BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Dengan semakin berkembangnya multimedia yang semakin pesat dan zaman yang semakin modern, maka suatu video memerlukan adanya keamanan dalam menjaga informasi yang ada pada video tersebut. Masalah keamanan merupakan salah satu aspek yang sangat penting dalam suatu data pada video. Selain ada pihak yang ingin menjaga agar data pada video tersebut tetap aman, namun ada juga pihak-pihak yang ingin agar dapat mengubah isi data pada video tersebut. Tidak semua video yang ada dibuat untuk konsumsi publik, banyak dari beberapa video yang bersifat pribadi yang hanya ditujukan untuk beberapa pihak tertentu saja. Seperti jika pemilik data dari beberapa video yang bersifat rahasia seperti data pemerintah atau data militer, maka keamanan informasi pada video tersebut tergolong sangat rahasia dan penting yang tidak boleh diketahui oleh publik (Yuniati, Indriyanta, & C, 2009).

Beberapa contoh dari dari ancaman keamanan pada suatu informasi yang ada pada video seperti *modification* dan *fabrication*. Pada standar *National of Institute of Standards and Technology* (NIST) dalam SP 800-27, Rev A dengan judul *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)* memiliki 33 prinsip tentang keamanan teknologi informasi, salah satu prinsipnya yaitu pada prinsip ke-26 untuk mengurangi ancaman serangan pada suatu informasi dengan menerapkan batasan hak akses *(least privilege)* (Stoneburner, Hayden, & Feringa, 2004). Ini dapat diartikan menerapkan pembagian tugas yang tepat dan terbatas. Dengan melakukan pembatasan hak akses *(least privilege)* maka hanya pihak yang memegang kunci hak akses yang dapat mengakses suatu informasi dan dengan syarat hak akses itu secara aman diberikan kepada orang yang benar-benar memiliki hak tersebut.

Masalah yang dibahas pada penelitian ini yaitu merupakan tindakan manipulasi yang dapat mengubah keaslian data pada suatu *file* video *Closed Circuit Television* (CCTV). Sudah banyak kasus yang terjadi tentang data rekaman video CCTV yang dimanipulasi dan direkayasa untuk kepentingan pihak yang tidak berhak. CCTV

memainkan peran yang sangat signifikan dalam melindungi publik dan membantu kepolisian dalam menginvestigasi kasus kriminal (Keval, 2009). Data yang dimanipulasi akan memiliki data yang berbeda, pada sebuah data yang dimanipulasi gambar atau *frame* yang didapatkan menjadi lebih kabur akibat pengurangan dari *frame* yang artinya file video tidak sama ukuran dengan yang asli di CCTV (Herani, 2016). Maka dalam penelitian ini akan diterapkan kriptografi video untuk meningkatkan keamanan pada data rekaman video CCTV, yaitu dengan menggabungkan algoritma fungsi *hash Secure Hash Algorithm – 256* (SHA-256) dan algoritma *Advanced Encryption Standard* (AES).

Data rekaman video rentan dengan berbagai bentuk manipulasi seperti penambahan *frame* yang seharusnya tidak ada dan dihilangkan sebagian *frame* yang ada pada data sehingga data tidak lengkap. Data rekaman video yang telah dimanipulasi dapat menyebabkan kerugian yang sangat besar untuk beberapa pihak yang terkait. Karena sangat rentan dimanipulasi, keamanan pada data perlu ditingkatkan untuk melindungi data agar tetap terjaga keasliannya. Seperti pada kasus kriminal Jessica dan Mirna saksi ahli menemukan kejanggalan berupa pengeditan dalam video CCTV Kafe Olivier yang merekam detik-detik kematian Mirna berupa jumlah *frame* yang seharusnya 98750 *frame* menjadi hanya 2227 frame. Lalu ukuran *file* yang tereduksi menjadi 96 x 576 piksel yang asalnya dari 1920 x 1080 piksel (Aditya, 2016). Dalam kasus tersebut sudah terjadi proses manipulasi karena tidak adanya keamanan dalam penjagaan suatu informasi pada video CCTV tersebut. Maka dalam penelitian ini akan diterapkan kriptografi video untuk meningkatkan keamanan pada data rekaman video, yaitu dengan menggabungkan algoritma AES dan fungsi hash SHA-256.

