

BAB I

PENDAHULUAN

1.1 Latar belakang

Kemajuan teknologi membuat penggunaan video *surveillance* di beberapa ruangan semakin penting guna meningkatkan keamanan dan *privacy* bagi penggunanya. Adanya video *real-time* yang berfungsi merekam suatu gambar pada suatu kegiatan tentu penting bagi beberapa instansi seperti perbankan, perkantoran, pertahanan negara, dan lain-lain. Namun pertukaran informasi tersebut tentu saja dapat menimbulkan resiko jika informasi yang dipertukarkan dapat diakses oleh pihak-pihak yang tidak bertanggung jawab. Maka dari itu kerahasiaan data pun semakin ditingkatkan, salah satunya dengan metode kriptografi yang menggunakan algoritma VEA.[1]

Kriptografi adalah proses mengubah data asli menjadi bersandi atau tidak dapat dipahami oleh pembaca jika tidak memiliki kunci sandinya. Kunci yang digunakan biasanya bersifat simetris dan asimetris. Pembaca yang telah memiliki kuncinya maka dapat mengubah data bersandi atau tidak bisa dibaca tadi menjadi data asli.

Pada algoritma ini byte-byte pada frame video, di-XOR-kan dengan suatu byte kunci tertentu yang telah didefinisikan. Hasil operasi XOR tersebut kemudian diterapkan pada data video, sehingga video yang dihasilkan memiliki kualitas gambar tidak sempurna [2]. Video hasil enkripsi itulah yang nantinya diterima oleh user yang tidak berhak memasukkan kunci tertentu yang telah didefinisikan. Alasan banyaknya penggunaan algoritma ini adalah karena tingkat keamanannya yang cukup memuaskan, komputasi yang ringan, dan cocok diimplementasikan di lingkungan video *streaming* karena algoritmanya yang dapat berbasis stream cipher maupun block cipher, tergantung kebutuhan saat *streaming* video tersebut.

1.2 Rumusan Masalah

Rumusan masalah dalam pembuatan Proposal Tugas Akhir ini adalah seperti yang dijelaskan dibawah ini:

- a) Modifikasi enkripsi dan dekripsi algoritma VEA dengan kunci Rabbit untuk pengamanan data video *real-time*
- b) Menerapkan proses enkripsi data *streaming* video dan mendekripsikannya langsung secara *real-time*
- c) Performansi sistem yang diukur meliputi pengukuran parameter *avalanche effect, delay, jitter, datarate, frame rate, dan bandwidth*.

1.3 Tujuan

Dengan merujuk pada rumusan masalah diatas, maka tujuan yang dibahas pada Tugas Akhir ini:

- a) Menerapkan dan memodifikasi algoritma VEA dengan kunci Rabbit pada proses enkripsi dan dekripsi video.
- b) Membuat sistem untuk mengenkripsi data *streaming* video *surveillance* dan mendekripsikannya langsung secara *real-time* menggunakan algoritma VEA dengan kunci Rabbit.
- c) Menganalisis hasil implementasi yang telah dilakukan dengan pengukuran parameter waktu proses, *avalanche effect, delay, jitter, datarate, frame rate, dan bandwidth*.

1.4 Batasan Masalah

Tugas Akhir ini mempunyai batasan masalah yaitu :

- a) Rekaman video *surveillance* berasal dari webcam
- b) Menggunakan kunci simetris

- c) Software yang digunakan berbasis java
- d) *Client* tidak terlibat distribusi kunci
- e) Sistem tidak menyimpan file berekstensi
- f) Pembobolan jaringan dan *server* tidak dibahas
- g) Admin tidak memerlukan proses autentifikasi

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan diantaranya:

- a. Studi Literature mencari dan mempelajari teori-teori dan konsep mengenai VEA dan kunci Rabbit, implementasi nya pada video *real-time*, dan modifikasi dari VEA dan Rabbit dari buku, artikel, jurnal dan referensi dari internet. Hasil studi literature yang didapatkan akan dijadikan sebagai bahan untuk dasar teori dalam pembuatan buku tugas akhir ini.
- b. Merancang flowchart / diagram alur sistem untuk implementasinya.
- c. Implementasi algoritma kriptografi pada Video *Real-Time* sesuai dengan sistem yang telah dirancang
- d. Uji performansi dan analisis hasil penelitian
- e. Pembuatan laporan dari hasil penelitian

1.6 Perancangan

Setelah melakukan analisis terhadap masalah yang di kaji, maka akan dilakukan perancangan perangkat lunak yang dibangun meliputi perancangan sistem kamera.

1.7 Sistematika Penulisan

BAB I PENDAHULUAN

Berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Berisi teori-teori dan materi mengenai video *streaming*, *surveillance*, kriptografi, modifikasi algoritma VEA, dan algoritma Rabbit yang diperlukan dalam pelaksanaan Tugas Akhir.

BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM

Berisi tentang skenario dan perancangan sistem yang akan dibangun

BAB IV PENGUJIAN DAN ANALISIS SISTEM

Berisi implementasi dari perancangan Tugas Akhir serta mengikutsertakan hasil uji coba dari sistem yang dibuat dan telah dicapai dalam Tugas Akhir ini.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan yang dapat diambil dari Tugas Akhir ini beserta saran untuk pengembangan selanjutnya.