Penyisipan Jalur Penerbangan UAV Rahasia dalam Media Digital dengan Steganografi Kunci Publik ElGamal

Leonard Matheus Wastupranata - 13519215
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
leo.matt.547@gmail.com

***Abstrak*—Untuk menyelesaikan misi penerbangan, UAV akan membutuhkan rute perjalanan yang harus ditempuh beserta koordinat lokasi yang spesifik. Akan tetapi, banyak misi yang harus diselesaikan secara rahasia, misalnya tugas kenegaraan, demi menjamin keselamatan terbang UAV dari serangan pihak-pihak yang tidak bertanggung jawab. Untuk itu, diperlukan mekanisme kriptografi data rute perjalanan dan steganografi pada suatu media digital agar keamanan pengiriman data lebih terjamin. Metode yang digunakan adalah kriptografi kunci publik ElGamal karena kecepatan dekripsi yang baik dan kalkulasi matematika yang lebih sulit sehingga meningkatkan keamanan data. Metode Steganografi yang digunakan adalah *Least Significant Bit* (LSB) sehingga kualitas media digital setelah dilakukan penyisipan data tidak jauh berbeda dari aslinya. Didapatkan hasil bahwa seluruh eksperimen mencapai nilai di atas 30 yang menunjukkan kualitas Steganografi kunci publik sangat baik.**

Keywords—UAV; Steganografi; ElGamal; Kriptografi Kunci Publik; Least Significant Bit

I. PENDAHULUAN

Dalam melakukan misi penerbangan, misalnya menjalankan tugas negara, UAV atau yang lebih familier disebut sebagai *drone* membutuhkan sebuah *file* jalur penerbangan yang akan dikunjungi. *File* jalur penerbangan ini akan menentukan letak koordinat spesifik tujuan terbang UAV tertentu. Pada praktiknya, banyak sekali ancaman yang telah disusun secara sistematis untuk melakukan kejahatan untuk menggagalkan misi penerbangan UAV tersebut. Untuk itu diperlukan sebuah strategi khusus supaya masukkan jalur penerbangan tidak diketahui oleh penyerang yang ingin mengacaukan misi penerbangan UAV.

Salah satu strategi yang banyak digunakan untuk mengamankan jalur penerbangan adalah dengan menggunakan kriptografi kunci publik. Teks pada *file* jalur penerbangan akan dienkripsi sedemikian rupa menggunakan kunci publik sehingga *file* ini hanya dapat dibuka kembali menggunakan kunci privat padanannya. Hanya saja, strategi ini memungkinkan penyerang mencoba segala kemungkinan kunci untuk mengetahui isi *file* jalur penerbangan secara spesifik.

Untuk itu, digunakan strategi tambahan berupa penyisipan jalur penerbangan secara rahasia pada media digital menggunakan prinsip steganografi pada *file* gambar, audio, dan video. Mekanisme penyisipan adalah dengan mengubah *Least Significant Bit* (LSB) pada *byte* penyusunnya mewakili representasi biner dari isi *file* jalur penerbangan. Dengan cara demikian, penyerang tidak akan mengetahui akan ada *file input* jalur penerbangan yang dikirimkan dari pemberi misi ke eksekutor misi.

Salah satu mekanisme steganografi kunci publik yang pernah dikembangkan oleh Mishra [1] dengan menggunakan gabungan steganografi dengan algoritma RSA. Metode ini menjamin transmisi data rahasia dengan konsistensi yang lebih tinggi sehubungan dengan teknik kriptografi yang dikembangkan terpisah dari teknik steganografi gambar, audio, dan video. Penyembunyian data juga bersifat searah yaitu pesan rahasia yang dikodekan oleh pengirim hanya dapat dipecahkan menggunakan kunci privat oleh penerima. Sayangnya, Algoritma RSA lebih cepat melakukan proses enkripsi, sedangkan lambat dalam melakukan proses dekripsi [2]. Untuk kasus penyisipan jalur penerbangan rahasia, diperlukan algoritma dengan waktu dekripsi yang lebih cepat dan keamanan yang relatif tinggi karena isi *file* penerbangan hanya berisi angka koordinat serta hanya memiliki ukuran *file* yang kecil.

Dalam makalah ini, akan dilakukan eksperimen penyisipan jalur penerbangan dengan menggunakan metode steganografi kunci publik menggunakan algoritma ElGamal. *File* Jalur Penerbangan akan dilakukan enkripsi sehingga menghasilkan keluaran sementara berupa representasi integer *byte* sementara yang akan disisipkan dengan metode LSB pada setiap representasi biner *file* stego yang ditentukan. Hal ini dilakukan agar penyisipan jalur penerbangan menjadi semakin aman dan misi penerbangan rahasia menjadi sukses.

Makalah ini terbagi menjadi lima bagian. Bagian pertama akan membahas mengenai latar belakang dan tujuan utama implementasi steganografi kunci publik. Bagian kedua akan mendasari konsep-konsep kriptografi dan steganografi yang akan diimplementasikan. Selanjutnya, bagian ketiga akan dijelaskan metode yang digunakan dalam melakukan

eksperimen beserta lingkungan pemrograman yang mendukung. Pada bagian keempat, akan dipaparkan hasil analisis dari eksperimen yang telah dilakukan. Terakhir, pada bagian ke lima, akan disimpulkan hasil yang telah didapatkan pada bagian analisis dan saran untuk peneliti selanjutnya.

