**TEKNIK “REC AND SHARE” PADA APLIKASI STEGANOGRAFI UNTUK FILE SUARA BERBASIS ANDROID**

**Achmad Aditya Ashadul Ushud**

Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur

Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260

 Email: achmad.aditya@budiluhur.ac.id

***Abstrak***

Perangkat berbasis Android seperti *handphone* atau *tablet* menawarkan berbagai fitur-fitur yang dapat menambah fungsi dari suatu aplikasi. Dengan menambah fungsi ini, suatu aplikasi dapat dikembangkan lebih jauh lagi. Dalam penelitian ini aplikasi steganografi untuk file audio, seperti wav atau mp3, dikembangkan dengan menggunakan fitur perekaman suara yang secara *default* sudah terinstal di dalam setiap perangkat Android. File *cover* steganografi tidak lagi menggunakan file suara yang sudah ada, tetapi bisa langsung dibuat dengan menggunakan perekaman suara tersebut. Penelitian ini berfokus pada kemudahan dan kecepatan dalam membuat file steganografi dan langsung mengirimkan atau menyebarkannya. Metode yang dipakai adalah metode LSB, yang menyisipkan bit terakhir pada file *cover*. Tujuan penelitian ini adalah dapat membuat dan menyebarkan file steganografi dengan cepat dan mudah tanpa kehilangan atau mengurangi tingkat keamanan dari file tersebut. Dengan menggunakan file yang dibuat sendiri melalui perekaman suara, maka keamanan file steganografi akan meningkat, karena file tidak mudah dikenali dan dibandingkan dengan file yang sudah ada.

***Kata kunci: Steganografi, audio, Android, LSB***

***Abstract***

*Android-based devices such as cellphones or tablets offer various features that can add to the functionality of an application. By adding this function, an application can be developed even further. In this study, a steganography application for audio files, namely wav or mp3, was developed using the sound recording feature which is installed by default on every Android device. Steganographic cover files no longer use existing sound files, but can be created directly using the sound recording. This research focuses on the ease and speed of creating steganographic files and sending or distributing them directly. The method used is the LSB method, which inserts the last bit in the cover file. The purpose of this research is to be able to create and distribute steganographic files quickly and easily without losing or reducing the security level of the files. By using self-created files through sound recording, the security of steganography files will be increased, because the files are not easily recognized and compared with existing files.*

***Keywords: Steganography, audio, Android, LSB***

**I. PENDAHULUAN**

**1.1. Latar Belakang**

Keamanan merupakan hal terpenting dalam berbagi data dimanapun di dunia ini. Terutama dalam dunia digital. Ketika suatu data diputuskan untuk dibuka untuk bisa diakses baik dengan hak akses bebas dan terbuka, maupun hak akses terbatas dengan syarat tertentu, maka data tersebut sudah rentan untuk bisa diakses oleh siapapun juga. Berbagai metode dan teknik dibuat dan diterapkan untuk melindungi data agar pemanfaatannya bisa sesuai dengan tujuan yang diharapkan. Salah satunya adalah steganografi.

Steganografi adalah suatu cara menyembunyikan pesan ke dalam suatu media, dimana media tersebut terlihat seakan-akan seperti media biasa pada umumnya sehingga tidak menimbulkan kecurigaan. Menurut Namita (Namita, 2010), steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Dengan steganografi ini seseorang dapat menyembunyikan pesan rahasia dengan tujuan pesan tersebut hanya dapat dibaca oleh orang yang dimaksudkan, atau bisa juga menyembunyikan trademark, hak cipta dan lain sebagainya.

Media yang digunakan dalam menyembunyikan pesan rahasia bisa dalam berbagai format, misalnya gambar, suara, video, atau hanya sekedar tulisan. Pesan rahasia ini akan membaur ke dalam media tersebut, sehingga akan sulit ditemukan. Media tempat menampung pesan rahasia ini disebut *cover*. Ada berbagai metode penyembunyian pesan rahasia di dalam steganografi, salah satunya adalah *Least Significant Bit* (LSB).

LSB adalah adalah mengganti bit yang paling kurang berarti atau signifikan dalam sebuah file dengan pesan rahasia yang ingin dimaksudkan. Diketahui pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti (*least significant bit* atau LSB). LSB ini merupakan metode yang paling sederhana dalam steganografi.

