Pengamanan File Gambar pada Media Video dengan Kriptografi Algoritma RSA dan Steganografi Algoritma End of File (EOF)

Afif Malvi[1], Painem[2]
[1,2] Program Studi Sistem Informasi, Fakultas Teknologi Informasi
Universitas Budi Luhur
Jalan Ciledug Raya, Petukangan Utara, Jakarta Selatan, DKI Jakarta, Indonesia
afifmalvi@gmail.com[1)], painem@budiluhur.ac.id[*2)]

Abstrak. Keamanan data merupakan suatu hal penting, karena berkaitan dengan privasi, integritas, otentikasi dan kerahasiaan. Apabila suatu data hilang atau diubah oleh pihak yang tidak bertanggung jawab, maka dapat merugikan bagi pemilik data. Keamanan data digital sangat penting pada perkembangan teknologi saat ini, termasuk di bidang percetakan. Pada bidang percetakan cover majalah dan pengeditan gambar dibutuhkan aplikasi pengamanan data untuk mencegah terjadinya pemalsuan data dan manipulasi data yang dilakukan oleh orang-orang yang tidak bertanggung jawab. Pada penelitian ini dikembangkan sebuah aplikasi yang berfungsi untuk mengamankan *file* gambar pada PT. Segoro Arto Sejati. Aplikasi yang dikembangkan menggunakan algoritma kriptografi RSA dan dipadukan dengan steganografi algoritma *End of File (EOF)*. Proses pengamanan *file* terdiri dari dua tahap, yaitu proses enkripsi *file* menggunakan metode RSA yang menghasilkan *file* terenkripsi (*encrypted file*), diikuti dengan tahap penyisipan *file* terenkripsi ke dalam media penampung menggunakan metode EOF. Berdasarkan hasil pengujian proses pengamanan *file* diperoleh tingkat keberhasilan aplikasi mencapai 100% dengan rata-rata waktu proses pengamanan *file* (*embedding*) sebesar 5,651 detik dan waktu proses ekstraksi *file* sebesar 17,533 detik.

Kata Kunci: Keamanan Data, Kriptografi, Steganografi, Gambar, Video

1 Pendahuluan

Seiring dengan perkembangan teknologi informasi yang berkembang semakin modern maka memerlukan informasi yang cepat dan akurat. Dalam hal ini, komputer memegang peranan penting sebagai alat bantu dalam pengolahan data, dimana dalam proses tersebut, kecepatan dan ketepatan data yang diolah menjadi informasi yang lebih berguna dan bermanfaat. Perkembangan teknologi digital membawa dampak pada ancaman keamanan data. Berdasarkan laporan dari *Risk Based Security*, pada kuartal pertama tahun 2020 jumlah pelanggaran terhadap data meningkat 58% dibanding kuartal yang sama di tahun 2019 [1]. Hal tersebut memberikan gambaran pentingnya pengamanan data digital.

PT. Segoro Arto Sejati merupakan salah satu perusahaan yang bergerak di bidang percetakan dan layanan pengeditan gambar digital. Pada bidang usaha percetakan dan pengeditan gambar, pengamanan data digital harus menjadi prioritas utama. Selain untuk menjaga kerahasiaan perusahaan, keamanan data digital diperlukan untuk menjaga kepercayaan pelanggan. Namun demikian, saat ini perusahaan belum memiliki sistem atau mekanisme pengamanan data digital yang dimiliki. Dengan perkembangan ancaman terhadap data digital hal tersebut dapat menjadi permasalahan serius bagi perusahaan. Oleh karena itu, pada penelitian ini diusulkan penerapan algoritma kriptografi dan steganografi untuk mengamankan data gambar yang dimiliki oleh perusahaan.

Kriptografi merupakan cara yang digunakan sebagai seni pengamanan pesan yang bertujuan supaya data atau dokumen yang diproses tidak bisa dibaca dengan mudah [2]. Metode kriptografi secara umum dapat dibagi menjadi dua jenis, metode simetris dan asimetris berdasarkan jenis kunci yang digunakan. Saat ini, ada beberapa algoritma enkripsi yang umum digunakan, termasuk DES, 3DES, AES, Blowfish, RC4, dan RSA. Algoritma DES adalah algoritma enkripsi yang cukup tua dan memiliki beberapa masalah keamanan [3], [4]. Algoritma 3DES merupakan pengembangan dari DES, tetapi masih kekurangan sisi waktu dari proses yang lambat. Kedua algoritma dirancang untuk diterapkan pada enkripsi berbasis perangkat keras. Sementara itu, RSA adalah algoritma kriptografi dengan kunci publik yang paling populer. Algoritma RSA dibuat oleh tiga orang peneliti dari MIT (*Massachusetts Institute*

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

of Technology), yaitu Ron Rivest, Adi Shamir, dan Len Adleman pada tahun 1976. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.

