Jurnal Teknologi Elektro, Universitas Mercu Buana
ISSN: 2086-9479

Pengamanan Dokumen Menggunakan Kriptografi RC4 dan Steganografi EOF dengan Media Video MP4 pada CV. Synergy Selaras

Syahputra Darmawan
Teknik Informatika Fakultas Teknologi Informasi
Universitas Budi Luhur
Jakarta, Indonesia
putradarmawan084@gmail.com

Imelda
Teknik Informatika Fakultas Teknologi Informasi
Universitas Budi Luhur
Jakarta, Indonesia
imelda@budiluhur.ac.id

***Abstrak*— Masalah keamanan dan kerahasiaan data proyek merupakan aspek yang sangat penting di perusahaan kontraktor. CV. Synergy Selaras merupakan perusahaan yang bergerak di bidang kontraktor. Perusahaan ini memiliki banyak dokumen yang bersifat rahasia seperti data proyek.Dokumen rahasia tidak boleh diketahui oleh pihak pihak luar karena dapat menimbulkan kerugian materi. Untuk mengamankan dokumen tersebut maka digunakan algoritma RC4 (*Rivest Code 4*) dan algoritma EOF (*End Of File*). Algoritma RC4 dipilih karena waktu prosesnya lebih cepat dibanding algoritma lain. Algoritma EOF dipilih karena tingkat keberhasilan menjalankan program sangat tinggi. Kontribusi paper ini adalah pengamanan dokumen menggunakan kriptografi RC4 dan steganografi EOF pada media video MP4. Ada 2 tahap yang digunakan pada pengamanan dokumen ini:*Embed* dan *Retrieve*. Tahapan *Embed* yang dilakukan adalah dokumen dienkripsi dengan RC4 lalu dokumen itu disisipkan ke video MP4 dengan algoritma EOF. Tahapan *Retrieve* yang dilakukan adalah video MP4 yang berisi dokumen di-*retrieve* menggunakan EOF lalu didekrip menggunakan RC4. Dari 30 data pengujian, tingkat keberhasilan tahap *Embed* dan tahap *Retrieve* mencapai 100% dengan waktu proses rata-rata 0,86 detik untuk *Embed* dan 2,61 detik untuk *Retrieve*.**

Kata Kunci*— *Kriptografi Rivest Code; MP4; Steganografi End Of File.

I. PENDAHULUAN

CV. Synergy Selaras adalah perusahaan yang bergerak di bidang jasa kontraktor. Banyak dokumen yang bersifat rahasia dan tidak bisa diubah oleh pihak yang tidak bertanggung jawab contohnya dokumen data proyek. Oleh karena itu, pengguna dokumen membutuhkan bantuan untuk keamanan akan dokumen yang disimpannya Untuk mengamankan dokumen maka digunakan algoritma RC4 (*Rivest Code 4*) dan algoritma EOF (*End Of File*). Algoritma RC4 merupakan salah satu metode kriptografi. Sedangkan algoritma EOF merupakan salah satu metode steganografi. Penerapan kriptografi pada CV. Synergy Selaras akan difokuskan bagaimana kriptografi dapat mengamankan dokumen yang tersimpan sehingga dokumen hanya dapat dibuka oleh pihak yang berhak untuk membukanya [1]. Penerapan steganografi difokuskan bagaimana dokumen disisipkan kedalam suatu media video agar fisik dari dokumen penting tersebut tidak terlihat, tanpa merusak media video yang disisipi data penting tersebut.

II. PENELITIAN TERKAIT

Banyak penelitian yang telah dilakukan untuk mengamankan data. Salah satu cara mengamankan data menggunakan kriptografi. Ada peneliti yang telah membandingkan algoritma RC4 dengan algoritma Affine Cipher. Hasilnya waktu proses dengan algoritmaRC4 untuk enkripsi dan dekripsi lebih cepat dibanding menggunakan algoritma Affine Cipher[1]. Peneliti lain menggunakan RC4 untuk *obfuscation source code* PHP sebagai sarana untuk menjaga keamanan hak cipta dan kerahasiaan *source code* program. Waktu eksekusi file PHP yang terobfuskasi cenderung lebih lama dibanding file *source code* asli dengan persentase 199,8658% [2].