Penelitian ini berfokus dalam menyembunyikan pesan rahasia ke dalam file audio atau suara. Biasanya file audio yang umum digunakan berformat wav atau mp3. Pesan rahasia disematkan dalam audio digital dalam sistem steganografi audio berbasis komputer. Pesan rahasia disematkan ke dalam file audio dengan sedikit mengubah urutan biner file audio tersebut. Dengan terhubung ke Internet, pengguna bisa berbagi, dan mengirimkan file tersebut secara online dan terbuka.

**1.2. Perumusan Masalah**

Masalah keamanan dalam berbagi data melalu Internet telah menjadi isu penting bagi semua orang. Betapapun ketatnya keamanan tidak semerta-merta menghilangkan semua kemungkinan data dapat diterobos oleh orang-orang yang tidak diinginkan. Steganografi mempunyai maksud salah satunya menyamarkan pesan ke dalam file sehingga file tersebut tidak dicurigai mengandung sesuatu yang tidak biasa. Untuk itu rumusan masalah dari penelitian ini adalah

1. Bagaimana cara menyamarkan pesan rahasia ke dalam file audio sehingga tidak terlihat mencurigakan?
2. Bagaimana cara membuat file audio yang dapat langsung dimasukkan pesan rahasia?
3. Bagaimana cara yang mudah dalam memasukkan pesan rahasia untuk selanjutnya file tersebut dapat dibagikan dengan mudah?

**2. PENYELESAIAN MASALAH**

Penelitian ini mencoba menyelesaikan uraian masalah diatas, dengan merancang sebuah aplikasi pada *smartphone* berbasis Android. Aplikasi ini diharapkan mampu menjawab uraian masalah di atas dengan mampu membuat file audio secara langsung, dimana file audio ini akan bersifat unik karena hanya dibuat sekali dan berbeda dari semua file yang telah ada. Pemanfaatan aplikasi perekaman suara yang telah tersemat di dalam setiap perangkat Android akan membuat aplikasi yang dirancang ini menjadi efisien.

**2.1. Teknik “Rec and Share”**

Teknik “Rec and Share” steganografi dalam penelitian ini adalah sebuah teknik merekam suara lalu langsung mendistribusi file audio tersebut setelah dimasukkan pesan rahasia di dalamnya. Melalui Teknik ini diharapkan proses membuat file steganografi menjadi lebih ringkas, mudah, langsung dapat disebarkan, tanpa mengurangi tingkat keamanan pesan rahasia yang ada di dalamnya. Secara umum proses Teknik “Rec and Share” ini digambarkan dalam gambar di bawah ini:



**Gambar 1.** Proses Teknik “Rec and Share”

Secara singkat proses Teknik “Rec and Share” ini adalah pengguna memulai perekaman suara untuk dijadikan file *cover*. Dari file yang telah direkam tersebut pengguna memasukkan pesan rahasia ke dalamnya. Metode yang digunakan adalah LSB, mengganti bit terkecil atau yang kurang signifikan dari file *cover* dengan bit pesan rahasia. Setelah itu pengguna dapat membagikan file stego tersebut melalui berbagai media, seperti email, Facebook, Twitter, Bluetooth, dan lain sebagainya. Bila file tersebut diterima oleh bukan penerima yang seharusnya, maka ia tidak mengetahui bahwa file tersebut sebenarnya berisi pesan rahasia. Hal ini dikarenakan file tersebut secara kasat mata tidak terlihat berbeda dengan file audio pada umumnya. Sedangkan bagi penerima yang dituju, file tersebut akan di-decode terlebih dahulu untuk dapat melihat pesan rahasia yang ada di dalamnya.

**3. HASIL DAN PEMBAHASAN**

**3.1. Perangkat yang Dibutuhkan**

Pada penelitian ini perangkat lunak yang digunakan adalah bahasa pemrograman Java dengan berbasis Android. Sedangkan perangkat keras yang digunakan adalah Laptop dengan spesifikasi seperti di bawah ini:

1. RAM 8 GB DDR 4
2. Prosesor Intel Core i5-6200 4 CPU 2,3 GHz
3. Hardisk SSD 250 GB
4. VGA Card NVidia GeForce 940MX 4GB

