RANCANG BANGUN APLIKASI STEGANOGRAFI UNTUK MENGAMANKAN PESAN MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) BERBASIS ANDROID

Rahmat Purnomo, Erna Dwi Astuti, M.Kom, Muslim Hidayat, M.Kom
Teknik Informatika, Fakultas Teknik dan Ilmu Komputer
Rahmatpurnomo808@gmail.com

ABSTRAK

Internet, jaringan yang saling terhubung, telah menjadi salah satu media komunikasi data yang paling luas di dunia. Dengan berkembangnya berbagai teknik pencarian informasi ilegal, banyak orang mencoba untuk mendapatkan informasi yang bukan milik mereka. Berbagai teknik untuk melindungi informasi sensitif dari orang yang tidak berwenang banyak digunakan untuk melindungi informasi penting. Steganografi adalah teknik untuk menyembunyikan *file* pesan dari publik yang mengetahui keberadaannya. Teknik ini sering digunakan untuk menghindari kecurigaan atau orang yang ingin mengetahui isi dari *file* pesan tersebut. Steganografi adalah ilmu dan teknik penulisan pesan tersembunyi sehingga tidak ada orang lain yang mengetahui keberadaannya. Oleh karena itu, aplikasi steganografi *plain-text* disisipkan ke dalam pembawa citra terenkripsi *Least Significant Bit* (LSB). Ini memungkinkan pengguna ponsel untuk mengirim pesan penulis ke penerima dengan aman.

Kata Kunci : Steganografi, Metode *Least Significant Bit* (LSB), *Android*.

ABSTRACT

The Internet, an interconnected network, has become one of the most widespread data communications medias in the world. With the development of various illegal information retrieval techniques, many people try to get information that does not belong to them. Various techniques to protect sensitive information from unauthorized persons are widely used to protect important information. Steganography is a technique for hiding message files from the public who know their existence. This technique is often used to avoid suspicion or people who want to know the contents of the message file. Steganography is the science and technique of writing hidden messages so that no one else knows about their existence. Therefore, the application of plain-text steganography is inserted into the Least Significant Bit (LSB) encrypted image carrier. This allows mobile users to send the author's message to the recipient securely..

Keywords ***:*** *Steganography, Least Significant Bit* (LSB) Method, *Android.*

1. PENDAHULUAN

1.1. Latar Belakang

Internet telah menjadi sarana komunikasi dan transmisi informasi yang sangat populer di seluruh dunia. Kemudahan memenuhi segala kebutuhan merupakan keunggulan internet dan bukan rahasia lagi di kalangan pengguna internet saat ini. Namun dengan berkembangnya internet dan aplikasi yang menggunakan internet, kejahatan dalam sistem informasi semakin meningkat. Dengan maraknya berbagai cara ilegal untuk mendapatkan informasi, banyak orang yang berusaha mendapatkan informasi secara ilegal hanya untuk kesenangan mereka sendiri. Untuk itu, sejalan dengan berkembangnya media *internet* yang sangat cepat dan *ter-update*, harus diikuti dengan perkembangan pengamanan dalam sebuah sistem informasi yang berada dalam media internet tersebut (Adiria, 2010).

Salah satu metode guna melindungi kerahasiaan sesuatu informasi menggunakan metode kriptografi, merupakan metode pengenkripsian informasi. Kriptografi mengganti isi informasi asli (*plain-text*) menjadi suatu informasi acak (*cipher-text*) (Munir, 2006). Proses pengubahan dalam kriptografi menggunakan suatu algoritma dan kunci yang hanya diketahui oleh pemilik atau pihak-pihak yang memiliki hak atas informasi rahasia tersebut. Untuk mengubah informasi yang telah terenkripsi menjadi informasi asli menggunakan kunci yang sama. Dengan begitu, orang yang tidak memiliki hak atas informasi rahasia tersebut hanya akan mendapatkan informasi acak yang sulit dimengerti. Namun, metode kriptografi ini memiliki kelemahan. Metode kriptografi ini dapat menimbulkan kecurigaan oleh pihak luar karena informasi acak tersebut. Informasi acak tersebut sangat jelas tidak mempunyai arti secara kasat mata. Pihak luar yang merasa curiga terhadap informasi tersebut dengan gampang mengganggu informasi ataupun melaksanakan suatu yang tidak di inginkan oleh pemilik informasi.

