ISSN : 2302-3805

IMPLEMENTASI TEKNIK STEGANOGRAFI DENGAN KRIPTOGRAFI KUNCI PRIVATE AES UNTUK KEAMANAN FILE GAMBAR BERBASIS ANDROID

Ari Muzakir

Ilmu KomputerUniversitas Bina Darma Palembang
Jl A. Yani No.03, Plaju, Palembang, Sumatera Selatan 30257
Email : arimuzakir@binadarma.ac.id

Abstrak

Teknologi berbasis mobile saat ini berkembang sangat cepat hampir diseluruh bidang industri dan sosial. Maka dari itu faktor keamanan sangat berperan penting, sehingga seluruh aplikasi berbasis mobile butuh keamanan. Saat ini tradisi selfie dikalangan anak-anak sampai dewasa menjadi suatu kebiasaan yang dari segi keamanan penting. Hampir semua masyarakat memiliki smartphone Android. Foto merupakan sesuatu karya pribadi yang dapat tersebar bebas di media. Maka dari itu dibutuhkan suatu sistem yang dapat menjaga privasi atau hak cipta dari karya tersebut. Teknik steganografi merupakan suatu seni penyembunyian informasi dengan cara penyisipan pada suatu media gambar. Dalam membangun perangkat lunak steganografi pada citra digital file gambar jpeg dengan menggunakan bahasa pemrograman java, yang mengeksploitasi sistem kekuatan penglihatan manusia, dengan menyembunyikan sebuah pesan tersembunyi atau informasi sehingga menghasilkan file gambar yang mempunyai kualitas tidak jauh berbeda dengan citra digital file gambar aslinya. Metode yang digunakan untuk penyembunyian pesan rahasia pada aplikasi ini adalah dengan cara menyisipkan pesan ke dalam bit standar AES (edvance encryption standard). Sistem steganografi disini mempunyai alur proses tersendiri yaitu proses sistem enkripsi dan deskripsi pesan yang berfungsi untuk menyisipkan pesan kedalam gambar jpeg dan mengungkap kembali pesan tersebut dari gambar jpeg. Hasil akhir dari penelitian ini adalah suatu aplikasi pengolahan citra gambar yang aman, dimana sumber gambar dapat diambil dari kamera langsung atau dari file galeri ponsel. Selanjutnya gambar dari hasil pengolahan dapat langsung di share via sosial media yang telah terinstal di ponsel android.

Kata kunci: *Steganografi, keamanan gambar, advance encryption standar*

1. Pendahuluan

Smartphone Android memiliki berbagai keunggulan sebagai *software* yang memakai basis kode komputer yang bisa didistribusikan secara *open source* sehingga pengguna dapat mengembangkan sistem operasi sesuai dengan kebutuhan dan keinginannya. *Smartphone* Android yang terus berkembang dan semakin cangggih sehingga mempermudah seseorang untuk bermedia sosial, bermain *games* selain itu juga penguna dapat berfoto-foto dan menghasilkan sebuah karya. Namun masih kurangnya pengamanan pada gambar yang dihasilkan sehingga gambar bisa di akui dan dipublikasikan oleh orang-orang yang tidak bertanggung jawab.

Dalam menjaga keamanan data mengkombinasikan teknik steganografi dengan algoritma AES yang merupakan kriptografi kunci private atau simetris. Metode steganografi merupakan metode yang bisa menyembunyikan pesan kedalam sebuah media gambar dengan sedemikian rupa sehingga orang lain tidak menyadari ada pesan di dalam gambar tersebut. Pesan inti tersebut tetap dipertahankan, hanya dalam penyimpananya dikaburkan atau disembunyikan dengan berbagai cara. Hanya pihak yang sah saja yang dapat mengetahui pesan tersebut. Kata steganografi terdiri dari dua kata yaitu steganos dan graphein yang berarti tulisan tersembunyi “menulis tulisan yang tersembunyi atau terselubung” [2].

