MODEL KEAMANAN PESAN PADA VIDEO MENGGUNAKAN METODE *ONE'S COMPLEMENT CRYPTOGRAPHY* DAN *TRACK FREE ATOM STEGANOGRAPHY*

TESIS

Oleh:
Pujianto
1111601090

PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

JAKARTA
2016

MODEL KEAMANAN PESAN PADA VIDEO MENGGUNAKAN METODE *ONE'S COMPLEMENT CRYPTOGRAPHY* DAN *TRACK FREE ATOM STEGANOGRAPHY*

TESIS

Diajukan untuk memenuhi salah satu persyaratan
Memperoleh gelar Magister Ilmu Komputer (MKOM)

Oleh:
Pujianto
1111601090

PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

JAKARTA
2016

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Pujianto
NIM : 11116010 90
Program Studi : Magister Ilmu Komputer (MKOM)
Program : Program Pascasarjana

Menyatakan bahwa Tesis yang berjudul:

MODEL KEAMANAN PESAN PADA VIDEO MENGGUNAKAN METODE ONE'S COMPLEMENT DAM TRACK FREE ATOM STEGANOGRAPHY

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik pihak lain.
2. Saya izinkan untuk dikelola oleh Universitas Budi Luhur sesuai norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila dikemudian hari pernyataan ini tidak benar .

Jakarta, Februari 2016

METERAI TEMPEL 23B4ADF430918711 6000 ENAM RIBU RUPIAH

(PUJIANTO)

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Pujianto
NIM : 1111601090
Kosentrasi : *Rekayasa Komputasi Terapan*
Jenjang Studi : Strata 2
Topik/Judul Tesis : Model Keamanan Pesan Pada Video Menggunakan Metode *One's Complement* Dan *Track Free Atom Steganography*

Jakarta, Februari 2016

Tim Penguji — Tanda Tangan

Ketua Penguji I,

Prof. Dr. Moedjiono, M.Sc ----------

Penguji II,

Hari Soetanto, S.Kom, M.Sc ----------

Pembimbing,

Dr., Ir. Nazori Az, M.T ----------

Ketua Program Studi

Dr. Ir. Nazori Az, M.T

ABSTRAK

Steganography merupakan ilmu dan seni yang mempelajari cara penyembunyian informasi rahasia ke dalam suatu media sehingga manusia tidak dapat menyadari keberadaan pesan tersebut. Penyembunyian pesan pada file video dikenal dengan istilah steganografi video. Pada tulisan ini, diusulkan sebuah kerangka penyisipan pesan rahasia pada video mp4. Penggunaan *Steganography* pada video dapat mempengaruhi kualitas video dengan menghasilkan sedikit perubahan yang terdapat pada video, tergantung dari metode yang digunakannya. Pada penelitian dan penulisan tesis ini, penulis mengusulkan metode *track free atom* yang digunakan untuk menyembunyikan pesan rahasia pada video. Metode *track free atom* merupakan metode penyisipan pesan pada hirarki *elements free* video mp4 yang penggunaannya mudah, cepat dan dapat menampung pesan rahasia dalam jumlah yang relatif banyak. Untuk meningkatkan keamanan pesan rahasia pada video dengan ditambahkan metode *One's Complement* pada *Cryptography*. Dengan menggunakan teknik gabungan *Cryptography* dan *Steganography,* pesan rahasia yang disisipkan pada video dapat lebih aman dan *stego video* yang dihasilkan tidak mengalami perubahan kualitas dibandingkan dengan *cover* videonya sehingga tidak menimbulkan kecurigaan bahwa ada pesan rahasia di dalam video, serta waktu yang dibutuhkan mulai dari penyisipan pesan ke dalam *cover video* sampai pengambilan pesan dari *stego video* relatif sangat cepat. Hasil analisis pengujian penyisipan pesan pada video mp4 menggunaan algoritma *track free atom* berhasil dilakukan dengan baik, bahkan tanpa mempengaruhi kualitas audio dan gambar yang ada didalamnya dikarenakan atom mdat yang digunakan untuk menyimpan sample audio dan gambar tidak dirubah. Ini menyebabkan nilai pengujian menggunakan PSNR adalah 100, APNSR adalah 100, MSE adalah 0, SSIM adalah 1, MSSSIM adalah 1, dan 3-Component SSIM INDEX adalah 1. Sehingga tidak ada perubahan kualitas antara video asli dengan video steganography.