Berdasarkan permasalahan dari metode kriptografi tersebut, digunakan metode penyembunyian informasi yang lain. Metode tersebut adalah steganografi. Penerapan steganografi bukan hanya untuk pengiriman informasi rahasia. Namun, steganografi juga dapat digunakan untuk melindungi informasi pribadi yang tersimpan pada media penyimpanan informasi seperti *hardisk, flashdisk*, dan CD (*Compact Disk*). Sama dengan pengiriman informasi rahasia, aplikasi steganografi juga dirancang untuk melindungi informasi dari gangguan orang lain. Tujuan dari gangguan bisa berupa membaca, mengedit dan menghapus informasi (Ainurrizan, 2014).

1.2. Rumusan Masalah

Kurangnya keamanan yang penuh terhadap informasi yang sangat penting mengakibatkan terjadinya kebocoran informasi yang disebabkan oleh pihak-pihak yang tidak bertanggung jawab secara ilegal, sehingga perlu adanya langkah-langkah dalam mengamankan informasi tersebut, salah satunya dengan menggunakan metode steganografi

1.3. Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari pembuatan aplikasi ini adalah "Membangun aplikasi yang dapat mengatasi permasalahan keamanan pesan dengan menggabungkan metode steganografi dan metode *Least Significant Bit (LSB)*".

2 METODE PENELITIAN

2.1 Pengertian Steganografi

Steganografi berasal dari Bahasa Yunani, yaitu *steganos* yang artinya "tulisan tersembunyi (*covered writing*)" dan *graphos* yang berarti tulisan. Steganografi adalah ilmu dan seni menyembunyikan informasi yang sangat penting didalam informasi lain (*hidding massage*) sehingga tidak diketahui letak informasi rahasia tersebut (Munir, 2004). Sedengkan menurut Dony Ariyus (2006), steganografi adalah cabang ilmu yang menjelaskan tentang bagaimana proses menyembunyikan suatu pesan rahasia didalam pesan lainnya (Arius, 2006).

2.2 Metode Steganografi

Steganografi sendiri mempunyai beberapa metode yang terdiri dari empat (4) macam yaitu: (Munir, 2004).

a. *Algorithms and Transformation*

Metode steganografi yang menggunakan teknik penyembunyian data dengan menggunakan fungsi matematika didalamnya. fungsi yang digunakan adalah *Discrete Cosine*

Transformation (DCT) dan *Discrete Wavelet Transformation* (DWT). Fungsi DWT adalah untuk merubah data dari satu tempat (*domain*) ke tempat (*domain*) yang lain. Pada saat yang sama, tugas DCT adalah mengubah data dari tempat *spatial domain* ke tempat *frequency domain*.

b. *Redundant Pattern Encoding*

Redundant Pattern Encoding adalah pertinjauan kecil dari pesan disebagian besar gambar. Metode ini mempunyai kelebihan yaitu dapat bertahan dari *cropping*, dari segi kekurangannya metode ini yaitu tidak dapat mengambil pesan yang lebih banyak.

c. *Spread Spectrum method*

Steganografi spectrum tersebar populer karena pesan diacak (*encrypt*) didalam gambar (berlawanan dengan LSB). Untuk dapat membaca pesan tersebut, penerima membutuhkan algoritma yaitu kunci dan gambar. Metode ini juga rentang terhadap serangan dengan merusak atau mengubah kompresi dan juga pemrosesan gambar. Faktor penggali dilambangkan dengan *cr* yang bernilai skala. Panjang bit-bit yang didapat dari proses penggalian ini menjadi *cr* dikalikan panjang bit aslinya, yaitu bit signifikan terkecil (LSB).

d. *Least Significant Bit (*LSB*)*

Metode penyembunyian pesan dimedia digital bermacam-macam. Misalnya, pesan dalam *file image* dapat disembunyikan dengan menerapkan teknik penyembunyian pada bit paling kecil atau bit yang paling kanan (LSB) pada data *pixel* yang menyusun sebuah *file* tersebut. Seperti yang diketahui untuk *file image* 24-bit maka setiap *pixel* pada *image* tersebut terdiri dari susunan tiga warna yang berupa warna merah, hijau, dan biru (RGB) yang masing-masing disusun oleh bilangan 8-bit dari 0 sampai 255 atau dalam bentuk biner 00000000 sampai 11111111

