APLIKASI STEGANOGRAFI DENGAN METODE *TRACK FREE* ATOM DAN KRIPTOGRAFI MENGGUNAKAN METODE AES-128 UNTUK PENGAMANAN PESAN PADA *FILE* MP4 BERBASIS ANDROID

Hidayatul Ichwan[1)], Dewi Kusumaningsih[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : Hidayatul.ichwan@budiluhur.ac.id[1)], Dewi.kusumaningsih@budiluhur.ac.id[2)]

ABSTRAK

Teknologi berbasis mobile saat ini berkembang sangat cepat hampir diseluruh bidang industry dan social . Maka dari itu faktor keamanan sangat berperan penting, sehingga seluruh aplikasi berbasis mobile butuh keamanan. Saat ini laporan kerja yang dilapangan secara langsung dapat menggunakan mobile seperti mengirim video laporan kerja dengan menggunakan rekaman video secara langsung, dan salah satunya perusahaan yang menggunakan system laporan kerja yang menggunakan video rekaman secara langsung adalah KSO Pertamina EP Axis Sambidoyong Energi yang juga menggunakan teknologi internet untuk melakukan bisnis dengan melakukan pertukaran atau informasi melalui internet. Oleh karena itu, KSO Pertamina EP Axis Sambidoyong Energi membutuhkan aplikasi yang dapat membantu untuk mengamankan data atau informasi tersebut. Teknik Steganografi merupakan suatu seni penyembunyian informasi dengan cara penyisipan pada suatu media salah satunya yaitu dengan media video. Aplikasi ini dibuat dengan algoritma Kriptografi Simetri AES-128(Advanced Encryption Standart) untuk mengenkripsi pesan dan mengoptimalkan penyembunyian pesan, pesan hasil proses enkripsi tersebut akan disispkan kedalam video dengan metode steganografi Free Track Atom. Aplikasi ini dibangun dengan bahasa pemograman java berbasis mobile. Aplikasi ini dapat mengamankan pesan dan menjaga kerahasiaan pesan dan informasi pada KSO Pertamina EP Axis Sambidoyong Energi. Pesan atau informasi yang bisa dienkripsi dan disisipkan hanya berupa pesan teks biasa sedangkan untuk file penampung pesan rahasia berupa file video yang berjenis .mp4 dari hasil rekaman langsung yang dapat disisipkan pesan atau informasi. Berdasarkan implementasi uji coba program, aplikasi steganografi menggunakan metode Free Track Atom dan Kriptografi dengan Algoritma AES-128 mampu mengamankan informasi/pesan yang disisipkan kedalam video, dengan baik. Dengan adanya aplikasi pengamanan pesan yang disisipkan kedalam video, pesan penting dapat lebih terjaga kerahasiaannya.

Kata kunci : *Kriptografi, AES-128, Steganografi, Free Track Atom*

1. PENDAHULUAN

Pada era teknologi seperti sekarang ini, keamanan dalam penyimpanan data atau informasi adalah hal yang sangat penting dan tidak dapat diabaikan. Terlebih jika pesan yang disimpan bersifat penting dan rahasia. Dengan makin berkembangnya teknologi yang begitu pesat maka bertukar informasi menjadi hal yang sangat mudah dan hanya mengandalkan internet sebagai media pertukaran. Salah satu dampak negatif dalam perkembangan teknologi informasi adanya pencurian data. karena suatu komunikasi jarak jauh belum tentu aman dari pecurian. Fasilitas internet memberikan kita kemudahan dan kecepatan dalam penyampaian informasi baik dalam sebuah bisnis atau kehidupan sehari-hari. Seperti pada KSO Pertamina EP Axis Sambidoyong Energi sebuah suatu badan kerja sama dalam bentuk Kerjasama Operasi (KSO) antara PT. PERTAMINA EP dengan PT. Axis Sambidoyong Energi berdasarkan Perjanjian Kerjasama Operasi yang ditandatangi tanggal 26 Juli 2012 yang bergerak dalam proyek-proyek migas. Perusahaan ini menggunakan internet dalam kegiatan bisnisnya, untuk pertukaran infomasi/data laporan kerja dilapangan yang berupa video antar cabang ataupun antar staff kepada pimpinan. Untuk mengamankan informasi atau deskripsi dari video itu tersebut agar pihak yang tidak berwenang tidak bisa memanipulasinya dari video aslinya. Untuk itu perlu adanya suatu aplikasi keamanan data agar kerahasiaan informasi, pesan maupun data bisa terjaga dari pihak-pihak yang tidak berhak menerimanya.Kriptografi adalah sebuah proses pengacakan data asli, sehingga dihasilkan data