Dalam proses penyembunyian pesan mengunakan algoritma kriptografi merupakan salah satu metode pengamanan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data serta keaslian pengiriman. AES (Advanced Encryption Standard) – Rijndael merupakan algoritma kriptografi bernama Rijndael didesain oleh Vincent Rijmen dan John Daemen asal Belgia. Algoritma Rijndael inilah yang kemudian dikenal dengan AES (Advanced Encryption Standards) yang diadopsi menjadi standard algoritma kriptografi [1]. Rijndael mendukung panjang kunci 128 *bit* sampai 256 *bit*, maka dikenal dengan AES-128, AES-192, dan AES-256 [4].

Saat ini banyak aplikasi pengolahan gambar yang tersedia bebas baik berbasis aplikasi desktop maupun aplikasi *smartphone* . Pada aplikasi *smartphone* yang paling banyak digunakan untuk ber-selfie, biasanya hanya menyediakan untuk proses editing serta manipulasi saja. Sehingga informasi yang terkandung dari dokumen

ISSN : 2302-3805

gambar tersebut dengan mudah di manipulasi oleh orang lain dan dapat dijadikan sebagai hak milik orang lain juga.

Berdasarkan penjelasan tersebut, maka solusi yang dilakukan dalam penelitian ini yaitu mengimplementasikan teknik steganografi menggunakan algoritma kunci private AES kedalam *smartphone* berbasis android, sehingga para pengguna ponsel Android yang memiliki hobi selfi dapat mengabadikan gambar mereka kemudian menyisipkan suatu hak cipta pada gambar tersebut.

2. Pembahasan

Metode yang digunakan dalam penelitian ini adalah metode deskriptif. Dimana metode deskriptif yaitu metode mengemukakan masalah dengan mengumpulkan data dan menyajikan data terhadap suatu objek penelitian, yang bertujuan untuk mengambil suatu kesimpulan dari pembahasan yang dilakukan.

Untuk membuat rancangan sebuah sistem harus memilih salah satu metode pengembangan sistem, metode yang dipakai yaitu metode mobile-D, yang merupakan metodologi pembangunan perangkat lunak khusus dirancang untuk pengembangan aplikasi mobile yang didasarkan pada praktek agile. Karakteristik pada metode mobile-D yaitu skala kecil, perangkat lunak aplikasi yang dikembangkan dalam lingkungan yang sangat dinamis oleh tim kecil menengah, dengan menggunakan pendekatan berorientasi objek, dalam siklus pengembangan yang relatif singkat. Bagian berikut memberikan gambaran singkat metode agile, berfokus pada kesesuaian mereka untuk pengembangan aplikasi mobile [3].

Tahapan mobile-D yaitu seperti pada gambar 1, yang terdiri dari explore, initialize, productinize, stabilize, system test and fix. Berdasarkan hasil dari perencanaan, perancangan, pengkodean dan pengujian ini, maka hasil yang di dapat adalah aplikasi pengamanan gambar berfoemat jpeg dengan teknik steganografi menggunakan algoritma AES berbasis Android.

Gambar 1. *Tahapan pada metode mobile-D*

Explore

Penulis melakukan perencanaan pembuatan aplikasi pengamanan gambar berbasis *android*. Berikut tahapan pada *explore :*

1. *Stakeholder establishment.* Terdiri dari :
   a)Gambar berformat jpeg sebagai bahan yang diperlukan penulis.
   b) Pengguna
2. *Scope definition.* Tahapan yang dilakukan adalah :
   a) Menetapkan waktu pembuatan aplikasi pengamanan berbasis *android*.
   b) Aplikasi pengamanan gambar berbasis *android ini,* mendukung sistem operasi *android versi* 4.0 *(ice cream sandwich)* sampai 5.0 *(Lolipop).*

Penulis mempersiapkan semua sumber daya baik fisik dan teknis, yaitu mempersiapkan :

1) *Software,* ADT dan *eclipse.*
2) Data-data gambar berformat jpge, tentang ukuran gambar, jenis gambar.
3) *Hardware,* yang menunjang pembuatan aplikasi pengamanan gambar berbasis *android* ini, yakni :
   a) *Notebook Acer Aspire* V5-132 Series, dengan RAM 2 GB, *harddisk* 500 GB, *processor intel inside.*
   b) *Smartphone Asus Zenfone* (*android* 5.0)

3. *Project establishment.* Berikut yang dilakukan pada tahapan *project establishment* :

   a) Pada lingkungan kerja pembuatan aplikasi pengamanan gambar berformat jpeg menggunakan *software* ADT, yang terdiri dari android-sdk dan eclipse-SDK-3.6.2-win32.
   b) Penulis mempersiapkan data-data gambar yang diambil dari jenis format gambar, yang berkaitan dengan jenis informasi yang penulis butuhkan, yaitu mengenai jenis gambar, ukuran gambar.