2.3 *Least Significant Bit* (LSB)

Least Significant Bit (LSB) merupakan metode steganografi yang paling sederhana untuk diimplementasikan ke dalam sebuah aplikasi. Metode ini menggunakan media citra digital sebagai wadah (*cover-text*). Pada susunan bit di dalam sebuah *byte* (1 byte = 8-bit), ada bit yang paling penting (*Most Significant Bit* atau MSB) dan bit yang paling kurang berarti (*least significant bit* atau LSB). Sebagai contoh *byte* **1**1010010, angkat bit 1 yang digaris bawahi adalah bit MSB dan angka bit 0 yang digaris bawahi adalah bit LSB (Adiria, 2010).

Dalam steganografi bit yang akan diganti adalah bit LSB, dikarenakan perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Dengan asumsi bahwa satu *byte* tersebut merepresentasikan warna merah, maka mengubah sedikit nilai bit LSB tidak mengubah warna merah tersebut secara signifikan, dan mata manusia tidak dapat melihat perubahan yang sangat kecil itu.

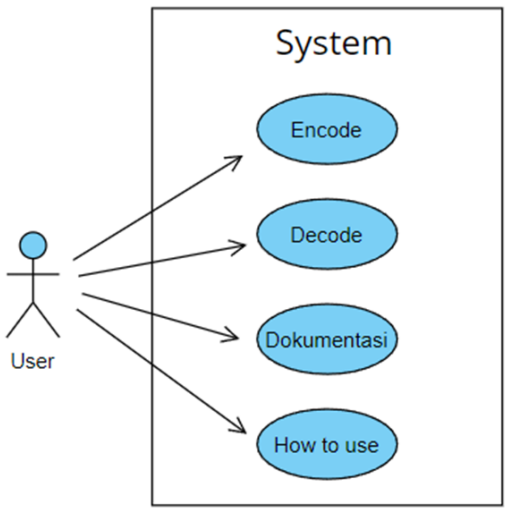
2.4 *Flutter*

Flutte adalah SDK untuk pengembangan aplikasi *mobile* yang dikembangkan oleh Google. Sama seprti *react native*, *framework* ini dapat digunakan untuk membuat atau mengembangkan aplikasi *mobile* yang dapat berjalan pada *device* iOS dan Android. Dibuat menggunkan Bahasa C, C++, Dart dan Skia. Pada *framework* ini semua kodenya di *compile* dalam kode *native* (Android NDK, LLVM, AOT-compiled) tanpa ada *intrepeter* pada prosesnya sehingga proses *compile*-nya menjadi lebih cepat. Dari segi penulisan kodenya, Flutter sangat berbeda dari *react native* dan lebih cenderung mendekati Java

3 HASIL DAN PEMBAHASAN

3.1 *Use Case Diagram*

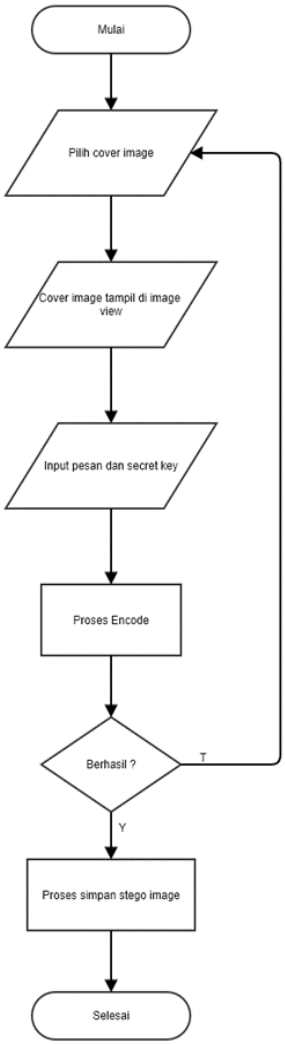
Use case diagram dari aplikasi steganografi pada penelitan ini dapat dilihat pada gambar 3.1 sebagai berikut:



Gambar 3.1 *Use Case Diagram*.

