p-ISSN: 1978-5232
e-ISSN: 2527-337X

PENGAMANAN PESAN TEKS MENGGUNAKAN TEKNIK STEGANOGRAFI SPREAD SPECTRUM BERBASIS ANDROID

[1]Achmad Noercholis, [2]Yohanes Nugraha

[1], [2]Teknik Informatika STMIK Asia Malang

Abstrak: *Keamanan dalam pengiriman informasi yang bersifat rahasia erupakan salah satu faktor penting yang harus dijaga. Salah satu teknik yang dapat dipakai untuk menangani hal tersebut adalah steganografi. Steganografi merupakan ilmu dan seni yang mempelajari cara penyembunyian informasi rahasia ke dalam suatu media sedemikian sehingga manusia tidak dapat menyadari keberadaan pesan tersebut. Dalam hal ini teknik steganografi yang digunakan adalah metode spread spectrum. Dalam teknik steganografi ini terdapat dua proses yaitu proses embedding dan proses extraction. Pada proses embedding pesan rahasia akan disisipkan ke dalam citra JPG dengan menggunakan metode spread spectrum. Dan proses extraction untuk mendapatkan hasil dari pesan rahasia yang telah disisipkan juga menggunakan spread spectrum. Dalam proses pengujian yang dilakukan dengan beberapa image dengan ukuran yang berbeda-beda dapat disimpulkan bahwa jumlah maksimal karakter pesan yang dapat ditampung oleh sebuah image mengikuti ukuran image tersebut. Semakin besar ukuran image atau cover yang digunakan untuk menyisipkan, semakin banyak jumlah karakter atau teks yang mampu disisipkan.*

Kata Kunci: Steganografi, *Spread Spectrum, Android.*

I. PENDAHULUAN

Dewasa ini kita dapat bertukar informasi atau mendapatkan sebuah informasi dengan dengan mudah dan waktu yang relatif singkat. Harga *smartphone* yang semakin terjangkau merupakan faktor penting yang menunjang kemudahan tersebut. Perkembangan ilmu teknologi ini sangat membantu dan memiliki dampak positif bagi manusia. Tetapi disamping memiliki dampak positif bagi dunia komunikasi tentunya perkembangan teknologi ini memiliki dampak negatif didalamnya, yaitu kemungkinan terjadinya pencurian data atau bocornya kerahasiaan dari sebuah data. Tentunya kita sendiri tidak bisa menghindari kemungkinan-kemungkinan terjadinya pencurian data ataupun bocornya kerahasiaan dari sebuah data. Hal ini disebabkan karena proses pertukaran informasi melalui media digital bisa dilakukan oleh siapa saja dimana saja dan kapan saja.

Dengan semakin banyak serangan yang mungkin terjadi dalam proses pertukaran data menyebabkan perlunya suatu metode agar dapat meningkatkan keamanan informasi. Salah satu metode yang dapat digunakan yaitu teknik steganografi. Steganografi memberikan solusi untuk penyembunyian pesan yang sering digunakan dalam proses pengiriman data. Steganografi adalah teknik menyisipkan pesan kedalam suatu media, dimana pesan rahasia yang akan dikirimkan tidak diubah bentuknya, melainkan disisipkan pada sebuah media lain (*cover-image*) yang digunakan dalam kehidupan sehari-hari. Media baru yang telah disisipi pesan rahasia (*stego-image*) kemudian dikirim kepada penerima tanpa menimbulkan kecurigaan dari pihak luar, karena perbedaan dari media asli (*cover- image*) dengan media yang telah disisipi pesan rahasia (stegoimage) tidak dapat disadari secara langsung oleh manusia. Steganografi pada masa kini dilakukan pada media digital berupa citra, audio, maupun video.

Salah satu metode yang dapat digunakan yaitu metode *Spread Spectrum*. Metode spread Spectrum tidak hanya tangguh dalam steganografi tetapi juga tangguh dalam *watermarking*, yang

p-ISSN: 1978-5232
e-ISSN: xxxx-xxxx

merupakan salah satu bidang pengaplikasian dari steganografi yang ditujukan untuk melindungi hak cipta atas produk digital. Untuk membaca suatu pesan, penerima memerlukan algoritma yaitu *Linear Congruential Generator*. Kelebihan metode ini dibandingkan metode yang lain yaitu sulit dideteksinya suatu pesan yang sudah tersembunyi.

