PENGECEKAN KEASLIAN GAMBAR MENGGUNAKAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* 128 (AES), *VIGENERE CIPHER* DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT* (LSB) BERBASIS ANDROID PADA CV.WIRATAMA

Diajeng Prastyanti Priyadi [1)], **Utomo Budiyanto** [2)]
[1, 2] *Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur*
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260

E-mail : diajengdiamon@gmail.com[1)], utomo.budiyanto@budiluhur.ac.id [2)]

Abstract

An information of a digital image is stored in a metadata called EXIF. The stored information is limited and can be easily read and deleted. This would be harmful because it can be used to manipulate the report. A combination of cryptography and steganography is used in order to accommodate the information more effectively and to maintain the security and authenticity of digital data as well. The password is first encrypted using Vigenere Cipher algorithm to obtain a ciphertext. The ciphertext is then used as a secret key message in the form of a text. The text will be encrypted using AES algorithm. The encrypted text is hidden into media digital image by using LSB. The result of this research is an Android based application to validate the authenticity of an image using AES, Vigener Cipher, and LSB methods. This application can provide information geottaging as validation. The encoding process takes approximately 7.76 seconds and the decoding process takes approximately 1.77 seconds. A message inserted into the cover image can not be seen, and need to be decrypted first to read the message.

Keywords: *Cryptography, Advance Encryption Standard 128 (AES), Vigenere Cipher, Steganography, Least Significant Bit (LSB), Geolocation*

Abstrak

Sebuah informasi dari sebuah gambar digital disimpan dalam metadata yang disebut EXIF. Informasi yang disimpan terbatas dan dapat dengan mudah dibaca dan dihapus. Ini akan berbahaya karena dapat digunakan untuk memanipulasi laporan. Kombinasi kriptografi dan steganografi digunakan untuk menampung informasi yang lebih efektif dan untuk menjaga keamanan dan keaslian data digital juga. password pertama dienkripsi menggunakan Vigenere Cipher algoritma untuk mendapatkan ciphertext a. ciphertext tersebut kemudian digunakan sebagai pesan kunci rahasia dalam bentuk teks. teks akan dienkripsi menggunakan algoritma AES. teks terenkripsi tersembunyi dalam gambar media digital dengan menggunakan LSB. Hasil dari penelitian ini adalah sebuah aplikasi berbasis Android untuk memvalidasi keaslian gambar menggunakan AES, Vigener Cipher, dan LSB metode. Aplikasi ini dapat memberikan informasi geottaging sebagai validasi. Proses encoding berlangsung sekitar 7.76 detik dan proses decoding berlangsung sekitar 1,77 detik. Sebuah pesan dimasukkan ke dalam gambar cover tidak dapat dilihat, dan harus didekripsi dahulu untuk membaca pesan.

Kata kunci*: Kriptografi, Advanced Encryption Standard 128 (AES), Vigenere Cipher, Steganografi, Least Significant Bit (LSB), Geolocation*

1. PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi dan informasi yang semakin pesat memberikan pengaruh cukup besar pada setiap aspek kehidupan manusia. Siapapun dapat memanipulasi data, yang bertujuan untuk menguntungkan dirinya sendiri. Semakin banyaknya kecurangan dalam berkerja dan penipuan terhadap laporan kerja. Dampak negatif dari perkembangan teknologi informasi membuat perusahaan mendapatkan kerugian.

Banyak terjadi kecurangan laporan dikarenakan aplikasi yang mendukung dan memfasilitasi penggunaan dengan mudah memanipulasi data. Informasi umum seperti halnya waktu, lokasi, dan pengaturan fotografi dapat secara mudah diperoleh dengan menggunakan kamera digital dan handphone yang ada saat ini. Informasi-informasi tersebut disimpan ke dalam metadata citra digital yang diambil disebut EXIF. Namun informasi yang dapat disimpan sangat terbatas hanya informasi mengenai pengambilan foto tersebut dan sangat

mudah dibaca dan dihapus oleh orang lain. Atas dasar hal tersebut maka dibutuhkan teknik lain untuk menyimpan informasi-informasi tersebut ke dalam sebuah gambar.

