Implementasi Metode *Advance Encryption Standard* dan *Least Significan Bit* pada Kriptografi Citra Digital

Implementation of the Advanced Encryption Standard and Least Significant Bit Methods in Digital Image Cryptography

Sitti Aisa*[1],Nurul Aini [*2]
[1] Program Studi Teknik Informatika, [2)] Manajemen Informatika, STMIK Dipanegara, Makassar
[1,2]Jalan Perintis Kemerdekaan KM.9 Makassar telp: 0411-588941, Kode Pos 90245
e-mail: ***[1]sittiaisa.11@gmail.com** , [2]nurulaini.m11@gmail.com

Abstrak

Perkembangan digital kian pesat tanpa kita sadari, salah satunya adalah kehadiran smartphone sudah menjadi salah satu kebutuhan pokok untuk masyarakat. Dimana, smarphone tidak hanya digunakan sebagai alat komunikasi tetapi juga sebagai alat bertukar informasi. Sistem pertukaran data dan informasi melalui Smartphone Android tidak memberi jaminan akan keamanan informasi khususnya untuk data yang bersifat rahasia. Pertukaran data dan informasi dengan cara seperti ini rentang terhadap bahaya pencurian data, sehingga perlu mencari solusi untuk hal tersebut. Diperlukan suatu sistem pengamanan data dan informasi terutama untuk data yang bersifat pribadi dan rahasia sehingga dapat sampai ke tangan yang berhak menerima. Salah satu metode yang sering digunakan untuk mengatasi hal tersebut dengan teknik kriptografi.salah satu metode yang digunakan adalah AES dan LSB Dengan metode AES ini, data diubah kedalam bentuk teks yang tidak diketahui maknanya agar orang lain tidak bisa membacanya dan untuk menghindari kecurigaan kepada orang lain maka si A menggunakan teknik steganografi dengan metode LSB. Aplikasi ini untuk mengamankan data yang akan dikirmkan pengamanan dilakukan dengan dua tahapan yang pertama tahap penyamaran pesan dengna metode AES dan tahap kedua adalah tahap penyisipan pesan dengan metode LSB, dimana cipherteks yang disimpan dalam bentuk file text, serta dapat disisipkan ke dalam file citra.

Kata kunci-- *kriptografi, Citra, Digital, Informasi*

Abstract

Digital development is growing rapidly without us knowing it, one of which is the presence of smartphones has become one of the basic needs for the community. Where, smartphone is not only used as a communication tool but also as an information exchange tool. Data and information exchange system through an Android Smartphone does not guarantee information security, especially for confidential data. Exchange of data and information in this way ranges from the danger of data theft, so it is necessary to find a solution to it. A system for securing data and information is needed, especially for data that is personal and confidential so that it can reach the right to receive it. One method that is often used to overcome this with cryptographic techniques. One of the methods used is AES and LSB. With the AES method, the data is converted into text that is not known so that other people cannot read it and to avoid suspicion to others then si A uses the steganography technique with the LSB method. This application to secure the data that will be sent security is done in the first two stages of the message disguise with the AES method and the second stage is the message insertion stage with the LSB method, where ciphertexts are stored in the form of text files, and can be inserted into image files.

Keywords— *Cryptography, Image, Digital, Information*

1. PENDAHULUAN

Saat ini, *Smartphone Android* telah menjadi kebutuhan pokok bagi sebagaian besar orang. *Smartphone Android* digunakan oleh para pebisnis hingga para pelajar. Hal ini disebabkan oleh fasilitas dan kemudahan yang dimiliki oleh *Smartphone Android* yaitu berbasis *Open Source,* aplikasi *Android* bias dikembangkan dan dimodifikasi secara bebas untuk kemudian disebarluaskan kepada para penggunanya maka *Smartphone Android* untuk saat ini sudah tidak asing lagi. Manfaat *Smartphone Android* tak hanya digunakan untuk menelpon, bermain game, dan Internetan tetapi juga dapat digunakan untuk bertukar data dan informasi digital termasuk pengiriman pesan yang tidak terbatas pada pesan yang berbentuk data teks saja melainkan juga bisa dalam bentuk audio dan video.