Berikut tahapan yang dilakukan pada *initialize :*

1. *Project set-up,* terdiri dari persiapan ADT untuk diinstal dalam *laptop*.
2. *Planning day,* tahapan yang dilakukan pada *planning day* yaitu :
   a) Mengelompokan data-data yang didapat sesuai dengan isi dari steganografi dengan AES yang akan dibuat.
   b) Mempersiapkan arsitektur steganografi dengan AES yakni *coding* yang dibuat masih dalam bentuk *pseudocode,* berarti bukanlah kode program yang sebenarnya, melainkan dengan menggunakan simbol-simbol yang mirip atau menyerupai kode program yang ditulis dengan menggunakan suatu bahasa pemrograman tertentu. Berikut diperlihatkan pada gambar 2.

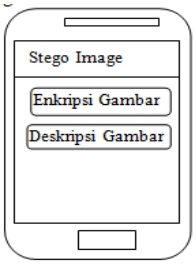
```
File  Edit  Format  View  Help
PROGRAM steganografi dengan aes
{
Program untuk mendapatkan output atau keluaran
hasil gambar yang telah di enkripsikan melalaui
steganografi image dengan aes
Masukan  : data gambar dan sisipkan pesan
Keluaran : info gamabr telah disisipi pesan
}
DEKLARASI
Datagambar : integer
Info gambartelah disisipi pesan : integer
ALGORITMA
Read (pesan yang disisipkan, step)
Read (info yang disisipkan, step)
```

Gambar 2. *Script Pseudocode* isi steganografi dengan AES

   c) Membuat jadwal pembuatan aplikasi yaitu :
3. Hari Percobaan (*Working Day* dan *Release Day*).

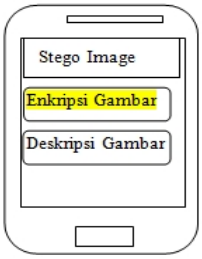
Membuat antar muka tampilan aplikasi pengamanan gambar dan merilis antar muka yang telah dibuat. Berikut gambar antar muka yang dirilis :

a) Rancangan Antar Muka. Pada gambar 3 memperlihatkan tampilan menu awal saat membuka aplikasi pengaman gambar berbasis *android*, yang terdiri dari : Menu. Berisi enkripsi, deskripsi, dan Tentang Aplikasi yang terdapat di aplikasi pengamanan gambar.



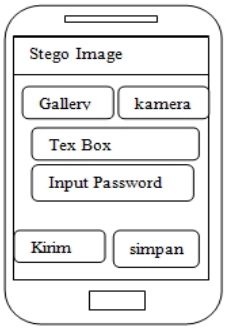
Gambar 3. Rancangan Antar Muka

b) Rancangan enkripsi. Gambar 4 adalah jenis informasi tentang penyisipan pesan. Dan saat memilih enkripsi maka akan muncul pilihan untuk pengambilan gambar dari kamera atau gambar yang tersimpan di dalam *gallery smartphone* . Sebagai contoh gambar 10, saat memilih tombol form card.



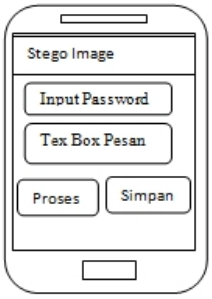
Gambar 4. Enkripsi pemilihan Gambar

a) Rancangan proses penyisipan pesan. Gambar 5 memperlihatkan bagai mana proses penyisipan pesan, maka akan tampil *detail* tentang nama gambar awal, dan input pesan yang akan disisipkan kemudian pilih proses enkripsi.