Salah satu unsur metadata yang biasa disimpan dalam EXIF dapat digunakan untuk menemukan atau memvalidasi suatu objek, misalnya data geotagging. Data geotagging ini dapat digunakan untuk mencari posisi objek sekaligus dapat melakukan verifikasi benar atau tidaknya objek berada di tempat tersebut. Oleh karena itu, keamanan ataupun privasi data dapat menjadi sangat penting bila data lokasi yang disimpan itu rahasia ataupun dibutuhkan untuk proses verifikasi.

Bentuk pengamanan informasi dapat dilakukan seperti dengan menggunakan steganografi dan kriptografi. Secara terminologi kedua bentuk pengamanan data tersebut adalah dua hal yang berbeda. Steganografi menyembunyikan informasi ke dalam suatu media tertentu, sedangkan kriptografi mengacak informasi sehingga tidak dapat dimengerti oleh orang lain. Pada teknik steganografi terkadang dapat merubah ukuran citra tergantung teknik atau algoritma apa yang digunakan. Berdasarkan perubahan itu, orang lain dapat mencurigai citra digital yang sudah disisipkan pesan rahasia. Dengan melakukan steganalisis, tentu saja sangat memungkinkan pesan rahasia yang dikirim dapat terbaca oleh orang lain. Untuk meningkatkan keamanan data tersebut maka ditambahkan teknik Kriptografi.

1.2. Tujuan

Penelitian ini mengimplementasikan algoritma kriptografi AES 128, *Vigenere Cipher*, dan metode steganografi LSB untuk menyembunyikan sebuah pesan dalam bentuk teks dan menyisipkanya ke dalam foto agar tidak bisa diakses oleh pengguna yang memang tidak mempunyai wewenang akan hal tersebut. Membuat aplikasi yang memberikan dan mengamankan informasi selain menggunakan EXIF berbasis android. Media steganografi yang digunakan sebagai *cover image* dengan ukuran minimal 600x800px setara dengan 0,94MB. *Password* yang dimasukan minimal 8 karakter dan hanya karakter alfabet dan angka saja

2. LANDASAN TEORI

2.1. Kriptografi

Kriptografi merupakan ilmu dan seni perlindungan keamanan pesan rahasia dengan cara mengacaukan dan menyandikan pesan rahasia menjadi kode-kode rahasia (*ciphertext*) [1]. Cara ini tidak menyembunyikan bahwa adanya pesan rahasia. Orang lain dapat menyadari keberadaan pesan rahasia tersebut, tetapi hanya orang yang mempunyai kuncinya yang dapat membuka pesan rahasia tersebut [2]. Kriptografi digunakan untuk menjaga kerahasiaan pesan yang dikirimkan menggunakan media tertentu sehingga pesan rahasia yang tersembunyi di media tersebut tidak diketahui oleh pihak-pihak yang tidak berhak menerima pesan tersebut.

2.2. Algoritma AES (*Advance Encryption Standard*)

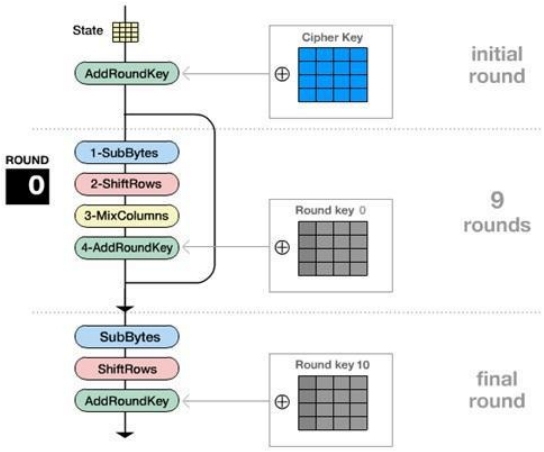
Rijndael termasuk dalam jenis algoritma kriptografi yang bersifat simetris dan *cipher blok*. Setiap pesan yang data akan dimasukkan ke dalam *cipher block* hingga nantinya menjadi *ciphertext*. dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. Secara umum desain algoritma AES terdiri dari *secret key* dan *plaintext* yang kemudian akan menghasilkan *ciphertext*. *Rijndael* merupakan ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit.

Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Untuk kunci 128 bit harus melalui 10 proses putaran. Selain itu pemilihan ukuran blok juga memperngaruhi hasil *ciphertext*. untuk kombinasi putaran blok bisa dilihat pada Tabel 2.1.

Tabel 2.1 : Key-Block Round Combination

Tipe	Jumlah Key (Nk)	Besar Blok (Nb)	Jumlah Round (Nr)
AES - 128	4	4	10
AES - 192	6	4	
AES - 256	8	4	

Algoritma AES menggunakan subtitusi dan permutasi, dan sejumlah putaran (cipher berulang), dimana setiap putaran menggunakan kunci yang berbeda (kunci setiap putaran disebut *round key*) [3]. Untuk gambaran secara umum pada proses enkripsi menggunakan AES bisa dilihat pada gambar 2.1.

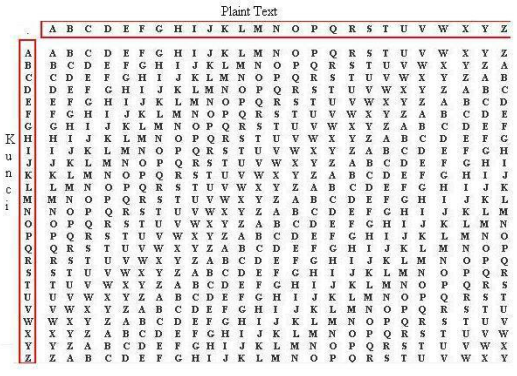


Gambar 2.1 : Diagram Proses Enkripsi AES

2.3. *Vigenere Cipher*

Vigenere Cipher merupakan algoritma kriptografi klasik. Operasi pada algoritma kriptografi klasik berbasis pada operasi karakter, sedangkan operasi pada algoritma kriptografi modern berbasis pasa operasi bit. Dalam kriptografi klasik *vigenere cipher* termasuk ke dalam cipheri subtitusi abjad majemuk, yang terbuat dari sejumlah cipher abjad tunggal, masing-masing dengan kunci yang berbeda.

Vigenere Cipher menggunakan bujur sangkar *vigenere* seperti pada gambar 2.2 untuk melakukan enkripsi. Pada bujursangkar tersebut, kolom paling kiri menyatakan huruf-huruf kunci, dan baris paling atas menyatakan *plaintext*, sedangkan karakter-karakter lainya menunjukkan karakter *ciphertext*. Karakter *ciphertext* ditentukan dengan menggunakan prinsip *Caesar Cipher*. Kunci : K = k1k2 … km ki untuk 1≤ i ≤ m menyatakan jumlah pergeserah pada huruf ke-i. karakter *ciphertext* ci(p) = (p + ki) mod 26 (*) [3].



Gambar 2.2 : Bujur Sangkar Vigenere Cipher

Bujur sangkar *vigenere* digunakan untuk mendapatkan *ciphertext* dengan menggunakan kunci yang telah ditentukan. Jika pajang kunci lebih pendek dari pada panjang *plaintext*, maka kunci diulang penggunaanya (sistem periodik). Jika panjang kunci adalah m, maka periodenya adalah m. secara singkat, enkripsi dapat di gambarkan sebagai berikut:

p (plainteks) : KRIPTOGRAFI
k (kunci) : LAMPIONLAMP
c (cipherteks) : VRUEBCTCARX

Penggunaan bujur sangkar vigenere pada enkripsi serupa dengan penjumlahan (dalam desimal) *plantext* dengan kunci, lalu modul 26, sehingga dapat di rumuskan sebagai berikut: $Enkripsi{:}ci=(pi)=(pi+ki) \quad mod \quad 26$ $Dekripsi{:}pi=D(ci)=(ci-ki) mod\ 26$.

Dekripsi *vigenere cipher* dengan menggunakan bujur sangkar *vigenere* dilakukan dengan cara berkebalikan enkripsi, yaitu dengan menarik garis mendatar dari huruf kunci sampai ke huruf *ciphertext* yang ditunjukan, kemudian dari huruf *ciphertext* tersebut tarik garis vertikal ke atas sampai ke huruf *plaintext*.