Penelitian tentang steganografi telah banyak dilakukan. Ada yang menggunakan algoritma LSB (Least Significant Bit) [3][4][5], DCT (Discrete Cosine Transform) [5], LBE (Low-Bit Encoding) [6], dan EOF (End of File) [6][7]. Ada penelitian tentang steganografi yang membandingkan antara algoritma LBE dengan algoritma EOF. Penelitiannya menggunakan media audio wave. Bila menggunakan algoritma LBE, ukuran data yang disisipkan tidak dapat melebihi ukuran audio wave. Bila menggunakan algoritma EOF, ukuran data yang disisipkan dapat melebihi ukuran file audio wave [5]. Ada pula penelitian yang membandingkan

antara algoritma LSB dengan algoritma DCT. Penelitiannya menggunakan media video. Hasil pengujian steganografi video dengan algoritma LSB adalah 38%, algoritma DCT adalah 90%, dan gabungan algoritma LSB-DCT adalah 64% [5]. Penelitian penyembunyian data pada media video memberi inspirasi untuk membuat penelitian sejenis. Kontribusi paper ini adalah mengimplementasikan kriptografi RC4 dan steganografi EOF pada media video MP4.

III. PENGAMANAN DOKUMEN MENGGUNAKAN KRIPTOGRAFI RC4 DAN STEGANOGRAFI EOF DENGAN MEDIA VIDEO MP4

Pengamanan dokumen pada CV. Synergy Selaras menggunakan kriptografi dengan algoritma RC4 dan steganografi dengan algoritma EOF. Ada 2 tahap yang digunakan pada pengamanan dokumen ini : *Embed* dan *Retrieve*. Tahapan *Embed* yang dilakukan adalah dokumen dienkripsi dengan RC4 lalu dokumen itu disisipkan ke video MP4 dengan algoritma EOF. Tahapan *Retrieve* yang dilakukan adalah video MP4 yang berisi dokumen di-*retrieve* menggunakan EOF lalu didekrip menggunakan RC4.

A. *Kriptografi RC4*

Semua tabel diberi nomor berdasarkan urutannya (contoh: Tabel 1; Tabel 2 ; dst..). Setiap tabel harus diberi judul dan diletakkan di atas tabel. Ukuran font judul tabel serta isi tabel adalah 10. Contoh table dapat dilihat pada Tabel 1.

RC4 merupakan salah satu kriptografi simetris. Kriptografi simetris memiliki kelebihan proses enkripsi dan dekripsi yang cepat. Ini karena kunci untuk enkripsi dan dekripsinya sama [8]. Pemilihan kriptografi dengan algoritma RC4 karena waktu prosesnya lebih cepat dibanding dengan algoritma Affine Cipher [1]. Langkah-langkah algoritma enkripsi RC4 adalah sebagai berikut [1] :

- *Inisialisasi array S-box pertama, S[0],S[1],...,S[255], diisi dengan bilangan 0 sampai 255, sehingga array S-box array S berbentuk S[0] = 0, S[1] = 1,...,S[255] = 255.*

  For r = 0 to 255

  S[r] = r

- *Inisialisasi array kunci (S-box lain), misal array kunci K dengan panjang 256. Jika panjang kunci K < 256, maka dilakukan padding yaitu penambahan byte semua sehingga panjang kunci menjadi 256 byte. Misalnya K = "abc" yang hanya terdiri 3 byte (3 huruf), maka lakukan padding dengan 86 penambahan byte (huruf) semu, misalnya K = "abcabcabc…" sampai panjang K mencapai 256 byte, sehingga S-box Array kunci K berbentuk K[0], K[1],...,K[255].*

  for i = 0 to 255

  K[i] = Kunci[i mod length];