Gambar 5. Antar muka Enkripsi

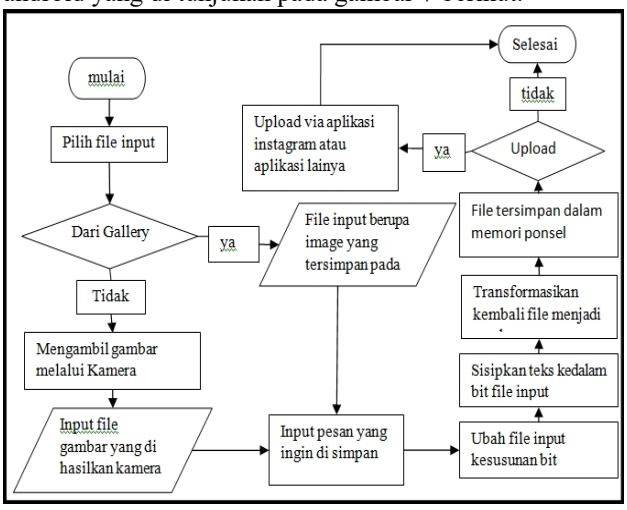
a) Rancangan antar muka deskripsi berisikan input password, hasil enkripsi pesan dalam gambar, proses, dan simpan yang ditunjukkan pada gambar 6 berikut.



Gambar 6. Deskripsi Gambar

Implementasi

Hasil dari penelitian ini akan diujicoba menggunakan *smartphone* Android dengan spesifikasi processor dual core 1,0Ghz, RAM 1Gb dan sistem operasi Android versi 5,0. Perancangan sistem merupakan suatu proses yang menggambarkan bagaimana sistem dibangun untuk memenuhi kebutuhan pada fase analisis dalam menggambarkan aplikasi pengamanan gambar berbasis android yang di tunjukan pada gambar 7 berikut.



Gambar 7. Rancangan Alur Aplikasi

Berikut ini adalah penjelasan dari perancangan alur aplikasi yaitu;

a. Buka aplikasi setelah aplikasi terbuka akan muncul pilihan untuk pengambilan gambar melalui *gallery* atau kamera.
b. Jika pilih ambil gambar dari *gallery* maka akn keluar notifikasi berbrntuk *teks box* untuk menyisipkan pesan, jika sudah ubah pesan *teks* dalam bentuk *bit* yang akan disisipkan pada gambar.
c. Jika pilih ambil gambar melalui kamera, ambil gambar terlebih dahulu jika sudah maka akn keluar *notifikasi* berbrntuk *teks box* untuk menyisipkan pesan jika sudah ubah pesan *teks* dalam bentuk *bit* yang akan disisipkan pada file gambar.
d. Gambar akan *otomatis mentansformasikan* kembali dalam bentuk gambar.
e. Jika sudah ditransformasikan di dalam aplikasi terdapat *tools* pilihan apakah akan dikirim kemedia sosial jika

ya, maka proses selesai, dan jika tidak maka gambar akan tersimpan pada memori ponsel dan proses selesai.

Productionize

Terdapat tiga tahapan dalam *productinize* yang di tunjukan pada gambar yaitu:

1) *Planning day.* Penulis membuat menu Home, Enkrpsi, Deskripsi, dan keterangan.
   a. Menu home adalah menu utama antar muka aplikasi pengamanan gambar berformat jpeg
   b. Menu enkripsi adalah menu untuk pengambilan gambar dan penyisipan pesan kedalam gambar.
   c. Menu deskripsi adalah menu dimana pengambilan gambar yang tersimpan di galleri *smartphone* dan pengekstrakan pesan yang terdapat dalam gamabr.
   d. Menu Keterangan adalah menu menu yang berisikan tentang aplikasi dan penulis.
2) *Working day.*

Penulis mencari *coding* program sesuai dengan rencana pembuatan aplikasi gambar. Pencarian coding dilakukan dengan cara,

a Studi Pustaka
Mengumpulkan data dengan cara mencari dan mempelajari data-data dari buku-buku ataupun *referensi* lain yang berhubungan dengan penulisan laporan penelitian ini.

b Dokumentasi
Mengumpulkan data-data atau *dokumen* atau *informasi* mengenai penelitian.

c Studi Literatur
Studi literature adalah mencari *refernsi* teori yang *relefan* dengan khasus atau permasalahan yang ditentukan. *Referensi* tersebut berisikan teori tentang, tentang tknik *steganografi*, metode-metode dalam *steganografi,* metode algoritma AES, serta enkripsi dan deskripsi algoritma AES, dan sumber ilmiah lain seperti situs internet ataupun artikel dokumen teks yang berhubungan dengan penelitian.

