PENGAMANAN DATA MENGGUNAKAN KRIPTOGRAFI ALGORITMA *RIVERST SHAMIR ADLEMAN* DAN STEGANOGRAFI METODE *END OF FILE* DENGAN MEDIA 3GP

Agung Setia Pambudi[1)], Imelda[2)]
[1,2]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : agungsetiapambudi@gmail.com[1)], imelda@budiluhur.ac.id[2)]

Abstract

Document Companies must be safeguarded from unauthorized parties to access, especially confidential information. This happens because a lot of wiretapping, theft or destruction of data by parties who are not responsible. To solve that problem, then made securing data using cryptographic algorithms Rivest Shamir Adleman (RSA) and steganography method End Of File (EOF) in the video media. With cryptography will change the contents of the original data files into file contents can not be read by others, and through steganography file will be inserted into the video media which will create files to be more secure and not be detected by others and eventually be able to restore files the original data intact without changes in the contents of the file. This application is made to the National Land Agency in the form of a message using the document file (.xlsx, * .xls) and media data container in the form of videos (.3gp). This application can make the data more secure in sending the message information as confidential documents undetectable human vision and does not attract the attention of others. RSA cryptography is quite good because it uses factoring large numbers into prime factors so that unauthorized parties are not easy to decode if it does not have the key. Steganography EOF chosen because it can insert its data file size larger than the size of the video. Of the 20 test data obtained an average processing time of 21:45 seconds.*

Keywords*: cryptography, Rivest Shamir Adleman, Steganography, End Of File, 3gp*

Abstrak

*Dokumen perusahaan harus dijaga keamanannya dari pihak yang tidak berhak untuk mengaksesnya, terutama informasi yang bersifat rahasia. Ini terjadi karena banyak penyadapan, pencurian data ataupun perusakan data oleh pihak yang tidak bertanggung jawab. Untuk mengatasi masalah itu, maka dibuatlah pengamanan data menggunakan kriptografi algoritma Rivest Shamir Adleman (RSA) dan steganografi metode End Of File (EOF) pada media video. Dengan kriptografi nantinya akan mengubah isi file data asli menjadi isi file yang tidak dapat dibaca oleh orang lain, dan melalui steganografi file tersebut akan disisipkan ke dalam media video yang nantinya akan membuat file menjadi lebih aman dan tidak terdeteksi oleh orang lain dan nantinya dapat mengembalikan file data asli secara utuh tanpa mengalami perubahan di dalam isi file. Aplikasi ini dibuat untuk Badan Pertanahan Nasional menggunakan dokumen pesan berupa file (*xlsx, *.xls) dan media penampung data berupa video (.3gp). Aplikasi ini dapat membuat data menjadi lebih aman dalam berkirim pesan informasi karena dokumen rahasia tidak terdeteksi secara penglihatan manusia dan tidak menarik perhatian pihak lain. Kriptografi RSA cukup baik karena menggunakan pemfaktoran bilangan yang besar menjadi faktor-faktor prima sehingga pihak yang tidak berhak tidak mudah men-decode jika tidak memiliki kuncinya. Steganografi EOF dipilih karena dapat menyisipkan file yang ukuran datanya lebih besar dari ukuran video. Dari 20 data pengujian diperoleh waktu proses rata-rata 21.45 detik.*

Kata Kunci : *Kriptografi, Rivest Shamir Adleman, Steganografi, End Of File, 3gp*

1. PENDAHULUAN

Kementrian Agraria dan Tata Ruang Atau Badan Pertanahan Nasional merupakan suatu perusahaan negara yang bergerak di bidang pertanahan dan perkebunan. Dokumen-dokumen penting dan sangat rahasia pada perusahaan harus terjaga keamanannya dari pihak yang tidak berhak untuk mengaksesnya. Oleh karena itu perlu dilakukan pengamanan terhadap dokumen yang tersimpan sampai dokumen tersebut dapat diakses oleh pihak yang berhak mengaksesnya. Pada paper ini, untuk mengamankan dokumen-dokumen tersebut maka dibuatlah pengamanan data menggunakan algoritma RSA dan EOF dengan media 3gp yang membahas mengenai bagaimana menyisipkan suatu dokumen yang telah dienkripsi ke dalam sebuah media berupa video pada aplikasi kriptografi dan steganografi di Kementrian Agraria dan Tata Ruang Atau Badan Pertanahan Nasional.