Sistem pertukaran data dan informasi melalui *Smartphone Android* tidak memberi jaminan akan keamanan informasi khususnya untuk data yang bersifat rahasia. Pertukaran data dan informasi dengan cara seperti ini rentang terhadap bahaya pencurian data, sehingga perlu mencari solusi untuk hal tersebut. Diperlukan suatu sistem pengamanan data dan informasi terutama untuk data yang bersifat pribadi dan rahasia sehingga dapat sampai ke tangan yang berhak menerima. Salah satu metode yang sering digunakan untuk mengatasi hal tersebut dengan teknik kriptografi. Dengan kriptografi, data diubah ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Untuk menghindari kecurigaan terhadap data yang sudah diubah tersebut, maka dapat disamarkan ke dalam sebuah media digital sebelum dikirim, cara ini dikenal dengan teknik steganografi. Penggunaan teknik steganografi dan kriptografi secara bersamaan dimaksudkan untuk memberikan keamanan berlapis dalam pengamanan pertukaran data..

Sebagai contoh si A mengirim pesan atau informasi kepada si B yang bersifat rahasia tanpa orang mengetahui isi pesan atau informasi tersebut, maka si A menggunakan teknik kriptografi dengan metode AES. Dengan metode AES ini, data diubah kedalam bentuk teks yang tidak diketahui maknanya agar orang lain tidak bisa membacanya dan untuk menghindari kecurigaan kepada orang lain maka si A menggunakan teknik steganografi dengan metode LSB. Dengan metode LSB ini, pesan teks yang tidak diketahui maknanya tersebut disisipkan kedalam citra digital untuk menghindari kecurigaan kepada orang lain. Sehingga pesan tersebut sampai ke si B dengan aman tanpa kecurigaan orang lain.

Dari pemaparannya dapat di simpulkan latar belakang dari penelitian ini adalah proses pertukaran data dan informasi secara langsung tidak memberi jaminan akan keamanan informasi sehingga dapat menyebabkan isi dari pesan tersebut diketahui oleh pihak yang tidak berhak, dan bagaimana membangun aplikasi tersebut tanpa mengurangi kualitas citra yang telah disisipi *ciphertext*.

Ada beberapa penelitian yang telah dilakukan sebelumnya sehubungan dengan penelitian ini, diantaranya :

1. Implementasi Steganografi Menggunakan Metode Least Significant Bit dan Kriptografi Advanced Encryption Standard, yang di tulis oleh sinta puspita, dkk. Dari penelitian ini aplikasi steganografi berhasil diimplementasikan pada mobile phone Android. Aplikasi ini dapat melakukan penyisipan pesan dari 160 karakter, 480 karakter, 1000 karakter hingga 6.500 karakter sesuai dengan gambar yang telah dilakukan uji coba. [1]
2. Implementasi teknik steganografi dengan kriptografi kunci private AES untuk keamanan file gambar berbasis android, yang ditulis oleh Ari Muzakir. Dari penelitian ini dihasilkan suatu aplikasi pengolahan citra gambar yang aman, dimana sumber gambar dapat di ambil dari kamera langsung atau daru file galeri ponsel. Selanjutnya, gambar dari hasil pengolahan dapat langsung di share via social media yang telah terinstal di ponsel android.[2]
3. Impelmentasi pengamanan data dan informasi dengan metode steganografi LSB dan Algoritma kriptografi AES, yang ditulis oleh syaiful Anwar. Dari hasil percobaan yang telah dilakukan maka dapat disimpulkan bahwa implementasi algoritma kriptografi aes dan

steganografi dengan metode ibs cukup berhasil. Pengujian terhadap beberapa sample membuktikan bahwa metode modified LSB memenuhi aspek imperceptibility, dimana keberadaan pesan rahasia pada citra digital sulit untuk dipersepsi oleh inderawi.[3]

steganografi sudah dikenal oleh bangsa Yunani sejak lama. Herodatus, penguasa Yunani mengirimkan pesan rahasia menggunakan kepala budak atau prajurit sebagai media. Caranya rambut budak dibotaki, lalu pesan rahasia ditulis pada kulit kepala budak. Ketika rambut sudah tumbuh, budak tersebut diutus untuk membawa pesan rahasia di balik rambutnya.[5]

Bangsa Romawi mengenal steganografi dengan menggunakan tinta tak tampak (*invisible ink*) untuk penulisan pesan. Tinta tersebut dibuat dari campuran sari buah, susu dan cuka. Jika tinta digunakan menulis maka tulisannya tidak tampak. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

Selama perang dunia II, agen-agen spionase juga menggunakan stegenografi untuk mengirim pesan. Caranya dengan menggunakan titik-titik yang sangat kecil sehingga keberadaanya tidak dapat dibedakan pada tulisan biasa yang diketik.
Dari contoh-contoh steganografi konvesional tersebut dapat dilihat bahwa semua teknik steganografi konvesional berusaha merahasiakan komunikasi dengan cara menyembunyikan pesan ataupun mengkamuflase pesan. Maka sesungguhnya prinsip dasar dalam steganografi lebih dikonsentrasikan pada kerahasiaan komunikasinya bukan pada datanya.