II. STUDI LITERATUR

A. Steganografi

Steganografi adalah suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi rahasia di dalam suatu informasi lainya. Ada beberapa terminologi yang digunakan pada steganografi, yaitu:

1. *Embedded message* atau *secret message*: pesan yang disembunyikan. Bisa berupa teks, gambar, audio, video, dll.
2. *Cover object*: media digital yang digunakan untuk menyembunyikan *embedded message*. Bisa berupa teks, gambar, audio, video, dll.
3. *Stego object* (stego-data): media yang sudah berisi pesan *embedded message*.
4. *Stego key*: kunci yang digunakan untuk ppenyisipan pesan dan mengekstraksi pesan dari *stego object*.

Dalam mencapai kualitas steganografi yang baik, ada beberapa kriteria yang perlu diperhatikan. Pertama, keberadaan pesan rahasia tidak dapat dipersepsi secara visual atau secara audial (*imperceptible*). Kualitas *cover object* juga tidak jauh berubah akibat penyisipan pesan rahasia (*fidelity*). Selanjutnya, pesan yang disembunyikan harus dapat diekstraksi kembali (*recovery*). Terakhir, ukuran pesan yang disembunyikan sedapat sebesar mungkin (*capacity*).

Metode yang digunakan dalam melakukan penyisipan pesan pada *cover object* adalah penyisipan *Least Significant Bit* (LSB). Metode ini merupakan metode steganografi yang paling populer karena memanfaatkan kelemahan indra visual manusia dalam mengamati perubahan sedikit pada *stego object*. Strategi yang dilakukan adalah mengganti bit LSB dari piksel dengan bit pesan [3].

Hal ini dilakukan karena dengan mengubah bit LSB, nilai byte hanya berubah satu nilai lebih tinggi atau satu nilai lebih rendah dari nilai sebelumnya. Oleh karena itu, pengubahan ini tidak berpengaruh terhadap persepsi visual atau auditori pengamat.

B. Kriptografi Kunci Publik

Kriptografi kunci-publik disebut juga kriptografi kunci-nirsimetri (*asymmetric key cryptography*) karena kunci enkripsi yang digunakan untuk menyembunyikan pesan tidak sama dengan kunci dekripsi. Istilah "publik" muncul karena kunci untuk enkripsi diumumkan kepada publik (tidak rahasia), misalnya disimpan di dalam repositori yang dapat diakses oleh publik. Dalam kriptografi kunci publik, kunci privat bersifat rahasia sehingga hanya pemiliknya yang mengetahui kunci privat tersebut sendiri.

Kelebihan kriptografi kunci-publik yaitu kunci privat perlu dijaga kerahasiaannya oleh setiap entitas yang berkomunikasi. Karena itu, tidak ada kebutuhan mengirim kunci privat sebagaimana pada kriptografi kunci simetri. Kelebihan lainnya adalah pasangan kunci publik dan kunci privat tidak perlu sering diubah, bahkan dalam periode waktu yang panjang.

Kekurangan dari kriptografi kunci publik ada pada proses enkripsi dan dekripsi pesan yang umumnya lebih lambat dari sistem kriptografi simetri, karena enkripsi dan dekripsi menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar. Kekurangan lainnya yaitu ukuran cipherteks lebih besar daripada plainteks (bisa dua sampai empat kali ukuran plainteks), serta ukuran kunci relatif lebih besar daripada ukuran kunci simetri [4].

C. Algoritma ElGamal

Algoritma ElGamal dibuat oleh Taher ElGamal[5] pada tahun 1985. Pada dasarnya, algoritma ini memiliki keamanan yang tinggi karena perhitungan yang lebih sulit menggunakan logaritma diskrit. Masalah logaritma diskrit dimodelkan dalam p yang adalah bilangan prima, g dan y adalah sembarang bilangan bulat, carilah x sedemikian sehingga memenuhi persamaan (1) sebagai berikut.

$$g^x \equiv y \ (mod\ p) \tag{1}$$

Adapun properti yang dimiliki algoritma ElGamal adalah sebagai berikut:

1. Bilangan prima, p (tidak rahasia)
2. Bilangan acak, g (g < p) (tidak rahasia)
3. Bilangan acak, x (x < p) (rahasia, kunci privat)
4. $y \equiv g^x \bmod p$ (tidak rahasia, kunci publik)
5. m (plainteks) (rahasia)
6. a dan b (cipherteks) (tidak rahasia)

Untuk melakukan pembangkitan kunci ElGamal, prosedur yang dilakukan adalah sebagai berikut:

1. Pilih sembarang bilangan prima p (p dapat dishare di antara anggota kelompok)
2. Pilih dua buah bilangan acak, g dan x, dengan syarat $g < p$ dan $1 \leq x \leq p - 2$
3. Hitung $y = g^x \bmod p$.