- *Permutasi terhadap nilai-nilai di dalam array S dengan cara menukarkan isi array S[I] dengan S[j], prosesnya adalah sebagai berikut:*

  j = 0

  For i = 0 to 255

  j = (j + S[i] + K[i]) mod 256

  isi S[i] dan isi S[j] ditukar

- *Membangkitkan aliran kunci (key stream) selanjutnya digunakan untuk enkripsi.*

  i = j = 0

  i = (i + 1) mod 256

  j = (j + S[i]) mod 256

  isi S[i] dan S[j] ditukar

  t = (S[i] + S[j]) mod 256

  K=S[t];

  Proses pembangkitan aliran kunci K dipilih dengan mengambil nilai S[i] dan S[j] dan menjumlahkannya dalam *modulo* 256. Hasil penjumlahan adalah nilai indeks t sedemikian sehingga S[t] menjadi kunci aliran K.

- *Kunci aliran K kemudian digunakan untuk mengenkripsi plaintext ke-idx sehingga didapatkan ciphertext, sedangkan untuk mendapatkan plaintext dengan cara ciphertext di-XOR-kan dengan kunci yang sama dengan proses enkripsi.*

Algoritma dekripsi RC4 mirip dengan algoritma enkripsinya, perbedaannya hanya pada saat *stream generation,* yaitu untuk menghasilkan *plainteks* semula, maka *ciphertext* nya akan dikenakan operasi XOR terhadap *pseudorandom* bytenya. Algoritma *key setup* pada proses dekripsi sama dengan algoritma enkripsinya yang diproses inisialisasi *S-Box,* penyimpanan kunci kedalam key byte array hingga proses inisialisasi *S-Box* berdasarkan *key byte array* nya. Untuk itu proses dekripsi dan enkripsi akan menghasilkan *key stream* yang sama. Perbedaannya hanya pada *stream* generationnya, yaitu yang dioperasikan bersama *key stream* adalah *ciphertext* untuk menghasilkan kembali *plaintext.* Langkah-langkah algoritmanya adalah sebagai berikut [1] :

- *Isi indeks i dan j dengan nilai 0*
- *Untuk i=0 hingga i=panjang ciphertext (panjang ciphertext = plaintext)*
- *Isi nilai i dengan hasil operasi (i+1) mod 256*
- *Isi nilai j dengan hasil operasi (j+S(i)) mod 256*
- *Tukar nilai S(i) dan S(j)*
- *Isi nilai t dengan hasil operasi (S(i)+(S(j) mod 256)) mod 256*
- *Isi nilai y dengan nilai S(t)*
- *Nilai y dikenakan operasi XOR terhadap ciphertext*
- *Tambahkan i dengan 1, kembali ke 2*

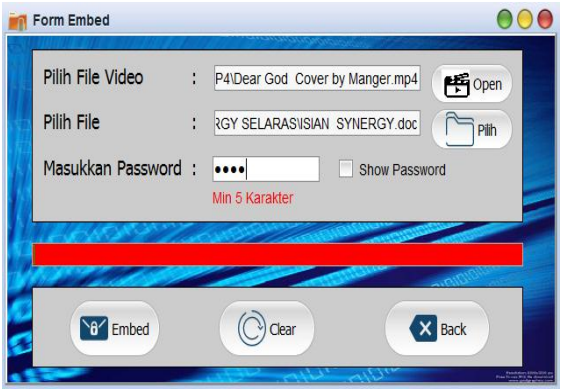
B. Steganografi EOF

Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Pesan tersebut hanya disembunyikan ke dalam suatu media berupa gambar, teks, musik, atau media digital lainnya dan terlihat seperti pesan biasa [7]. Teknik EOF atau *End Of File* merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini digunakan dengan cara menambahkan data atau pesan rahasia pada akhir dokumen. Teknik ini dapat digunakan untuk menambahkan data yang ukurannya sesuai dengan kebutuhan. Perhitungan kasar ukuran dokumen yang telah disisipkan data sama dengan ukuran dokumen sebelum disisipkan data ditambah ukuran data rahasia yang telah diubah menjadi encoding file [7].

