

# Pemanfaatan File Sharing untuk Menyampaikan Pesan Secara Rahasia Menggunakan Steganografi pada Andorid

Dedy Prasetyady / 13510102  
Program Studi Teknik Informatika  
Sekolah Teknik Elektro dan Informatika  
Institut Teknologi Bandung, Jl. Ganessa 10 Bandung 40132, Indonesia  
13510102@std.stei.itb.ac.id

**Abstract**—Peper ini berisi rancangan sistem dan juga aplikasi yang memungkinkan untuk mengirimkan pesan secara rahasia. Agar pesan rahasia yang dikirimkan tidak diketahui, tidak dibaca dan juga tidak menimbulkan kecurigaan orang lain maka pesan akan disisipkan pada media lain dalam hal file gambar dengan memanfaatkan teknik dan prinsip steganografi. Setelah pesan berhasil disisipkan kedalam file gambar kemudian file gambar yang bersangkutan akan dikirimkan dengan memanfaatkan fasilitas file sharing dengan menggunakan internet. Pesan yang tersembunyi didalam gambar kemudian dapat diambil kembali dengan memanfaatkan aplikasi yang sama. Agar proses-proses untuk mengirimkan pesan secara rahasia tersebut dapat dilakukan kapan saja dan dimana saja maka proses tersebut harus dapat dilakukan pada perangkat mobile. Perangkat yang dipilih dalam hal ini adalah perangkat *smartphone* berbasis Android karna perangkat ini dapat melakukan proses-proses yang dibutuhkan dan sudah dimiliki dan dimanfaatkan oleh masyarakat luas.

**Kata Kunci**—Android, Steganografi, Pesan rahasia, File Sharing, Gambar.

## I. PENDAHULUAN

Terkadang dibutuhkan menyampaikan pesan yang bersifat pribadi atau rahasia yang ingin disampaikan kepada orang tertentu saja dan tidak ingin orang lain mengetahuinya. Jika dapat bertemu langsung dengan orang yang bersangkutan tentu pesan rahasia tersebut dapat disampaikan langsung kepada orang tersebut namun terkadang karena terpisah jarak dan waktu tidak dimungkinkan untuk bertemu langsung sehingga pesan rahasia tersebut harus dikirimkan. Saat ini sudah terdapat banyak media yang dapat digunakan untuk berkomunikasi atau menyampaikan pesan kepada orang lain dari jarak jauh seperti sms, email, *chatting*, telpon, *video call* dan lain sebagainya. Meski pesan rahasia dapat dikirimkan hanya kepada orang tertentu saja namun ada resiko pesan rahasia yang dikirimkan di curi dan dibaca oleh orang lain saat dalam perjalanan.

Agar pesan yang dikirimkan terjaga kerahasiaannya dan tidak dapat baca oleh orang lain selain orang yang dituju pesan yang dikirimkan sebenarnya dapat diacak (enkripsi)

terlebih dahulu sebelum dikirimkan dan kemudian akan disusun kembali (dekripsi) oleh si penerima pesan. Dengan mengenkripsi pesan maka pesan yang dikirimkan akan berbeda dari pesan semula akan menjadi pesan yang acak. Jika dalam perjalanan pesan yang sudah diacak tersebut disadap atau dicuri oleh orang lain selama orang tersebut tidak dapat mendekripsi kembali pesan tersebut maka orang tersebut tetap tidak akan dapat membaca dan memahami pesan tersebut namun hal ini akan menimbulkan kecurigaan karena pesan tersebut sudah berbentuk acak.

Untuk dapat mengirimkan pesan rahasia kepada orang lain secara rahasia dan tanpa dicurigai maka pesan rahasia dapat disembunyikan pada medium dengan memanfaatkan prinsip dan teknik steganografi dan kemudian medium yang sudah berisi pesan tersebut dikirimkan dan kemudian penerima akan mengambil pesan yang disembunyikan pada medium tersebut.