Saat ini RSA menjadi salah satu algoritma kriptografi yang paling banyak digunakan di berbagai penelitian. Kurniawan berhasil memanfaatkan algoritma RSA untuk mengamankan beberapa jenis *file* dokumen seperti *Microsoft Word*, *Open Office* dan PDF [5]. Sementara itu, Pambudi dan Imelda juga menerapkan algoritma RSA untuk mengamankan *file* dokumen [6]. Penelitian tersebut juga menggabungkan algoritma enkripsi dengan steganografi untuk menyisipkan *file* terenkripsi ke dalam media video 3GP.

Steganografi merupakan teknik penyembunyian pesan yang memanfaatkan kekurangan sistem indera manusia [7] seperti mata (*human visual system*) dan telinga (*human auditory system*). Dengan teknik steganografi, pesan rahasia tidak dapat diketahui kehadirannya oleh indera manusia (indera penglihatan atau indera pendengaran) dengan mudah dan mampu menghadapi proses-proses pengolahan sinyal digital dengan tidak merusak kualitas data yang telah disisipi sampai pada tahap tertentu. Saat ini jenis media penyembunyian pesan sudah sangat beragam, mulai dari teks, citra, audio hingga video. Demikian juga metode penyembunyian pesan juga banyak diusulkan oleh para peneliti. Beberapa metode steganografi yang banyak digunakan antara lain *Least Significant Bit* (LSB), *Bit Plane Complexity Segmentation* (BPCS) [8], *Pixel Value Differencing* (PVD), *Tri-Way Value Differencing* (TPVD), *Edges based data embedding* [9], *Discrete Cosine Transform* (DCT) dan *End Of File* (EOF) [10].

Video merupakan jenis media penyembunyian pesan yang potensial dan banyak digunakan. Data yang dapat disisipkan atau disembunyikan pada media video memiliki kapasitas yang jauh lebih besar dibanding media lainnya seperti teks, citra dan audio. Selain itu, video tersedia dalam berbagai format sehingga dapat digunakan pada berbagai keperluan. Penerapan steganografi dengan media video memiliki banyak alternatif metode. Hampir semua metode steganografi yang dapat diterapkan pada citra, dapat pula diterapkan pada video karena pada dasarnya video merupakan kumpulan dari sejumlah citra tunggal. Saat ini, berbagai teknik dan metode penyembunyian data berupa teks atau *file* pada media video banyak diusulkan oleh para peneliti termasuk *Less Significant Frame* (LSF) [11] dan *End of File* (EOF) [10].

Pada penelitian ini dikembangkan sebuah aplikasi yang berfungsi untuk mengamankan *file* gambar pada PT. Segoro Arto Sejati. Aplikasi yang dikembangkan menggunakan algoritma kriptografi RSA dan dipadukan dengan steganografi algoritma *End of File* (EOF). Penelitian ini secara khusus hanya membahas pengamanan *file* gambar berjenis JPG dan PNG. Pemilihan algoritma RSA dilatarbelakangi oleh kelebihan dari sisi keamanannya dibanding algoritma sejenis. Sementara itu untuk penyisipan *file* gambar, digunakan algoritma EOF dengan pertimbangan kemudahan dalam proses penyisipan dan tidak bergantung pada ukuran media penampung.

2 Metode Penelitian

2.1 Analisis Masalah dan Solusi

Begitu banyak terjadinya pencurian data, yang mana hal tersebut dapat menimbulkan kerugian terhadap pemilik data, baik itu data yang bersifat pribadi atau data-data lain. Hal ini terjadi karena tidak adanya pengamanan pada data yang disimpan, sehingga data tersebut mudah dicuri atau dimanipulasi oleh orang-orang yang tidak bertanggung jawab. PT. Segoro Arto Sejati masih menggunakan tingkat pengamanan yang terbilang klasik dan masih banyak kelemahannya.