teracak dan berbeda dengan aslinya, sedangkan steganografi merupakan seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain pengirim dan penerima tidak ada seorangpun yang mengetahui dan menyadari bahwa ada suatu pesan rahasia .Berdasarkan uraian diatas maka penulis skripsi ini membahas bagaimanakah mengamankan sebuah informasi/data yang telah dienkripsi, dengan menyisipkan kedalam media berupa video mp4 dengan metode Track Free atom dengan kombinasi algoritma AES-128 sehingga menghindari kecurigaan pihak luar terhadap informasi/data tersebut.

2. LANDASAN TEORI

2.1 Steganografi

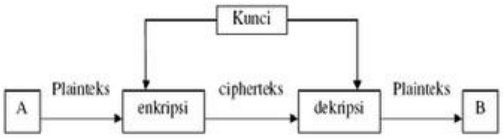
Kata Steganography berasal dari bahasa Yunani yaitu "steganos" yang berarti tersembunyi atau terselubung dan "graphy" yang berarti tulisan atau gambar [1]. Steganography membutuhkan 2 media untuk pengimplementasiannya yaitu media penyimpan (*cover object*) dan pesan rahasia yang akan disisipkan ke dalam media penyimpanan[1] Steganography muncul untuk menyempurnakan kekurangan *Cryptography* dalam menyembunyikan data penting di dalam sebuah *cover object*, sehingga hanya pihak tertentu yang dimaksudkan bisa mendapatkan pesan yang ingin disampaikan. Kelebihan Steganography dibandingkan dengan *Cryptography* adalah pesan-pesannya tidak menarik perhatian orang lain[1].

2.2 Kriptografi

Crytography adalah bidang ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data dan autentikasi. *Cryptography* adalah ilmu dan seni yang digunakan untuk keamanan pesan rahasia yang akan dikirimkan dengan cara mengacaukan, menyamarkan atau menyandikan pesan rahasia menjadi bentuk yang tidak dibaca dan tidak dapat dimengerti dengan menggunakan teknik yang disebut encode (enkripsi), kemudian pesan rahasia yang telah diubah menjadi ciphertext tidak dapat dibaca oleh orang lain selain pengirim dan penerima pesan rahasia tersebut dan proses kebalikan dari encode adalah decode (dekripsi) [1].
Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut dengan melakukan pembangkitan kunci, enkripsi dan dekripsi[2].

2.2.1 Algoritma Simetris

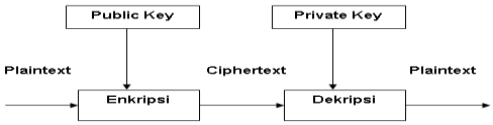
Algoritma simetris terbagi menjadi dua buah bergantung pada datanya, yaitu chiper aliran (stream chiper) dan chiper blok (block chiper). Chiper aliran memproses satu bit pesan sekali dalam satu waktu, sedangkan chiper blok memproses sekumpulan bit sekaligus sebagai satu unit. Ukuran blok yang umum dipakai adalah 64 bit. Dari segi kecepaan komputasi, algoritma simetri lebih cepat daripada algoritma asimetri. Kelemahan utama dari opsi ini adalah dalam mendistribusikan kunci ke pihak-pihak yang berkepentingan. Namun jika dipakai dalam suatu lingkungan yang tidak membutuhkan pendistribusian kunci (seperti penggunaan pribadi), maka algoritma ini merupakan yang terbaik [2].