Hasil dari algoritma ini berupa kunci publik: triplet (y, g, p) dan kunci privat yang berupa pasangan (x, p). Untuk melakukan enkripsi, prosedur yang dilakukan adalah sebagai berikut:

1. Susun plainteks menjadi blok-blok m_1, m_2, …, (nilai setiap blok di dalam selang [0, p – 1].
2. Pilih bilangan acak k, yang dalam hal ini $1 \leq k \leq p - 2$.
3. Setiap blok m dienkripsi dengan rumus

$$a = g^k \ mod\ p \tag{2}$$

$$b = y^k m \bmod p \quad (3)$$

Pasangan a dan b adalah cipherteks untuk blok pesan m. Jadi, ukuran cipherteks dua kali ukuran plainteksnya. Sedangkan, Prosedur Dekripsi adalah sebagai berikut:

1. Gunakan kunci privat x untuk menghitung seperti persamaan(4)

$$(a^x)^{-1} = a^{(p-1-x)} \bmod p \quad (4)$$

2. Hitung plainteks m sesuai dengan persamaan (5)

$$m = b(a^x)^{-1} \bmod p \quad (5)$$

D. Peak-Signal-to-Noise Ratio (PSNR)

PSNR merupakan metrik untuk mengukur kualitas (*fidelity*) citra setelah proses manipulasi. Pengukuran baik buruknya manipulasi sebuah *stego object* selalu dibandingkan dengan *stego object* semula (yang belum dimanipulasi). Misalkan I = *cover-image* dan $\hat{I}$ = *stego-image*, ukuran citra M x N, maka

$$PSNR = 20 \times \log_{10}\left(\frac{MAX}{rms}\right) \quad (6)$$

MAX berarti jumlah selisih RMS yang mungkin dicapai oleh suatu manipulasi bit pada praktik steganografi. Pada Steganografi gambar dan video, nilai MAX didefinisikan sebesar 255 bit. Pada steganografi audio, nilai MAX didefinisikan sebesar 8 bit saja. Adapun rumus rms untuk steganografi gambar dan video dapat dilihat pada persamaan (7), rumus rms untuk steganografi audio dapat dilihat pada persamaan (8).

$$rms = \sqrt{\frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(I_{ij} - \hat{I}_{ij}\right)^2} \quad (7)$$

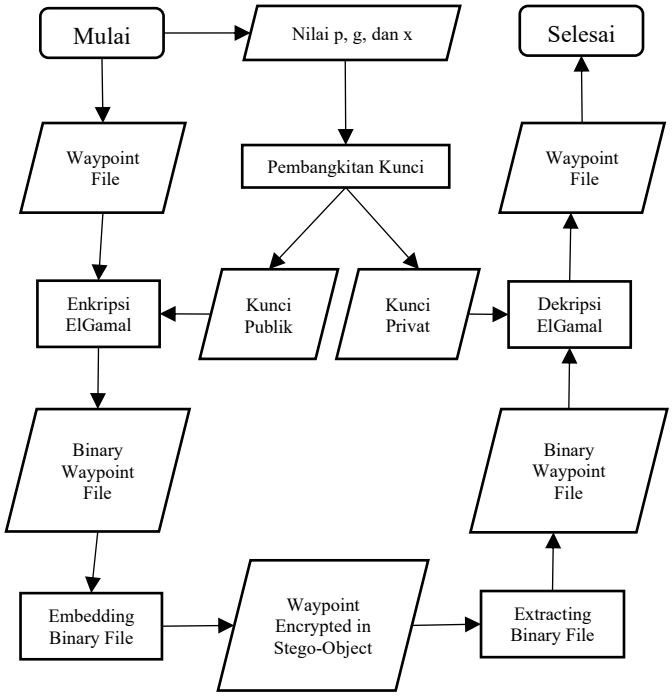
$$rms = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(I_i - \hat{I}_i)} \quad (8)$$

Dengan rms = *root mean square*

Satuan PSNR yang digunakan adalah desibel (dB). Nilai PSNR berbanding terbalik dengan rms. PSNR yang besar mengindikasikan nilai rms yang kecil, sedangkan rms kecil berarti dua buah *stego object* mempunyai hanya sedikit perbedaan. PSNR yang kecil mengindikasikan nilai rms yang besar; rms besar berarti kedua *stego object* memiliki perbedaan yang besar (degradasi). PSNR yang dapat diterima/ditoleransi adalah jika > 30 [6].

