INTISARI

MODEL KOMPRESI-KRIPTOGRAFI PADA CITRA DIGITAL MENGGUNAKAN PEMBANGKIT KUNCI DINAMIS BERBASIS CHAOS DAN PENDISTRIBUSIAN KUNCI SIMETRIS DENGAN METODE END OF FILE

Oleh

EMY SETYANINGSIH
16/405307/SPA/00564

Permasalahan pertukaran data yang berbentuk citra digital adalah ukurannya yang cenderung semakin besar dan pemenuhan aspek kerahasiaannya pada saat ditransmisikan melalui jalur yang tidak aman. Model kriptosistem menggunakan penggabungan metode kompresi-kriptografi yang dikembangkan saat ini memiliki kinerja yang baik, tetapi masih terbuka peluang untuk dapat ditingkatkan. Selain itu, model-model tersebut masih memiliki kelemahan dalam hal manajemen kunci terkait dengan penggunaan kriptografi simetris.

Penelitian ini mengembangkan model kriptosistem yang dapat mengatasi permasalahan manajemen kunci serta menjaga keamanan data citra yang ditransmisikan. Model yang dikembangkan terdiri dari 3 proses. Proses pertama adalah pembangkitan kunci simetris dan kunci sesi dinamis yang bertujuan untuk membangkitkan kunci simetris dan kunci sesi yang berbeda untuk setiap data citra yang akan ditransmisikan. Proses kedua adalah pengamanan data citra. Proses ini menggunakan metode kompresi yang dilanjutkan dengan kriptografi selektif yang memanfaatkan tiga buah kunci aliran dan dua buah S-Box yang dibangkitkan berdasarkan metode *chaos logistic map*. Proses ketiga adalah mendistribusikan kunci simetris secara aman dan efisien. Proses ini diawali dengan pemberian otentikasi dari pengirim dan dilanjutkan dengan penyandian kunci simetris. Kemudian, kunci tersebut disisipkan ke cipher image menggunakan metode *End of File* (EoF) untuk dikirimkan secara bersamaan.

Hasil pengujian menunjukkan model yang dikembangkan mampu membangkitkan kunci simetris yang bersifat acak dan dinamis, sehingga data citra aman dari serangan *ciphertext only attack*. Selain itu ruang kunci yang terbentuk juga cukup besar, yaitu lebih dari 2^{200} bit untuk kunci simetris dan lebih dari 2^{216} bit untuk kunci sesi, sehingga aman dari serangan *brute-force*. Model kriptosistem yang dikembangkan juga berhasil mereduksi ukuran data dengan mengurangi redudansi data citra rata-rata 37% dengan tetap mempertahankan kualitas dan keamanan data citra yang

ditransmisikan. Model ini terbukti kuat terhadap serangan *entropy, statistical attack, differential attack*, dan *brute-force attack*. Dari sisi komputasi, model ini memiliki kompleksitas waktu $O(n)$.

Kata-kata kunci : kunci simetris, kunci sesi, kompresi-kriptografi, S-Box, otentikasi, end of file.

ABSTRACT

DIGITAL IMAGE COMPRESSION-CRYPTOGRAPHY MODEL USING CHAOS-BASED DYNAMIC KEY GENERATOR AND END OF FILE METHOD FOR SYMMETRIC KEY DISTRIBUTION

By

EMY SETYANINGSIH
16/405307/SPA/00564

The problem of digital image data exchange is related with the increasing size of images and the requirement to provide the confidentiality of the images when transmitted through unsecure channel. The existing cryptosystem models that are basd on compression-cryptography techniques have sufficient performance, but there is still room for improvement. In addition, these models still have weaknesses in terms of key management that are related to the use of symmetric cryptography.

In this research, a cryptosystem model that is able to overcome key management problems and maintain the data security of transmitted images is developed. The model consists of 3 processes. The first process is the generation of dynamic symmetric and session keys that aims to generate different symmetric and session keys for each image to be transmitted. The second process is related to data confidentiality. This process uses a compression method that is followed by selective cryptography by utilizing three stream keys and two S-Boxes that are generated based on the chaos logistic map method. The third process is the process of distributing symmetric keys safely and efficiently. This process is started by giving authentication of the sender, continued with symmetric key encoding. The key is then inserted into the image cipher using the End of File (EoF) method to be sent simultaneously.

The evaluation shows that the model is able to generate symmetric keys that are random and dynamic, so that image data is safe from ciphertext attack only. The key space is also quite large, which is more than 2^{200} bits for symmetric keys and more than 2^{216} bits for session keys, hence, the keys are safe from brute-force attacks. The proposed cryptosystem model also succeeds in reducing the size of the data while maintaining the quality and confidentiality of the image data to be transmitted. This model is proven to be strong against entropy attacks, statistical attacks, differential attacks and brute-force attacks. In terms of computation time, this model is quite efficient with time complexity of $O(n)$.

Keywords : symmetric key, session key, compression-cryptography, S-Boxes, authentication, end of file.