Gambar 1. Skema Kriptografi Simetri

2.2.2 Algoritma Asimetris

Algoritma asimetris adalah algoritma yang menggunakan kunci pada proses enkripsinya berbeda dengan kunci pada proses dekripsi. Pada algoritma ini kunci dekripsinya tidak dibuka atau rahasia, sedangkan kunci enkripsinya bisa diberikan secara umum. Untuk memperoleh atribut ini, algoritma dirancang pada mekanisme yang sulit untuk dipecahkan secara matematika[2].



Gambar 2. Skema Kriptografi Asimetri

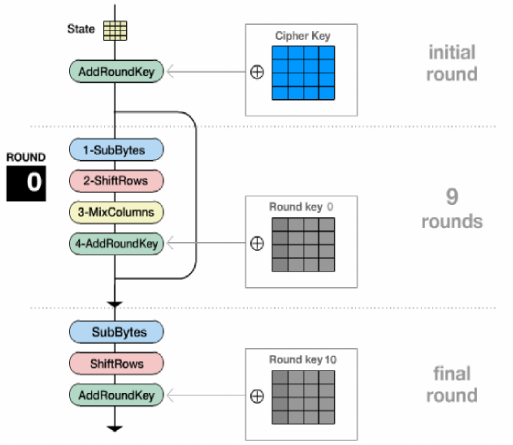
2.3 Algoritma AES-128

Advanced Encryption Standard (AES) dipublikasikan oleh NIST (National Institute of Standard and Technology) pada tahun 2001. AES merupakan block kode simetris untuk menggantikan DES (Data Encryption Standard). DES terbukti menjadi algoritma enkripsi yang aman didunia selama puluhan tahun. Pada tahun 1990 panjang kunci DES dianggap terlalu pendek dan terbukti pada tahun 1998, 70 ribu PC di internet berhasil membobol satu kunci DES dalam tempo 96 hari, tahun 1999 dalam tempo 22 hari. Karena sudah berhasil dipecahkan, maka dibuatlah mesin khusus untuk memecahkan algoritma DES yang mampu memecahkan 25% kunci DES dalam waktu 2,3 hari dan dapat memcahkan seluruh kunci DES dalam waktu rata-rata 4,5 hari. Karena alasan tersebut maka kemudian diadakan kompetisi

oleh NIST untuk mengganti algoritma DES. Melalui seleksi yang ketat, maka pada 2 Oktober 2000 terpilih algoritma Rijndael [2].

2.3.1 Proses Enkripsi AES

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Pada awal proses enkripsi, *input* yang telah dicopykan ke dalam *state* akan mengalami transformasi byte *AddRoundKey*. Setelah itu, state akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai *round function*. *Round* yang terakhir agak berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, state tidak mengalami transformasi *MixColumn*s, dibawah ini adalah gambar proses enkripsi AES[2].



Gambar 3. Proses Enkripsi AES-128

2.3.2 Proses Dekripsi

Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada *invers cipher* adalah *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey*.

2.4 Steganografi *Free Track* Atom

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 menyisipkan pesan kedalam video maka *file* video harus menjadi byte array, cari index dari atom *free*. Jika index atom *free* lebih dari nol maka ambil byte array *size* dari atom *free*. Jika panjang *size* dari atom *free* lebih dari atau sama dengan dari delapan maka akan menampilkan pesan sudah ada