Oleh karena itu perusahaan menginginkan agar *file-file* penting khususnya gambar desain dan logo pelanggan untuk diamankan sehingga dapat terhindar dari manipulasi data oleh pihak yang tidak bertanggung jawab. Untuk mencegah segala hal yang tidak diinginkan maka diperlukan sistem keamanan yang lebih baik dan modern untuk menjaga kerahasiaan setiap data *file* penting.

Berdasarkan permasalahan diatas, diperlukan sebuah solusi untuk mengamankan data pelanggan, sehingga dapat terciptanya kepuasan pelanggan dari segi pelayanan dan kepercayaan terhadap perusahaan. Salah satu solusi yang

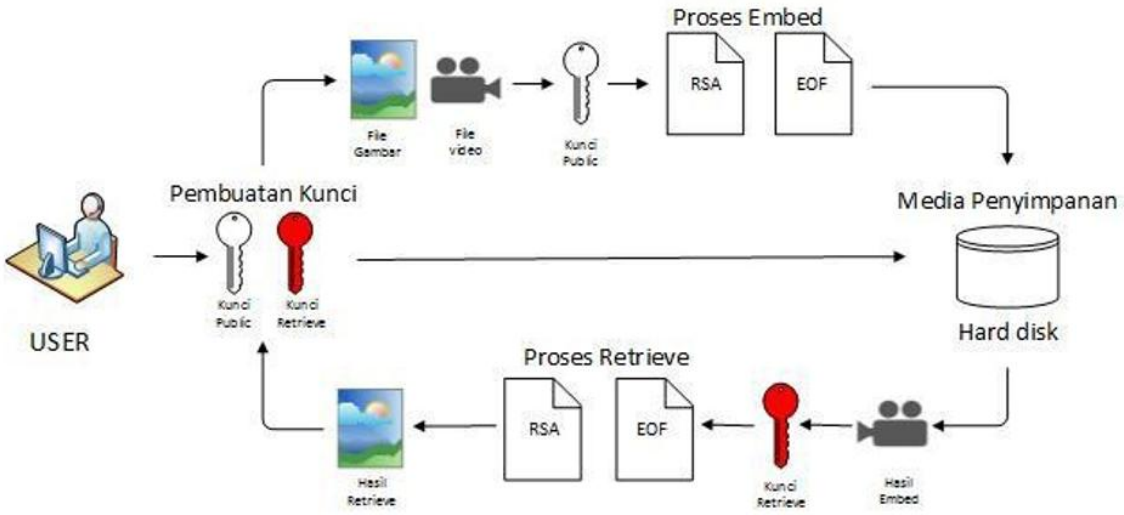
ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

diterapkan pada perusahaan adalah dengan dibuatnya aplikasi berbasis *desktop* yang berfungsi untuk mengamankan data-data pelanggan yang berupa gambar. Aplikasi ini berguna untuk menyembunyikan sebuah gambar ke dalam video dengan kombinasi dari metode algoritma kriptografi RSA dan Steganografi EOF. Sehingga diharapkan dapat aplikasi tersebut dapat mengamankan gambar dengan baik dan dapat digunakan pada aplikasi *desktop* dengan baik.