Penilaian sebuah algoritma steganografi yang baik dapat dinilai dari beberapa faktor yaitu :

1. *Imperectibility.* Keberadaan pesan rahasia dalam media penampung tidak dapat dideteksi oleh inderawi. Misalnya, jika *covertext* berupa citra, maka penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan *covertext*-nya. Jika *covertext* berupa audio (misalnya berkas file *mp3*, *wav*, *midi* dan sebagainya), maka indera telinga tidak dapat mendeteksi perubahan pada file *stegotext*-nya.
2. *Fidelity.* Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan itu tidak dapat dipersepsi oleh inderawi. Misalnya, jika *covertext* berupa citra, maka penyisipan pesan dapat membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *covertext*-nya. Jika *covertext* berupa audio (misalnya berkas file *mp3*, *wav*, *midi* dan sebagainya), maka audio *stegotext* tidak rusak dan indera telinga tidak dapat mendeteksi perubahan pada file *stegotext*-nya.
3. *Recovery*. Pesan yang disembunyikan harus dapat diungkapkan kembali (*reveal*). Karena tujuan steganografi adalah *data hiding*, maka sewaktu-waktu pesan rahasia di dalam *stegotex*t harus dapat diambil kembali untuk digunakan lebih lanjut.[5]

Metode LSB merupakan teknik subtitusi pada steganografi, biasanya arsip 24-bit atau 8-bit digunakan untuk menyimpan citra digital. Representasi warna dari pixel-pixel bisa diperoleh dari warna-warna primer, yaitu merah, hijau dan biru. Citra 24-bit menggunakan 3 byte untuk masing-masing pixel, dimana setiap warna primer direpresentasikan dengan ukuran 1 byte. Penggunaan citra 24-bit memungkinkan setiap pixel direpresentasikan dengan nilai warna sebanyak 16.777.216 macam. Dua bit saluran warna tersebut bisa digunakan untuk menyembunyikan data yang akan mengubah jenis warna pixel-nya menjadi 64-warna. Namun hal itu mengakibatkan sedikit perbedaan yang bisa dideteksi secara kasat mata oleh manusia. Penggunaan metode LSB memungkinkan adanya sejumlah besar informasi tanpa adanya degradasi tampilan dari citra itu sendiri.

Advanced Encryption Standard (AES) merupakan algoritma kriptografi yang dapat digunakan untuk mengamakan data (*paper*). Algoritma AES adalah blok *ciphertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut *ciphertext*, sebaliknya dekripsi adalah merubah *ciphertext* data menjadi bentuk semula yang kita kenal sebagai *plaintext*. Algoritma AES menggunakan kunci kriptografi 128, 192 dan 256 bit untuk mengenkripsi dan mendekripsi data pada blok 128 bit. [6]

Secara harafiah, citra (image) adalah gambar pada bidang dua dimensi (dwimatra). Ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (continue) dari intensitas cahaya pada bidang dwimatra. Sumber cahaya menerangi objek, objek memantulkan kembali sebagian dari berkas cahaya tersebut.Pantulan cahaya ini ditangkap oleh alat-alat optik, misalnya mata pada manusia, kamer. Pemindai (scanner), dan sebagainya, sehingga bayangan objek yang disebut citra tersebut terekam.[4]

2. METODE PENELITIAN

2.1 Tempat dan Waktu Penelitian

Penelitian di lakukan di kampus STMIK Dipanegara yang beralamat di Jalan Perintis kemerdekaan KM.9 Makassar. Waktu penelitian dilakukan selama 5 bulan.

2.2 Metode Pengumpulan data

Metode pengumpulan data yang digunakan dalam pembuatan aplikasi ini adalah berupa pencarian sumber-sumber bacaan yang dapat menunjang topik. Sumber-sumber bacaan tersebut penulis letakkan pada daftar pustaka, sumber bacaan berupa buku panduan pemrograman, kumpulan soal-soal dan berbagai tutorial-tutorial di internet.

