IMPLEMENTASI ALGORITMA AES DAN SHA-256 DALAM PENGKODEAN PADA SEBAGIAN *FRAME* VIDEO CCTV MPEG-2

Oleh

Anisha Yahdiani Mulyadi – anishayahdiani@gmail.com

1301015

ABSTRAK

Perkembangan yang sangat pesat dalam pertukaran data pada teknologi internet dan informasi menyebabkan keamanan informasi menjadi masalah utama dalam penyimpanan data. Beberapa data memiliki informasi yang bersifat rahasia dan harus dilindungi, terutama dalam bentuk video yang mungkin mencakup beberapa informasi sensitif yang tidak diperuntukkan bagi konsumsi publik. Masalah muncul ketika informasi tersebut dapat dimanipulasi dan diubah keasliannya, salah satunya pada suatu file video *Closed Circuit Television* (CCTV). Oleh karenanya, tingkat keamanan dan privasi dalam suatu file video CCTV memiliki peranan yang vital. Penelitian ini membahas rancangan dan implementasi model pengamanan video CCTV MPEG-2 menggunakan teknik enkripsi. Proses enkripsi pada video akan menghasilkan video dengan sebagian *frame* yang acak sehingga dapat mencegah tindakan manipulasi. Metode enkripsi yang digunakan yaitu *Advanced Encryption Standard* (AES) 128 bits dan *Secure Hash Algorithm* – 256 (SHA-256), dimana AES digunakan pada proses enkripsi dan dekripsi, sedangkan SHA-256 digunakan untuk meningkatkan kompleksitas pada kunci yang akan digunakan dan diuji oleh *Randomness Test*. Dengan menggunakan *Peak Signal to Noise Ratio* (PSNR) dan *Mean Squared Error* (MSE), model pengamanan video CCTV MPEG-2 yang dihasilkan menunjukkan kinerja yang cukup baik dengan nilai PSNR dan MSE maksimum secara berturut-turut yaitu 27.8 dB dan 107.19 pada hasil enkripsi. Sedangkan pada hasil dekripsi, nilai PSNR dan MSE maksimum secara berturut-turut yaitu 43.43 dB dan 3.01.

Kata Kunci —Kriptografi, Metode AES128, SHA256, MPEG-2, enkripsi, dekripsi

ALGORITHMS IMPLEMENTATION OF AES 128 AND SHA-256 IN CODING ON PARTIAL FRAMES OF MPEG-2 CCTV VIDEO

Arranged by

Anisha Yahdiani Mulyadi – anishayahdiani@gmail.com

1301015

ABSTRACT

The relentless growth of data exchange on internet and informtion technolgy has made information security being a major issue in data storage. Some data have confidential information and must be protected. Some data have confidential information and should be protected, especially in the form of videos that may include some sensitive information not reserved for public consumption. Problems arise when the information can be manipulated and changed its authenticity, one of them is a Closed Circuit Television (CCTV) video file. Therefore, the level of security and privacy in a CCTV video file has a vital role. This study discusses the design and implementation of CCTV MPEG-2 video security model using encryption technique. The encryption process on the video will produce a video with partial random frames that can prevent manipulation. Encryption method used is Advanced Encryption Standard (AES) 128 bits and Secure Hash Algorithm - 256 (SHA-256), where AES is used in encryption and decryption process, while SHA-256 is used to increase the complexity of the key to be used and tested by Randomness Test. The results of the *frames* will be using the Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE), the MPEG-2 CCTV video security model produced shows good performance with maximum PSNR and MSE values respectively 27.8 dB and 107.19 on the encryption result . While on the decryption, the maximum value of PSNR and MSE respectively are 43.43 dB and 3.01.

Keywords —Cryptography, AES128, SHA256, MPEG-2, encryption, decryption