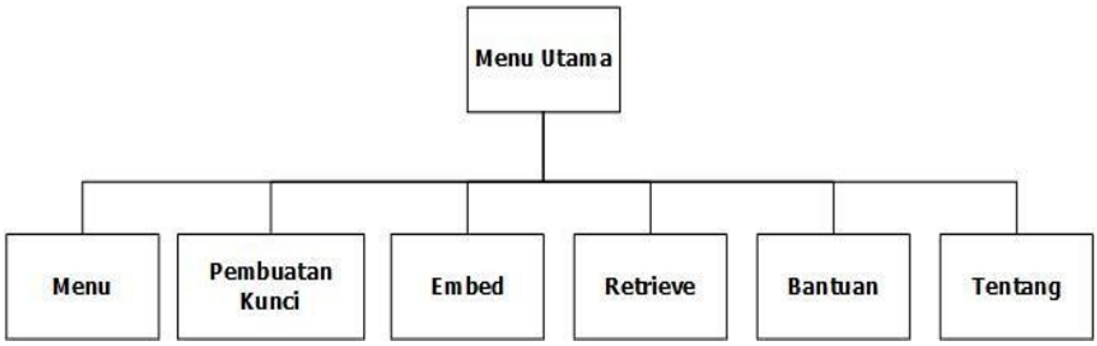
2.2 Arsitektur Aplikasi

Arsitektur aplikasi merupakan suatu proses/tahapan yang menjelaskan tentang penggunaan dari aplikasi yang telah dirancang. Gambar 1 menunjukkan rancangan arsitektur aplikasi pengamanan *file* gambar yang diusulkan. Pertama, pengguna dapat membuat kunci setelah melakukan *login* ke aplikasi. Untuk melakukan proses pengamanan *file*, pengguna mempersiapkan *file* gambar yang akan diamankan, video sebagai media penampung *file*, dan kunci *public* yang telah dibangkitkan di tahap sebelumnya. *File* yang telah diamankan dapat disimpan di media penyimpanan atau didistribusikan ke media lain.

Pada proses *retrieve* atau mendapatkan kembali *file* yang telah diamankan, pengguna harus memiliki kunci untuk membuka *file*. Gambar yang telah disisipkan ke *file* video dapat dipisahkan kembali dari media penampungnya menggunakan kunci yang sama dengan kunci pada proses *embed*. Jika kunci yang dimasukkan benar, maka gambar dapat dipisahkan dari media penampungnya.



Gambar 1. Arsitektur aplikasi proses pengamanan *file*.



Gambar 2. Rancangan menu aplikasi

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

Berdasarkan arsitektur aplikasi pada Gambar 1, dirancang struktur menu dari aplikasi pengamanan *file* yang diusulkan pada penelitian ini. Rancangan menu dapat dilihat pada Gambar 2. Aplikasi memiliki 3 (tiga) menu utama yaitu pembuatan kunci, proses *embed*, dan proses *retrieve*, serta memiliki beberapa menu pendukung seperti menu "bantuan" berisi petunjuk penggunaan aplikasi, dan menu "tentang" berisi informasi singkat mengenai pengembang aplikasi.

2.3 Algoritma Proses Pengamanan *File* dan Ekstraksi *File*

Penelitian ini mengembangkan sebuah aplikasi pengamanan data gambar menggunakan algoritma enkripsi RSA dan algoritma steganografi EOF. Proses utama terdiri dari 2 (dua) bagian, yaitu proses pengamanan *file* dan proses ekstraksi *file*. Pada proses pengamanan *file*, gambar dilakukan enkripsi dengan algoritma RSA dan selanjutnya disisipkan pada media video dengan algoritma EOF. Hasil dari proses tersebut adalah *file* gambar terenkripsi yang tersisipkan secara sempurna pada sebuah media penampung. Berikut ini algoritma proses pengamanan *file* yang diterapkan pada aplikasi.

Algoritma Proses Pengamanan File

```
 1  Tampil Form Embed
 2  Input Pilih
 3  IF Pilih = "Gambar" Then
 4      Browse Gambar
 5      Input Pilih
 6      IF Pilih = "Open" Then
 7          Tampil Nama Gambar
 8      END IF
 9  END IF
10
11  IF Pilih = "Video" Then
12      Browse Video
13      Input Pilih
14      IF pilih = "Open" Then
15          Tampil Nama Video
16      END IF
17  END IF
18
19  IF pilih = "Public Key" Then
20      Browse Tempat Penyimpanan
21      Input pilih
22      IF Pilih Open
23          Tampil Tempat Penyimpanan
24      END IF
25  END IF
26
27  IF pilih = "Simpan" Then
28      Pilih Tempat Penyimpanan
29      Input pilih
30      IF Pilih Open
31          Tampil Tempat Penyimpanan
32      END IF
33  END IF
34
35  IF pilih = "Embed" Then
36      IF pilih gambar , pilih video, pilih public key, pilih penyimpanan
    = "Null" Then
37          Tampil Alert "Form Belum Lengkap Atau Masih Kosong"
38      ELSE
```

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

```
39          Proses enkripsi, dan penyisipan file
40          Simpan file
41          Tampil alert "File Berhasil Di Enkripsi Dan Disisipkan"
42      END IF
43  ELSE IF ="Batal" Then
44      Bersihkan form embed
45  ELSE IF = "Keluar" Then
46      Kembali Ke Menu Utama
47  END IF
```

Sementara itu, pada proses ekstraksi *file*, gambar yang sudah diamankan dan disisipkan ke dalam sebuah media penampung video dapat diperoleh kembali melalui serangkaian proses. Pertama, *file* gambar harus dipisahkan dari media penampungnya. Selanjutnya, *file* gambar yang sudah dipisahkan dilakukan proses dekripsi menggunakan kunci yang sama pada proses pengamanan *file*. Berikut ini algoritma lengkap proses ekstraksi *file*.