III. METODE PENELITIAN

A. Alur Kerja Sistem Penyisipan Jalur Penerbangan Rahasia

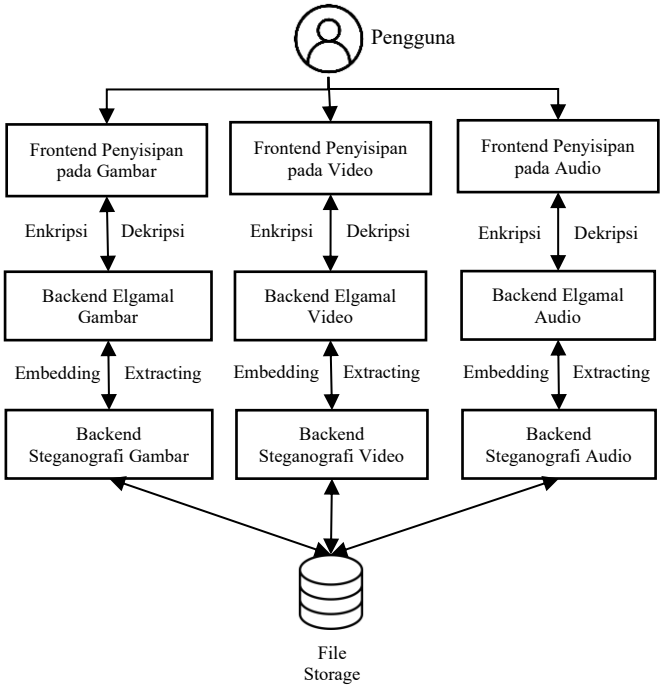


Gambar 1. Diagram Alur Kerja Sistem Penyisipan Jalur Penerbangan Rahasia

Pada Gambar 1, terlihat bahwa sistem akan meminta masukkan berupa *file waypoints* dan nilai yang dibutuhkan untuk pembangkitan kunci. Pada makalah ini, akan digunakan *file waypoints* yang digunakan pada percobaan yang dilakukan oleh Wastupranata dalam membuat rute pengantaran obat-obatan[7] dan pencegahan klaster kerumunan [8]. Setelah itu, akan dilakukan enkripsi ElGamal terhadap *file waypoints* dengan memasukkan kunci publik yang telah dibangkitkan sebelumnya. Selanjutnya, *binary file* akan dilakukan *embedding* terhadap *stego object* yang didefinisikan sebelumnya, baik berupa visual maupun audio. *Stego object* ini nantinya dapat dibagikan kepada penerima dengan sistem keamanan yang lebih terjamin.

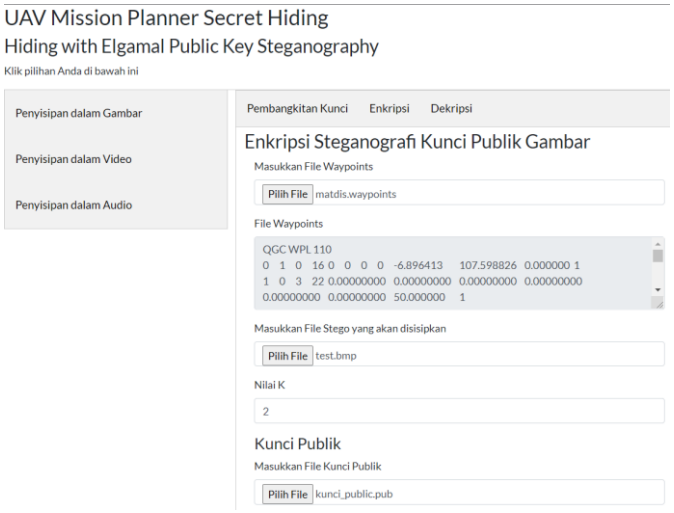
Untuk membaca *file waypoint* seperti semula, dibutuhkan mekanisme ekstraksi pada *stego object* untuk mendapatkan *binary file* kembali. Setelah itu, akan dilakukan dekripsi ElGamal terhadap *binary file* dengan memasukkan kunci privat yang telah dibangkitkan sebelumnya. Pada akhirnya, akan didapatkan kembali *file waypoint* yang utuh sehingga tidak dapat disadap oleh penyerang.

B. *Arsitektur Sistem Web Penyisipan*



Gambar 2. Diagram Arsitektur Sistem Web Penyisipan

Pada Gambar 2, Arsitektur sistem akan mengandalkan tiga bagian utama, yaitu penyisipan jalur penerbangan pada gambar, video, dan audio. Masukkan pengguna akan ditangani pada *frontend* masing-masing bagian seperti terlihat pada Gambar 3.



Gambar 3. Tampilan *Frontend* Sistem Web Penyisipan

Untuk penyisipan pada gambar, hanya menerima tipe PNG atau BMP. Hal ini dilakukan karena hanya tipe inilah yang mampu mencegah kehilangan data pada kompresi [9]. Berbeda dengan penyisipan pada video, tipe yang diterima hanyalah berformat AVI karena setiap *frame* video akan diekstraksi ke dalam tiap *file* gambar yang terpisah [10]. Untuk *file* audio, tipe yang dapat diterima hanya bertipe WAV karena sifatnya yang *lossless* sehingga pada saat dilakukan *embedding*, data yang ingin disisipkan cenderung sulit untuk dihilangkan [11].

Selanjutnya, *backend* steganografi pada tiap bagian akan melakukan penyisipan dengan metode LSB. Hasil penyisipan ini akan dimasukkan ke dalam suatu *file storage* sehingga pengguna dapat memperoleh *stego object* yang telah diolah. Proses ini berlaku dua arah, artinya baik penyisipan maupun pengekstraksian dilakukan pada *backend* dan *frontend* yang sama.

C. *Environment Pendukung Simulasi*

Program akan dijalankan pada Sistem Operasi Windows versi 11 karena sebagian besar aplikasi akan dijalankan pada lingkungan Web Windows. Untuk mengecek apakah input jalur penerbangan telah terdekripsi dengan baik, digunakan aplikasi Ardupilot Misson Planner sehingga rencana penerbangan UAV dapat terlihat. Aplikasi penyisipan dikembangkan berbasis web menggunakan kakas Flask dengan lingkungan pemrograman Python 3.9 supaya ffmpeg dapat berjalan dengan baik.