Kata Kunci : steganography, cryptograpy,stego-video, video, one' complement,free atom, track

ABSTRACT

Steganography is the art and science which studies how confidential information hiding into a medium so that man can not be aware of the existence of the message. Concealment message on the video file is known as steganography video. In this paper, proposed a framework secret message insertion in video mp4. The use of steganography in video may affect the quality of the video by producing little changes contained in the video, depending on the method used. On the research and writing of this thesis, the authors propose a method of track free of atoms that used to hide secret messages in the video. Free track atom method is a method of inserting a message in the hierarchy of elements free mp4 video is easy to use, fast, and can hold a secret message in a relatively large amount. To enhance the security of confidential messages on the video with added methods One's Complement in Cryptography. By using the combined technique Cryptography and steganography, secret messages embedded in the video can be more secure and stego video produced unchanged quality compared to cover the video so as not to arouse suspicion that there is a secret message in the video, as well as the time it takes from the insertion of a message into the cover of the video until the retrieval of video stego relatively very fast. The results of the analysis of the video test message insertion algorithm uses track free mp4 atom successfully carried out properly, even without affecting audio quality and the included images due mdat atom that is used for storing audio samples and pictures are not changed. This led to testing using PSNR value is 100, APNSR is 100, MSE is 0, the SSIM is 1, MSSSIM is 1, and 3-Component SSIM INDEX is 1. So there is no change in quality between the original video with a video steganography.

Keywords: steganography, cryptography, stego-video, video, one 'complement, free atom, track

KATA PENGANTAR

Puji syukur penulis haturkan atas berkat rahmat Allah SWT. Yang Maha Pemurah Lagi Maha Penyayang, yang telah memberikan anugrah, rahmat serta hidayah-Nya kepada penulis, sehingga karena kuasa-Nya penulis dapat menyelesaikan tesis dengan judul "Model Keamanan Pesan Rahasia Pada Video Menggunakan Metode *One's Complement Cryptography* dan *Track Free Atom Steganography*". Tesis ini disusun dengan maksud untuk memenuhi salah satu persyaratan dalam memperoleh gelar Magister Komputer.

Dalam Penyusunan tesis ini, penulis menyampaikan terima kasih yang tulus kepada :

1. Bapak dan Ibu atas do'a, cinta dan dukunganya yang tak henti-hentinya diberikan.
2. Istri tercinta yang telah memberikan semangat dalam mengerjakan tesis.
3. Bapak Prof. Dr. Moedjiono, M.Sc, selaku Direktur Program Pascasarjana Universitas Budi Luhur.
4. Bapak Dr. Ir. Nazori AZ, M.T. selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur dan selaku pembimbing yang banyak membimbing dan memberi masukan dalam penyusunan tesis ini.
5. Bapak Mardi Hardjianto, M.Kom, yang tak henti-hentinya memberikan dukungan.
6. Seluruh Dosen Program Magister Ilmu Komputer Universitas Budi Luhur yang banyak memberikan ilmu selama perkuliahan.
7. Teman-teman, sahabat dan pihak-pihak lain yang tidak bisa penulis sebutkan satu persatu juga saya sampaikan terima kasih.

Penulis menyadari bahwa penulis tesis ini jauh dari sempurna. Untuk itu penulis berharap mendapatkan kritik dan saran yang dapat berguna untuk membangun demi kesempurnaan tulisan tesis ini.

Jakarta, Januari 2016

PUJIANTO

DAFTAR ISI

Halaman

ABSTRAK i
ABSTRACT ii
KATA PENGANTAR iii
DAFTAR ISI iv
DAFTAR GAMBAR vii
DAFTAR TABEL ix
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Masalah Penelitian 3
1.2.1 Identifikasi Masalah 3
1.2.2 Batasan Masalah 3
1.2.3 Rumusan Masalah 3
1.3 Tujuan dan Manfaat Penelitian 4
1.3.1 Tujuan Penelitian 4
1.3.2 Manfaat Penelitian 4
1.4 Sistematika Penulisan 4
1.5 Istilah 5
BAB II LANDASAN PEMIKIRAN 6
2.1 Tinjauan Pustaka 6
2.1.1 Steganografi 6
2.1.2 Cryptography 9
2.1.3 One's Complement 10
2.1.4 MPGEG-4 Part 14 (MP4) 11
2.1.5 Teknik Kompresi video mp4 14
2.1.6 *Peak Signal to Noise Ratio* (PSNR) 15
2.1.7 *Align Peak Signal to Noise Ratio* (APSNR) 16
2.1.8 *Structural Similiarity* (SSIM) 18
2.1.9 *Multi-Scale Structural Similiarity* (MSSSIM) 19
2.1.10 3-Component SSIM INDEX 20