Algoritma Proses Ekstraksi File

```
 1  Tampil Form Retrieve
 2  Input Pilih
 3  IF Pilih = "Video" THEN
 4      Browse Video
 5      Input Pilih
 6      IF Pilih = "Video" THEN
 7          Tampil Nama Video
 8      END IF
 9  END IF
10
11  IF pilih = "Private Key" THEN
12      Browse Tempat Penyimpanan
13      Input pilih
14      IF Pilih Open
15          Tampil Tempat Penyimpanan
16      END IF
17  END IF
18
19  IF pilih = "Simpan" THEN
20      Pilih Tempat Penyimpanan
21      Input pilih
22      IF Pilih Open
23          Tampil Tempat Penyimpanan
24      END IF
25  END IF
26
27  IF pilih = "Retrieve" THEN
28      IF   pilih   video, pilih private     key,  pilih   penyimpanan   =
    "Null" THEN
29          Tampil Alert "Form Belum Lengkap Atau Masih Kosong"
30      ELSE
31          Proses dekripsi, dan pengeluaran file
32          Simpan file
33          Tampil alert "File Berhasil Di Dekripsi Dan Dikeluarkan"
34      END IF
35  ELSE IF ="Batal" THEN
36      Bersihkan form Retrieve
37  ELSE IF = "Keluar" THEN
38      Kembali Ke Menu Utama
39  END IF
```

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

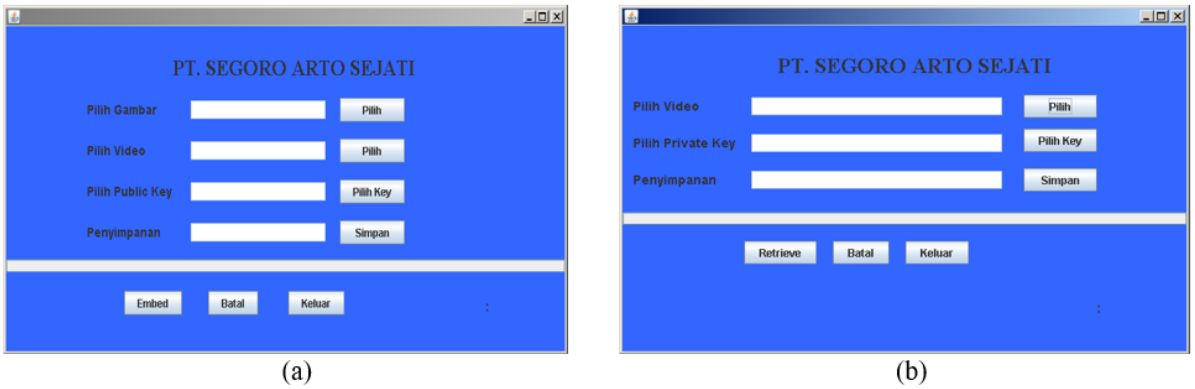
3 Hasil dan Pembahasan

3.1 Implementasi Aplikasi

Aplikasi yang dikembangkan membutuhkan spesifikasi perangkat lunak dan perangkat keras agar aplikasi dapat berjalan baik. Aplikasi yang dibangun menggunakan bahasa pemrograman Java membutuhkan *platform J2SDK runtime* dengan versi 1.7 ke atas. Selain itu, aplikasi membutuhkan ruang kapasitas penyimpanan yang cukup untuk menyimpan *file* video dan gambar yang akan diamankan. Kebutuhan ruang penyimpanan sangat bergantung pada besarnya *file* yang digunakan. Sementara itu, untuk kapasitas memori (RAM) tidaklah membutuhkan kapasitas yang besar, cukup dengan RAM minimal 2GB sudah dapat menjalankan aplikasi.