Kakas ffmpeg sendiri digunakan untuk melakukan steganografi pada *file* gambar dan video, sedangkan kakas wave digunakan untuk melakukan steganografi pada *file* audio. Nantinya, hasil PSNR akan menggunakan bantuan kakas numpy untuk perhitungan mean dan kakak opencv untuk mencari selisih perubahan pada *stego object* berbasis gambar.

IV. Hasil dan Pembahasan

Telah dilakukan simulasi penyisipan *file* bernama matdis.waypoint dan dinamis.waypoint yang berisi lokasi spesifik seperti yang terlihat pada Tabel I dan Tabel 2.

TABEL I. LOKASI RUTE MATDIS.WAYPOINTS

No. WP	*Command*	Lat	Long	Alt
0	HOME	-6.896413	107.598826	0
1	TAKEOFF	0	0	50
2	WAYPOINT	-6.89725410	107.59710430	50
3	WAYPOINT	-6.89684410	107.59661610	50
4	WAYPOINT	-6.89616240	107.59647670	50
5	WAYPOINT	-6.89605590	107.59690580	50
6	WAYPOINT	-6.89536350	107.59642840	50
7	WAYPOINT	-6.89494810	107.59621920	50
8	WAYPOINT	-6.89460200	107.59589730	50
9	WAYPOINT	-6.89433570	107.59621380	50
10	WAYPOINT	-6.89446880	107.59675030	50
11	WAYPOINT	-6.89436760	107.59736720	50
12	WAYPOINT	-6.89457000	107.59776950	50
13	WAYPOINT	-6.89531560	107.59787680	50
14	LAND	-6.89643400	107.59882090	0

TABEL II. LOKASI RUTE DINAMIS.WAYPOINTS

No. WP	Command	Lat	Long	Alt
0	HOME	-6.885423	107.608179	0
1	WAYPOINT	-6.88564150	107.61012380	100
2	WAYPOINT	-6.88694630	107.61007820	100
3	WAYPOINT	-6.88789700	107.61035440	100
4	WAYPOINT	-6.88926570	107.61037050	100
5	WAYPOINT	-6.88996600	107.61036250	100
6	WAYPOINT	-6.89035210	107.61036780	100
7	WAYPOINT	-6.89091660	107.61037590	100
8	WAYPOINT	-6.89123350	107.61038390	100
9	WAYPOINT	-6.89166490	107.61005400	100
10	WAYPOINT	-6.89242910	107.61014790	100
11	WAYPOINT	-6.89239720	107.61069240	100
12	WAYPOINT	-6.89308950	107.61064950	100
13	WAYPOINT	-6.89312940	107.61163920	100
14	LAND	-6.89312940	107.61163920	0

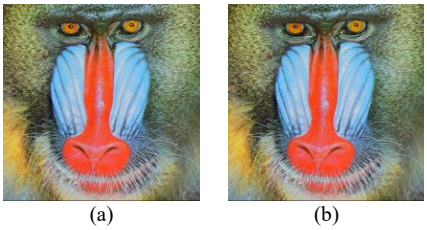
Pembangkitan kunci dilakukan dengan memasukkan nilai P sebesar 313, nilai G sebesar 105, dan nilai X sebesar 7. Selanjutnya, kunci publik dihasilkan membentuk pasangan (281, 105, 313) dan kunci privat dengan pasangan (7, 313). Penyisipan file ini telah diujikan pada skenario-skenario yang akan dijelaskan pada bagian berikutnya.

A. Penyisipan Jalur Penerbangan pada File Gambar

Untuk pengujian, akan digunakan *Cover Object* berupa *file* gambar yang dapat dilihat pada Gambar 4

Gambar 4. Tampilan *Cover Object* Bertipe BMP

Percobaan pertama akan dilakukan dengan menyisipkan *file* Matdis.waypoints dengan memasukkan kunci publik dan kunci privat yang sesuai. Didapatkan nilai PSNR sebesar 72.6146. Perbandingan Cover Object dan Stego Object dapat dilihat pada Gambar 5.

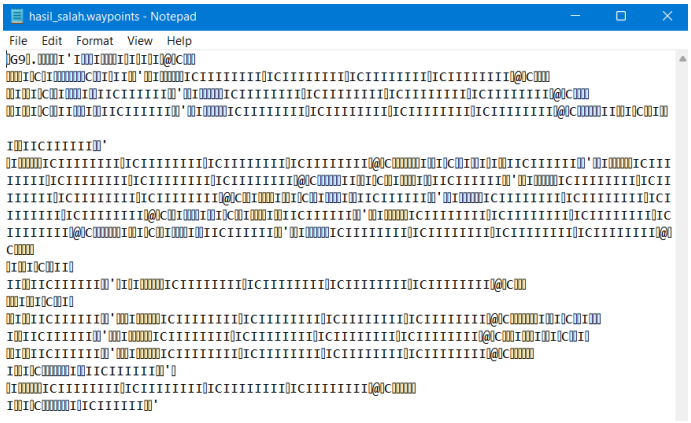


(a) (b)

Gambar 5. Tampilan *Cover Object* (a) sebelum disisipkan jalur penerbangan dan Tampilan *Stego Object* (b) setelah disisipkan jalur penerbangan

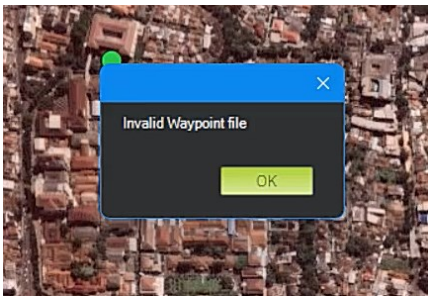
Terlihat dari percobaan pertama, tidak terlihat perbedaan yang jauh dari kedua citra yang ditampilkan apabila dilihat dari sudut pandang visual. Akan tetapi, nilai PSNR 72 menunjukkan bahwa steganografi berhasil karena melewati batas *threshold* yang didefinisikan sebesar 30.

