APLIKASI ENKRIPSI VIDEO MPEG DENGAN *VIDEO ENCRYPTION ALGORITHM* (VEA) YANG DIMODIFIKASI DENGAN ALGORITMA RC4

SKRIPSI

Disusun Sebagai Salah Satu Syarat

Untuk Memperoleh Gelar Sarjana Komputer

Pada Departemen Ilmu Komputer/Informatika

Disusun oleh:

Yusuf Fahmi Adiputera

24010310130068

DEPARTEMEN ILMU KOMPUTER/INFORMATIKA

FAKULTAS SAINS DAN MATEMATIKA

UNIVERSITAS DIPONEGORO

2017

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini:

Nama	:	Yusuf Fahmi Adiputera
NIM	:	24010310130068
Judul	:	Aplikasi Enkripsi Video MPEG dengan *Video Encryption Algorithm* (VEA) yang dimodifikasi dengan Algoritma RC4

Dengan ini saya menyatakan bahwa dalam tugas akhir/ skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Semarang, 1 Februari 2017

Yusuf Fahmi Adiputera
24010310130068

HALAMAN PENGESAHAN

Judul	:	Aplikasi Enkripsi Video MPEG dengan *Video Encryption Algorithm* (VEA) yang dimodifikasi dengan Algoritma RC4
Nama	:	Yusuf Fahmi Adiputera
NIM	:	24010310130068

Telah diujikan pada sidang tugas akhir pada tanggal 30 Desember 2016 dan dinyatakan lulus pada tanggal 27 Januari 2017.

Semarang, 1 Februari 2017

Mengetahui,
Ketua Departemen Ilmu Komputer/Informatika
FSM UNDIP

Ragil Saputra, S.Si, M.Cs
NIP. 19801021 200501 1 003

Panitia Penguji Tugas Akhir
Ketua,

Drs. Eko Adi Sarwoko, M.Kom
NIP. 19651107 199203 1 003

HALAMAN PENGESAHAN

Judul : Aplikasi Enkripsi Video MPEG dengan *Video Encryption Algorithm* (VEA) yang dimodifikasi dengan Algoritma RC4

Nama : Yusuf Fahmi Adiputera

Nim : 24010310130068

Telah diujikan pada sidang tugas akhir pada tanggal 30 Desember 2016

Semarang, 1 Februari 2017

Pembimbing

Dr. Eng. Adi Wibowo, S.Si, M.Kom

NIP. 19820309 200604 1 002

ABSTRAK

Video adalah salah satu konten multimedia yang sering digunakan seiring maraknya penggunaan *smartphone*. Seiring dengan perkembangan teknologi maka faktor keamanan untuk menjaga kerahasiaan dari video menjadi hal yang penting agar orang yang tidak berkepentingan tidak dapat melihat gambar dari video. Salah satu metode untuk mengamankan gambar dari video adalah dengan melakukan enkripsi. Metode enkripsi video yang dapat digunakan yaitu algoritma *video encryption algorithm* (VEA), algoritma ini melakukan enkripsi pada frame I dari video MPEG. Dalam tugas akhir ini algoritma VEA dimodifikasi dengan algoritma RC4 untuk menambah keamanannya. Aplikasi ini dibangun dengan menggunakan metode pengembangan perangkat lunak *unified process* dan implementasinya menggunakan bahasa pemrograman Java. Dari hasil pengujian, diperoleh hasil bahwa algoritma RC4 dapat meningkatkan tingkat keamanan dari algoritma VEA yang dapat dilihat dari nilai MSE rata-rata video hasil enkripsi algoritma VEA yang dimodifikasi dengan algoritma RC4 lebih tinggi dari nilai MSE rata-rata video hasil enkripsi algoritma VEA, selain itu pengujian juga memperlihatkan bahwa waktu enkripsi yang linier dengan durasi video dan resolusi video.

Kata kunci: VEA, RC4, kriptografi, video.

ABSTRACT

Video is one of the multimedia content that is frequently used as the increase popularity of smartphone. With the development of technology, security factor is becoming more important to prevent unauthorized person from seeing the video. One way to secure the frame of a video is by encrypting the frame. Encryption method used in this application is video encryption algorithm (VEA), this algorithm encrypt frame type I of MPEG video. In this application VEA is modified with RC4 algorithm to increase the security. This application is created using software development methods Unified Process and its implementation using the Java programming language. Testing results reveal that RC4 algorithm can increase the security of VEA which can be seen from average MSE of encrypted video by VEA and RC4 is higher than average MSE of encrypted video by VEA only. Testing results also reveal that encryption time is linier with the duration of video and resolution of video.