3) *Release day.*

Penulis mengumpulkan coding program yang telah lolos tes dan menangani setiap kesalahan dalam pembuatan aplikasi pengamanan gambar.

Stabilize

Pada tahapan *stabilize* terdapat empat tahapan yaitu :

1) Planning day.

Penulis memilih dan merencanakan isi dari menu enkripsi dan deskripsi, penulis melakukan tes penggunaan (yaitu apakah ada cacat) dan didokumentasikan, tes dilakukan pada *emulator*.

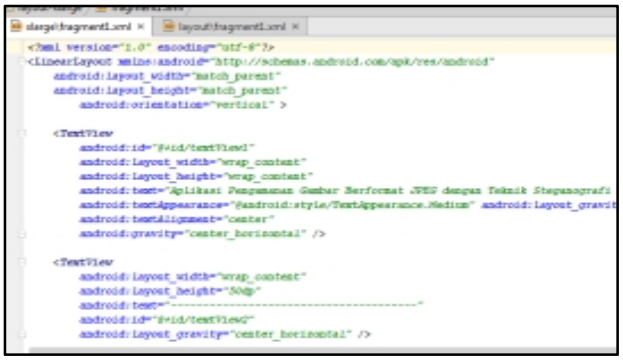
2) Working Day.

Tahapan yang dilakukan pada *working day* adalah :

a. Memecahkan masalah dalam pembuatan aplikasi pengamanan gambar, yakni setiap kesalahan *coding* yang terjadi maka akan dilakukan perbaikan.
b. Sebelum *coding* dilakukan, penulis menulis coding ditempat lain (ditulis sebelum kode program dijalankan pada *eclipse*). Hasil backup coding dapat dilihat pada gambar 8.

Gambar 8. *Backup Coding*

c. Kegiatan memulai pembuatan aplikasi pengamanan gambar berbasis *android*. Penggalan coding dalam pembuatan program dapat dilihat pada gambar 9.



Gambar 9. Coding program aplikai pengamanan gambar

d. Hasil tampilan awal aplikasi pengaman gambar berformat jpg.

3) *Documentation wrap-up.* Pada tahapan ini yang dilakukan, yaitu :

a. Aplikasi pengamanan gambar ini dibuat dengan jangka waktu yang pendek, yaitu dari bulan April 2015 dan selesai pada bulan Juli 2015.

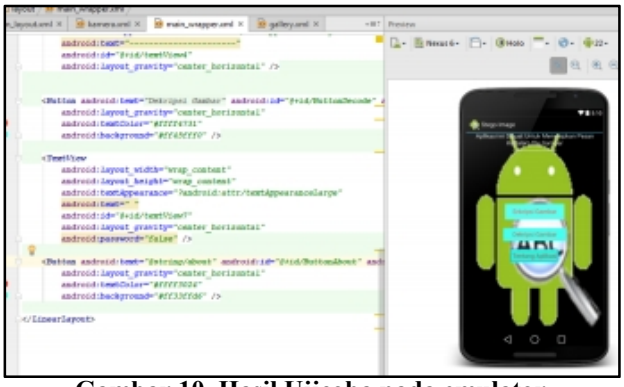
b. Aplikasi pengamanan gambar dibuat agar mudah dimengerti bagaimana cara pengoperasiannya.

4) *Release day*. Penulis memastikan bahwa aplikasi pengamanan gambar berbasis *android* sudah siap digunakan**,** dan memastikan pembuatan aplikasi pengaman gambar telah sesuai dengan rancangan awal.

System test and fix

Pada tahapan ini penulis melihat apakah aplkiasi menghasilkan fungsi dengan benar, dan telah memperbaiki kekurangan yang ditemukan. Tahapan yang dilakukan yakni :

1) *System tes.* Melakukan tes apakah terdapat kesalahan pada aplikasi pengamanan gambar berbasis *android,* penulis melakukan tes pada *emulator*.