Beberapa peneliti telah menggunakan pengamanan data menggunakan **metode steganografi. Ada yang menggunakan steganografi dengan metode LSB** sebagai sarana

kampanye, pengumuman, komunikasi organisasi. Penelitian ini menyisipkan pesan rahasia ke dalam file audio **mp3 [1]**. Ada pula yang menggunakan steganografi LSB untuk menyamarkan eksistensi (keberadaan) data rahasia sehingga sulit dideteksi [2].

Beberapa peneliti lain menggunakan algoritma RSA. Peneliti berhasil mengenkripsi file teks yang panjang karakternya tidak lebih dari 1000 karakter [3]. Peneliti lain berhasil meningkatkan pemanfaatan layanan e-mail melalui internet dengan cara mengenkripsi pesan yang akan dikirim menggunakan kunci publik yang telah dibangkitkan oleh pihak pengirim [4]. Peneliti lainnya berhasil membuat aplikasi untuk keamanan komunikasi yang sangat penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata sehingga keberadaan data tersebut tidak dapat diketahui [5].

Namun belum ada yang membahas pengamanan data menggunakan kriptografi dengan algoritma RSA dan steganografi dengan algoritma EOF pada media 3gp. Oleh karena itu, kontribusi paper ini adalah pengamanan data menggunakan kriptografi RSA dan steganografi EOF dengan media 3gp pada Kementerian Agraria dan Tata Ruang atau Badan Pertanahan Nasional.

2. LANDASAN TEORI

2.1 Kriptografi RSA

Kriptografi dipilih untuk pengamanan data karena dapat menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi RSA cukup baik karena menggunakan pemfaktoran bilangan yang besar menjadi faktor-faktor prima sehingga pihak yang tidak berhak tidak mudah men-decode jika tidak memiliki kuncinya. Kriptografi RSA termasuk *asymmetric* karena memiliki kunci publik dan kunci privat. Saat enkripsi digunakan kunci publik karena semua orang boleh mengetahui kuncinya, namun hanya orang tertentu yang dapat melakukan dekripsi terhadap pesan tersebut menggunakan kunci privat [1].

2.2 Perhitungan Algoritma RSA

Proses pembangkitan kunci, proses enkripsi pesan, dan proses dekripsi pesan dalam penggunaan algoritma RSA dapat dilihat sebagai berikut :

Pilih dua buah bilangan prima secara *random* yakni p=**19** dan q=**41**.

Hitung n = p.q = 19x41 = **779**.

Hitung phi(n) = (p-1)(q-1) = (19-1)(41-1) = **720**.

Kemudian bangkitkan kunci publik (e), dimana nilai e relatif prima terhadap phi(n). Nilai GCD(phi(n), e) harus bernilai 1. Untuk menentukan nilai kunci publik (e) yang relatif prima terhadap phi(n) ditunjukkan pada perhitungan dibawah ini:

Tabel 1 : Perhitungan Kunci Publik[2]

Mulai dari	Nilai GCD(phi(n), e)
e = 2	720 mod 2 = 0 GCD(720, 2) = 2
e = 3	720 mod 3 = 0 GCD(720, 3) = 3
e = 4	720 mod 4 = 0 GCD(720, 4) = 4
e = 5	720 mod 5 = 0 GCD(720, 5) = 5
e = 6	720 mod 6 = 0 GCD(720, 6) = 6
e = 7	720 mod 7 = 6 7 mod 6 = 1 6 mod 1 = 0 **GCD(720, 7) = 1**

Jadi, nilai dari kunci publik (e) yang diperoleh adalah **7**.

Hitung kunci privat (d) dengan menggunakan pesamaan d = (1+k.phi(n))/e. Nilai k dapat dihitung dengan mencoba nilai-nilai = 1,2,3,4…. sehingga diperoleh nilai d bilangan bulat.

Tabel 2 : Perhitungan Kunci Privat[2]

Nilai k	d = (1+k.phi(n))/e	Hasil
1	d = (1+1.720)/7	**103**
2	d = (1+2.720)/7	205,85
3	d = (1+3.720)/7	308,71
4	d = (1+4.720)/7	411,57

Jadi, nilai dari kunci privat (d) yang diperoleh adalah **103**.