Untuk memecahkan *Vigenere Cipher*, perlu mengetahui kuncinya. Jika periode atau panjang kunci (m) diketahui, maka kunci dapat diterka dengan *exhaustive search*. Namun, diperlukan hingga 26^m kali percobaan untuk mendapatkan kunci yang menghasilkan *plaintext* sesuai.

2.4. Steganografi

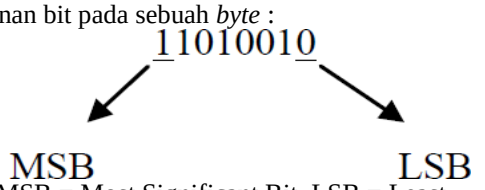
Steganografi (steganography) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding massage*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia [4]. Steganografi memanfaatkan media digital untuk menyisipkan pesan rahasia melalui kode biner pada media digital tersebut, seperti gambar, audio, teks atau file biner.

2.5. Metode *Least Significant Bit* (LSB)

Least Significant Bit (LSB) merupakan salah satu metode steganografi, metode ini digunakan untuk menyisipkan data rahasia ke bit paling kecil dari nilai piksel yang ada di *stego image* [5]. Teknik steganografi dengan menggunkan metode *Least Significant Bit* (LSB) adalah teknik yang paling sederhana, pendekatan yang sederhana untuk menyisipkan informasi di dalam suatu citra digital . Metode ini memodifikasi bit-bit yang termasuk bit LSB pada setiap *byte color* pada sebuah piksel. Bit-bit LSB ini akan dimodifikasi dengan menggantikan setiap LSB yang ada dengan bit-bit pesan rahasia yang ingin disembunyikan. Penyembunyian pesan rahasia selesai pada saat semua bit pesan rahasia menggantikan bit LSB file tersebut.

Metode ini menyisipkan bit-bit pesan rahasia pada bit rendah atau bit yang paling kanan (LSB) pasa data *pixel* yang menyusun file tersebut. Pada berkas bitmap 24 bit, setiap *pixel* (titik) pada gambar tersebut terdiri dari susunan tiga warna yaitu merah, hijau, dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (*byte*) dari 0

sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikin, pada setiap *pixel* berkas bitmap 24 bit dapat menyisipkan 3 bit data. Contoh penggunaan LSB, sebuah susunan bit pada sebuah *byte* :



(MSB = Most Significant Bit, LSB = Least Significant Bit)

Jika digunakan image 24 bit color sebagai cover, sebuah bit dari masing-masing komponen *Red*, *Green*, dan *Blue*; dapat digunakan sehingga 3 bit dapat disimpan pada setiap piksel. Sebuah *image* 800 x 600 piksel dapat digunakan untuk menyembunyikan 1.440.000 bit (180.000 *bytes*) data rahasia. Misalnya, terdapat piksel dari image 24 bit:

Color :
(00100111 11101001 11001000) (00100111 11001000 11101001 11001000 00100111 11101001)

Jika diinginkan menyembunyikan karakter A dengan nilai biner 01000001 dihasilkan :
(00100110 11101001 11001000) (00100110 11001000 11101000) (11001000 00100111 11101001)

Dapat dilihat bahwa hanya 3 bit saja yang perlu diubah untuk menyembunyikan karakter A ini. Perubahan pada LSB ini akan terlalu kecil untuk terdeteksi oleh mata manusia sehingga pesan dapat disembunyikan secara efektif. Jika digunakan *image* 8 bit color sebagai *cover image*, maka hanya satu bit saja dari setiap piksel warna yang dapat dimodifikasi sehingga pemilihan image harus dilakukan dengan sangat hati-hati, karena perubahan LSB dapat menyebabkan terjadinya perubahan warna yang ditampilkan pada *image*. Akan lebih baik jika berupa *grayscale* karena perubahan warnanya akan lebih sulit dideteksi oleh mata manusia.