3.2 *Flowchart*

Proses penyisipan sebuah pesan atau encode dapat dilihat pada *flowchart* berikut:



Gambar 3.2 *Flowchart encode*.

3.3 Implementasi Desain Interface

Pada proses implementasi *interface* ke dalam aplikasi ini yaitu mengubah desain sistem, *interface* menjadi sistem yang dapat digunakan *user* dimulai dari implementasi sampai dengan fungsional sistem. Pada tahap ini merupakan lanjutan dari tahap perancangan. Berikut beberapa *interface* yang terdapat dalam aplikasi:

1. Tampilan halaman Menu

Tampilan halaman menu sebagai halaman utama dalam menggunakan aplikasi steganografi ini.

Gambar 3.3 Tampilan Halaman Menu.

2. Tampilan Halaman Encode

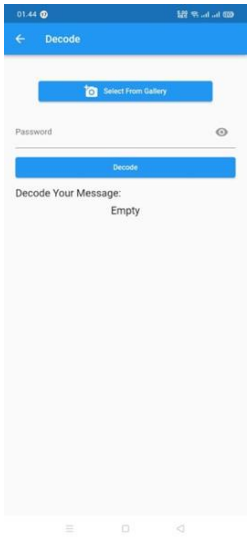
Selanjutnya jika memilih fitur encode, maka *user* akan diarahkan ke halaman encode. Dihalaman encode mempunyai beberapa form yang harus diisi oleh *user* mulai dari memasukan *cover-image* berupa **jpg* atau **png* yang dipilih memalui *gallery*. Selanjutnya *user* diharuskan untuk mengisi *form message* yang akan disisipkan pada *cover-image*. Dan *user* harus mengisi *form password* yang berfungsi sebagai *stego-key*. Setelah semuanya terisi untuk mendapatkan *stego-image* yaitu dengan cara menekan tombol *button* encode dan otomatis *stego-image* akan tersimpan di *gallery*.

Gambar 3.4 Tampilan Halaman Encode.

3. Tampilan Halaman Decode

Sesuai pada gambar 3.5, pada fitur decode *user* diarahkan untuk memasukan gambar yang

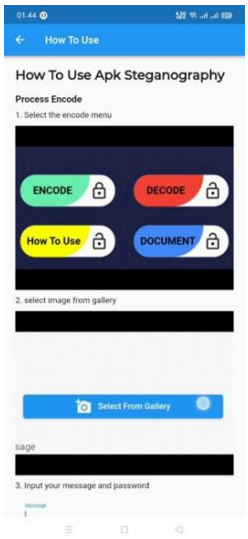
berisi *secret message* didalamnya atau *stego-image*. Setelah mendapatkan gambarnya, *user* harus memasukan *password* yang berfungsi untuk mengembalikan *secret message*. Setelah semuanya terisi pesan akan terlihat pada bagian *Decode Your Message*



Gambar 3.5 Tampilan Halaman Decode.

4. Tampilan Halaman *How To Use*

Pada tampilan How To Use berfungsi sebagai informasi bagaimana cara pemakaian aplikasi steganografi, mulai dari cara menggunakan fitur encode dan decode.



Gambar 3.6 Tampilan Halaman How To Use.

5. Tampilan Halaman Document

Pembuatan halamana *documentation* berfungsi untuk menampilkan informasi dan penjelasan tentang apa itu steganografi, sejarah steganografi dan lainya

Gambar 3.7 Tampilan Halaman Document.

4 PENUTUP

4.1. Kesimpulan

Dari pembahasan yang telah dijelaskan pada bab-bab sebelumnya, dapat ditarik kesimpulan bahwa aplikasi steganografi dengan menggunakan metode *Least Significant Bit* (LSB) berbasis android berhasil melakukan penyisipan pesan berupa *text* pada gambar RGB 24-bit dan berhasil melakukan ekstraksi pesan *stego-image* yang sebelumnya sudah melalui proses pengiriman melalui media sosial. Gambar hasil dari proses penyisipan pesan steganografi menggunakan metode *Least Significant Bit* (LSB) tidak mengalami perubahan secara kasat mata, sehingga aplikasi steganografi dengan metode *Least Significant Bit* (LSB) dapat mengamankan pesan tanpa menimbulkan kecurigaan dari pihak lain.