Keywords: VEA, RC4, cryptograph, video

KATA PENGANTAR

Segala puji syukur bagi Allah SWT atas karunia-Nya yang diberikan kepada penulis sehingga penulis dapat menyelesaikan penulisan laporan Tugas Akhir ini. Laporan Tugas Akhir yang berjudul "Aplikasi Enkripsi Video MPEG dengan *Video Encyption Algorithm* (VEA) yang dimodifikasi dengan Algoritma RC4" ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana komputer pada Departemen Ilmu Komputer / Informatika Universitas Diponegoro. Pada penelitian Tugas Akhir ini, mahasiswa dituntut untuk mengimplementasikan ilmu yang telah didapatkan di bangku perkuliahan untuk menyelesaikan suatu permasalahan yang ada dengan menggunakan teknik penelitian ilmiah.

Pada penyusunan laporan ini, tentulah Penulis banyak mendapat bimbingan dan bantuan dari berbagai pihak. Untuk itu, pada kesempatan ini penulis mengucapkan rasa hormat dan terima kasih kepada :

1. Ragil Saputra, S.Si, M.Cs. selaku Ketua Departemen Ilmu Komputer / Informatika FSM Universitas Diponegoro
2. Helmi Arif Wibawa, S.Si, M.Cs. selaku koordinator tugas akhir Departemen Ilmu Komputer / Informatika Universitas Diponegoro
3. Dr. Eng. Adi Wibowo, S.Si, M.Kom selaku dosen pembimbing tugas akhir
4. Semua pihak yang telah membantu kelancaran dalam pelaksanaan tugas akhir ini yang tidak dapat penulis sebutkan satu persatu

Penulis menyadari bahwa dalam laporan ini masih banyak kekurangan baik dari segi materi ataupun dalam penyajiannya karena keterbatasan kemampuan dan pengetahuan Penulis. Oleh karena itu, kritik dan saran sangat penulis harapkan. Semoga laporan ini dapat bermanfaat bagi pembaca pada umumnya dan penulis pada khususnya.

Semarang, Januari 2017

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR KODE

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

Bab ini menyajikan latar belakang, rumusan masalah, tujuan dan manfaat dan ruang lingkup mengenai tugas akhir aplikasi enkripsi video MPEG dengan *Video Encryption Algorithm* (VEA) yang dimodifikasi dengan RC4.

1.1. Latar Belakang

Dewasa ini, konten multimedia telah berkembang sangat pesat dan digunakan dalam berbagai bidang. Salah satu konten multimedia yang umum digunakan dalam masyarakat adalah video. Video saat ini digunakan dalam bidang komunikasi sebagai sarana dalam *video chat* dan juga dalam bidang hiburan yaitu berupa film. Salah satu format video yang sering digunakan adalah video MPEG atau *Moving Pictures Expert Group*, yang merupakan standar industri dalam *video processing* (Agi & Gong, 1996). Seiring dengan perkembangan teknologi maka faktor keamanan untuk menjaga kerahasiaan dari video menjadi hal yang penting agar orang yang tidak berkepentingan tidak dapat melihat isi dari suatu video. Salah satu cara untuk menjaga kerahasiaan dari suatu data adalah dengan melakukan enkripsi pada video.

Beberapa algoritma untuk melakukan enkripsi video mpeg telah diteliti, antara lain *naïve algorithm, selective algorithm, zig-zag permutation algorithm,* dan *video enrcryption algorithm* (VEA). *Naïve algorithm* memperlakukan baris bit file MPEG seperti hanya data teks tradisional dan tidak menggunakan sedikit pun bentuk spesial dari struktur file MPEG. Algoritma enkripsi tersebut, bagaimanapun sangat rumit dan melibatkan komputasi yang besar. Implementasi perangkat lunak dengan cara ini tidak cukup cepat untuk memproses jumlah data yang dihasilkan oleh aplikasi multimedia (Shi, et al., 1999). *Selective algorithm* bekerja dengan melakukan enkripsi hanya pada *header* dari video MPEG. *Zig-zag permutation algorithm* memiliki ide dasar dengan memetakan blok 8x8 kedalam vektor 1x64 dalam urutan yang zig-zag. Algoritma VEA bekerja dengan memperhatikan struktur file dari sebuah file MPEG dengan hanya beroperasi pada *sign bits* dari koefisien DCT pada frame I dari sebuah file video MPEG

(Bhargava, et al., 2002). Algoritma VEA dipilih karena merupakan algoritma yang cepat dan efisien dalam melakukan proses enkripsi (Qiao & Nahrstedt, 1997).