2.6. Geotagging

Geotagging dapat membantu untuk menemukan berbagai macam informasi lokasi yang cukup spesifik. *Geotagging* itu sendiri merupakan proses menambahkan identifikasi geografis seperti garis lintang dan bujur [7]. Data yang dimasukan biasanya terdiri dari *logitude*, *latitude*, *altitude*, *bearing* (navigasi), jarak, akurasi data, dan nama tempat. Dengan menggunakan *geotagging*, pengguna dapat menemukan suatu lokasi dengan informasi yang lebih spesifik. Pengguna dapat menemukan gambaran pada lokasi tertentu dengan memasukan arah lintang dan bujur. Dengan teknik geotaging ini dapat menunjukan lokasi tersebut.

Untuk memasukan geolocation ke dalam sebuah media tentunya harus mengetahui terlebih dahulu koordinat ataupun informasi geografis yang terkait lokasi tersebut. Dewasa ini semakin canggih kamera maupun ponsel mereka sudah dilengkapi dengan GPS dan *software* pendukung sehingga dapat secara otomatis untuk melakukan *geotagging* ke dalam sebuah media. Namun juga bisa melakukan geotagging secara manual ke dalam sebuah media seperti photo dengan menggunakan aplikasi-aplikasi untuk memasukan informasi ke dalam sebuah photo.

3. ANALISA MASALAH DAN PERANCANGAN PROGRAM

3.1 Analisa Masalah

CV. Wiratama adalah perusahaan atau instansi bergerak di bidang konstruksi dan instalasi listrik. CV. Wiratama memiliki beberapa data yang akan dijadikan laporan hasil kerja para pegawai. Data yang berupa foto objek pekerjaan yang sedang dilakukan. Data ini berfungsi sebagai validasi hasil kerja dan peningkatan hasil kerja mereka. Untuk mengamankan kemungkinan data dimanipulasi oleh pegawai, dan kemungkinan terjadi kecurangan pada saat memberikan laporan pekerjaan. Maka dari itu kemanan data sangat penting untuk meningkatan keamanan data agar tidak ada pihak yang dirugikan. Kemanan data sangat diperlukan untuk memberikan keamanan, keakuratan, dan keaslian data. Maka dari itu salah satu cara agar data yang diberikan oleh para pegawai benar-benar valid dan terjaga keasliannya adalah dengan menyisipkan data dengan informasi tentang titik koordinat dimana foto tersebut diambil dan juga berisikan pesan yang akan disisipkan ke dalam foto yang telah diambil, sehingga pegawai tidak bisa memanipulasi data.

Penyelesaian masalah dari permasalahan yang diuraikan di atas, untuk mengamankan data harus ada mekanisme untuk mengamankan data. Mekanisme yang dipilih adalah dengan menyisipkan pesan ke dalam sebuah bit pada foto yang sebelumnya pesan sudah diacak sehingga tidak dapat dibuka. Pengguna dapat melihat data yang sudah diamankan jika mempunyai kunci, jika kuci yang di miliki sesuai dengan kuci yang sebenarnya maka data tersebut dapat dilihat tanpa mengalami perubahan.

Metode yang dipilih untuk menyisipkan pesan kedalam foto dengan metode algoritma LSB dan metode yang digunakan untuk mengacak pesan tersebut dengan menggunakan algoritma AES. Aplikasi ini dibuat berbasis android yang dibangun dengan bahasa pemograman Java. Dengan adanya aplikasi ini diharapkan suatu data dapat terjaga keasliannya.

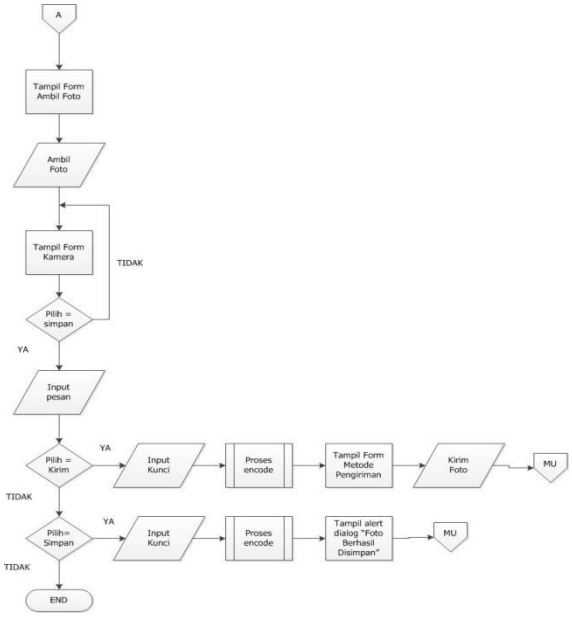
Agar tidak disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab dan mampu menjaga keamanan data tersebut sehingga memenuhi aspek keamanan kriptografi dan steganografi.