IV. HASIL DAN ANALISA

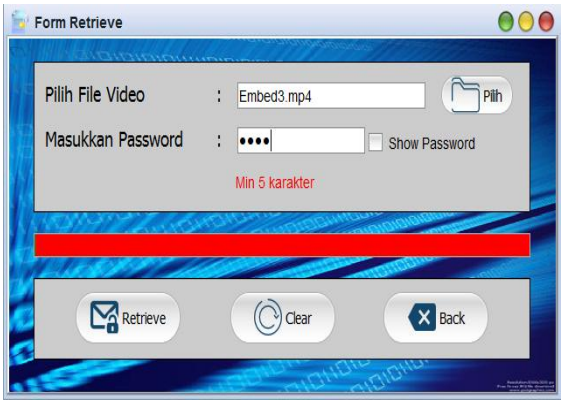
A. Hasil

Implementasi pengamanan dokumen ini memiliki dua tahap utama. Pertama, tahap *Embed*. Kedua, tahap *Retrieve*. Pada tahap *Embed*, pertama user perlu mempersiapkan dokumen dan video. Kemudian usermemilih video lalu memilih dokumen yang akan di sisipkan ke video. Setelah itu user memasukan *password* minimal 5 karakter lalu tekan tombol *embed* untuk menjalankan proses *embed*, seperti Gambar 1. Hasil *embed* adalah video yang di-*embed* atau disebut juga video stego.



Gambar 1. Tahap Embed

Tahap Retrieve dilakukan apabila *user* ingin melakukan *retrieve* atau pengembalian dokumen yang telah di-*embed*. Tahap *retrieve* dimulai dari pemilihan *video stego* yang ingin di-*retrieve*. Setelah memilih *video stego*, kemudian *user* meng-*input password* yang sama dengan password yang digunakan pada tahap embed, seperti Gambar 2. Hasilnya adalah dokumen hasil *retrieve*.



Gambar 2 Tahap Retrieve

B. Pengujian

Pengujian dilakukan pada tahap *embed* dan tahap *retrieve*. Tujuan pengujian pengamanan dokumen pada tahap *embed* untuk memastikan bahwa dokumen berhasil disisipkan ke video MP4. Tujuan pengujian pengamanan dokumen pada tahap *retrieve* untuk memastikan bahwa proses pengembalian dokumen berhasil. Format dokumen yang diuji adalah .doc, docx, .xls, .xlsx.

Spesifikasi *hardware* yang digunakan saat pengujian adalah sebagai berikut:.

- *Processor* : Intel(R) Core(TM) i5CPU M 450 @ 2.40 GHz (4 CPUs),~2.4GHz
- *RAM : 4 GB*
- *Harddisk : 300 GB*
- *Monitor : 14.0"*
- *Mouse : USB Mouse*
- *Keyboard : Internal Keyboard Laptop*

Spesifikasi *software* yang digunakan saat pengujian adalah sebagai berikut:.

- Sistem Operasi : Windows 7 Ultimate 64-bit
- Bahasa Pemprograman : Java Desktop
- Editor : Netbeans IDE 8.0.2
- Database : MySQL Front 5.3

C. Pengujian Tahap Embed

Tabel 1 menunjukkan bahwa contoh beberapa hasil pengujian tahap Embed. Pengujian tahap Embed dilakukan pada 30 dokumen dan 30 video mp4. Dokumen yang diuji terdiri dari 15 dokumen yang berekstensi .doc, .docx, dan 15 dokumen yang berekstensi .xls, .xlsx. Tabel 1 memperlihatkan 7 dari 30 pengujian yang telah dilakukan. Tabel 1 berisi nama video, ukuran video, nama dokumen, ukuran dokumen, ukuran video hasil embed, waktu proses embed, status. Ukuran video yang telah di embed lebih besar dari ukuran video asli. Ini karena sudah ada tambahan dokumen didalamnya. Namun perbedaannya sangat kecil. Dari 30 data pengujian, tingkat keberhasilannya mencapai 100% dengan waktu proses rata-rata 0,86 detik.