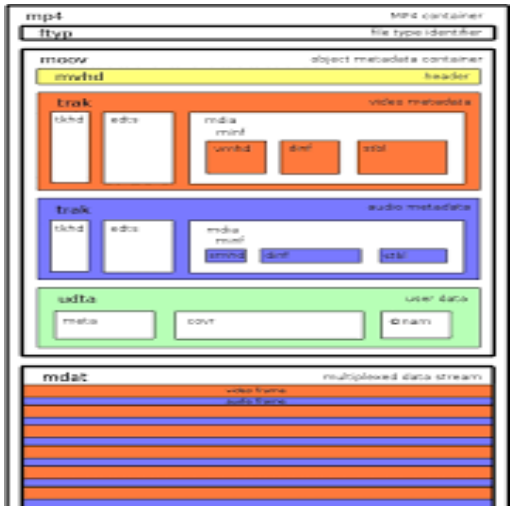
Tabel 2. Perbandingan Tipe Aes

Tipe	Panjang kunci (NK)	Ukuran Blok (NB)	Jumlah Putaran (NR)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

jika tidak maka menghitung panjang pesan kemudian menggeser tabel dari atom stco sejauh panjang pesan dan menambahkan pesan kedalam atom *free*. Lalu mengenerate *file* stego video. Jika index atom *free* kurang dari nol maka mencari index atom *ftyp* kemudian mencari panjang atom *ftyp*, setelah itu menggeser tabel *offset* dari atom *stco* sejauh panjang pesan + 8. Lalu menambahkan pesan kedalam atom *free*. Sisipkan atom *free* setelah panjang atom *ftyp*. Terakhir men-*generate* atau membuat *file* stego video dari byte array video[3].

2.5 MPEG-4 Part 14 (MP4)

MPEG-4 sub-bagian 14 atau lebih di kenal sebagai MP4 adalah salah satu format bekas pengkodean suara dan menggunakan pengembangan dari format *QuickTime* dari *computerApple.* MP4 Metadata yang sangat penting adalah *file* Index, indeks menunjuk ke *offset file* dimana muatan (misalnya video). Format standar untuk MPEG-4 dinamakan MP4. Terkadang ini menyebabkan orang bingung dan menganggapnya sebagai format audio seperti MP3. Sebenarnya MP3 terkait dengan MPEG-1. MP3 merupakan bagian audio dari standar MPEG yang asli [3].



Gambar 4. Struktur Berkas MP4

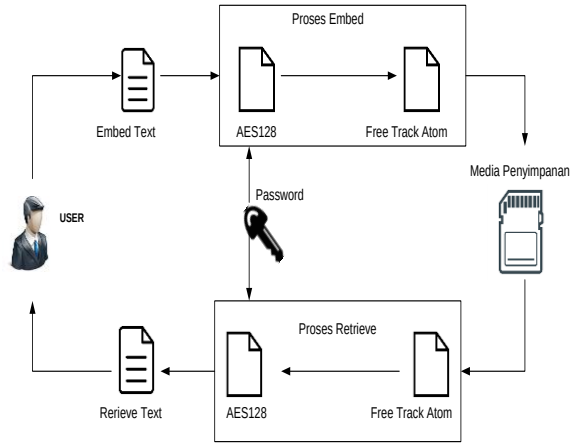
3.RANCANGAN SISTEM DAN APLIKASI

Tahapan-tahapan yang terjadi dalam proses sistem aplikasi ini dapat dijelaskan sebagai berikut :

3.1 Desain Konsep Aplikasi

Desain konsep aplikasi merupakan alur pembuatan video mulai dari proses embed dan retrieve kemdian melakuakan proses enkripsi dan dekripsi Algoritma AES-128 membutuhkan password yang sama untuk proses enkripsi dan dekripsi.

Untuk dapat menggunakan aplikasi ini *user* terlebih dahulu harus melakukan proses *Embed* dengan cara memilih *Form* Menu *Embed* yang ada pada Menu Utama, setelah itu *user* mulai membuat rekaman video kemudian mengisi kolom pesan dan kolom key yang ada pada *Form* Menu *Embed.* Ketika *User* memilih tombol *Embed* maka proses Enkripsi dan penyisipan teks akan berjalan lalu disimpan dalam media penyimpanan memori. Begitu pula untuk proses *Retrieve* dengan cara memilih Form Menu *Retrieve* yang ada pada Menu Utama kemudian *user* memilih video dan mengisi kolom *key* ketika memilih tombol *Retrieve* maka proses dekripsi akan berjalan, jika videonya sudah disisipkan pesan maka pesan tersebut akan otomatis keluar di Kolom Pesan.