**3.2. Desain**

 1. Rancangan Menu

Pada tampilan awal, pengguna akan diminta memilih menu *Encode* atau *Decode*. Menu *Encode* adalah menu untuk membuat file steganografi, sedangkan menu *Decode* untuk mengeluarkan pesan rahasia dari file stego. Di dalam menu *Encode* terdapat dua menu pilihan, yaitu menu *Create Cover*, dimana jika menu ini dipilih pengguna akan membuat file *cover* yang akan digunakan sebagai media tempat menyimpan pesan rahasia. Menu ini akan membuka perekam suara, dan pengguna diminta merekam suaranya. Sedangkan menu kedua yaitu *Open Gallery*, dimana pengguna bisa menggunakan file yang sudah ada pada media penyimpanan untuk dijadikan file *cover*. Setelah file *cover* tersedia, maka barulah pengguna dapat memasukkan pesan rahasia ke dalamnya. Sistem akan memasukkan pesan rahasia dengan metode LSB. Setelah selesai pengguna dapat langsung membagikan file stego melalu berbagai media yang ada di perangkatnya.

Menu *Decode* akan menampilkan pilihan *Open Gallery* kepada pengguna untuk memilih file stego yang akan dikeluarkan dan ditampilkan pesan rahasianya.

Menu

Decode

Encode

Open Gallery

Create Cover

Open Gallery

Insert Message

Decode

Share

**Gambar 2.** Rancangan Tampilan Menu Aplikasi

2. Rancangan Layar Aplikasi

Rancangan layar aplikasi ini adalah format bentuk tampilan dari aplikasi.

1. Rancangan Layar Awal

Rancangan layar awal adalah tampilan ketika aplikasi pertama kali dijalankan. Pengguna diminta untuk memilih salah satu menu yang ditampilkan.

MAIN MENU

Encode

Decode

**Gambar 3.** Rancangan Layar Menu Utama

1. Rancangan Layar *Encode*

Pada Rancangan layar *Encode* ini terdapat dua menu, *Create Cover* untuk membuat file *cover* dan *Open Gallery* untuk memilih file yang sudah ada untuk dijadikan file *cover*.

ENCODE

Create Cover

Open Gallery

**Gambar 4.** Rancangan Layar *Encode*

1. Rancangan Layar *Insert Message*

Pada rancangan layar *insert message* ini, pengguna memasukkan pesan rahasia ke dalam file *cover* yang telah dibuat atau dipilih sebelumnya.

INSERT MESSAGE

OK

**Gambar 5**. Rancangan Layar *Insert Message*

1. Rancangan Layar *Share*

Rancangan layar ini muncul setelah rancangan layar sebelumnya, yaitu *insert message* selesai dilakukan.

SHARE

Email

Facebook

Twitter

Bluetooth

**Gambar 6**. Rancangan Layar *Share*

1. Rancangan Layar *Decode*

Rancangan layar *decode* memunculkan satu menu yaitu *open gallery*, yang akan membuka file *explorer* untuk mencari file stego yang ada di dalam media penyimpanan perangkat.

DECODE

Open Gallery

**Gambar 7**. Rancangan Layar *Decode*

1. Rancangan Layar *View Message*

Rancangan layar ini memunculkan pesan rahasia yang telah berhasil di-*decode* oleh sistem.

MESSAGE

Xxxxxxxxx

Xxxxxxxxx

xxxxxxxxx

**Gambar 7.** Rancangan Layar *View Message*

**3.3. Implementasi**

Implementasi dari aplikasi yang dibuat dalam penelitian ini untuk menguji apakah sistem dapat berfungsi sesuai harapan.

1. Implementasi Tampilan Layar Awal

Tampilan layar awal akan memunculkan dua pilihan menu, yaitu *Encode* dan *Decode* seperti gambar di bawah.



**Gambar 9.** Tampilan Layar Awal

1. Implementasi Tampilan *Encode*

Tampilan *Encode* memunculkan dua menu untuk menyiapkan file *cover*, yaitu *Create Cover* untuk membuat file *cover* baru atau *Open Gallery* untuk memilih file yang sudah ada.



**Gambar 10.** Tampilan *Encode*

Ketika pengguna memilih *Create Cover*, maka sistem akan membuka perekam suara. Lalu pengguna melakukan perekaman suara. File audio tersebut akan digunakan sebagai file *cover*.



**Gambar 11.** Tampilan Perekaman Suara

1. Implementasi Tampilan *Insert Message*

Tampilan ini meminta pengguna untuk memasukkan pesan rahasia ke dalam file *cover* yang telah dibuat atau dipilih.

****

**Gambar 12.** Tampilan *Insert Message*

1. Implementasi Tampilan *Share*

Tampilan ini adalah tampilan membagikan file stego yang telah dibuat melalui berbagai media yang tersedia di dalam perangkat Android.