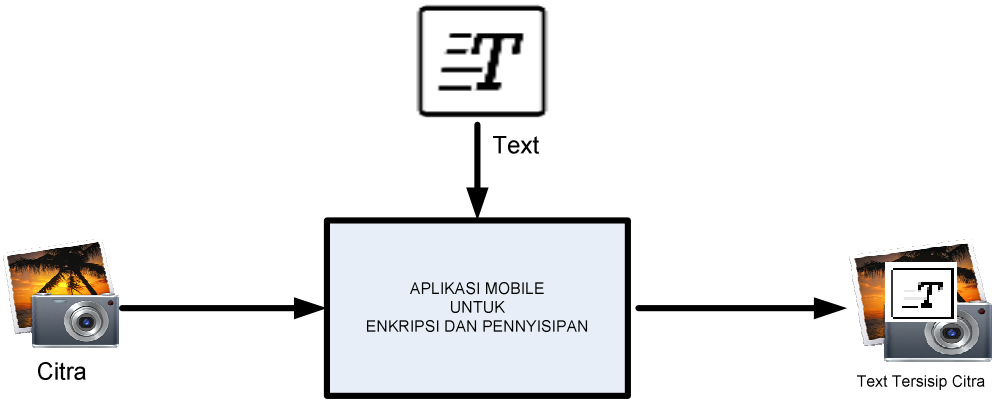
2.3 Bahan Penelitian

Adapun bahan yang digunakan dalam penelitian berupa perangkat lunak (*software*). Dalam melakukan perancangan sistem maka diperlukan beberapa *software* dan file diantaranya :

1. Media Digital Gambar format (.png) dan (.jpg)
2. Teks (.txt)

2.4 Arsitektur Sistem

Arsitektur sistem untuk merancang aplikasi ini terbagi 2 yaitu, konsep enkripso dan penyisipan, serta konsep deskripsi dan ekstraksi gambar.



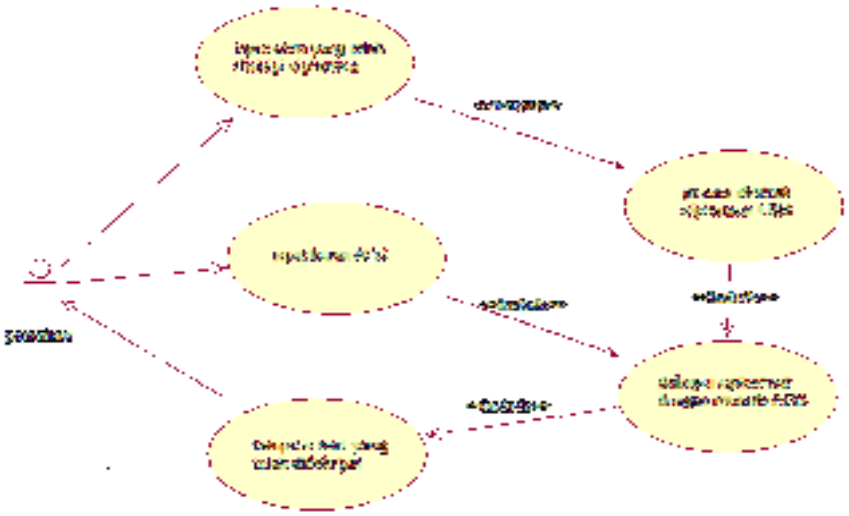
Gambar 1 : Konsep Enkripsi dan Penyisipan

Gambar 1. Konsep Deskripsi dan Ekstraksi

2.5 Desain Aplikasi

Dalam perancangan aplikasi ini, dirancang dengan mengunakan *UML (Unifield manipulation language)*.

Gambar 2. Use Case Diagram Enkripsi dan Penyisipan Citra



Gambar 3. Use Case Diagram Deskripsi dan Ekstraksi

3. HASIL DAN PEMBAHASAN

3.1 Implementasi metode

3.3.1 Implementasi metode Kriptografi AES

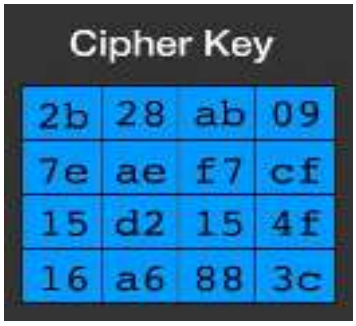
AES ini merupakan algoritma block cipher dengan menggunakan sistem permutasi dan substitusi (P-Box dan S-Box) adaa tiga jenis AES yaitu :

1. AES-128
2. AES-192
3. AES-256

Jenis AES yang digunakan adalah AES-128. Angka-angka di belakang kata AES menggambarkan panjang kunci yang digunakan pada tipa-tiap AES. Selain itu, hal yang membedakan dari masing-masing AES ini adalah banyaknya round yang dipakai. AES-128 menggunakan 10 round.

