisipkan *payload* terenkripsi ke dalam citra PNG menggunakan metode LSB. Pengujian dilakukan melalui analisis kualitas citra, akurasi ekstraksi pesan, validasi integritas, ketahanan terhadap serangan, kapasitas penyisipan, dan performa waktu pemrosesan. Hasil pengujian menunjukkan bahwa sistem berhasil menyisipkan dan mengekstraksi pesan tanpa perubahan visual yang signifikan. Nilai MSE sebesar 0,000085 dan PSNR sebesar 88,859 dB menunjukkan kualitas *stego-image* yang sangat baik, sedangkan MAR mencapai 100% yang berarti pesan hasil ekstraksi identik dengan pesan asli. Pengujian manipulasi *payload* dan percobaan dekripsi dengan kunci tidak sesuai menghasilkan kegagalan verifikasi *Poly1305* sehingga proses dekripsi ditolak. Namun, metode LSB masih rentan terhadap *cropping* dan kompresi citra *lossy* yang diuji dalam penelitian ini, seperti JPG dan WebP *lossy*, karena perubahan nilai piksel dapat merusak *payload* yang disisipkan. Berdasarkan hasil tersebut, kombinasi *ChaCha20-Poly1305*, *Secure Storage* berbasis Android Keystore, dan LSB efektif digunakan untuk pengamanan pesan digital berbasis *mobile*, terutama ketika citra tidak mengalami modifikasi atau menggunakan format yang mempertahankan data piksel, seperti PNG, BMP, dan WebP *lossless*.

Kata kunci: *ChaCha20-Poly1305*, *Least Significant Bit*, steganografi, Android Keystore, aplikasi *mobile*.

ABSTRACT

JANUMELAH. Mobile-Based Digital Message Security Using ChaCha20-Poly1305 and Least Significant Bit (LSB) Steganography. Supervised by Nurul Hayaty, S.T., M.Cs. and Feri Irawan, S.Kom., M.Kom.

The exchange of digital messages through mobile devices is vulnerable to data leakage, eavesdropping, and message manipulation, creating a need for security mechanisms that ensure confidentiality, integrity, and concealment of information. This study evaluates the effectiveness of combining the ChaCha20-Poly1305 authenticated encryption algorithm with the Least Significant Bit (LSB) steganography method for securing digital messages on the Android platform. The developed system, named Cryptixel, encrypts messages using ChaCha20-Poly1305, stores cryptographic keys locally through Secure Storage backed by the Android Keystore, and embeds encrypted payloads into PNG images using the LSB technique. System evaluation was conducted through image quality analysis, message extraction accuracy, integrity validation, attack resistance testing, embedding capacity assessment, and processing time measurement. The results demonstrate that the system successfully embeds and extracts messages without noticeable visual degradation. An MSE value of 0.000085 and a PSNR value of 88.859 dB indicate excellent stego-image quality, while a Message Accuracy Rate (MAR) of 100% confirms that the extracted messages are identical to the original messages. Payload manipulation and decryption attempts using incorrect keys failed Poly1305 verification, causing the decryption process to be rejected. However, the LSB method remains vulnerable to image cropping and lossy compression formats, such as JPEG and lossy WebP, as pixel modifications may damage the embedded payload. These findings indicate that the combination of ChaCha20-Poly1305, Android Keystore-based Secure Storage, and LSB is effective for securing mobile digital messages, particularly when images remain unmodified or use formats that preserve pixel data, such as PNG, BMP, and lossless WebP.

Keywords: ChaCha20-Poly1305, Least Significant Bit, steganography, Android Keystore, mobile application.