**Gambar 13.** Tampilan *Share*

1. Implementasi Tampilan *Decode*

Tampilan ini adalah tampilan untuk mengeluarkan pesan rahasia dan menampilkan pesan tersebut setelah dilakukan pengkodean ulang terhadap file stego yang ada atau yang diterima.



**Gambar 14.** Tampilan *Decode*

**3.4. Pengujian**

Pengujian dilakukan menggunakan metode *black box testing*. Bertujuan untuk menemukan kesalahan fungsi pada aplikasi. Berikut adalah pengujian *black box testing* pada aplikasi ini.

1. **Pengujian Layar Menu Awal**

Berikut tabel pengujian menu awal.

**Tabel 1.** Pengujian Menu Awal

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Pengujian** | **Yang diharapkan** | **Hasil** | **Kesimpilan** |
| 1 | Plih Menu *Encode* | Layar berpindah ke layar *Encode* | Menu *Encode* berfungsi | Berhasil |
| 2 | Pilih Menu *Decode* | Layar berpindah ke layar *Decode* | Menu Panduan berfungsi | Berhasil |

1. **Pengujian Layar *Encode***

Berikut tabel pengujian layar *encode*.

**Tabel 2.** Pengujian Layar *Encode*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Pengujian** | **Yang Diharapkan** | **Hasil** | **Kesimpulan** |
| 1 | Pilih Menu *Create Cover* | Membuka Perekam Suara | Membuka Perekam Suara | Berhasil |
| 2 | Pilih *Open Gallery* | Membuka File *Explorer* | Membuka File *Explorer* | Berhasil |

1. **Pengujian Layar *Insert Message* dan *Share***

Berikut tabel pengujian *Insert Message* dan *Share*.

**Tabel 3.** Pengujian layar *Insert Message* dan *Share*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Pengujian** | **Yang diharapkan** | **Hasil** | **Kesimpulan** |
| 1 | Memasukkan pesan rahasia | Pesan rahasia tersimpan ke dalam file *cover* | Pesan rahasia tersimpan ke dalam file *cover* | Berhasil  |
| 2 | Pilih menu *Share* | Tampil berbagai pilihan *Share* | Tampil berbagai pilihan *Share* | Berhasil  |

1. **Pengujian Layar *Decode***

Berikut tabel pengujian layar *decode*.

**Tabel 4.** Pengujian Layar *Decode*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Pengujian** | **Yang diharapkan** | **Hasil** | **Kesimpulan** |
| 1 | Pilih File stego dari media penyimpanan pada perangkat | Pesan rahasia tampil | Pesan rahasia tampil | Berhasil |

**4. KESIMPULAN**

Berdasarkan hasil perancangan dan analisa program pada aplikasi ini, dapat diambil beberapa kesimpulan antara lain.

1. Dengan membuat file *cover* sendiri, dalam hal ini merekam sendiri, maka file menjadi lebih aman, karena file tidak ada pembanding atau hanya ada satu-satunya.
2. Dalam aplikasi ini, pembuatan file *cover* dan proses memasukkan pesan rahasia menjadi satu di dalam aplikasi, sehingga pengguna tidak perlu pindah antar aplikasi atau membuka aplikasi tambahan, sehingga memudahkan pengguna.
3. Dalam aplikasi ini juga sudah ditambahkan fitur untuk bisa membagikan file stego yang telah dibuat dengan memanfaatkan fasilitas yang ada di dalam sistem Android.

**DAFTAR PUSTAKA**

Ritesh Pratap Singh and Neha Singh, Steganography in Multimedia Messaging Service of Mobile Phones Using CDMA Spread Spectrum, AKGEC Journal of Technology, vol. 1, 2008.

Prof. B.N. Jagdale, Prof. R.K. Bedi, Sharmishta Desai, Securing MMS with High Performance Elliptic Curve Criptography, International Journal of Computer Application, vol. 8, Oktober 2010.

Wesam S. Bhaya, Text Hiding in Mobile Phone Simple Message Service Using Fonts, Journal of Computer Science 7, 2011.

Yogendra Kumar Jain, Roopesh Kumar and Pankaj Agarwal (2011), Securing Data Using Jpeg Image over Mobile Phone, Global Journal of Computer Science and Technology, Volume 11, Issue 13, Version 1.0, August 2011.

S. Mohanapriya, Design and Implementation of Steganography Along with Secured Message Services in Mobile Phones, International Journal of Emerging Technology and Advanced Engineering, vol. 2, Mei 2012.