Tabel 1. Hasil pengujian tahap Embed

No	Nama Video	Ukuran Video	Nama dokumen	Ukuran dokumen	Ukuran Video Hasil *Embed*	Waktu Proses *Embed* (detik)	Status
1	Avenged Sevenfold - Afterlife [Live].MP4	19.46 MB	01.Data Proyek FG 2016 fix..xlsx	344 KB	20,38 MB	0.71	BERHASIL
2	Cassandra - Cinta Terbaik (Official Video).MP4	20.99 MB	FORMULIR ISIAN KUALIFIKASI.docx	48 KB	21.11 MB	0.48	BERHASIL
3	Dear God Cover by Manger.MP4	18.80 MB	ISIAN SYNERGY.doc	254 KB	19.48 MB	0.66	BERHASIL
4	Asking Alexandria _A Prophecy.mp4	18.09 MB	dokumen kualifikasi kontruksi.doc	332 KB	18.97 MB	0.64	BERHASIL
5	Bat Country (Official Music Video).mp4	34.53 MB	List material.xls	35 KB	34.63 MB	0.69	BERHASIL
6	Delon - Indonesia Jaya.mp4	11.23 MB	SURAT PERJANJIAN KONTRAK KERJA BANGUN RUMAH.doc	46 KB	11.35 MB	0.38	BERHASIL
7	Dewa 19 – Kangen.mp4	12.80 MB	Schedule.xls	21 KB	12.86 MB	0.2	BERHASIL

D. Pengujian Tahap Retrieve

Tabel 2 menunjukkan bahwa hasil pengujian tahap *Retrieve*. Pengujian tahap *Retrieve* dilakukan pada 30 dokumen dan 30 video mp4. Input dokumen tahap *Retrieve* adalah 30 video mp4 yang telah di embed. Tabel 2 memperlihatkan 7 dari 30 pengujian yang telah dilakukan. Tabel 2 berisi nama video stego, ukuran video stego, nama dokumen hasil retrieve, ukuran dokumen asli, ukuran dokumen hasil retrieve, waktu proses retrieve, status. Dari hasil pengujian terlihat ukuran dokumen asli sama dengan ukuran dokumen hasil retrieve. Dari 30 data pengujian, tingkat keberhasilannya mencapai 100% dengan waktu proses rata-rata 2,61 detik.

Tabel 1. Hasil pengujian tahap *Retrieve*

No	Nama Video *Stego*	Ukuran Video *Stego*	Nama Dokumen	Ukuran Dokumen	Ukuran Dokumen Hasil *Retrieve*	Waktu Proses *Retrieve* (detik)	Status
1	Embed1	20.38 MB	01.Data Proyek FG 2016 fix.xlsx	344 KB	344 KB	2.04	BERHASIL
2	Embed2	21.11 MB	FORMULIR ISIAN KUALIFIKASI.docx	48 KB	48 KB	1.87	BERHASIL
3	Embed3	19.48 MB	ISIAN SYNERGY.doc	190 KB	190 KB	2.26	BERHASIL
4	Embed4	18.09 MB	dokumen kualifikasi kontruksi.doc	332 KB	332 KB	2.07	BERHASIL
5	Embed5	34.53 MB	List material.xls	35 KB	35 KB	3.28	BERHASIL
6	Embed6	11.35 MB	SURAT PERJANJIAN KONTRAK KERJA BANGUN RUMAH.doc	46 KB	46 KB	1.18	BERHASIL
7	Embed7	12.38 MB	Schedule.xls	21 KB	21 KB	2.03	BERHASIL

E. Analisa

Tujuan Analisa untuk mengetahui kelebihan dan kekurangan aplikasi yang telah diimplementasi. Dalam analisa ini ditemukan beberapa kelebihan dan kekurangannya antara lain:

F. Kelebihan Aplikasi

- Video mp4 yang di-*embed* tetap sama seperti video mp4 biasa.
- Dokumen yang sudah di-embed dapat dikembalikan secara utuh tanpa mengalami perubahan ukuran dan bentuk.
- Secara penglihatan manusia, dokumen tidak akan terdeteksi bahwa ada dokumen rahasia di dalam video mp4.