Pesan yang dikirimkan secara digital dapat disisipkan dan disembunyikan didalam media lain seperti file gambar, file suara, atau file video. Diantara medium-medium tersebut file gambar merupakan adalah file yang dianggap paling baik untuk menyisipkan pesan-pesan yang berukuran kecil. Alasan pemilihan file gambar sebagai medium untuk menyisipkan pesan adalah karena file gambar dapat disisipkan tanpa merusak tampilan dari file gambar yang bersangkutan berbeda dengan file suara yang jika disisipkan pesan maka dapat disadari perbedaannya dengan file yang asli. Alasan lain adalah karena file gambar relatif berukuran lebih kecil dari file suara ataupun file video sehingga beban untuk mengirimkan file gambar relatif lebih kecil. Selain alasan diatas bertukar atau mengirimkan file gambar merupakan hal yang sudah biasa sehingga dapat mengurangi kecurigaan.

Untuk mengirimkan file gambar dapat dimanfaatkan fasilitas file sharing dengan memanfaatkan internet. Saat ini sudah terdapat sistem tersebar yang mendukung file sharing seperti google drive, dropbox, mediafire, facebook, instagram, dll.

Dengan kemajuan teknologi sekarang ini sudah terdapat alat mobile yang dapat mendukung proses proses yang dibutuhkan untuk mengirimkan pesan secara rahasia

seperti yang sudah dijelaskan diatas yaitu *smartphone*. Salah satu *smartphone* yang sudah digunakan luas oleh masyarakat adalah *smartphone* berbasis android. Dengan membuat aplikasi steganografi untuk menyisipkan pesan pada file gambar pada platform android serta dengan memanfaatkan fasilitas file sharing pada jaringan internet maka kedepannya mengirimkan pesan rahasia kepada orang lain tanpa menimbulkan kecurigaan dapat dilakukan dengan lebih mudah kapan saja dan dimana saja.

## II. DASAR TEORI

### A. *Steganografi*

Steganografi merupakan ilmu dan juga seni menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada orang lain yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Kata steganografi berasal dari bahasa Yunani yaitu *steganos* yang artinya tersembunyi atau terselubung dan *graphein* yang berarti menulis.

Kini istilah steganografi juga digunakan untuk penyembunyian data digital dalam file komputer. Teknik steganografi meliputi banyak metode untuk menyembunyikan pesan rahasia didalam berkas lain tanpa menunjukkan ciri-ciri perubahan yang nyata dari berkas semula. Contohnya menyisipkan file teks kedalam sebuah file gambar dengan mengubah bit-bit akhir yang merepresentasikan warna pada pixel gambar sesuai dengan nilai bit-bit file teks yang disisipkan. Tujuan dari steganografi adalah merahasiakan dan menyembunyikan keberadaan dari sebuah informasi tanpa menimbulkan kecurigaan.

### B. *Steganografi pada Citra Digital*

Citra digital terdiri atas sejumlah pixel. Citra 200x150 berarti memiliki 200x150 pixel = 30000 pixel. Setiap pixel panjangnya n-bit. Contoh: citra 8 - bit, citra 24-bit, dsb. Nilai pada setiap pixel menyatakan derajat keabuan. Pada citra 24-bit (*real image*), 1 pixel = 24 bit, terdiri dari komponen RGB (Red-Green-Blue)

Teknik yang digunakan :

- Spatial (time) domain

Memodifikasi langsung nilai byte dari cover-object (nilai byte dapat merepresentasikan intensitas/warna pixel atau amplitudo) Memodifikasi langsung nilai byte dari cover-object

Contoh: Metode modifikasi LSB

- Transform domain

Memodifikasi hasil transformasi sinyal dalam ranah frekuensi

Contoh: Metode Spread Spectrum

Pada makalah kali ini teknik yang digunakan adalah

spatial domain yaitu metode LSB.

Metode LSB memanfaatkan indra visual manusia dalam mengamati perubahan sedikit pada gambar. Caranya dengan mengganti bit LSB pixel dengan bit data. Mengubah bit LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya dan hal ini tidak akan berpengaruh terhadap persepsi.