Percobaan kedua akan menggunakan dinamis.waypoints, tetapi kunci privat yang digunakan untuk mendekripsi *binary file* berbeda dari padanan kunci publiknya. Dari percobaan, nilai PSNR yang dihasilkan sebesar 72.3948. Pada saat uji coba dekripsi ElGamal dengan kunci privat yang berbeda, hasilnya dapat dilihat pada Gambar 6.



Gambar 6. Tampilan *waypoints file* hasil dekripsi pada *Stego Image* dengan kunci privat yang salah

Terlihat bahwa *file* benar-benar tidak terbaca oleh mata manusia. Akibatnya, *file* ini tidak bisa dimasukkan ke dalam aplikasi Mission Planner. Penolakan masukkan *file* tersebut dapat dilihat pada Gambar 7.



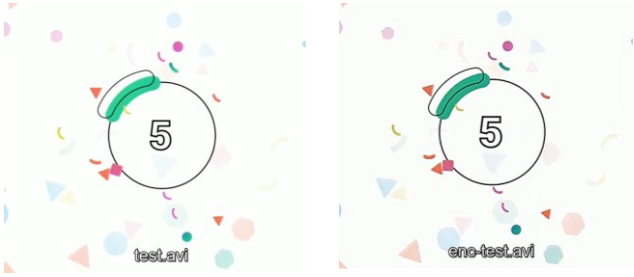
Gambar 7. Tampilan kegagalan saat memasukkan data *waypoints* yang salah

Hal ini menunjukkan bahwa walaupun steganografi berhasil diekstraksi oleh penyerang, tetap saja *file waypoints* tetap aman dari serangan karena masih terlindungi oleh enkripsi ElGamal tersebut.

B. Penyisipan Jalur Penerbangan pada File Video

Untuk pengujian penyisipan pada video, akan digunakan *Cover Object* berupa video bertipe AVI. Percobaan pertama akan dilakukan pada matdis.waypoints dengan memasukkan kunci publik dan kunci privat yang sesuai. Didapatkan nilai PSNR sebesar 122. Angka ini didapatkan dari hasil *embedding file* pada tiap frame PNG yang diekstraksikan dari *Cover* Object yang pada akhirnya dicampur dengan audio yang ada.

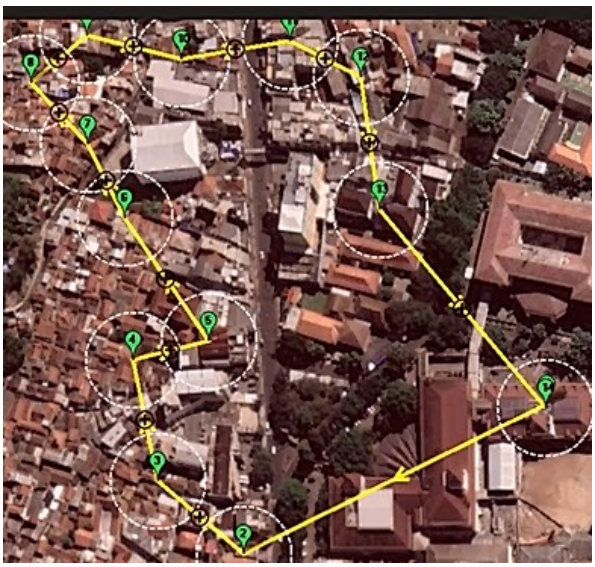
Perbandingan Cover Object dan Stego Object dapat dilihat pada Gambar 8.



(a) (b)

Gambar 8. Tampilan *Cover Object* (a) sebelum disisipkan jalur penerbangan dan Tampilan *Stego Object* (b) setelah disisipkan jalur penerbangan

Setelah dimasukkan ulang dengan kunci privat yang benar dan diproses ke dalam aplikasi Mission Planner, hasil sukses dapat dilihat pada Gambar 9.