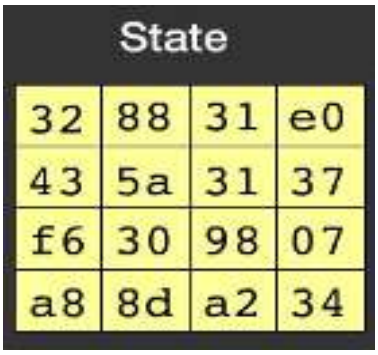
AES memiliki ukuran block yang tetap sepanjang 128 bit dan ukuran kunci sepanjang 128 bit. Berdasarkan ukuran block yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap-tiap sel matriks terdiri atas 1 byte (8 bit). Berikut adalah Tahapan algoritma enkripsi AES-128:

1. Siapkan array berukuran 4x4 bernama Kunci
2. Masukan Kunci
3. Konversikan teks kunci tersebut ke dalam bentuk bit menggunakan kode ASCII



Gambar 4. Array 4x4 yang telah diisi kunci

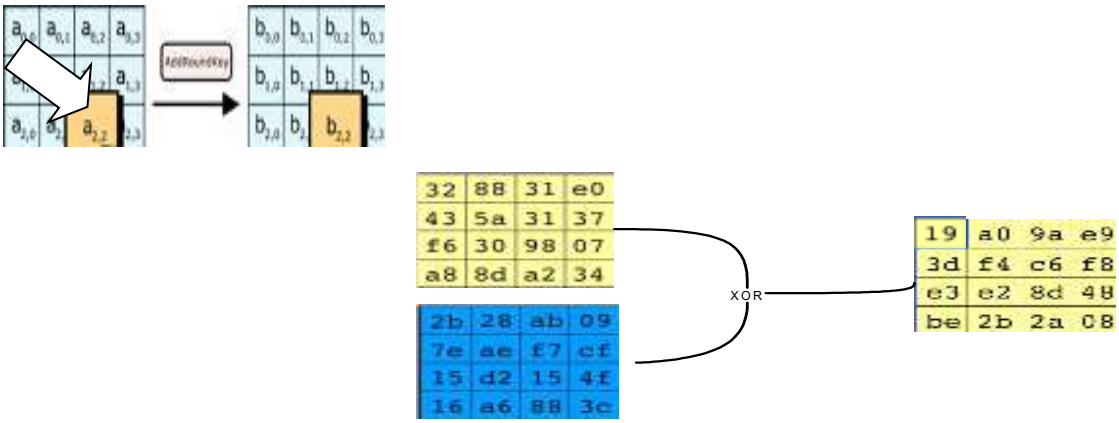
4. Siapkan array berukuran 4x4 bernama State
5. Masukkan Plainteks
6. Konversikan teks tersebut ke dalam bentuk bit menggunakan kode ASCII.



Gambar 5. Array 4x4 yang telah diisi state

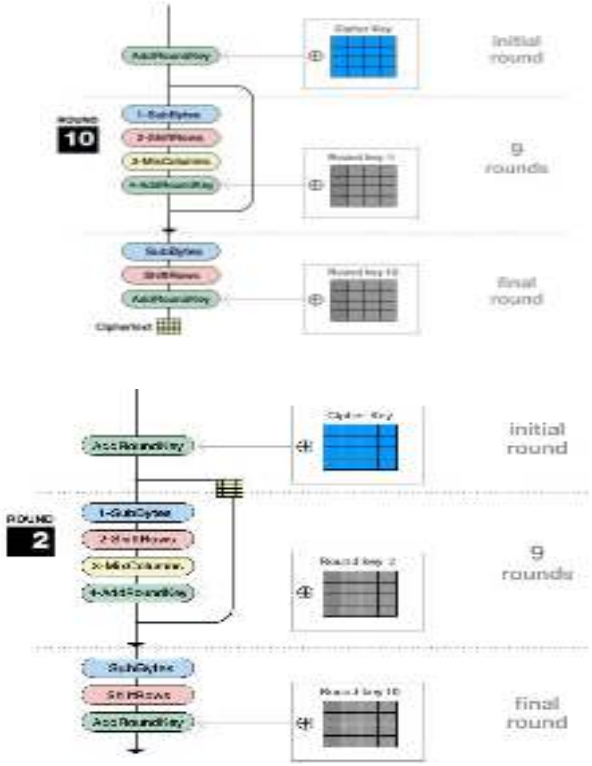
7. Konversikan kode ASCII tersebut ke dalam heksadesimal

8. Lakukan langkah AddRoundKey
   Pada proses ini subkey digabungkan dengan state. Proses penggabungan ini menggunakan operasi XOR untuk setiap byte dari subkey dengan byte yang bersangkutan dari state. Untuk setiap tahap, subkey dibangkitkan dari kunci utama dengan menggunakan proses key schedule. Setiap subkey berukuran sama dengan state yang bersangkutan.