3.1. Perancangan Program

Skema proses ambil foto dapat diuraikan pada gambar 3.1 dan gambar 3.2.

1. Tampil *Form* Ambil Foto
2. Ambil Foto
3. *If* pilih Simpan = ya *then*
4. Tampil *Form* Ambil Foto
5. Else If = tidak *then*
6. Tampil *Form* Kamera
7. *End If*
8. *Input* Pesan
9. *If* pilih = Kirim *then*
10. *Input* Kunci
11. Tampil *Form* Metode Pengiriman
12. Kirim Foto
13. *Else* pilih = Simpan *then*
14. *Input* Kunci
15. Tampil Foto Berhasi Disimpan
16. *End If*
17. *End*

Gambar 3.1 Skema Proses Ambil Foto



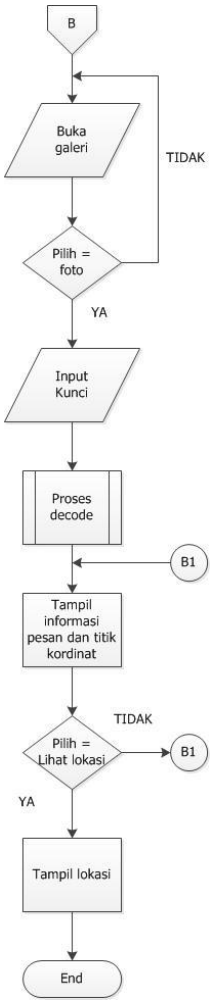
Gambar 3.2 : Skema Proses Ambil Foto

Skema

Proses buka foto dapat diuraikan pada gambar 3.3 dan gambar 3.4.

1. Tampil *Form* Buka Foto
2. Buka Galeri
3. *If* pilih Foto = ya *then*
4. *Input* Kunci
5. *Else* = tidak *then*
6. Buka Galeri
7. *End If*
8. Tampil Informasi pesan dan titik koordinat
9. *If* pilih Lihat Lokasi = ya *then*
10. Tampil Lokasi
11. *Else* pilih = tidak *then*
12. Tampil Informasi pesan dan titik koordinat
13. *End If*
14. *End*

Gambar 3.3 : Skema Proses Buka Foto



Gambar 3.4 : Skema Proses Buka Foto

4. IMPLEMENTASI DAN UJI COBA PROGRAM

4.1. Pengujian Program

Dalam pengujian program kali ini akan membahas perbandingan antara proses encoding dan decoding. Pengujian yaitu meliputi waktu proses encoding, waktu proses decoding seperti pada tabel 4.1 dan tabel 4.2

Tabel 4.1 Hasil Uji Coba Proses Encoding

Isi pesan	Password	Waktu Encoding	Ukuran foto
pemasangan pipa untuk instalasi listrik pada tower c lantai 3	ajeng123	6,59 detik	829 Kb
hydrant pada tower b lantai 3	12345678	6,33 detik	585 Kb
plambing pada tower c lantai 3	qwe12345	8,92 detik	861 Kb
instalasi listrik pada tower b lantai 3	diajengp	7,19 detik	676 Kb
hydran tower c lantai 3	321ajeng	5,85 detik	895 Kb

Tabel 4.2 Hasil Uji Coba Proses Decoding

Isi pesan	Password	Waktu Decoding	Ukuran foto
pemasangan pipa untuk instalasi listrik pada tower c lantai 3	12345678	2,09 detik	829 Kb
hydrant pada tower b lantai 3	12345678	1,39 detik	585 Kb
plambing pada tower c lantai 3	Qwe12345	2,10 detik	861 Kb
instalasi listrik pada tower b lantai 3	diajengp	1,72 detik	676 Kb
hydran pada tower c lantai 3	321ajeng	1,58 detik	895 Kb