Gambar 10. Hasil Ujicoba pada emulator

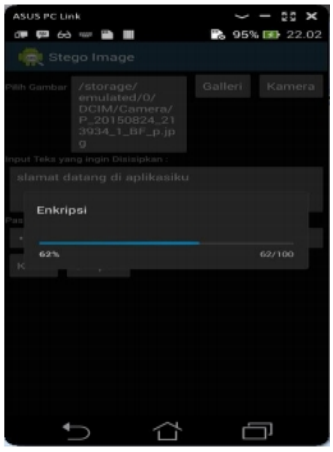
2) *Planning day*. Meningkatkan proses pembuatan aplikasi pengamanan gambar agar sesuai kebutuhan yang penulis rencanakan, penulis merencanakan adanya menu Enkripsi dan deskripsi yang akan membantu pengguna untuk menyisipkan pesan dan mendeskripsikan pesan yang disisipkan.

3) *Working day*. Penulis melakukan perbaikan sesuai fungsi yang direncanakan pada hari perencanaan, yaitu membuat menu enkripsi pada aplikasi pengamanan gambar.

Gambar 11. Hasil ujicoba menu enkripsi gambar

Pada gambar 12 berikut memperlihatkan proses pemilihan gambar pada galeri. Cara lain yang bisa dilakukan juga adalah mengaktifkan modul kamera sehingga pengambilan objek melalui kamera ponsel.

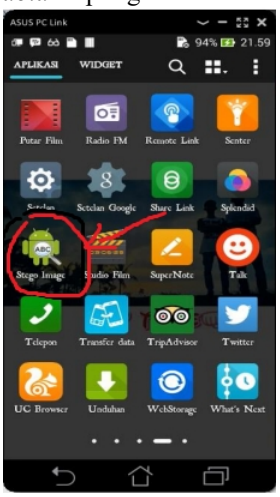
Gambar 13. Hasil ujicoba pengambilan dan enkripsi melalui modul kamera



Gambar 14. Hasil proses enkripsi gambar

4) *Release day.* Tahapan yang dilakukan, yaitu :

a. Mempersiapkan aplikasi pengamanan gambar yang telah jadi. Untuk kemudian memasukan apk ke *smartphone* android.
b. Memasukan apk ke dalam *smartphone android*.
c. Aplikasi pengamanan gambar berformat jpeg berbasis *andoid* siap digunakan



Gambar 15. Aplikasi terinstal di *smartphone* Android

ISSN : 2302-3805

3. Kesimpulan

Berdasarkan dari penelitian yang telah dilaksanakan dan diuraikan pada penjelasan sebelumnya, maka model pengamanan gambar menggunakan teknik steganografi dengan algoritma AES dapat disimpulkan sebagai berikut:

1. Aplikasi pengamanan gambar berformat jpeg dengan teknik steganografi mengunakan algoritma aes berbasis android telah berhasil dibangun sebagai aplikasi penyisipan teks gambar menggunakan perangkat mobile android.
2. Dalam menentukan lokasi penyimpanan gambar yang terdapat dua pilihan yaitu penyimpanan kedalam gallery smart phone berbasis android dan penyimpanan gambar melaui media sosial atau dikirim melalui BBM dan lain-lain.

Daftar Pustaka

[1] Pradana,R.O., *Analisis Perbandingan Algoritma Rijndael dan Algoritma Twofish Pada Proses Pengiriman Data Teks Menggunakan Jaringan LAN (Local Are Network)*.2011.

[2] Sellears, D., An Introduction to Steganography. http://totse.mattfast1.com/en/privacy/encryption/163947.html.1996

[3] Spataru,A,C., *Agile Development Methods for Mobile Applications*, School of Informatics, University of Edinburgh, https://www.inf.ed.ac.uk/publications/thesis/online/IM100767.pdf. 2010.

[4] Wahyudi, K., *Aplikasi Steganografi Untuk Pertukaran Pesan Dengan Menggunakan Teknik Steganografi Dan Algoritma AES*.2008.

Biodata Penulis

Ari Muzakir, memperoleh gelar Sarjana Komputer (S.Kom), Program Studi Teknik Informatika Universitas Bina Darma Palembang, lulus tahun 2009. Memperoleh gelar *Master* of Computer Science (M.Cs) Program Pasca Sarjana Magister Ilmu Komputer Universitas Gajah Mada Yogyakarta, lulus tahun 2012. Saat ini menjadi Dosen di Universitas Bina Darma Palembang.