Gambar 6. Proses addRoundKey

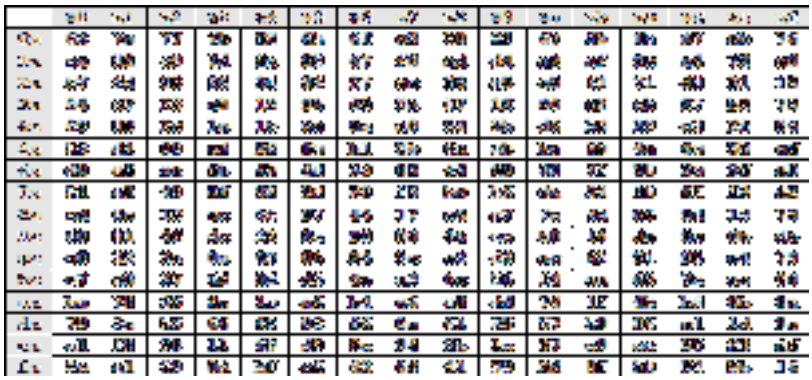
9. Kemudian akan dilakukan 4 transformasi sebagai berikut sebanyak 9 kali :
   1. SubBytes
   2. ShiftRows
   3. MixColumns
   4. AddRoundKey
10. Setelah itu, untuk round ke-10 dilakukan 3 transformasi sebagai berikut :
   1. SubBytes
   2. ShiftRows
   3. AddRoundKey



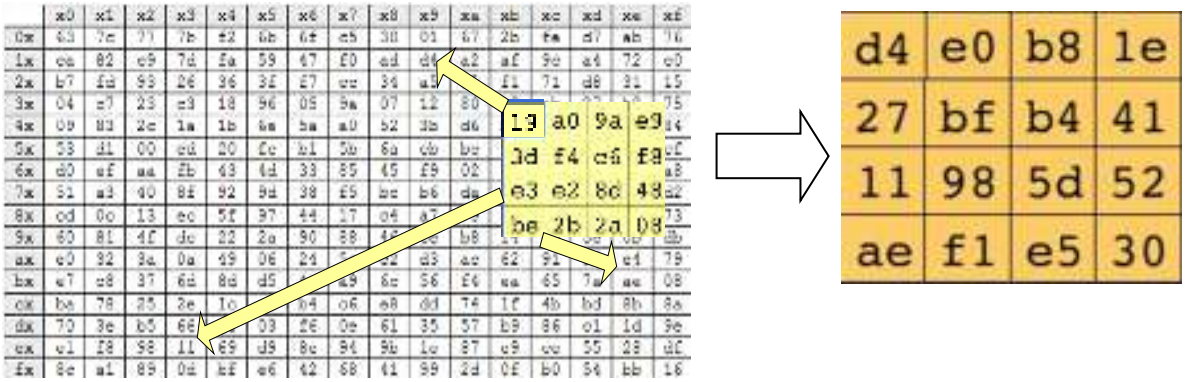
Gambar 7. Proses *round* 1 sampai 10

1. Proses SubBytes

Proses SubBytes adalah operasi yang akan melakukan substitusi tidak linear dengan cara mengganti setiap byte state dengan byte pada sebuah tabel yang dinamakan tabel SBox. Sebuah tabel S-Box terdiri dari 16x16 baris dan kolom dengan masing-masing berukuran 1 byte. Tabel S-Box diperlihatkan pada Gambar 12 sedangkan proses SubBytes diperlihatkan pada Gambar 13 di bawah ini