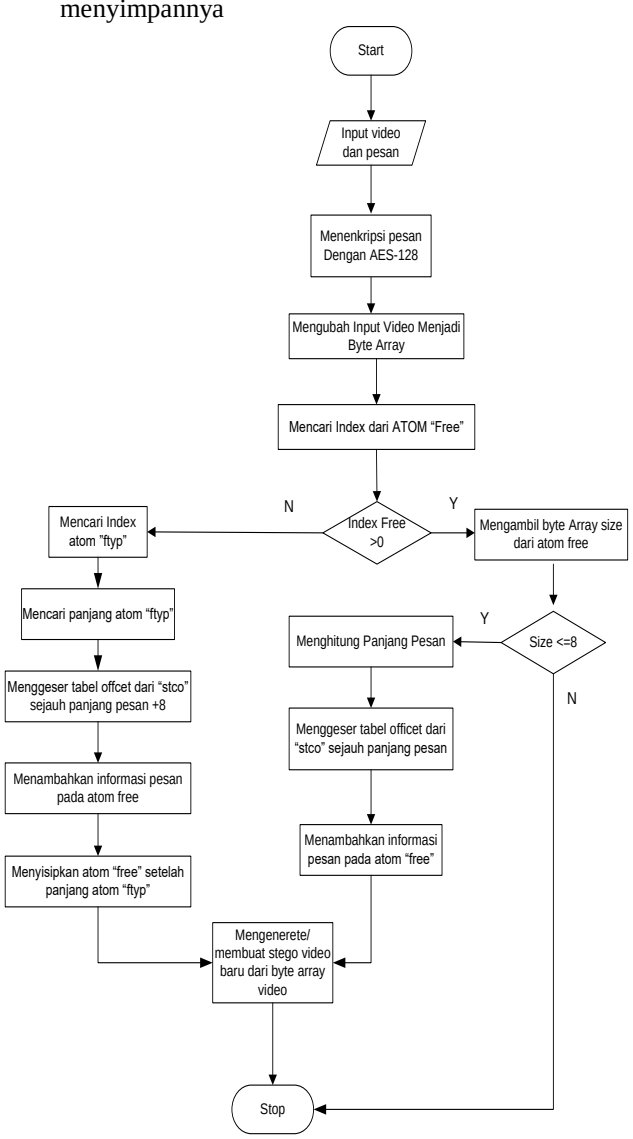
Gambar 5 : Skema proses Aplikasi

3.2 *Flowchart Embed* dan *Retrive*

Untuk memecahkan masalah ke dalam segmen-segmen yang lebih kecil atau detail dan membantu dalam menganalisis alternatif-alternatif lain dalam pengoperasian dari aplikasi maka dibutuhkan flowchart pada saat perancangan aplikasi. Flowchart ini akan menjelaskan alur kerja dari aplikasi untuk dijadikan pedoman pada saat implementasi dan menghubungakan masing-masing langkah tersebut menggunakan tanda panah. Urutan menggambarkan proses kerja sistem yang menjelaskan langkah langkah dalam kerja sistem.