Pesan yang akan dikirim adalah P = **AGUNG** atau dalam *decimal* (kode ASCII) adalah **65 71 85 78 71**. Sebelumnya telah diketahui kunci publik adalah n = **779** dan e = **7**. Maka pesan P dapat dienkripsikan dengan rumus $C_i = P_i^e \bmod n$ sebagai berikut :

$C_1 = 65^7 \bmod 779 = 274$
$C_2 = 71^7 \bmod 779 = 744$
$C_3 = 85^7 \bmod 779 = 137$
$C_4 = 78^7 \bmod 779 = 508$
$C_5 = 71^7 \bmod 779 = 744$

Sehingga *ciphertext* yang dihasilkan adalah **274 744 137 508 744**.

Selanjutnya pesan yang terenkripsi tersebut dikirim ke penerima pesan, yang mana telah memiliki kunci privat n = **779** dan d = **103**. Maka *ciphertext* dapat didekripsikan dengan rumus $P_i = C_i^d \bmod n$ sebagai berikut :

$P_1 = 274^{103} \bmod 779 = 65$
$P_2 = 744^{103} \bmod 779 = 71$
$P_3 = 137^{103} \bmod 779 = 85$
$P_4 = 508^{103} \bmod 779 = 78$
$P_5 = 744^{103} \bmod 779 = 71$

Sehingga akan dihasilkan kembali pesan P = **65 71 85 78 71**, yang dalam pengkodean ASCII dapat dibaca P = **AGUNG**.

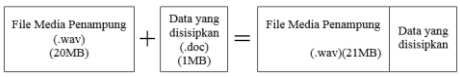
2.3 Steganografi

Steganografi *(steganography)* adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Jika kriptografi merahasiakan makna pesan sementara eksistensi pesan tetap ada, maka steganografi menutupi

keberadaaan pesan. Steganografi dapat dipandang sebagai kelanjutan kriptografi dan dalam prakteknya pesan rahasia dienkripsi terlebih dahulu, kemudian *ciphertext* disembunyikan di dalam media lain sehingga pihak ketiga tidak menyadari keberadaannya. Pesan rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti aslinya.[3]

2.4 Metode EOF

Metode ini disebut dengan teknik EOF karena teknik ini menyisipkan data pada akhir *file* media penampung. Teknik ini dapat dikatakan sebagai metode *injection*, dimana teknik ini memasukkan secara langsung data di dalam *file* media penampung. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran *file* yang telah disisipkan data sama dengan ukuran *file* sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam *file* tersebut. Dalam teknik ini, data disisipkan pada akhir *file* dengan diberi tanda khusus sebagai pengenal *start* dari data tersebut dan pengenal akhir dari data tersebut.



Gambar 1 : Teknik End Of File[4]

2.5 Penyembunyian Data

Berikut adalah langkah-langkah metode *End Of File* dalam menyembunyikan sebuah data[5] :

a. Baca penanda akhir *(End Of File)* dari *file* penampung.
b. Sisipkan sebuah *file* setelah penanda *End Of File* dari *file* penampung dengan diberikan penanda awal dan penanda akhir dari *file* yang akan disembunyikan.
c. *File* penampung yang telah disisipkan data di petakan menjadi sebuah *file (stego file)*.

2.6 Pengekstraksan Data

Berikut adalah tahapan dalam melakukan proses pengekstraksan data [5]:

a. Baca penanda EOF *file* penampung.
b. Ambil data yang terletak setelah penanda EOF *file* penampung.
c. Buang penanda awal dan penanda akhir sehingga menyisakan data rahasia yang masih terenkripsi.

2.7 Media Video 3gp

Video merupakan sebuah film atau gambar hidup yang dihasilkan dengan rekaman dari orang dan benda (termasuk fantasi dan figure palsu) dengan menggunakan kamera, dan memiiki fungsi dua dimensi yang terbentuk dari penglihatan dalam suatu tempat (scene) yang merupakan basis dari pembentukan video. Walaupun jenis kompresi yang lainnya beberapa memiliki kualitas yang lebih baik, namun 3gp belum dapat tersaingi hingga saat ini [6]. Maka dari itu penggunaan 3gp sebagai salah satu media steganografi merupakan langkah yang baik. Lalu lintas pertukaran 3gp di internet merupakan hal biasa sehingga steganografi menggunakan 3gp adalah teknik yang baik untuk mengamankan pesan rahasia melalui media internet.