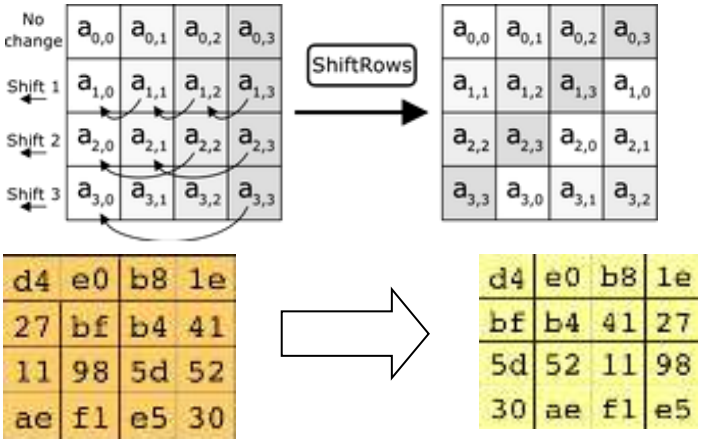
Gambar 8. Refrensi Tabel S-Box



Gambar 9.Proses AddRoungKey

2. Proses Shift Rows

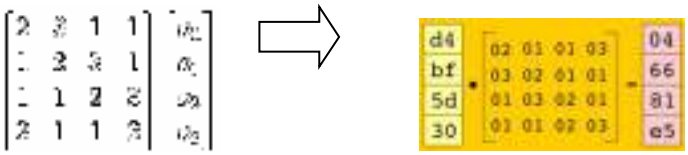
Proses Shift Rows akan beroperasi pada tiap baris dari tabel state. Proses iniakan bekerja dengan cara memutar byte-byte pada 3 baris terakhir (baris 1, 2, dan 3) dengan jumlah perputaran yang berbeda-beda. Baris 1 akan diputar sebanyak 1 kali, baris 2 akan diputar sebanyak 2 kali, dan baris 3 akan diputar sebanyak 3 kali. Sedangkan baris 0 tidak akan diputar. Proses ShiftRows diperlihatkan pada Gambar 14 di bawah ini



Gambar 10. Proses Shift Rows

3. Proses Mix Columns

Proses MixColumns akan beroperasi pada tiap kolom dari tabel state. Operasi ini menggabungkan 4 bytes dari setiap kolom tabel state dan menggunakan transformasi linier Operasi Mix Columns memperlakukan setiap kolom sebagai polinomial 4 suku dalam Galois field dan kemudian dikalikan dengan c(x) modulo (x4+1),Operasi MixColumns juga dapat dipandang sebagai perkalian matrix. Langkah MixColumns dapat ditunjukkan dengan mengalikan 4 bilangan di dalam Galois field oleh matrix berikut ini.



Sehingga :

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

Gambar 11. Proses Mix Columns Untuk Round 1

3.3.2 Implementasi Metode Stenografi LSB

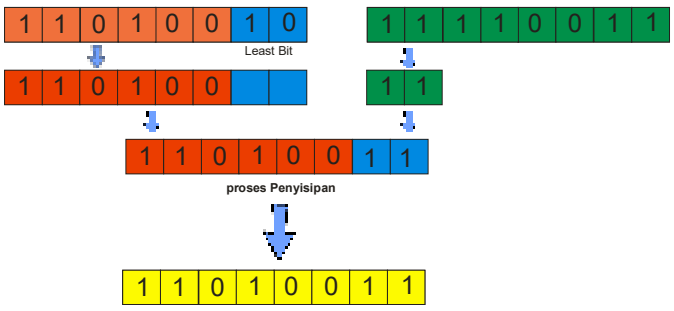
Untuk mengimplementasikan algoritma Least Significant Bit ada beberapa tahapan berikut.

a. Tahapan Proses Penyisipan

1. Mengubah Data Citra dalam bentuk rangkaian biner.
2. Mengubah Data Text dalam bentuk rangkaian biner.
3. Sisipkan Data text ke dalam Citra dengan metode LSB.
4. Buat File Citra dengan Nama File yang telah ditentukan.

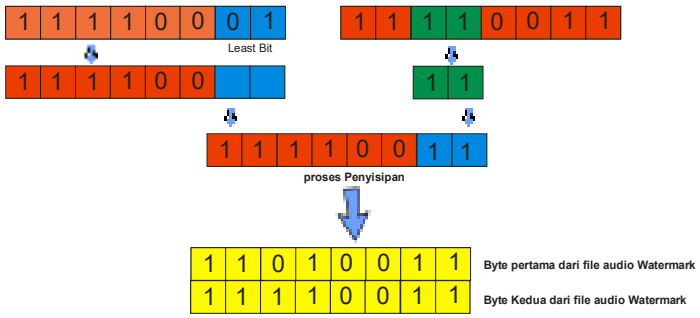
Gambar di bawah ini memperlihatkan proses penyisipan citra dengan langkah-langkah di atas

1. Skema byte pertama



Gambar 12. Penyisipan Byte Pertama

2. Skema Byte Kedua



Gambar 13. Penyisipan Byte Kedua

Skema diawali dengan mengosongkan dua bit pada byte pertama file audio kemudian disiapkan dua bit pengganti yang diambil dari dua bit pertama dari byte file citra, kemudian bit tersebut di tempatkan pada byte pertama yang telah dikosongkan sebelumnya, skema ini di ulang terus menerus sampai bit terakhir pada file citra.