Gambar 3. Tampilan aplikasi pengamanan *file*, (a) tampilan menu dan halaman utama, (b) tampilan pembangkitan kunci

Pada Gambar 3 disajikan tampilan aplikasi pengamanan *file* pada PT. Segoro Arto Sejati. Gambar 3 (a) merupakan tampilan aplikasi setelah pengguna melakukan login ke aplikasi. Menu utama terletak di bagian atas, antara lain menu Home, Pembuatan Kunci, *Embed, Retrieve*, Bantuan dan Tentang. Sementara itu, pada Gambar 3 (b) menyajikan tampilan halaman pembangkitan kunci yang dapat dilakukan oleh pengguna. Kunci dapat disimpan di lokasi yang ditentukan oleh pengguna. Kunci tersebut dapat dimanfaatkan pada proses *embed* atau pengamanan *file*.



Gambar 4. Tampilan aplikasi proses utama pengamanan *file*, (a) proses pengamanan *file* (enkripsi dan *embedding*), (b) proses ekstraksi *file* (pemisahan dan dekripsi).

Proses utama aplikasi adalah proses pengamanan *file* yang digambarkan pada Gambar 4 bagian (a) dan (b). Pada tampilan menu (a), pengguna diminta memilih *file* gambar yang akan diamankan, *file* video sebagai media penampung *file*, *file* kunci *public* yang telah dibangkitkan, dan lokasi penyimpanan *file* yang telah diamankan. Sementara itu, pada proses ekstraksi *file* (Gambar 4 bagian b), pengguna cukup memasukkan *file* video yang berisi *file* rahasia, lalu memasukkan *file* kunci dan lokasi penyimpanan *file* hasil proses *retrieve*.

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

3.2 Pengujian Pengamanan Gambar

Untuk mengetahui kualitas aplikasi pengamanan *file* gambar menggunakan metode kriptografi RSA dan steganografi EOF, dilakukan serangkaian pengujian. Tabel 1 menyajikan data *file* gambar yang dijadikan data uji. *File* gambar tersebut merupakan contoh gambar digital yang akan diamankan. Jenis *file* gambar yang diuji coba adalah JPG dan PNG karena kedua jenis gambar tersebut merupakan jenis gambar yang paling banyak digunakan. Sementara itu, pada Tabel 2 disajikan data *file* video yang akan dijadikan penampung *file* gambar. Jenis video yang dijadikan penampung adalah MP4 dengan variasi ukuran lebih dari 1 MB.

Tabel 1. Data uji *file* gambar

No	Gambar	Nama Gambar	Ukuran
1		Gambar 1.jpg	63 KB
2		Gambar 2.jpg	64 KB
3		Gambar 3.png	283 KB

Tabel 2. Data uji video penampung

No	Nama Video	Ukuran	Format
1	Video1.mp4	8.494 KB	.mp4
2	Video2.mp4	9.999 KB	.mp4
3	Video3.mp4	1.321 KB	.mp4

Berdasarkan hasil pengujian seperti disajikan pada Tabel 3, terlihat bahwa 100% *file* gambar dapat terenkripsi dan tersisipi dengan baik. Selain itu proses pengamanan *file* juga relatif cepat. Berdasarkan pengujian, rata-rata waktu proses pengamanan *file* untuk setiap data uji sebesar 5,651 detik. Selain itu, berdasarkan pengujian ternyata ukuran *file* terenkripsi menjadi lebih besar. Hal tersebut dapat terjadi karena proses algoritma RSA melakukan pengacakan data asli.

Tabel 3. Hasil pengujian proses pengamanan *file*

No	Video Penampung	*File* Gambar	Ukuran *File* Terenkripsi	Nama Video Tersisipi	Waktu Proses
1	Video1.mp4	Gambar 1.jpg	1.268 KB	Embed_video 1.mp4	7,531 detik
2	Video2.mp4	Gambar 2.jpg	1.293 KB	Embed_video 1.mp4	4,234 detik
3	Video3.mp4	Gambar 3.png	2.449 KB	Embed_video 1.mp4	5,188 detik
				Rata-rata	5,651 detik

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

Sementara itu, pada pengujian proses ekstraksi *file* seperti terlihat pada Tabel 4, seluruh *file* gambar dapat dipisahkan kembali dari video penampung dan berhasil didekripsi kembali. Ukuran *file* gambar yang berhasil dipisahkan juga sama dengan gambar aslinya. Adapun rata-rata waktu proses ekstraksi *file* adalah 17,533 detik. Proses ini lebih lama dibanding proses pengamanan *file*.