1) Fowchart Proses Embed Free Track Atom

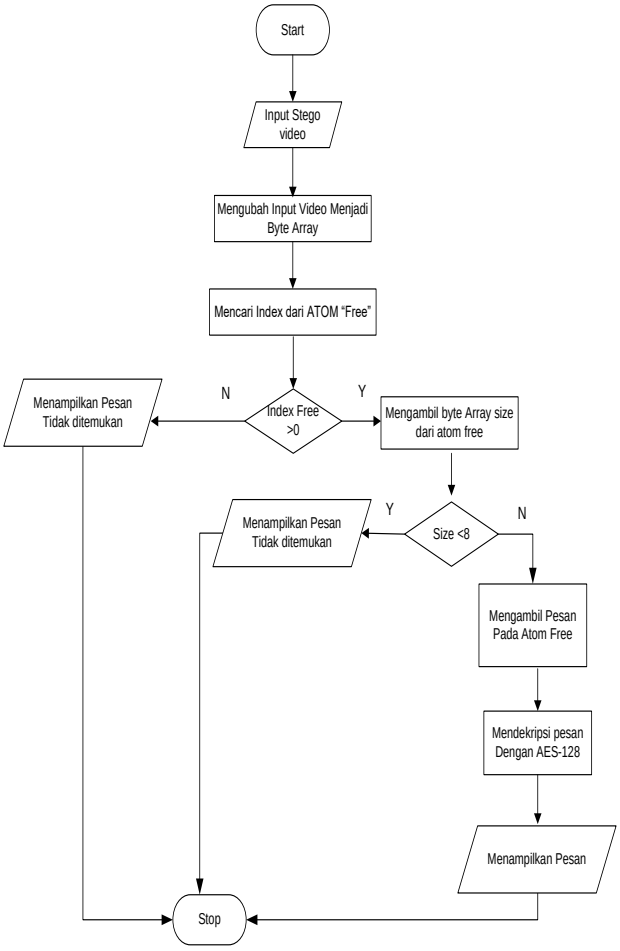
Pada *Flowachart* ini menjelaskan alur proses dalam *Embeeding Free Track* Atom. Dalam Proses ini dijelaskan, bagaimana pesan *secret* dan *file* video digabung hingga membentuk *file* hasil *embed* dan kemudian menyimpannya



Gambar 6 :Flowchart Proses Embed Frree Track Atom

2) Flowchart Proses Retrieve Free Track Atom

Pada *Flowachart* ini menjelaskan alur proses dalam *Retrieve Free Track* Atom. Dalam Proses ini dijelaskan, mulai dari proses pemilihan *file embed* hingga menampilkan pesan hasil proses *Retrieve.*



Gambar 6 :Flowchart Proses Retrieve Frree Track Atom

4. HASIL DAN PEMBAHASAN

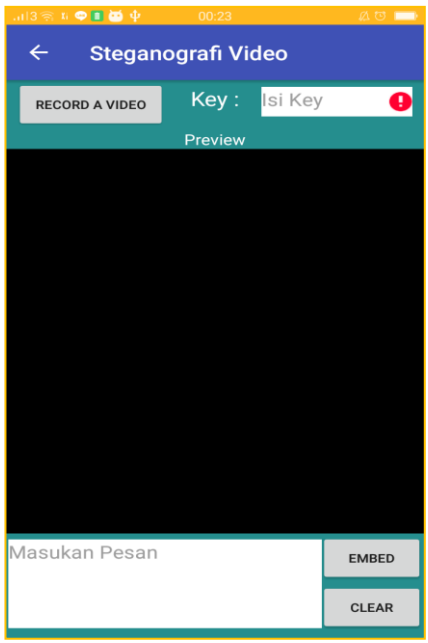
4.1 Tampilan Halaman Menu Utama

Halaman Menu Utama adalah menu pertama kali akan tampil pada saat aplikasi dijalankan. Bentuk tampilannya bisa di lihat pada gambar 7 di bawah ini.