Adapun hasil perubahan nilai biner setelah penyisipan pada dua langkah di atas dapat dilihat pada gambar di bawah ini

Gambar 14. Hasil Perubahan byte

3.2 Hasil Program

1. Input pesan

Gambar 15. Proses Enkripsi Pesan

Bila Sistem telah menerima input Kunci dan Plainteks dari user, maka aplikasi akan mengenkripsi dengan metode AES.

2. Penyisipan Gambar

Gambar 16. Penyisipan Gambar

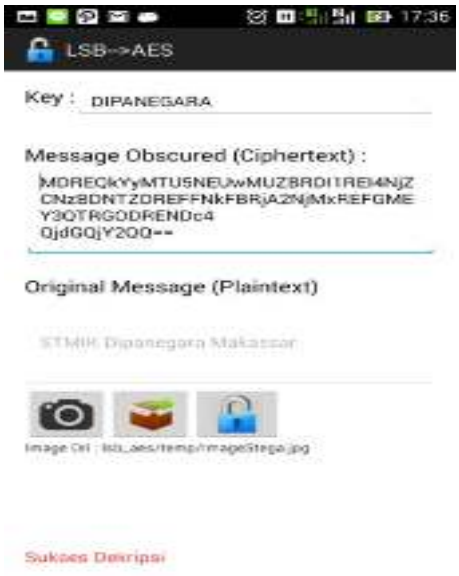
Bila Proses enkripsi telah menghasilkan Cipherteks, dan user telah memilih Citra, maka aplikasi akan melakukan proses penyisipan teks ke dalam citra

3. Proses Ekstraksi

Gambar 17. Proses Ekstraksi

Bila user telah memilih citra yang telah tersisipi file teks, maka aplikasi akan mengekstrak file teks tersebut yang berupa cipherteks.

4. Proses Dekripsi



Gambar 18. Proses Dekripsi

Setelah teks diekstrak dari file citra, dan user tela hmenginput kunci, maka aplikasi akan melakukan proses dekripsi untuk mendapatkan pesan asli (Plainteks)

4. KESIMPULAN

Berdasarkan hasil pengujian aplikasi Kriptografi dan steganografi dengan metode AES dan LSB berbasis Android maka diketahui bahwa aplikasi ini dibuat untuk mengamankan data yang akan dikirmkan pengamanan dilakukan dengan dua tahapan yang pertama tahap penyamaran pesan dengna metode AES dan tahap kedua adalah tahap penyisipan pesan dengan metode LSB, Aplikasi ini mengasilkan sebuah cipherteks yang disimpan dalam bentuk file text, serta dapat disisipkan ke alam file citra yang didukung oleh sistem operasi android (.JPG, .PNG .BMP), serta 3 berdasarkan hasil yang didapat pada pengujian perangkat lunak yang menggunakan metode *black box*, untuk menguji spesifikasi, baik itu spesifikasi keamanan maupun spesifikasi validasi dari aplikasi yang dibagun maka dapat disimpulkan aplikasi ini tidak di temukan kesalahan fungsional sesuai sepsifikasi yang telah di jelaskan sebelumnya

5. SARAN

Adapun pengembangan untuk aplikasi ini selanjutnya bisa membaca semua jenis ekstensi gambar, ada tambahan fitur untuk kompresi pesan agar file pada media penampung tidak penuh sehingga pesan yang disisipkan bisa lebih banyak, serta penggunaan metode yang lain sehingga bisa dilakukan pembandingan agar mendapatkan hasil yang paling baik.

DAFTAR PUSTAKA

[1] Sinta Puspita, dkk, 2012, Implementasi Steganografi Menggunakan Metode Least Significant Bit dan Kriptografi Advanced Encryption Standard, Jurnal ultimatics vol.4 no 1.

[2] Ari Muzakir, 2015, Implementasi Teknik Steganografi Dengan Kriptografi Kunci Private Aes Untuk Keamanan File Gambar Berbasis Android Berbasis Android, *Seminar Nasional teknologi, informasi dan Multimedia*, STMIK AMIKOM Jogjakarta.

[3] Syaiful Anwar, 2017, Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES, Jurnal Format Vol.6 No.1.

[4] Rinaldi Munir, 2006, "Kriptografi*",* Informatika, Bandung.

[5] Alatas, Putri. 2009. "Implementasi Teknik Steganografi D Bit engan Metode LSB Pada Citra Digital".

[6] Wahyudi, Kunjung. 2008. "Aplikasi Steganografi Untuk Pertukaran Pesan Dengan Menggunakan Teknik Steganografi Dan Algoritma AES.