KEAMANAN BERLAPIS PADA DOKUMEN MENGGUNAKAN STEGANOGRAFI DAN *HONEY ENCRYPTION*

OLEH

Gabriel Nathanael Purba

2215101044

Program Studi Ilmu Komputer

Fakultas Teknik dan Kejuruan

Universitas Pendidikan Ganesha

ABSTRAK

Meningkatnya penggunaan dokumen digital mempertinggi risiko ancaman siber seperti serangan *brute-force* dan analisis steganografi (*steganalysis*). Enkripsi konvensional menjaga kerahasiaan, tetapi menampilkan indikator kegagalan yang jelas saat kunci salah digunakan, sehingga membantu penyerang memvalidasi tebakan kunci. Penelitian ini mengusulkan sistem keamanan dokumen berlapis yang mengintegrasikan *Honey Encryption* dan steganografi *Least Significant Bit* (LSB) berbasis algoritma AES-CBC. Pendekatan kuantitatif eksperimental diterapkan untuk merancang dan mengevaluasi sistem. Dokumen PDF dikodekan dalam kerangka kerja Honey Encryption untuk menghasilkan *output* meyakinkan (*plausible*) jika kunci salah. Data hasil pengodean dienkripsi dengan AES-CBC lalu disisipkan ke citra penampung PNG melalui metode LSB. Evaluasi meliputi pengujian fungsional, simulasi *brute-force*, pengukuran waktu pemrosesan, analisis kualitas visual (PSNR dan MSE), serta pengujian analisis steganografi memakai StegExpose. Hasil menunjukkan sistem menghasilkan dokumen umpan (*decoy*) yang valid secara struktural saat kunci salah diterapkan, sehingga menghilangkan umpan balik eksplisit untuk serangan *brute-force*. Pengujian kualitas visual menunjukkan nilai PSNR tinggi dan MSE rendah, mengindikasikan distorsi minimal. Hasil analisis steganografi menunjukkan data tersemat tetap berada dalam ambang batas deteksi yang aman. Studi ini membuktikan penggabungan *Honey Encryption* dan steganografi LSB memperkuat perlindungan dokumen melalui manipulasi kriptografi dan penyisipan terselubung. Penelitian mendatang dapat difokuskan pada peningkatan pemodelan encoder dan ketahanan terhadap metode analisis steganografi tingkat lanjut.

Kata kunci: *honey encryption*, steganografi, AES-CBC, keamanan berlapis, serangan *brute-force*

MULTI-LAYER SECURITY FOR DOCUMENTS USING

STEGANOGRAPHY AND HONEY ENCRYPTION

BY

Gabriel Nathanael Purba

2215101044

Computer Science Study Program

Faculty of Engineering and Vocational

Universitas Pendidikan Ganesha

ABSTRACT

The increasing use of digital documents has heightened exposure to cyber threats such as brute-force attacks and steganalysis. Conventional encryption preserves confidentiality but typically reveals clear failure indicators when incorrect keys are used, potentially aiding attackers in validating key guesses. This research proposes a multi-layer document security system that integrates Honey Encryption and Least Significant Bit (LSB) steganography using the AES-CBC algorithm. An experimental quantitative approach was employed to design and evaluate the system. PDF documents are encoded within a Honey Encryption framework to generate plausible outputs for incorrect keys. The encoded data is encrypted using AES-CBC and embedded into PNG cover images through the LSB method. Evaluation includes functional testing, brute-force simulation, processing time measurement, visual quality analysis using Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE), and steganalysis testing using StegExpose. The results indicate that the system produces structurally valid decoy documents when incorrect keys are applied, eliminating explicit feedback that could support brute-force attacks. Visual quality testing shows high PSNR and low MSE values, indicating minimal distortion. Steganalysis results suggest that the embedded data remains within acceptable detection thresholds. This study demonstrates that combining Honey Encryption and LSB steganography strengthens document protection through cryptographic deception and covert data embedding. Future work may focus on improving encoder modeling and resistance to advanced steganalysis methods.

Keywords: honey encryption, steganography, AES-CBC, multi-layer security, brute-force attack