4.2. Evaluasi Program

Berdasarkan pengujian untuk proses encoding dan decoding yang telah dilakukan, yang meliputi waktu encoding dan decoding, didapatkan beberapa kelebihan dan kekurangan dari aplikasi ini, sebagai berikut :

Kelebihan Aplikasi

a. Aplikasi ini dapat memberikan informasi *geolocation* di dalam data digital.
b. Pesan yang disisipkan ke dalam *cover image* tidak dapar terlihat secara kasat mata dan jika orang lain dapat memecahkan pesan yang disisipkan tetapi belum tentu bisa memecahkan pesan yang sudah diacak terlebih dahulu.
c. Proses encoding memakan waktu rata-rata kurang lebih 7,76 detik dan proses decoding memakan waktu rata-rata kurang lebih 1,77 detik

Kekurangan Aplikasi

a. Aplikasi ini hanya dapat mengencode pesan teks saja.
b. Aplikasi ini tidak bisa menggunakan *password* berkarakter seperti !, @, #, spasi dan sebagainya.

5. KESIMPULAN

Berdasarkan perancangan, pembuatan, analisa program dan serangkaian uji coba dari aplikasi ini, maka dapat diambil suatu kesimpulan antara lain :

a. Proses penyimpanan informasi atau pesan rahasia ke dalam sebuah *image* menggunakan teknik steganografi sehingga mampu menampung lebih banyak pesan dibandingkan dengan penyimpanan pada meta data *image* atau yang di kenal EXIF.
b. Untuk menyembunyikan pesan ke dalam *image* dan meningkatkan keamanan pesan dapat dilakukan meggunakan metode kriptografi AES, *Vigenere cipher*, dan steganografi LSB. Dengan menggabungkan metode tersebut dapat meberikan keamanan ganda dan jauh lebih baik. Dengan penambahan *geolocation* dapat dijadikan sebagai validasi sebuah data digital.

6. Saran

Adapun saran yang mungkin diperlukan untuk membuat aplikasi ini dapat berjalan lebih baik lagi antara lain :

a. Aplikasi yang dibuat hanya dapat mengirim gambar melalui email. Tidak dapat digunakan untuk teknologi lain (social media) yang menggunakan kompresi untuk mengecilkan ukuran gambar yang akan di kirim sehingga dapat merusak bit-bit pada gambar tersebut.
b. Jika perlu di tambahkan pesan berupa *file* dan ditambahkan kompresi sehingga dapat menghemat ruang penyimpanan.

DAFTAR PUSTAKA

[1] Arius, D., 2008, "Pengatar Ilmu Kriptografi Teori Analisis dan Implementasi". Yogyakarta: Penerbit ANDI.

[2] Kaur, R. & Aggarwal, D., 2013, "Analysis of Secure Text Embedding using Steganography". International Journal of Latest Trend in Engineering and Technology, 2(1), pp.120–126, http://ijltet.org/wpcontent/uploads/2013/01/20.pdf.21 Oktober 2015.

[3] Munir, R., 2006b, "Pengantra Kriptografi". Bandung: Departemen Teknik Informatika.

[4] Munir, R., 2006a, "Diktat Kuliah IF5054 Kriptografi". Bandung: Sekolah Teknik Elektro dan Informatika Intstitut Teknologi.

[5] Entreprise, J., 2010, " 13 Ancaman PC dan Cara Mengatasinya". Jakarta: PT Elex Media Komputindo.

[6] Walia, D.E., Jain, P. & Deep, N., 2010, "An Analysis of LSB & DCT Based Steganography". Global Journal of Computer Science and Technology, 10(1), pp.4–8. https://www.academia.edu/1491402/Information_Hiding_A_New_Approach_in_Text_Steganography.. 2 Oktober 2015.

[7] Muchbarak, A. & Budi, U., 2015., "PROTOTIPE VALIDASI DAN PROTEKSI DATA PADA FILE IMAGE DENGAN MENGGUNAKAN ADVANCED ENCRYPTION STANDARD DAN LEAST SIGNIFICANT BIT", http://pelita-informatika.com/berkas/jurnal/429.pdf. 2 Oktober 2015.