Gambar 7 : Tampilan Halaman Menu Utama

1.2 Tampilan Halaman *Embed*

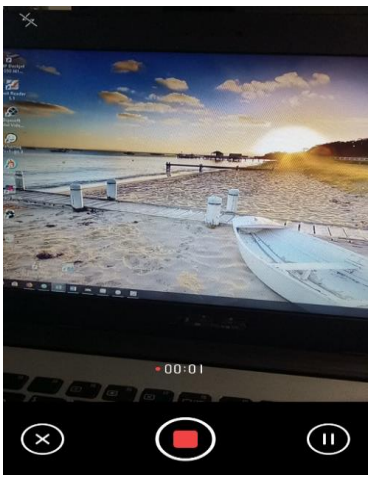
Jika pengguna ingin melakukan proses pembuatan video dan akan menyisipkan pesan rahasia kedalam video maka pengguna memilih menu *embed*, kemudian pengguna menekan tombol *record a* video untuk membuat/merekam video baru yang akan disisipkan pesan, jika pengguna sudah membuat video, kemudian pengguna harus mengisi *Key* dan isi pesan terlebih dahulu, jika semua *form* sudah terisi semua, maka pengguna menkan tombol *embed* untuk menyimpan video dan menyisipkan pesan rahasia kedalam video, jika pengguna memilih tombol *clear* maka pengguna akan membersihkan *form* isi *key* da nisi pesan.



Gambar 8 : Tampilan halaman Embed

1.3 Tampilan Halaman *Record A* Video

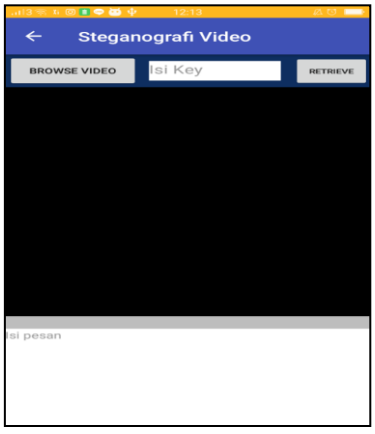
Untuk membuat sebuah video yang akan disisipkan pesan atau informasi rahasia *user* dapat memilih tombol *RECORD A* VIDEO. *User* juga dapat memainkan video yang telah dibuat . Tampilan layar *RECORD A* VIDEO dapat dilihat pada Gambar 9 dibawah ini:



Gambar 9 : Tampilan layar Record a Video

4.4 Tampilan Halaman *Retrieve*

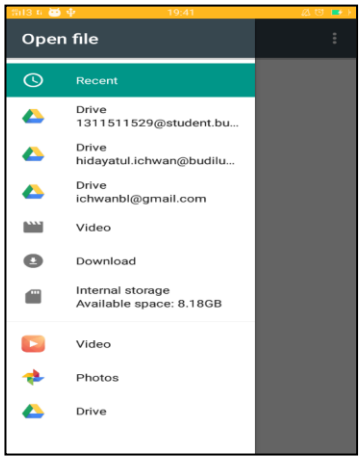
Tampilan layar dari *form* Menu *Retrieve* ini muncul pada saat *Button Retrieve* dipilih di Menu Utama. *User* dapat melakukan proses dekripsi pesan rahasia dan menampilkan pesan dari video yang sudah dilakukan proses *embed*. Pertama user memilih video yang sudah di *embed* dengan cara mengklik tombol *Browse* Video. Kemudian *user* diminta untuk memasukan *password*/kunci awal yang sama pada saat ketika melakukan proses *embed*. *User* dapat memilih tombol *Retrieve* untuk menjalankan proses dekripsi dan menampilkan pesan rahasia yang ada dalam media video. Tombol *Back* untuk kembali kemenu utama. Tampilan layar *form* Menu *Retrieve* dapat dilihat pada Gambar 10 dibawah ini;



Gambar 10 : Tampilan layar Menu Retrieve

4.5 Tampilan Halaman *Browse Video*

Untuk memilih sebuah *file* yang ingin didekripsi dan dikeluarkan dari media video kembali seperti awal, *user* dapat mengklik tombol *Browse* Video. *User* juga dapat memainkan Video yang dipilih dan ter-*embed*. Tampilan layar *Browse* Video dapat dilihat pada Gambar 11 dibawah ini:



Gambar 11 : Tampilan halaman Browse video

4.6 Tampilan Halaman *File* Video Hasil Embed

Untuk memilih *file* video yang sudah di-*embed* maka *user* akan dibedakn nama *file* video dengan nama *encode.* Tampilan layar *file* video yang sudah di-*embed* dengan nama *encode*.