2.2 Tinjauan Studi 21
2.3 Tinjauan Objek Penelitian 36
2.3.1 Perangkat *Hardware* 36
2.3.2 Perangkat Lunak 37
2.4 Kerangka Konsep 37
2.5 Hipotesis 38
BAB III METODOLOGI DAN RANCANGAN PENELITIAN 40
3.1 Metode Penelitian 40
3.1.1 Eksperiment: Masukan 40
3.1.2 Eksperiment: Proses 40
3.1.3 Eksperiment: Hasil Keluaran 40
3.2 Metode Pemilihan Sample 41
3.3 Metode pengumpulan data 41
3.4 Teknik Analisis, Rancangan, dan Pengujian 41
3.4.1 Analisis Proses dan Analisis Algoritma 42
3.4.2 Analisis Proses Pengujian 46
3.5 Langkah Penelitian 47
3.6 Jadwal Penelitian 49
BAB IV PEMBAHASAN HASIL PENELITIAN 51
4.1 Analisa Data 51
4.1.1 Struktur File 51
4.1.2 Penyisipan Pesan 53
4.1.3 Enkripsi pesan 54
4.1.4 Inkonsistensi Waktu 54
4.2 Rancangan Aplikasi 55
4.3 Implementasi Pengujian Algoritma 56
4.3.1 Pengujian *Objective* 57
4.3.2 Pengujian *Subjective* 67
4.4 Analisa Hasil Pengujian 69
4.5 Implikasi Penelitian 70
4.5.1 Aspek Sistem 70
4.5.2 Aspek Penelitian Lanjutan 71

4.6 Rencana Implementasi Pengujian 71
BAB V PENUTUP..... 74
5.1 Kesimpulan 74
5.2 Saran 75
5.3 Rencana Implementasi 76
DAFTAR PUSTAKA 77
LAMPIRAN-LAMPIRAN..... 81

DAFTAR GAMBAR

Gambar Halaman

II-1 Cryptography[Lenna 1997] 7
II-2 Steganography[Lenna 1997] 7
II-3 Encode dan Decode Steganografi 8
II-4 Encode Steganografi 8
II-5 Decode Staganografi 9
II-6 Encode dan Decode 10
II-7Struktur Atom Video MP4 secara keseluruhan 12
II-8 Struktur Atom secara umum 12
II-9 Struktur format atom file video mp4 pada file sampleMovie.m4v 13
II-10 Struktur format atom file video mp4 pada file monera.mp4 13
II-11 Urutan Frame pada video 15
II-12 Perubahan Ukuran Window di APNSR 17
II-13 Ilustrasi posisi frame yang hilang 18
II-14 Sistem Pengukuran Gambar dengan MSSSIM. L: low-pass filtering; 2 ↓: downsampling dengan 2[Wang et al. 2003] 19
II-15 Hasil Pengukuran dengan 3SSIM 20
II-16 Diagram untuk Kalkulasi 3-SSIM[Li and Bovik 2010] 21
II-17 Diagram Konsep Penelitian 38
III-1Flowchart One's Complement Encoding 42
III-2 Flowchart One's Complement Decoding 43
III-3Flowchart Proses Penyisipan Pesan pada file video mp4 45
III-4 Flowchart Menampilkan pesa dari stego video mp4 46
III-5 Diagram langkah penelitian 48
IV-1 Struktur Container Video mp4 51
IV-2Struktur File MP4 52
IV-3 :"Free" Atom 53
IV-4 Atom media data (mdat) 54
IV-5 Tampilan Layar Aplikasi Proses Penyisipan Pesan 55
IV-6 Tampilan Layar Aplikasi Proses Pembacaan Pesan 56