4.2. Saran

Dalam penerapan steganografi menggunakan metode *Least Significant Bit (LSB)* berbasis android, terdapat beberapa hal yang harus diperhatikan sepaya menjadi lebih baik kedepanya, diantaranya sebagai berikut:

1. Pengembangan lebih lanjut dapat difokuskan penerapan metode LSB untuk tipe *file* lain seperti **doc, *txt, *mp4, *mp3*.
2. Aplikasi steganografi berbasis android dapat dilakukan modifikasi pada algoritma yang digunakan.

3. Menambahkan dukungan fungsi-fungsi untuk pengembangan aplikasi steganografi.

5 DAFTAR PUSTAKA

Adiria. (2010). Analisis Dan Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Metode LSB (Least Significant Bit). 1-264.

Ainurrizan. (2014). Implementasi Steganografi Pada File Image Menggunakan Teknik Spread Spectrum. Semarang.

Amin, M. M. (2014). Image Steganography Dengan Metode Least Significant Bit (LSB). CSRID, 53-64.

Ariyus, D. (2006). Kriptografi Keamanan Data dan Komunikasi. Yogyakarta: Graha Ilmu.

Darwis, D. (2016). Implementasi Teknik Steganografi Least Significant Bit (LSB) Dan KompresiI Untuk Pengamanan Data Pengiriman Surat Elektronik. 1-7.

Darwis, D., & Kisworo. (2017). Teknik Steganografi untuk Penyembunyian Pesan Teks Menggunakan Algoritma End Of File. Telekomunikasi, Multimedia, dan Informasi.

Donavan, K., Ekojono, E., & Rozi, I. F. (2015). Aplikasi Steganography untuk Enkripsi Image to Image dengan Metode Spread Spectrum. 29-33.

Fanani, A., & Ulinnuha, N. (2016). WaterMarking Citra Digital Menggunakan Metode Transformasi Kosinus Diskrit. 1-7.

Fateh, M., Rezvani, M., & Irani, Y. (2021). A New Method of Coding for Steganography Based on LSB Matching Revisited. Security and Communication Networks, 1-15.

Flutter-dev. (2022, Juni 02). Flutter Documentation. Retrieved from Flutter Documentation, https://docs.flutter.dev/.

Harnanto, J. (1999). Analisis dan Disain Sistem Informasi: Pendekatan. Terstrutur Teori dan Praktek Aplikasi Bisnis Edisi 2. Yogyakarta: Andi.

Liana, L. (2015). Pengujian Perangkat Lunak (Software Testing).

Mohanapriya, S. (2012). Design and Implementation of Steganography Along with Secured Message Services in Mobile Phones. 69-72.

Mulyanto, Febriyana, R. V., & Wicaksono Putra, A. B. (2019). Penyisipan Pesan Teks pada Citra Menggunakan Metode LSB dan 2-Wrap Length. Seminar Nasional APTIKOM (SEMNASTIK).

Munir, R. (2004). Pengolahan Citra Digital dengan Pendekatan Algoritmik. Bandung: Informatika, 2004.

Narsuki, I. (2011). Rancang Bangun Aplikasi Untuk Penyisipan Text Dan File Ke Dalam Image Dan Audio File Dengan Metode Least Significant Bit (LSB). Skripsi.

Prawirawan, A., Isnawaty, & Ramadhan, R. (2015). Implementasi Discrete Wavelet Transform Untuk Penyisipan Teks Pada Gambar. 11-18.

S, R. A., & Shalahuddin, M. (2014). Rekayasa Perangkat Lunak: Terstruktur dan Berorientasi Objek. Bandung: Informatika Bandung , 2014.

sani, D. A., Sarwani, M. Z., & Setiawan, M. A. (2020). An Implementation of MMS Steganography With The LSB Method. International Journal of Artificial Intelligence & Robotics (IJAIR), 8-12.

Santoso, B. W., & Alhadi, F. R. (2017). Perbandingan Hasil Implementasi Steganografi dan Kriptografi Menggunakan Least Significant Bit (LSB) dengan End of File.

Sembiring, S. (2013). Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Gambar Dengan Metode End Of File. 45-51.

T, S., W, B. R., & Nuswantoro, U. D. (2009). Teori pengolahan citra digital. Yogyakarta: Andi.