II. LANDASAN TEORI

A. Steganografi

Menurut Ariyus (2009), Teknik steganografi sudah ada sejak 4000 tahun yang lalu di kota Menet Khufu, Mesir. Awalnya adalah penggunaan hieroglyphic yakni menulis menggunakan karakter-karakter dalam bentuk gambar. Ahli tulis menggunakan tulisan Mesir kuno ini untuk menceritakan kehidupan majikannya. Tulisan Mesir kuno tersebut menjadi ide untuk membuat pesan rahasia saat ini. Oleh karena itulah, tulisan Mesir kuno yang menggunakan gambar dianggap sebagai steganografi pertama di dunia.

Menurut Kipper (2004), Steganografi adalah jenis komunikasi yang tersembunyi, yang secara harfiah berarti "tulisan tertutup." Pesannya terbuka, selalu terlihat, tetapi tidak terdeteksi bahwa adanya pesan rahasia. Deskripsi lain yang popular untuk steganografi adalah *Hidden in Plain Sight* yang artinya tersembunyi di depan mata. Sebaliknya, kriptografi adalah tempat pesan acak, tak dapat dibaca dan keberadaan pesan sering dikenal.

Sedangkan menurut Ariyus (2009), Steganografi merupakan istilah yang berasal dari bahasa yunani, yaitu steganos yang berarti penyamaran atau penyembunyian dan graphein yang berarti tulisan. Jadi, steganografi bisa diartikan sebagai seni menyembunyikan pesan dalam data lain tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hampir terlihat sama.

1. Teknik Steganografi

Menurut Ariyus (2009), ada tujuh teknik dasar yang digunakan dalam steganografi, yaitu *Injection*, Substitusi , Transform Domain, *Spread Spectrum, Statistical Method, Distortion* dan *Cover Generation*.

2. Metode Spread Spectrum

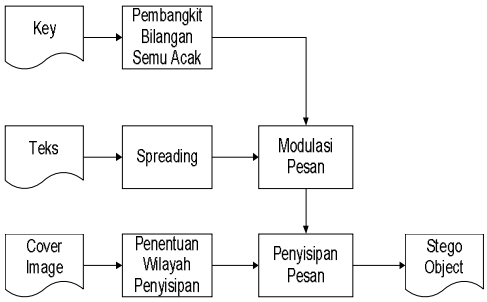
Spread spectrum merupakan bagian dari ranah transform. Sebuah teknik pentransmisian dengan menggunakan *pseudo-noise code*, yang independen terhadap data informasi, sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwith*) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise code* tersinkronisasi.

Berdasarkan definisi dapat dikatakan bahwa steganografi menggunakan metode *spread spectrum* memperlakukan *cover-object* baik sebagai derau (*noise*) ataupun sebagai usaha untuk menambahkan derau semu (*pseudo-noise*) ke dalam *cover-object*.

Di dalam metode spread spectrum, penyisipan pesan atau informasi terdapat kunci atau *key* yang digunakan untuk mengenkripsi pesan. *Key* tersebut kita dapatkan melalui pembangkit bilangan semu acak dengan algoritma LCG (*Linear Conruential enerator*). Sebelum pesan disisipkan kedalam cover image, maka terlebih dahulu menentukan wilayah penyisipannya. Setelah menentukan wilayah penyisipan, selanjutnya adalah proses *spreading*. Proses *spreading* dilakukan sesuai dengan bilangan pengali skalar yang ditentukan. Pada proses ini citra rahasia diambil nilai intensitas per-pixel nya, lalu diubah kedalam bilangan biner. Kemudian bilangan biner tersebut disebar sesuai bilangan pengali skalar yang telah ditentukan, maka hasil keluaran dari proses spreading ini adalah deret bilangan biner yang telah tersebar dengan panjang setiap deretnya sebesar 32 bit.

p-ISSN: 1978-5232
e-ISSN: xxxx-xxxx

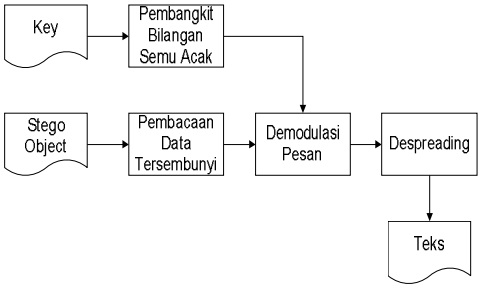
Setelah proses spreading yang selanjutnya adalah proses modulasi pesan. Proses ini merupakan proses pengacakan pesan yang telah disebar dengan bilangan *pseudonoise* yang telah dibangkitkan menggunakan algoritma LCG. Panjang dari bilangan *pseudonoise* ini disesuaikan dengan panjang dari pesan. Jika panjang pesan lebih kecil dari panjang bilangan *pseudonois*e, bilangan *pseudonoise* tersebut akan dipotong sesuai dengan ukuran pesan. Sebaliknya, jika panjang pesan lebih besar dari panjang bilangan *pseudonoise*, maka bilangan tersebut akan diulang sampai panjangnya sama dengan panjang pesan. Proses modulasi tersebut dilakukan dengan menggunakan fungsi XOR (*Exclusive OR*). Nilai yang dihasilkan dari proses modulasi inilah yang kemudian akan disisipkan ke dalam berkas *cover image*. Setelah pesan disisipkan maka outputnya merupakan *stego-object* yang sudah tersisipi sebuah pesan. Skema penyisipan pesan dapat dilihat pada Gambar 1