### C. *Platform Android*

Android merupakan sistem operasi yang berbasis Linux yang didesain khusus untuk perangkat mobile yang menggunakan layar sentuh seperti telepon pintar dan komputer tablet. Awalnya android dikembangkan oleh Andorid, Inc. yang kemudian dibeli oleh Google, Inc. Untuk mengembangkan Android kemudian dibentuk Open Handset Alliance, konsorsium dari 34 perusahaan besar yang bergerak di bidang perangkat keras, perangkat lunak, serta telekomunikasi antara lain HTC, Intel, Qualcomm, T-Mobile, dan Nvidia.

Android merupakan *open source* dan Google merilis kode android dengan lisensi Apache. Kode *open source* serta lisensi yang diberikan memungkinkan pengembang untuk dengan leluasa memodifikasi dan mendistribusikan perangkat yang menggunakan android. Android juga memiliki komunitas pengembang yang besar yang membuat aplikasi-aplikasi yang dapat memperbanyak dan memperluas fungsionalitas dari perangkat berbasis android. Pada Oktober 2012 terdapat sekitar 700.000 aplikasi yang tersedia untuk Android dan perkiraan jumlah yang sudah di download dari Google Play mencapai sekitar 25 miliar. Karena hal tersebut saat ini Android merupakan platform untuk *smartphone* yang paling banyak digunakan di dunia.

Fitur yang umumnya tersedia di Android antara lain:

- Kerangka aplikasi: memungkinkan penggunaan dan penghapusan komponen yang tersedia.
- Dalvik mesin virtual: mesin virtual yang dioptimalkan untuk perangkat telepon seluler.
- Grafis: grafik di 2D dan grafis 3D berdasarkan pustaka OpenGL.
- SQLite: untuk penyimpanan data.
- Mendukung media: audio, video, dan berbagai format gambar (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF)
- GSM, Bluetooth, EDGE, 3G, 4G dan WiFi (tergantung piranti keras)
- Kamera, Global Positioning System (GPS), kompas, NFC dan accelerometer (tergantung piranti keras)

### D. *File Sharing*

File sharing merupakan pendistribusian atau penyediaan akses ke informasi yang tersimpan secara digital, seperti program komputer, multimedia, dokumen elektronik, dan lain lain. Pengimplementasiannya dapat dilakukan dengan berbagai cara.

Saat ini terdapat banyak aplikasi sistem tersebar terkait file sharing yang dapat dimanfaatkan untuk pendistribusian file melalui jaringan internet. Beberapa contoh aplikasi sistem tersebar yang mendukung file sharing antara lain dropbox, mediafire, instagram, dll.

### III. ANALISIS DAN IMPLEMENTASI

#### A. Analisis Kebutuhan

Aplikasi Sembunyiin ini digunakan untuk menyembunyikan pesan teks kedalam file gambar pada perangkat dengan sistem operasi Android. Pesan disembunyikan kedalam file gambar dengan cara menyisipkan file teks kedalam file gambar menggunakan metode LSB. Untuk menambah tingkat keamanan maka penyisipan kedalam file gambar menggunakan kunci yang akan membangkitkan bilangan random. Gambar yang sudah disisipi pesan rahasia kemudian akan dikirimkan menggunakan aplikasi sistem tersebar yang memiliki fasilitas file sharing. Disisi penerimayang dilakukan adalah mengambil file gambar yang bersangkutan dengan memanfaatkan aplikasi sistem tersebar yang sama seperti yang digunakan pengirim. Setelah gambar yang mengandung rahasia didapatkan kemudian penerima melakukan pengambilan kembali isi pesan rahasia yang disimpan dengan menggunakan Sembunyiin dan untuk dapat mengambil pesan rahasia yang tersembunyi maka penerima harus mengetahui kunci yang digunakan pengirim untuk menyisipkan pesan. Setelah pengirim memasukkan kunci yang benar maka pesan rahasia yang tersembunyi akan kembali dimunculkan.