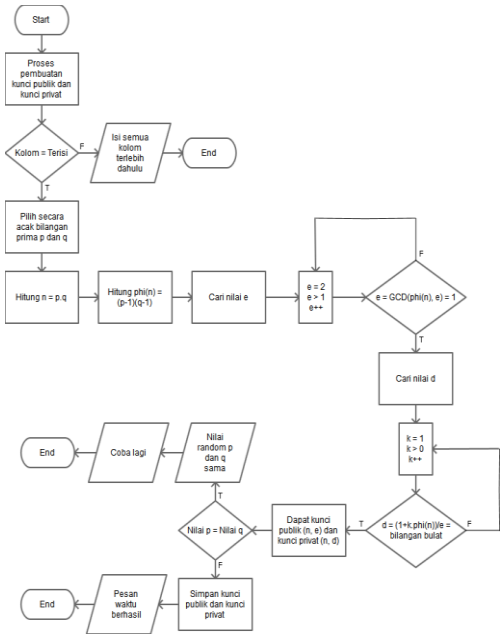
3. ANALISA DAN PERANCANGAN APLIKASI

3.1 Proses Aplikasi

Tahap awalnya harus membuat kunci publik dan kunci privatnya terlebih dahulu, dengan kunci publik *file* akan dienkripsi menjadi *file* berisi *ciphertext*, kemudian hasil enkripsi akan disisipkan atau di-*encode* ke dalam media audio dan diberi penanda khusus sebagai batas penampung audio dan *file* hasil enkripsi, lalu *output*-nya adalah *stego object* berupa audio yang di dalamnya sudah berisi *file* hasil enkripsi yang nantinya akan dikembalikan lagi melalui proses *decode* dengan membaca penanda khusus sebagai batas *file* hasil enkripsi lalu akan didekripsi dengan kunci privat sehingga kembali menjadi *file* data asli.

3.2 Flowchart Key

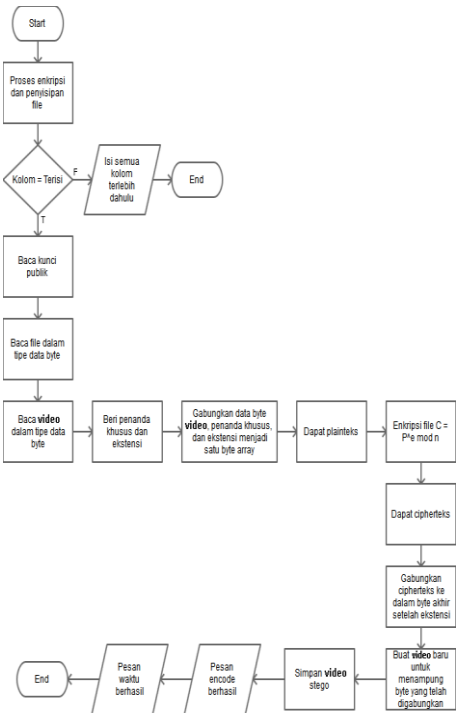
Proses untuk membuat kunci publik dan kunci privat.



Gambar 2 : Flowchart Key

3.3 Flowchart Encode

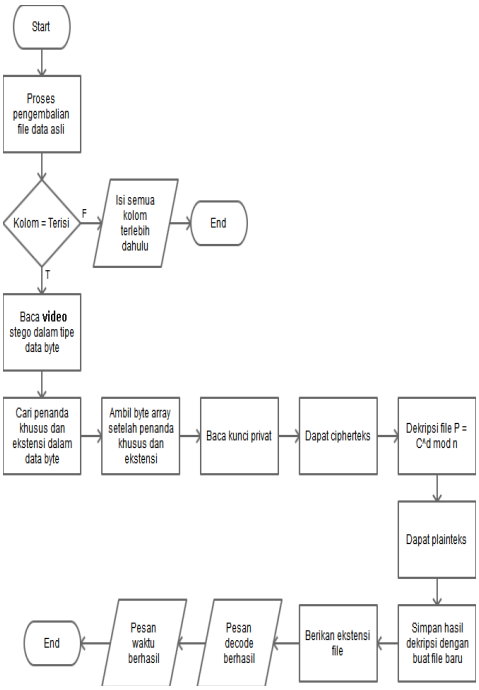
Proses untuk steganografi dan kriptografi-nya.