Kriptografi merupakan suatu ilmu mengenai teknik matematis yang ditujukan pada aspek pengamanan data yang meliputi tingkat kepercayaan terhadap data tersebut, integritas data, ontetikasi entitas data, otentifikasi terhadap keaslian data (Menezes, Oorschot, & Vanstone, 1996). Kriptografi *(cryptography)* berasal dari Bahasa Yunani yaitu *"cryptos"* yang artinya *"secret"* atau rahasia. Sedangkan *"gráphein"* artinya *"writing"* atau tulisan. Jadi kriptografi merupakan *"secret writing"* atau tulisan rahasia (Munir, 2006). Terdapat empat tujuan mendasar dari ilmu kriptografi yang juga merupakan aspek dari keamanan informasi yaitu kerahasiaan *(confidentiality)*, otentikasi *(authentication)*, integritas data *(data integrity)* dan ketiadaan penyangkalan *(non-repudiation)*. Dalam penelitiaan ini akan mengacu

pada kerahasiaan dan integritas data. Integritas data yaitu layanan yang menjamin bahwa data masih asli dan utuh atau belum pernah dimanipulasi (Munir, 2006). Tujuan dari integritas data tersebut sudah sangat jelas bahwa integritas data mencegah terjadinya manipulasi pada suatu informasi oleh pihak-pihak yang tidak berhak dalam mengakses suatu informasi tersebut. Manipulasi data dapat berupa melakukan penyisipan, menghapus dan merubah suatu data.

Terdapat penelitian sebelumnya yang menjadi dasar untuk melakukan penelitian ini. Penelitian-penelitian berikut ini berkaitan dengan Algoritma AES dan fungsi hash SHA-256 untuk enkripsi dan dekripsi pada *video*. Beberapa penelitian menyatakan bahwa implementasi algoritma AES memiliki performa yang lebih baik dibandingkan dengan algoritma kriptografi lain. Dalam penelitiannya yaitu dengan membandingkan algoritma (*Data Encryption Standard)* DES, RSA dan AES menjelaskan bahwa walaupun algoritma DES telah terbukti sebagai algoritma yang aman. Namun algoritma AES memberikan keamanan yang lebih baik dan memiliki kebutuhan memori yang sangat rendah. Maka dari itu algoritma AES memiliki algoritma enkripsi yang paling efisien dan menjadi salah satu algoritma yang paling kuat dibandingkan algoritma lainnya (Saleh, Tahir, Hisham, & Hashim, 2015).

Penelitian algoritma enkripsi lainnya yang berkaitan dengan algoritma AES dilakukan, yaitu pada implementasi algoritma AES-256 dan fungsi *hash* SHA-1 dalam pengamanan *file*. Implementasi yang dilakukan pada penelitian ini dilakukan proses enkripsi yang dimulai dengan pemilihan *file input* dan kunci enkripsi (Siregar, Syahfitri, & Tommy, 2017). Setelah itu, proses dilanjutkan dengan menghitung nilai *hash* kunci dengan menggunakan metode SHA. Algoritma SHA-1 dapat digunakan untuk mengamankan kunci sebelum diterapkan dalam proses enkripsi dan dekripsi agar kunci yang dihasilkan menjadi lebih kompleks dan lebih sulit untuk dipecahkan. Kombinasi dari algoritma AES-256 dan fungsi SHA-1 dapat meningkatkan keamanan dari pesan yang akan dikirimkan.

Maka berdasarkan hal-hal yang ada di atas yang akan dilakukan pada penelitian ini yaitu implementasi algoritma AES dengan fungsi *hash* SHA-256. AES memiliki komputasi yang ringan dan cocok digunakan dalam suatu proses enkripsi video dan dapat dikombinasikan dengan fungsi *hash* SHA-256 yang bertujuan meningkatkan

kompleksitas kunci. Panjang kunci AES yang digunakan pada penelitian ini adalah kunci AES dengan panjang kunci 128 *bits*, 128 *bits* dipilih karena fleksibel dan dengan kunci 128 *bits*, AES tahan terhadap serangan *exhaustive key search*. Dengan penelitian yang akan dilakukan, diharapkan implementasi dari algoritma AES dan fungsi *hash* SHA-256 ini yang juga telah dilandasi oleh penelitian sebelumnya dapat menghasilkan sebuah aplikasi keamanan video yang memiliki tujuan untuk mencegah terjadinya proses manipulasi data pada video serta meningkatkan keamanan pada video.