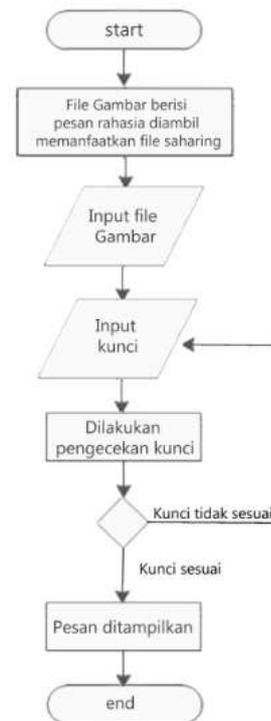
Agar aplikasi Sembunyiin sesuai dengan rancangan diatas maka aplikasi Sembunyiin harus memiliki beberapa kemampuan dan batasan. Kemampuan yang harus dimiliki aplikasi Sembunyiin dan juga batasannya adalah sebagai berikut:

- Dapat menerima dan membaca file Gambar
- Dapat membaca pesan
- Dapat membangkitkan nilai random dari kunci
- Dapat menyisipkan pesan kedalam file Gambar dengan memanfaatkan bilangan random yang dibangkitkan oleh kunci.
- Dapat mengambil pesan yang tersimpan didalam file Gambar dengan memanfaatkan kunci yang sesuai.

Fungsi utama dari aplikasi Sembunyiin ini dapat digolongkan menjadi dua bagian besar yaitu fungsi menyembunyikan pesan dan fungsi pengambilan pesan. Aplikasi ini tergolong aplikasi yang sederhana dan langkah-langkah dalam menjalankan tiap fungsi dari sistem ini juga tidak terlalu rumit. Langkah-langkah yang harus dijalankan untuk menjalankan fungsi menyembunyikan dan pengambilan pesan bisa dilihat pada diagram berikut.



Gambar 1. Alur Proses Penyisipan Pesan



Gambar 2. Alur Proses Pengambilan Pesan

#### B. Komponen yang Digunakan

Implementasi aplikasi Sembunyiin pada makalah ini dilakukan dengan memanfaatkan perangkat lunak Eclipse Indigo sebagai alat bantu pengembangan. Aplikasi dibangun dengan bahasa Java dan dibangun pada platform Android 2.2.

#### C. Implementasi

Dalam pengimplementasian aplikasi Sembunyiin ini dibagi menjadi 4 kelas yaitu kelas yaitu KomponenUtama, LSBHandler, Penyembunyi, Pengambil.

## 1. Kelas KomponenUtama

Kelas ini berfungsi sebagai interface utama dari aplikasi Sembunyiin. Kelas ini yang pertama kali dibangkitkan saat pemanggilan program yang kemudian berfungsi menerima pilihan user untuk memilih opsi menyembunyikan pesan atau menampilkan pesan.



Gambar 3. Interface KomponenUtama

## 2. LSBHandler

Kelas ini berfungsi menangani operasi penyisipan bit-bit pesan pada bit-bit akhir tiap komponen pixel pada citra digital yang digunakan.

Citra digital yang digunakan dalam pemrosesan ini sudah diubah terlebih dahulu menjadi bitmap dengan memanfaatkan library BitmapFactory yang sudah tersedia pada library Android. Citra digital yang sudah dalam bentuk bitmap tersebut tiap pixelnya tidak terdiri dari tiga element rgb seperti pada umumnya melainkan terdiri dari empat element yaitu Alpha, Red, Green, Blue atau disingkat argb. Tiap pixel direpresentasikan oleh nilai integer. Nilai pixel yang direpresentasikan dalam integer tidak memungkinkan untuk langsung diubah LSBnya karena hal ini akan merubah warna secara mencolok. Agar proses penyisipan dapat berlangsung dengan baik maka representasi nilai pixel harus diubah dari integer menjadi byte.

```
public static byte[] KonversiIntToByte(int[] array) {
    byte[] newarray = new byte[array.length * 3];
    for (int i = 0; i < array.length; i++) {
        newarray[i * 3] = (byte) ((array[i] >> 16) & 0xFF);
        newarray[i * 3 + 1] = (byte) ((array[i] >> 8) & 0xFF);
        newarray[i * 3 + 2] = (byte) ((array[i]) & 0xFF);
    }
    return newarray;
}
```

Gambar 4. Kode program Konversi Integer ke Byte

Pada proses konversi yang dilakukan integer yang merepresentasikan nilai argb diubah menjadi array byte yang merepresentasikan nilai rgb saja. Hal ini dilakukan karena nilai Alpha tidak akan digunakan dalam penyisipan.