Gambar 3 : Flowchart Encode

3.4 Flowchart Decode

Flowhart decode merupakan proses untuk mengeluarkan isi *file* dari 3gp.



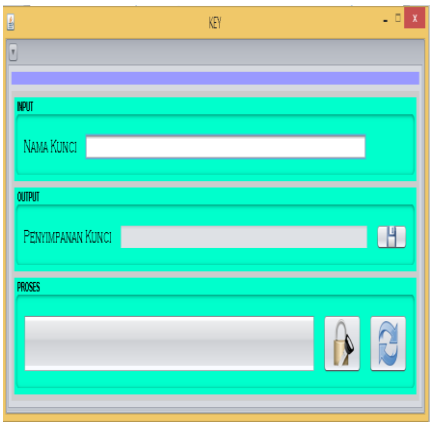
Gambar 4 : Flowchart Decode

4. HASIL DAN PEMBAHASAN

4.1 Tampilan Layar

Pada bagian ini akan dijelaskan mengenai tampilan layar pada saat aplikasi dijalankan dari tampilan layar *form key*, *form encode* dan *form decode*.

a. Tampilan Layar *Form Key*.

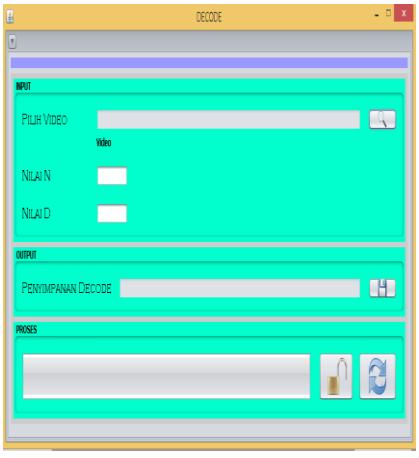


Gambar 5 : Form Key

b. Tampilan Layar *Form Encode*.

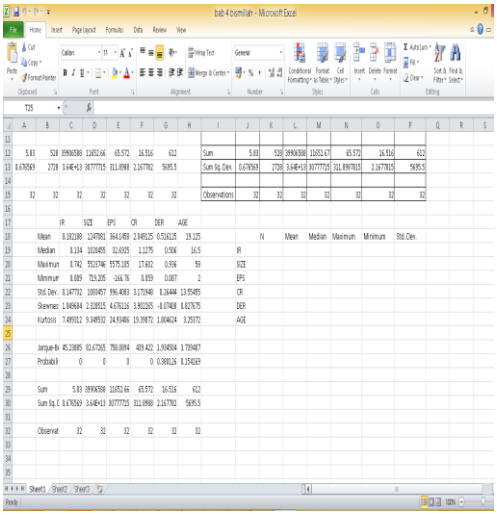
Gambar 6 : Form Encode

c. Tampilan Layar *Form Decode*.