IV-7 Pengujian menggunakan PSNR 61
IV-8 Pengujian Menggunakan MSE 61
IV-9 Perhitungan Menggunakan APSNR 62
IV-10 Pengujian Menggunakan SSIM 63
IV-11 Pengujian Menggunakan MSSSIM 64
IV-12 Pengujian Menggunakan 3-Component SSIM INDEX 65
IV-13 Struktur file video sebelum penyisipan pesan 65
IV-14 Struktur file video sebelum penyisipan pesan 66
IV-15 Format Hexadecimal Sesudah Penyisipan 66
IV-16 Format Hexadecimal Sebelum Penyisipan 67
IV-17 Video Sebelum Penyisipan Pesan 68
IV-18 Video Sesudah Penyisipan Pesan 68
IV-19 Informasi Properti video sebelum(kanan) dan sesudah penyisipan pesan(kiri) 69

DAFTAR TABEL

Tabel Halaman

II-1 Tabel One's Complement 11
II-2 Rangkuman studi yang relevan mengenai steganografi pada media video.... 27
III-1 Sample teks uji 41
III-2Jadwal Penelitian 49
IV-1 Hasil Pengujian Video Steganografi dengan file Video yang berbeda 57
IV-2 Pengujian Steganografi Video Berdasarkan Ukuran Teks 58
IV-3 Pengujian Steganografi Video Berdasarkan Ukuran Video 59
IV-4 Hasil Pengujian Video Steganografi..... 69
IV-5 Perencaan Implementasi 71

DAFTAR PUSTAKA

[Adnan 2010] A.-A. G. Adnan, "Pixel Indicator Technique for RGB Image Steganography." *Journal of Emerging Technologies in Web Intelligence*, vol. 2, (2010): .

[Alfred 1996] M. Alfred, *Handbook of Applied Cryptography*. Massachussets: Massachussets Institute of Techology (MIT), 1996.

[Alwan 2013] W. hasan Alwan, "Dynamic least significant bit technique for video steganography." *Journal of Kerbala University*, vol. 11, no. 4, (2013): pp. 7–16.

[AN101 2014] A. N. AN101, *Elements of the H . 264 Video / AAC Audio*. Cimarron System, 2014.

[Andri et al. 2015] Andri, A. A. Lubis, et al., "Perancangan Aplikasi Steganografi Berbasis Matrix Pattern dengan Metode Random Blocks." *JSM STMIK Mikroskil*, vol. 16, no. 1, (Apr. 2015): .

[Bateman 2008] P. Bateman, "Images Steganography and Steganalysis." University of Surrey, 2008.

[Chan et al. 2010] A. Chan, K. Zeng, et al., "Metrics for Evaluating Video Streaming Quality in Lossy IEEE 802.11 Wireless Networks." *Proceedings IEEE INFOCOM*, (Mar. 2010): pp. 1–9.

[Cipher 2013] Cipher, "Codes and Ciphers," 2013. [Online]. Available: http://www.braingle.com/brainteasers/codes/caesar.php. [Accessed: 20-Oct-2015].

[Cruz et al. 2012] J. P. Cruz, N. J. Libatique, et al., "Steganography and data hiding in flash video (FLV)." *TENCON 2012 IEEE Region 10 Conference*, (2012): pp. 1–6.

[Divya and Mahesh 2014] K. P. Divya and K. Mahesh, "Random Image Embedded in Videos using LSB Insertion Algorithm." *International Journal of Engineering Trends and Technology (IJETT)*, vol. 13, no. 8, (Jul. 2014): pp. 381–385.

[Februariyanti 2010] H. Februariyanti, "Steganografi File Audio Mp3 menggunakan Mp3Stego." *Jurnal Teknologi Informasi DINAMIK*, vol. XV, no. 1, (Jan. 2010): pp. 57–65.

[Flores 1963] I. Flores, *The Logic Of Computer Arithmetic*, 1st ed. Amerika: PRENTICE-HALL, INC., 1963.

[Hapsari and Banowosari 2009] D. D. Hapsari and L. Y. Banowosari, "APLIKASI VIDEO STEGANOGRAPHY DENGAN METODE LEAST SIGNIFICANT BIT (LSB)." *Konferensi Nasional Sistem dan Informatika*, (Nov. 2009): pp. 118–124.

[Hari Rahmawanto and Atika Sari 2104] E. Hari Rahmawanto and C. Atika