Diakhir proses penyisipan maka kumpulan byte yang merepresentasikan pixel dalam rgb harus dapat kembali di ubah dalam integer yang merepresentasikan argb.

```
public static int[] KonversiArrayToIntArray(byte[] b) {
    Log.v("Ukuran byte array", b.length+"");
    int size=b.length / 3;
    Log.v("Size Int array",size+"");
    System.runFinalization();
    System.gc();
    Log.v("Memory", Runtime.getRuntime().freeMemory()+"");
    int[] result = new int[size];
    int off=0;
    int index = 0;
    while (off<b.length) {
        result[index++] = byteArrayToInt(b, off);
        off= off+ 3;
    }
    return result;
}
```

Gambar 5. Kode program Konversi Byte ke Integer

Kelas ini juga berfungsi untuk menangani penyisipan pesan kedalam nilai nilai bit pada gambar.

```
public static byte[] SembunyiinPesan(int[]
fileGambar, int Kolom, int Baris,String Pesan,
String Kunci) {
    Pesan += "#!@";
    Pesan = "@!#" + Pesan;
    byte[] msg = Pesan.getBytes();
    int Kunci = (Int)Kunci. getBytes().[0];
    int channels = 3;
    int shiftIndex = 4;
    byte[] result = new byte[Baris * Kolom *
channels];
    int msgIndex = 0;
    int resultIndex = 0;
    boolean msgEnded = false;
    for (int row = 0; row < Baris; row++) {
        for (int col = 0; col < Kolom; col++) {
            int element = row * Kolom + col;
            byte tmp = 0;
            for (int channelIndex = Kunci; channelIndex <
channels; channelIndex++) {
                if (!msgEnded) {
                    tmp = (byte) (((fileGambar[element] >>
binary[channelIndex] & 0xFF) & 0xFC) |
((msg[msgIndex] >> toShift[(shiftIndex++)
% toShift.length] & 0x3)) // 6
if (shiftIndex % toShift.length == 0) {
                    msgIndex++;}
                if (msgIndex == msg.length) {
                    msgEnded = true;}
                else {
                    tmp = (byte) (((fileGambar[element] >>
binary[channelIndex] & 0xFF));}
                    result[resultIndex++] = tmp;}}
            return result;}
}
```

Gambar 6. Kode Program untuk Menyembunyikan Pesan

Pada penyembunyian pesan digunakan string “#!@” untuk menandai awal dari pesan yang disisipkan dan “@!#” untuk menandakan akhir dari pesan yang disisipkan. Teknik penyisipan yang digunakan adalah LSB 2 bit. Pemilihan teknik penyisipan LSB 2 bit adalah untuk memaksimalkan ukuran pesan yang bisa disimpan namun tetap menjaga kualitas file gambar yang sudah disisipkan tetap tidak terlalu berbeda dengan gambar aslinya.

Kelas ini juga berfungsi dalam pengambilan pesan yang sudah disembunyikan.

```

public static String AmbilPesan(byte[] fileGambar,
int Kolom,
int Baris, String Kunci) {
Vector<Byte> v = new Vector<Byte>();
String builder = "";
int shiftIndex = 4;
int Kunci = (Int)Kunci. getBytes()[0];
byte tmp = 0x00;
for (int i = Kunci; i < fileGambar.length; i++) {
tmp = (byte) (tmp | ((fileGambar[i] <<
toShift[shiftIndex
% toShift.length]) & andByte[shiftIndex++ %
toShift.length]));
if (shiftIndex % toShift.length == 0) {
v.addElement(new Byte(tmp));
byte[] nonso = { v.elementAt(v.size() -
1).byteValue() };
String str = new String(nonso);
// if (END_MESSAGE_COSTANT.equals(str)) {
if
(builder.endsWith(END_MESSAGE_COSTANT))
{
break;
} else {
builder = builder + str;
if (builder.length() ==
START_MESSAGE_COSTANT.length()
&&
!START_MESSAGE_COSTANT.equals(builder)) {
builder = null;
break;
}
}
tmp = 0x00;
}
}
if (builder != null)
builder =
builder.substring(START_MESSAGE_COSTANT.l
ength(), builder
.length()
- END_MESSAGE_COSTANT.length());
return builder;
}