Gambar 12 : Tampilan halaman file video Hasil Embed

4.6 Evaluasi Sistem

Setelah dilakukan analisis dari hasil pengujian aplikasi ini, terdapat beberapa kelebihan dan kekurangan dari aplikasi ini ;

i. Kelebihan Aplikasi

1) Tampilan layar yang memudahkan user menggunakan aplikasi
2) Pesan rahasia yang sudah di-*embed* tidak bisa dibaca ataupun dibuka sebelum di-*retrieve*
3) Video hasil *embed* dibuka dengan aplikasi lain maka pesan *embed* tidak akan bisa dibaca.

ii. Kekurangan Aplikasi

1) Program ini hanya mengenkripsi *text* dan menyisipkan pesan kedalam video
2) Aplikasi ini hanya mengamankan isi pesan
3) Video yang bisa disispkan hanya video hasil rekaman dengan menggunakan aplikasi ini yang berektensi .mp4.
4) Video yang bisa di-*retrieve* hanya video hasil embed dengan menggunakan aplikasi ini.

5. KESIMPULAN

Berdasarkan analisis yang telah dilakukan terhadap permasalahan yang ada, terdapat kesimpulan dan saran untuk pengembangan aplikasi mendatang.

1.1 Kesimpulan

Dari hasil perancangan dan percobaan aplikasi ini. Dapat diambil kesimpulan sebagai berikut :

i. Dengan adanya aplikasi ini, informasi atau data penting yang dimiliki KSO Pertamina EP Axis Sambidoyong Energi dapat terjamin keamanannya dan kerahasiaanya dan mempermudah pengiriman laporan kerja yang berupa video.
ii. Ilmu Kriptografi algoritma AES(Advanced Encryption Standart) dan Steganografi dengan metode Free Track Atom dapat diimplementasikan pada aplikasi keamanan data berbasis mobile.
iii. Aplikasi ini juga dapat mengembalikan data yang sudah diamankan Steganografi dengan metode Free Track Atom tanpa mengalami perubahan sedikitpun pada pesan yang disisipkan.

1.2 Saran

Selain kesimpulan, penulis juga membuat saran-saran agar dapat memperbaiki kekurangaan aplikasi sehingga menjadi aplikasi yang lebih baik lagi. Berikut saran-saran dari pembuatan aplikasi yaitu:

i. Aplikasi ini hanya dapat menyisipkan pesan berupa teks, untuk itu kedepannya perlu dikembangkan tambahan pesan suara, *file* dll.
ii. Untuk kedepannya diharapkan tampilan *icon* menu dan *background* bisa diperbaiki lagi sehingga lebih terlihat menarik.
iii. Algoritma dan metode yang dibuat sebaiknya selalu ditingkatkan, karena dengan semakin berkembangnya ilmu pengetahuan kriptografi dan steganografi maka tidak dapat dipastikan apakah algoritma dan metode ini masih bisa diandalkan.

6. DAFTAR PUSTAKA

[1]Ariyus, D. (2008). *Pengantar Ilmu Kriptografi*, Teori, Analisis, dan Implementasi. Yogyakarta, Andi.

[2] Haryanto, H, Wiryadinata, H.R , Afif, M. (2014). Implementasi Kombinasi Algoritma Enkripsi Aes 128 Dan Algoritma Kompresi Shannon-Fano, Jurnal SETRUM Vol.3, No. 1 Juni 2014.

[3] Pujianto (2016). "Model Keamanan Pesan Pada Video Menggunakan Metode *One's omplement Cryptogaphy Dan Track Free Atom Steganogrphy", Tesis.* Pasca Sarjana Universitas Budi Luhur Jakarta.