1.2 Rumusan Masalah Penelitian

Rumusan masalahnya antara lain adalah:

1. Bagaimana implementasi proses enkripsi dan dekripsi pada *file* video CCTV dengan menggunakan algoritma AES dan SHA-256??
2. Bagaimana hasil dari pengujian kompleksitas AES dengan SHA-256 dan tanpa SHA-256?
3. Bagaimana hasil dari implementasi enkripsi dan dekripsi pada *file* video CCTV dengan menggunakan algoritma AES dan SHA-256?

1.3 Tujuan Penelitian

Tujuan dari dilakukannya penelitian ini adalah sebagai berikut, yaitu:

1. Merealisasikan suatu proses enkripsi dan dekripsi dengan masukan berupa *file* video CCTV MPEG-2 yang menggunakan algoritma AES dan SHA-256.
2. Membuktikan Kerahasiaan Video CCTV yang tidak dapat dimanipulasi menggunakan Algoritma AES dan SHA-256.
3. Mendapatkan hasil pengujian kompleksitas dari kunci AES 128 *bits* dan SHA-256 dengan menggunakan *Randomness Test*.
4. Menganalisis hasil dari pengujian faktor *fidelity* dengan menggunakan MSE dan PSNR.

1.4 Batasan Masalah

Batasan masalah dari ruang lingkup penelitian ini yang dilakukan adalah sebagai berikut:

1. Kunci yang digunakan pada algoritma AES dalam penelitian ini memiliki ukuran panjang 128 *bits*.
2. Informasi yang akan dienkripsi dan didekripsi dapat berupa format video seperti .avi, .mp4 dan format mpeg lainnya namun

pada penelitian ini penulis hanya menggunakan video dengan format MPEG-2.

3. Dalam proses pengujian aplikasi tidak melakukan validasi *file* video apakah video tersebut merupakan video MPEG-2 atau tidak.
4. Proses enkripsi akan dilakukan pada video MPEG statik (bukan untuk video *streaming*).
5. Pengujian hasil aplikasi akan dilakukan pada video yang berukuran 320 x 240 pixel.
6. Video CCTV yang diuji hanya berdurasi 4 detik.
7. Pengujian *Randomness Test* dilakukan dengan bantuan software Cryptool 1.4.4.5.
8. Video CCTV diambil dari beberapa berita televisi internasional yaitu Fox News, Korean Ent serta dari halaman *https://youtube.com*.
9. Simulasi ini akan dilakukan dengan menggunakan Matlab R2016a.

1.5 Sistematika Penulisan

Sistematika penulisan yang akan disampaikan pada penelitian ini, yaitu:

BAB I PENDAHULUAN

Pada bab ini dijelaskan latar belakang masalah yang melandasi dilakukannya penelitian mengenai implementasi enkripsi dan dekripsi frame video dengan menggunakan algoritma AES dan fungsi *hash* SHA-256 pada suatu kasus pada video. Dan bab ini juga akan diuraikan mengenai rumusan masalah, tujuan dari penelitian yang dilakukan, batasan masalah dan sistematika penulisan.

BAB II KAJIAN PUSTAKA/ LANDASAN TEORETIS

Pada bab ini akan dijelaskan landasan teoritis yang mendukung dan berhubungan dengan penelitian yang diilakukan. Bagian ini menjelaskan tentang teori-teori dan konsep algoritma-algoritma yang digunakan dalam penelitian.

BAB III METODE PENELITIAN

Pada bab ini akan menjelaskan dan mengarahkan pembaca agar mengetahui bagaimana langkah-langkah yang dilakukan oleh peneliti dalam penelitian ini.

BAB IV TEMUAN DAN PEMBAHASAN

Pada bab ini akan dibahas secara mendalam mengenai permasalahan yang telah dirumuskan pada bagian rumusan masalah. Adapun inti dari bab ini yaitu membahas hasil dari penelitian yang dilakukan.

BAB V KESIMPULAN DAN SARAN

Bab kesimpulan berisi tentang rangkuman dari hasil penelitian yang telah dilakukan. Selain kesimpulan, pada bab 5 disampaikan saran untuk penelitian selanjutnya.