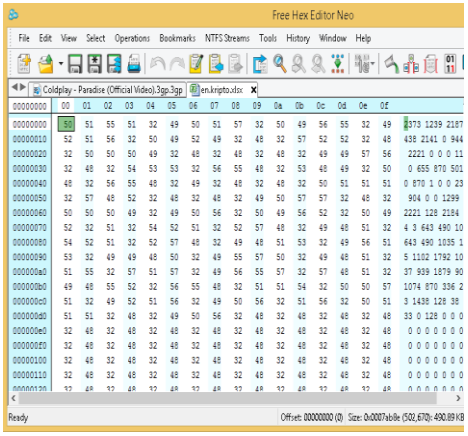


Gambar 7 : Form Decode

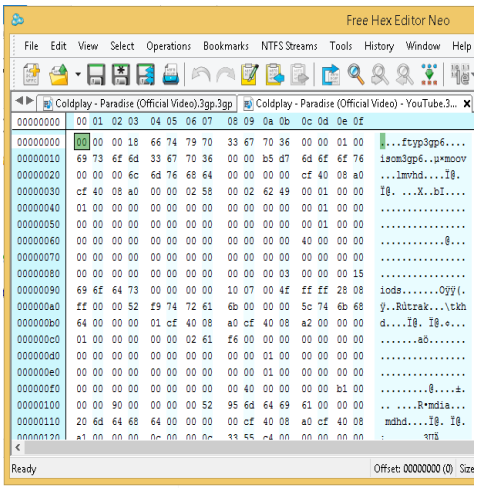
4.2 Uji Coba Program



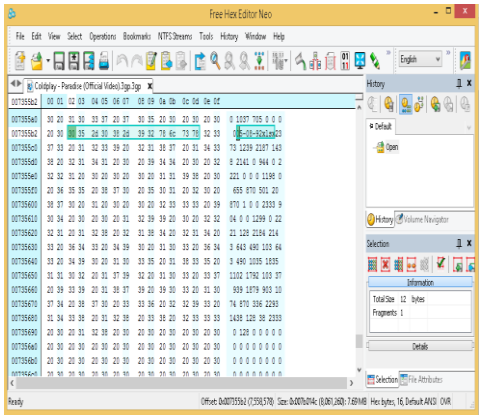
Gambar 8 : Sebelum Di Enkripsi



Gambar 9 : Hasil Enkripsi



Gambar 10 : Sebelum Di Encode



Gambar 11 : Hasil Encode

4.3 Pengujian Aplikasi

Pengujian dilakukan pada 20 file xls dan 20 video 3gp. Tabel 3 menunjukkan pengujian proses encode. Semua data berhasil di-encode dengan waktu proses rata-rata 21,45 detik. Semakin besar ukuran file maka semakin lama proses encode.

Tabel 3 : Pengujian Proses Encode

Nama Video	Ukuran Video	Ukuran Video Hasil Encode	Nama File	Ukuran File	Ukuran File Hasil Enkripsi	Waktu Proses Encode (Detik)	Status
All Time Low – Missing You.3gp	3.082 KB	3.159 KB	Book1.xls	27 KB	77 KB	7.437	Berhasil
Avenged Sevenfold – The Stage.3gp	13.823 KB	13.892 KB	Revenue. xlsx	24 KB	70 KB	99.08	Berhasil
Blink 182 – Bored To Death.3gp	2.387 KB	4.990 KB	Izin alih 2012.xls	799 KB	2633 KB	4.781	Berhasil
Bullet For My Valentine – Don't Need You.3gp	7.987 KB	8.054 KB	Data ini.xlsx	23 kb	68 Kb	1.257	Berhasil
coldplay – Paradise.3gp	7.382 KB	7.873 KB	Kripto.xls	110 KB	491 KB	76.27	Berhasil
Green Day – Still Breathing.3gp	7.111 KB	7.186 KB	Proyek.xls x	26 KB	76 KB	50.23	Berhasil
Simple Plan – Perfectly Perfect.3gp	7.872 KB	7.923 KB	Olah data eviews.xls x	16 KB	52 KB	70.15	Berhasil
Simple plan – Save You.3gp	6.708 KB	6.754 KB	Bab 4 bismillah. xlsx	12 KB	47 KB	5.563	Berhasil
Sum 41 – Fake My Own Death.3gp	1.874 KB	2.444 KB	Pengaspal an rt0304.xls	134 KB	570 KB	4.497	Berhasil
Yellow Card – Only One.3gp	2.409 KB	2.709 KB	HGU 2012.xls	95 KB	301 KB	5.888	Berhasil

Tabel 4 menunjukkan pengujian proses encode. Semua data berhasil di-encode dengan waktu proses rata-rata 32,51 detik.

Tabel 4 : Pengujian Proses Decode

Nama Video Stego	Ukuran Video Stego	Nama File	Ukuran File Hasil Enkripsi	Ukuran File Hasil Dekripsi	Waktu Proses Decode (Detik)	Status
All Time Low – Missing You.3gp	3.082 KB	Book1.xls	77 KB	27 KB	88.44	Berhasil
Avenged Sevenfold – The Stage.3gp	13.823 KB	Revenue.xlsx	70 KB	24 KB	50.12	Berhasil
Blink 182 – Bored To Death.3gp	2.387 KB	Izin alih 2012.xlsx	2633 KB	799 KB	418.961	Berhasil
Bullet For My Valentine – Don't Need You.3gp	7.987 Kb	Data ini.xlsx	68 KB	23 KB	11.16	Berhasil
Coldplay – Paradise.3gp	7.382 KB	kripto.xls	491 KB	47 KB	69.751	Berhasil
Green Day – Still Breathing.3gp	7.111 KB	Proyek.xlsx	76 KB	26 KB	2.09	Berhasil
Simple Plan – Perfectly Perfect.3gp	7.872 KB	Olah data eviews.xlsx	52 KB	16 KB	10.09	Berhasil
Simple Plan – Save You.3gp	6.708 KB	Bab 4 bismillah.xlsx	47 KB	12 KB	40.281	Berhasil
Sum 41 – Fake My Own Death.3gp	1.874 KB	Pengaspalan rt0304.xls	570 KB	134 KB	2.007	Berhasil
Yellow Card – Only One.3gp	2.409 KB	HGU 2012.xls	301 KB	95 KB	17.605	Berhasil