```

Gambar 7. Kode Program untuk Mengambil Pesan

### 3. Kelas Penyembunyian

Kelas ini berfungsi sebagai interface dan juga berfungsi menangani pemanggilan fungsionalitas penyembunyian pesan kedalam gambar. Kelas ini menangani pemilihan file gambar yang akan dipakai sebagai media untuk

penyisipan, membaca pesan yang ingin disembunyikan dan membaca kunci yang akan digunakan untuk pembangkitan bilangan random. Kelas ini kemudian akan memanggil fungsi untuk menyisipkan pesan kedalam file gambar.



Gambar 8. Interface Penyembunyian Pesan

### 4. Kelas Pengambil

Kelas ini berfungsi sebagai interface dan juga berfungsi menangani pemanggilan fungsionalitas penyembunyian pesan kedalam gambar. Kelas ini menangani pemilihan file gambar yang akan diambil pesan rahasianya dan juga membaca kunci yang akan digunakan untuk pembangkit bilangan random.



Gambar 8. Interface Pengambilan Pesan

## III. PENGUJIAN

Pengujian dilakukan pada telpon seluler Android Lenovo S-560 yang menggunakan firmware Android 4.0 ICS. Saat pengujian ternyata aplikasi belum dapat berfungsi sebagaimana mestinya. Program hanya bisa menampilkan tampilan namun saat menyisipkan pesan masih terdapat kesalahan. Saat penyisipan pesan program menampilkan pesan error terkait ukuran array integer. Program hanya berhasil menampilkan tampilan saja

## V. SIMPULAN DAN SARAN

### A. Simpulan

Untuk mengirimkan pesan secara rahasia tanpa menimbulkan kecurigaan orang lain dapat digunakan teknik steganografi. Steganografi dapat diterapkan dalam dunia digital dan menyembunyikan pesan dalam media digital seperti menyembunyikan pesan teks ke dalam citra digital. Untuk menyampaikan pesan yang tersembunyi di dalam citra digital dapat dilakukan dengan mengirimkan file yang sudah berisi pesan yang disisipkan memanfaatkan file sharing yang sudah banyak disediakan oleh aplikasi sistem tersebar seperti dropbox, instagram, dan lain lain. Untuk meningkatkan kemudahan dalam berkirim pesan secara rahasia pemanfaatan perangkat mobile dapat menjadi solusi. Salah satu perangkat mobile yang dapat digunakan untuk mengirimkan pesan secara rahasia dengan teknik steganografi adalah perangkat *mobile* berbasis Android. Dibutuhkan aplikasi yang dapat melakukan steganografi pada android untuk mendukung pengiriman pesan secara rahasia. Perangkat berbasis Android sudah mendukung proses-proses yang dibutuhkan untuk melakukan steganografi dan juga pengiriman pesan. Aplikasi untuk melakukan steganografi yang disiapkan belum berhasil diimplementasi dengan baik.

### B. Saran

Aplikasi yang dibangun masih belum dapat berfungsi dengan baik dan benar untuk itu perbaikan fungsionalitas dijadikan prioritas utama kedepannya. Jika fungsionalitas sudah berhasil diperbaiki kedepannya adabainya melakukan perbaikan terkait hal hal berikut :

- Aplikasi didesain dengan interface menarik
- Aplikasi dapat mengirimkan file secara langsung ke beberapa aplikasi sistem tersebar yang memiliki fasilitas file sharing
- Aplikasi dapat langsung mengakses file yang terdapat di aplikasi sistem tersebar yang menyimpan file gambar yang berisi pesan rahasia.

## DAFTAR PUSTAKA

- [1] <http://developer.android.com/index.html>
- [2] <http://www.android-indonesia.com/forum/developers/>
- [3] Wayner, Peter (2009). Disappearing cryptography 3rd Edition: information hiding: steganography & watermarking

## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 25 Maret 2013

ttd



Dedy Prasetya / 13510102