Tabel 4. Hasil pengujian proses ekstraksi *file*

No	Nama Video Tersisipi	Ukuran *File* Terenkripsi	Ukuran Gambar Terekstraksi	Waktu Proses
1	Embed_video 1.mp4	1.268 KB	63 KB	26,016 detik
2	Embed_video 1.mp4	1.293 KB	64 KB	11,691 detik
3	Embed_video 1.mp4	2.449 KB	283 KB	14,891 detik
			Rata-rata	17,533 detik

4 Kesimpulan

Berdasarkan analisis yang telah dilakukan terhadap permasalahan dan pengujian aplikasi yang telah dikembangkan, maka dapat ditarik kesimpulan bahwa dengan adanya aplikasi ini, maka data *file* gambar dan data lainnya yang dianggap penting bagi perusahaan dapat terjaga kerahasiaannya dari pihak yang tidak bertanggung jawab. Algoritma kriptografi RSA (*Rivest Shamir Adleman*) dan steganografi EOF (*End Of File*) berhasil diimplementasikan dalam pengembangan aplikasi pengamanan *file* yang terdiri dari dua proses utama. Berdasarkan hasil pengujian, proses pengamanan data juga termasuk cepat, yaitu rata-rata waktu sekitar 5 detik. *File* gambar digital yang sudah dienkripsi dan disisipkan ke dalam *file* video dapat dikembalikan menjadi *file* asli tanpa ada perubahan. Adapun rata-rata waktu proses ekstraksi *file* gambar asli adalah 17 detik.

Selain menarik beberapa kesimpulan, dapat pula diajukan saran-saran yang mungkin bisa dijadikan pertimbangan dan pengembangan sistem dan penelitian selanjutnya. Waktu proses pengamanan dan ekstraksi *file* dapat lebih dipercepat terutama untuk *file* yang berkapasitas besar. Selain itu, penelitian lanjutan juga dapat mengkaji efektivitas media penampungan dibandingkan dengan media penampung MP4. Untuk mengatasi ukuran *file* yang besar, dapat juga ditambahkan algoritma kompresi untuk mempercepat proses penyisipan pesan di media penampung.

Referensi

[1] RiskBased Security, "2020 Q1 Report Data Breach QuickView," 2020.

[2] D. Ariyus, *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*. Yogyakarta: Andi Offset, 2008.

[3] T. Pornin, "Comparison of DES, Triple DES, AES, blowfish encryption for data," *StackOverflow.Com*, 2011. [Daring]. Tersedia pada: https://stackoverflow.com/questions/5554526/comparison-of-des-triple-des-aes-blowfish-encryption-for-data. [Diakses: 24-Apr-2018].

[4] A. Solichin dan E. W. Ramadhan, "Enhancing data security using DES-based cryptography and DCT-based steganography," in *2017 3rd International Conference on Science in Information Technology (ICSITech)*, 2017, hal. 618–621.

[5] R. Kurniawan, "Rancang Bangun Aplikasi Pengaman Isi *File* Dokumen dengan Algoritma RSA," *Algoritm. J. Ilmu Komput. dan Inform.*, vol. 1, no. 1, hal. 46–52, 2017.

[6] A. S. Pambudi dan Imelda, "Pengamanan Data Menggunakan Kriptografi Algoritma Riverst Shamir Adleman dan Steganografi Metode End of *File* Dengan Media 3GP," *J. BIT*, vol. 14, no. 1, hal. 45–50, 2017.

[7] R. Sigit, *Step By Step Pengolahan Citra Digital*. YOGYAKARTA: Andi Publisher, 2007.

[8] E. Kawaguchi dan R. O. Eason, "Principles and applications of BPCS steganography," in *Proceedings of SPIE*, 1999, hal. 464–473.

[9] M. Hussain dan M. Hussain, "A Survey of Image Steganography Techniques," *Int. J. Adv. Sci. Technol.*, vol. 54, no. May, hal. 113–124, 2013.

[10] Martono dan Irawan, "Penggunaan Steganografi dengan Metode End of *File* (EOF) pada Digital Watermarking," *J. TICOM*, vol. 2, no. 1, hal. 36–42, 2013.

[11] A. Solichin dan Painem, "Motion-based Less Significant Frame for Improving LSB-based Video Steganography," in *2016 International Seminar on Application for Technology of Information and Communication*, 2016, hal. 179–183.

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)