ABSTRACT

Vulnerabilities and threats to CCTV cameras have recently been an increasingly common issue. Data from CCTV, whether in the form of images or videos, is vulnerable to leaks, personal data theft, data manipulation, and criminality. This problem becomes serious unless it is addressed immediately. One attempt to address this issue is the implementation of cryptography methods through data encryption and decryption operations. This study focuses on the security of images obtained from CCTV cameras in private and public places.

Encryption and decryption are used to safeguard the integrity of images and prevent information from being leaked or modified. The cryptographic method used is the Advanced Encryption Standard (AES) 128 bit with Cipher Block Chaining (CBC). This study not only encrypts and decrypts images, but it also uses the dictionary attack approach to test the strength of the keywords employed in the process. Furthermore, this study computes the entropy value of terms to determine their saturation level.

The findings showed that the images were successfully encrypted and decrypted using AES 128-bit with CBC. Measurements of the six photos' Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) parameters yielded positive results, indicating that there was no significant difference between the original and decrypted images. Testing with the dictionary attacks method reveals that keywords that are simple to guess and often used are extremely sensitive to attacks. Therefore, it is vital to employ terms of great complexity and uniqueness. The entropy value indicates the degree of randomness of the terms employed.

Keywords: CCTV Images, encryption, decryption, AES-128bit, Cipher Block Chaining, Dictionary Attacks, entropy, MSE, and PSNR.

INTISARI

Kerentanan dan ancaman pada kamera *CCTV* menjadi masalah yang semakin sering terjadi belakangan ini. Data dari *CCTV*, baik berupa gambar maupun video, rentan terhadap kebocoran, pencurian data pribadi, manipulasi data, dan kejahatan siber. Masalah ini menjadi serius jika tidak segera ditangani. Salah satu upaya yang dilakukan untuk mengatasi masalah ini adalah menerapkan metode kriptografi melalui proses enkripsi dan dekripsi data. Penelitian ini berfokus pada keamanan data gambar yang diambil dari kamera *CCTV*, baik dari rumah pribadi maupun ruang publik.

Tujuan dari enkripsi dan dekripsi ini adalah untuk menjaga integritas gambar sehingga tidak ada informasi yang bocor atau dimanipulasi. Metode kriptografi yang digunakan adalah *Advanced Encryption Standard* (*AES*) 128-bit dengan *Cipher Block Chaining* (*CBC*). Selain melakukan enkripsi dan dekripsi gambar, penelitian ini juga menguji kekuatan kata kunci yang digunakan dalam proses tersebut menggunakan metode dictionary attacks. Selanjutnya, penelitian ini menghitung nilai entropi kata kunci untuk mengevaluasi tingkat keacakannya.

Hasil penelitian menunjukkan bahwa proses enkripsi dan dekripsi gambar menggunakan *AES* 128-bit dengan *CBC* berjalan dengan baik. Pengukuran parameter *Mean Square Error* (*MSE*) dan *Peak Signal-to-Noise Ratio* (*PSNR*) terhadap enam gambar menunjukkan hasil yang baik, menandakan bahwa tidak ada perbedaan signifikan antara gambar asli dan gambar yang didekripsi. Pengujian dengan metode *dictionary attacks* menunjukkan bahwa kata kunci yang mudah ditebak dan umum digunakan sangat rentan terhadap serangan. Oleh karena itu, penting untuk menggunakan kata kunci dengan kompleksitas tinggi dan keunikan. Perhitungan nilai entropi menunjukkan tingkat keacakan kata kunci yang digunakan.

Kata kunci: Gambar *CCTV*, Enkripsi, Dekripsi, *AES*-128bit, *Cipher Block Chaining*, *Dictionary Attacks*, Entropi, *MSE, PSNR*