Penelitian algoritma VEA sebelumnya diantaranya dengan menambahkan algoritma DES dan fungsi *hash* MD5 untuk penerapannya dalam video streaming (Savitri, 2007). Dalam tugas akhir ini algoritma VEA dimodifikasi dengan tambahan algoritma RC4 untuk meningkatkan keamanannya.

RC4 merupakan jenis algoritma kriptografi *stream cipher* (cipher aliran) yang beroperasi pada bit tunggal. Oleh karena termasuk dalam cipher aliran maka dalam proses enkripsinya memakan waktu yang sangat singkat (Sadikin, 2012). Algoritma RC4 merupakan algoritma enkripsi simetris, yang berarti hanya satu kunci yang digunakan dalam proses enkripsi dan dekripsi (Kim, et al., 2007). Dengan algoritma enkripsi simetris maka tingkat keamanan tergantung pada pengguna dalam menyimpan kunci yang digunakan, jika kunci diketahui oleh penyerang maka data dapat dengan mudah didekripsi (Kadam & Deshmukh, 2016).

Berdasarkan hal tersebut di atas, maka pada tugas akhir ini akan diteliti tentang enkripsi video dengan menggunakan algoritma VEA yang dimodifikasi dengan algoritma RC4. Untuk menambah keamanan maka dilakukan enkripsi pada keseluruhan frame I dan P. Aplikasi ini diharapkan dapat menjadi alternatif dalam pengamanan video MPEG.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang dapat dirumuskan permasalahannya adalah bagaimana membuat aplikasi enkripsi video MPEG dengan algoritma VEA yang dimodifikasi dengan algoritma RC4.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dari penelitian ini yaitu membuat aplikasi yang dapat melakukan enkripsi terhadap video MPEG dengan algoritma VEA yang dimodifikasi dengan RC4 untuk menjaga kerahasiaan gambar(*frame*) video.

Adapun manfaat yang diharapkan dari penelitian ini adalah mendapatkan aplikasi yang dapat memberikan pengamanan terhadap video MPEG dengan mengimplementasikan algoritma VEA yang dimodifikasi dengan algoritma RC4.

1.4. Ruang Lingkup

Adapun ruang lingkup dalam pembuatan aplikasi enkripsi video MPEG dengan *Video Encryption Algorithm* (VEA) yang dimodifikasi dengan algoritma RC4 adalah sebagai berikut:

1. Aplikasi yang dikembangkan adalah berbasis *desktop*
2. *Input* dari aplikasi berupa video mpeg-1
3. Aplikasi hanya melakukan enkripsi pada *frame* video
4. Bahasa pemrograman yang digunakan adalah Java
5. *Media player* yang digunakan yaitu windows media player
6. Aplikasi bekerja secara *offline*.
7. Pengujian dilakukan dengan menghitung nilai *mean squared eror*(MSE) dengan menggunakan aplikasi MSU Video Quality Measurement Tool.

1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi dalam beberapa pokok bahasan, yaitu:

BAB I PENDAHULUAN

Merupakan pendahuluan yang berisi latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan.

BAB II LANDASAN TEORI

Berisi kumpulan studi pustaka yang berkaitan dengan tugas akhir. Dasar teori meliputi Video MPEG, Kriptografi, *Video Encryption Algorithm* (VEA), Algoritma RC4, *Mean Squared Errori* (MSE), konsep berorientasi objek, metode pengembangan *unified process*, *unified modeling language*, dan bahasa pemrograman Java.

BAB III INSEPSI DAN ELABORASI

Membahas analisis kebutuhan dan perancangan sistem yang dibangun. Tahap analis dan perancangan dimulai dari fase *inception* sampai dengan *elaboration*. Analisis dan perancangan aplikasi ini menggunakan metode pengembangan *unified process* dengan satu

iterasi karena ruang lingkup yang diangkat dalam pembentukan aplikasi ini tidak terlalu luas.

BAB IV KONSTRUKSI DAN TRANSISI

Membahas tahap implementasi dan rincian pengujian sistem yang dibangun dengan metode *black box*.

BAB V PENUTUP

Berisi kesimpulan yang diambil berkaitan dengan sistem yang dikembangkan dan saran-saran untuk pengembangan sistem lebih lanjut.