G. Kekurangan Aplikasi

- Ukuran video hanya dibatasi sampai 60 MB.
- Media penampung data yang digunakan hanya video dengan ekstensi *.mp4.
- Dokumen yang dapat digunakan hanya berupa file*.docx, *.doc, *.xls, *xlsx.

V. KESIMPULAN

Adapun simpulan berdasarkan penelitian yang telah dilakukan adalah sebagai berikut:

- Pengamanan dokumen dengan kriptografi menggunakan metode Rivest Code 4 (RC4) dan steganografi menggunakan metode End Of File (EOF) telah berhasil diimplementasikan. Dengan demikian dokumen penting yang ada di CV. Synergy Selaras lebih aman kerahasiaannya dari orang-orang yang tidak bertanggung jawab.
- Pada tahap *Embed*, video MP4 yang telah disisipi dokumen masih dapat dipergunakan seperti biasa.
- Pada tahap *Retrieve*, dokumen yang telah di-embed dapat dikembalikan seperti semula menggunakan Steganografi EOF dan KriptografiRC4 menjadi data yang orisinil tanpa mengalami perubahan sedikitpun.

Pada penelitian selanjutnya diharapkan dapat dilakukan juga untuk video, audio maupun citra. Selain itu penelitian selanjutnya diharapkan dapat digabung dengan metode kompresi sehingga dapat memperkecil ukuran videonya.

Ucapan Terima Kasih

Ucapan terima kasih diberikan kepada Yayasan Budi Luhur Cakti yang telah memberikan dukungan sehingga tulisan ini dapat dipublikasikan.

Daftar Pustaka

[1] Agung, H., Budiman. 2015. Implementasi Affine Cipher Dan RC4 Enkripsi File Tunggal. Seminar Nasional Teknologi dan Informatika (SNATIF) Ke - 2, Kudus, hal. 243.

[2] Setiawan, O., Fiati, R., dan Listyorini, T. 2014. Algoritma Enkripsi RC4 Sebagai Metode Obfuscation Source Code PHP. Seminar Nasional Teknologi dan Informatika (SNATIF) Ke -1, Kudus, hal. 117.

[3] Cahyadi, T. 2012. Implementasi Steganografi LSB dengan Enkripsi Vigenere Cipher Pada Citra JPEG. TRANSIENT, 4(1), Semarang, hal. 282-283.

[4] Lovebbi, Sudirman, Z.D., 2012, Rancang Bangun Aplikasi Steganografi dengan Metode Least Significant Bit di Audio pada Sistem Operasi Android, ULTIMATICS,1(4), Tangerang, hal.7-10.

[5] Yunus, M.,Harjoko, A.,2014. Penyembunyian Data pada *file* video Menggunakan Metode LSB dan DCT. Jurnal Ilmu Komputer, Vol 8 Januari 2014, pp 81-90.

[6] Kurniawan, I., 2013. Implementasi dan Studi Perbandingan Steganografi pada File Audio WAVE Menggunakan Teknik Low-Bit Encoding dengan Teknik End Of File. Journal of Informatics and Technology, 3(2), Semarang, p.1-12.

[7] Wasino, Rahayu P. T., dan Setiawan. 2012. Implementasi Steganografi Teknik End Of File dengan Enkripsi Rijndael. Seminar Nasional Teknologi Informasi dan Komunikasi 2012 (SENTIKA 2012) Yogyakarta, 10 Maret 2012, hal. 151.

[8] Nugroho, D. A. 2014. Penggabungan Algoritma Kriptograi Simetris dan Kriptografi Asimetris untuk Pengamanan Pesan. Kriptografi, Bandung, hal. 1-3.