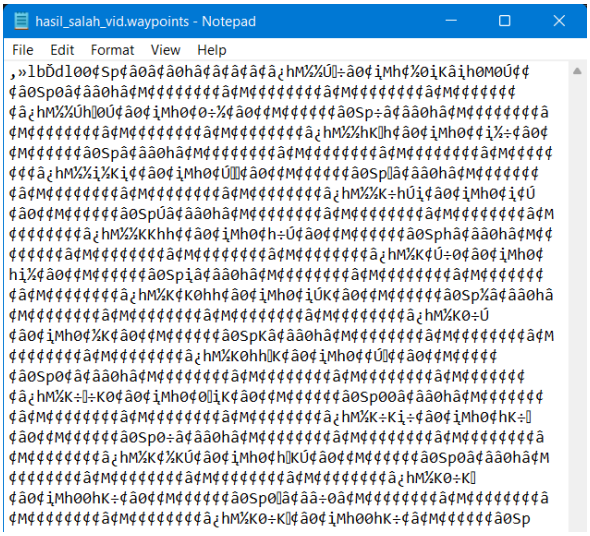


Gambar 9. Tampilan Jalur Penerbangan yang berhasil diekstraksi dari *Stego Object* bertipe Video dan didekripsi menggunakan algoritma ElGamal

Percobaan kedua dilakukan dengan memasukkan target *Cover Object* yang bukan bertipe AVI. Sistem langsung melakukan penolakan dan meminta *Cover Object* dengan format yang benar. Tampilan kesalahan oleh sistem dapat dilihat pada Gambar 10.

Gambar 10. Tampilan kegagalan saat memasukkan *Stego Video* dengan tipe yang salah

Percobaan ketiga dilakukan pada *file* dinamis.waypoints dengan mencoba padanan kunci publik dan kunci privat yang berbeda. Didapatkan nilai PSNR sebesar 122, sama seperti percobaan pertama. Hal ini terjadi lantaran jumlah gambar yang diproses sama dengan percobaan pertama. Setelah dilakukan dekripsi ElGamal, sistem akan memproses permintaan tersebut dan kembali memberikan hasil dekripsi *file* yang salah seperti terlihat pada Gambar 11.

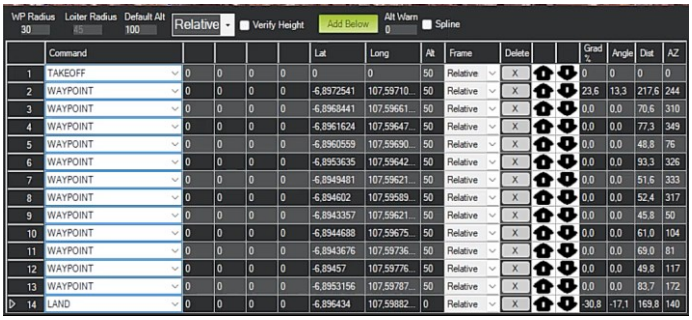


Gambar 11. Tampilan *waypoints file* hasil dekripsi pada *Stego Video* dengan kunci privat yang salah

Hal ini membuktikan bahwa keamanan *waypoints* terletak pada algoritma kriptografi kunci publik ElGamal. Steganografi tidak memberikan keamanan terhadap serangan, hanya menyembunyikan data sehingga tidak diketahui oleh penyerang bahwa ada *file* penting yang ingin diketahui isinya.

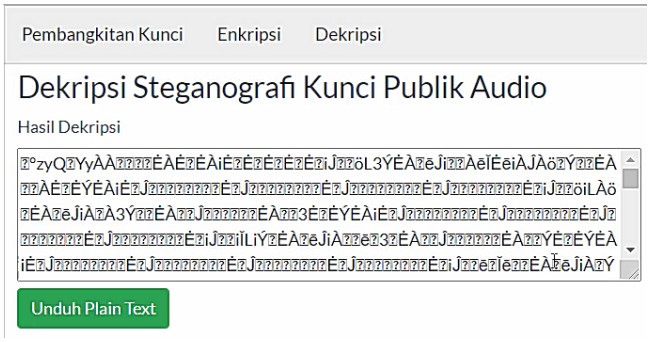
C. Penyisipan Jalur Penerbangan pada File Audio

Untuk pengujian penyisipan pada audio, akan digunakan *Cover Object* berupa audio bertipe WAV. Percobaan pertama akan dilakukan pada matdis.waypoints dengan memasukkan kunci publik dan kunci privat yang sesuai. Didapatkan nilai PSNR sebesar 36.7713. Angka ini didapatkan dari hasil *embedding file* pada tiap frame Audio yang didapatkan dari *splitting* tiap bagian data. Setelah dimasukkan ulang dengan kunci privat yang benar dan diproses ke dalam aplikasi Mission Planner, hasil sukses dapat dilihat pada Gambar 12.



Gambar 12. Tampilan Tabel Jalur Penerbangan yang berhasil diekstraksi dari *Stego Object* bertipe Audio dan didekripsi menggunakan algoritma ElGamal

Percobaan kedua dilakukan pada *file* dinamis.waypoints dengan mencoba padanan kunci publik dan kunci privat yang berbeda. Didapatkan nilai PSNR sebesar 36.6483. Setelah dilakukan dekripsi ElGamal, sistem akan memproses permintaan tersebut dan kembali memberikan hasil dekripsi *file* yang salah seperti terlihat pada Gambar 13.



Gambar 11. Tampilan *waypoints* hasil dekripsi pada *Stego Audio* dalam Web dengan kunci privat yang salah

Hal yang menarik adalah PSNR pada Audio berkisar di angka 30 hingga 40 saja. Hal ini dikarenakan pada audio, *splitting* dilakukan pada bit satu dimensi. Berbeda dengan gambar dan video yang berbentuk dua dimensi, *file* audio hanya memiliki 8 bit pada setiap *frame* yang ada. Oleh karena itu, kualitas audio yang dihasilkan menjadi kurang baik dan ada kemungkinan penyerang mengetahui ada yang disembunyikan dari *file* audio tersebut.