Semua data berhasil di-decode dengan waktu proses rata-rata 71,05 detik

5. PENUTUP

5.1 Kesimpulan

Melalui proses pembuatan dan pengujian dalam penelitian ini, maka dapat diberikan kesimpulan, antara lain :

a. Kriptografi algoritma *Rivest Shamir Adleman* (RSA) dan steganografi metode *End Of File* (EOF) dapat diimplementasikan untuk aplikasi keamanan dokumen.
b. Dengan adanya aplikasi kriptografi dan steganografi untuk keamanan dokumen, penyimpanan dan pertukaran informasi menjadi lebih aman.
c. Media video yang telah disisipkan *file* rahasia tidak akan terdeteksi secara penglihatan menusia sehingga tidak menimbulkan kecurigaan dalam berkirim pesan informasi.
d. Aplikasi ini dapat mengembalikan *file* data asli secara utuh dalam proses *decode* tanpa mengalami perubahan di dalam isi *file*.
e. Kecepatan pada saat proses *encode* dan *decode* tergantung pada *hardware*, *software*, dan ukuran *file* rahasia maupun media video yang digunakan.

5.2 Saran

Beberapa saran yang dapat diberikan untuk pengembangan aplikasi dengan harapan menghasilkan penelitian yang lebih baik lagi selanjutnya, berikut saran yang dapat diberikan :

a. Dalam aplikasi ini format media video agar ditambahkan lagi, tidak hanya audio (.3gp) saja.
b. Dalam aplikasi ini format *file* rahasia agar ditambahkan lagi, tidak hanya *file* (*xlsx, *.xls) saja.
c. Ukuran *file* yang dapat digunakan diharapkan bisa lebih besar dari 1 MB.
d. Waktu proses *encode* dan *decode* diharapkan dapat lebih cepat lagi.

Algoritma dan metode yang dibuat sebaiknya selalu ditingkatkan, karena dengan semakin berkembangnya ilmu pengetahuan tentang kriptografi dan steganografi, maka tidak dapat dipastikan apakah algoritma dan metode ini masih bisa diandalkan.

6. DAFTAR PUSTAKA

[1] H. Syaputra and H. F. Herdiyatmoko, "APLIKASI ENKRIPSI DATA PADA FILE TEKS DENGAN ALGORITMA RSA (RIVEST SHAMIR ADLEMAN)," no. Semantik 2012, pp. 229–234, 2012.

[2] M. S. Lubis, M. A. Budiman, and K. L. Manik, "Penggunaan Algoritma RSA dengan Metode The Sieve of Eratosthenes dalam Enkripsi dan Deskripsi Pengiriman Email," no. SNATI, pp. 28–33, 2013.

[3] C. D. A. B. Tarigan, "STEGANOGRAFI PADA FILE AUDIO MP3 UNTUK PENGAMANAN DATA MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB)," *Pelita Inform. Budi Darma*, vol. VI, no. 3, pp. 26–29, 2014.

[4] I. Kurniawan, "Implementasi dan Studi Perbandingan Steganografi pada File Audio WAVE Menggunakan Teknik Low-Bit Encoding dengan Teknik End Of File," *J. Informatics Technol.*, vol. 2, no. 3, pp. 0–11, 2013.

[5] A. Al Jufri, T. Abdillah, and M. Rohandi, "IMPLEMENTASI KRIPTOGRAFI DIFFIE-HELLMAN, KRIPTOGRAFI VIGENERE CIPHER DAN STEGANOGRAFI END OF FILE UNTUK KEAMANAN DATA."

[6] A. S. Raharjo, A. Hidayatno, and R. Isnanto, "IMPLEMENTASI STEGANOGRAFI PADA BERKAS MP3," pp. 1–7.