Tetapi, kelemahan pada penyisipan audio mampu diatasi dengan memberikan perlindungan menggunakan Algoritma Kriptografi Kunci Publik ElGamal, sehingga masalah logaritma diskrit yang sulit untuk dipecahkan menjadi nilai tambah bagi skema pengamanan jalur penerbangan rahasia.

V. KESIMPULAN

Penyisipan Jalur Penerbangan UAV Rahasia berhasil dilakukan pada berbagai Media digital berbentuk gambar, video, dan audio. Representasi biner dari berkas jalur terbang UAV dienkripsi dengan algoritma ElGamal sehingga representasi data tiap *byte* dapat disisipkan pada *Least Significant Bit* (LSB) penyusun media digital. Kriptografi kunci publik sangat berperan dalam meningkatkan keamanan data biner sehingga isinya tidak dapat diinterpretasikan oleh penyerang.

Selain itu, Steganografi turut membantu penyisipan data sehingga penyerang tidak menyadari ada data yang disembunyikan pada media digital yang diterimanya. Seluruh eksperimen mendapatkan nilai PSNR di atas 30. Nilai ini menunjukkan kualitas penyisipan data yang sangat baik. Nilai PSNR sangat berpengaruh pada tingkat kecurigaan penyerang mengenai adanya data yang disembunyikan pada media digital terkait.

VI. SARAN

Sistem dapat dikembangkan untuk penyisipan data penting lainnya seperti keadaan geografis dari suatu wilayah untuk informasi yang akan mendukung misi penerbangan rahasia lainnya. Selain itu, penyisipan audio dapat dilakukan dengan metode lain yang lebih efektif sehingga kualitas audio tetap terjaga dan dapat meningkatkan nilai PSNR lebih baik untuk menurunkan kecurigaan penyerang data.

VIDEO LINK PADA YOUTUBE

https://youtu.be/o2PhTfD4ePg

UCAPAN TERIMA KASIH

Pertama-tama, Saya mengucapkan syukur kepada Tuhan Yang Maha Esa karena dengan rahmatNya, Makalah berjudul "Penyisipan Jalur Penerbangan UAV Rahasia dalam Media Digital dengan Steganografi Kunci Publik ElGamal" dapat terselesaikan dengan baik dan tidak ada hambatan sedikit pun. Terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, MT yang telah mengajar mata kuliah IF4020 Kriptografi dan membimbing selama satu semester ini. Terima kasih terhadap segala pihak yang tidak dapat disebutkan satu persatu sehingga turut membantu terselesaikan pembuatan makalah ini.

DAFTAR PUSTAKA

[1] M. Mishra, G. Tiwari, dan A. K. Yadav, "Secret communication using public key steganography," Sep 2014.

[2] Z. Sann, T. thi Soe, K. W. M. Knin, dan Z. M. Win, "Performance Comparison of Asymmetric Cryptography (Case study- Mail message)," *APTIKOM J. Comput. Sci. Inf. Technol.*, vol. 4, no. 3, hal. 105–111, 2019.

[3] R. Munir, "Steganografi (Bagian 1)," hal. 1–41, 2021, [Daring]. Tersedia pada: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Steganografi-Bagian1-2020.pdf.

[4] R. Munir, "Kriptografi Kunci-Publik," 2021, [Daring]. Tersedia pada: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Kriptografi-Kunci-Publik-2020.pdf.

[5] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," in *Advances in Cryptology*, 1985, hal. 10–18.

[6] R. Munir, "Steganografi (Bagian 2)," hal. 29–30, 2021, [Daring]. Tersedia pada: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Steganografi-Bagian2-2020.pdf.

[7] L. M. Wastupranata, "Strategi Rute UAV untuk Pengantaran Obat-obatan bagi Penderita Covid-19 saat Isolasi Mandiri dengan Algoritma Cheapest Link & Sirkuit Hamilton," hal. 1–6, 2020, [Daring]. Tersedia pada: https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Makalah/Makalah-Matdis-2020 (208).pdf.

[8] L. M. Wastupranata, "Perencanaan Rute UAV Ulang-Alik untuk Mengantisipasi Timbulnya Klaster Kerumunan COVID-19 dengan Pendekatan Program Dinamis," 2021, [Daring]. Tersedia pada: https://informatika.stei.itb.ac.id/~rinaldi.munir/Stmik/2020-2021/Makalah2021/Makalah-Stima-2021-K4 (5).pdf.

[9] B. Sinha, "Comparison of PNG & JPEG Format for LSB Steganography," 2013, [Daring]. Tersedia pada: https://www.ijsr.net/archive/v4i4/29031501.pdf.

[10] C. Science, C. Science, dan C. Science, "Data Hiding Using Video Steganography -A Survey," vol. 5, no. 6, hal. 206–213, 2015, [Daring]. Tersedia pada: https://www.ijert.org/research/data-hiding-using-video-steganography-IJERTV3IS040807.pdf.

[11] Y. Perkhasa, W. Suadi, dan B. A. Pratomo, "Implementasi Kriptografi dan Steganografi pada *File* Audio Menggunakan Metode DES dan Parity Coding," hal. 1–6, 2011.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Jakarta, 20 Desember 2021

Leonard Matheus Wastupranata - 13519215