Gambar 1 Skema Penyisipan Pesan

Proses yang berikutnya di dalam metode *spread spectrum* setelah dilakukan penyisipan pesan adalah proses ekstraksi. Di dalam proses ekstraksi terlebih dahulu dilakukan pembacaan data yang disisiipkan di dalam *stego object* dalam hal ini adalah *image*. Pembacaan data yang dilakukan berdasarkan informasi wilayah penyisipan pesan. Pembacaan akan dilakukan secara berselang-seling pada matriks frekuensi yang terdapat pada citra dan berlangsung sampai data yang dibaca besarnya sama dengan informasi ukuran berkas yang disisipkan.

Setelah data tersembunyi berhasil dikumpulkan, dilakukan proses demodulasi terhadap data tersebut. Proses demodulasi ini melibatkan bilangan acak yang dibangkitkan dari kunci masukan menggunakan algoritma LCG. Adapun proses pembangkitan bilangan acak yang dilakukan pada tahap ekstraksi pesan sama seperti proses pembangkitan bilangan acak pada tahap penyisipan pesan. Hasil dari proses demodulasi tersebut akan mengalami proses *de-spreading*. Proses despreading ini bekerja menggunakan faktor besaran pengali yang dimasukkan oleh pengguna pada proses penyisipan pesan. Proses *de-spreading* ini adalah proses yang dilakukan untuk mendapatkan bit-bit dari pesan tersembunyi, maka hasil keluaran dari proses de-spreading ini adalah deret bilangan biner yang telah disusutkan dengan panjang setiap deretnya sebesar 8 bit. Lalu bit-bit tersebut dikonversi kedalam bilangan desimal, yang selanjutnya akan disusun sebagai nilai intensitas tiap pixel pada citra rahasia. Skema proses ekstraksi dapat dilihat pada gambar 2.



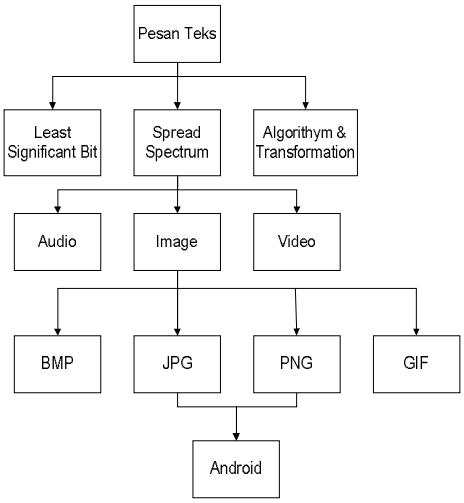
Gambar 2. Skema Proses Ekstraksi Pesan

p-ISSN: 1978-5232
e-ISSN: xxxx-xxxx

III. PERANCANGAN SISTEM

A. Analisa Masalah

Analisa Permasalahan di dalam penelitian ini dapat dilihat melalui blok diagram berikut dengan penjelasannya.



Gambar 3 Blok Diagram Analisa Masalah

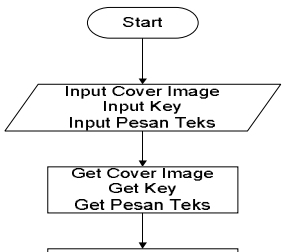
Pada blok diagram dapat dilihat alur analisa permasalahan yang ditunjukkan dengan teks berwarna merah. Prosesnya diawali dari sebuah pesan teks dengan menggunakan sebuah teknik dan metode di dalam steganografi yaitu spread sprectrum yang harus disisipkan kedalam sebuah media penampung yaitu image dengan format JPG dan PNG yang diimplementasikan kedalam sebuah perangkat mobile Android.

1. Flowchart Sistem

Dalam perancangan program aplikasi steganografi, sebagai media untuk mendeskripsikan semua proses maka dipergunakan diagram alir (flow chart). Flowchart ini berguna sebagai gambaran proses steganografi dalam hal ini proses embedding atau penyisipan dan proses extraction atau ekstraksi. Dalam perancangan ini terdapat 2 diagaram alir (flow chart) untuk proses embedding dan proses extraction.

a. Proses Embedding

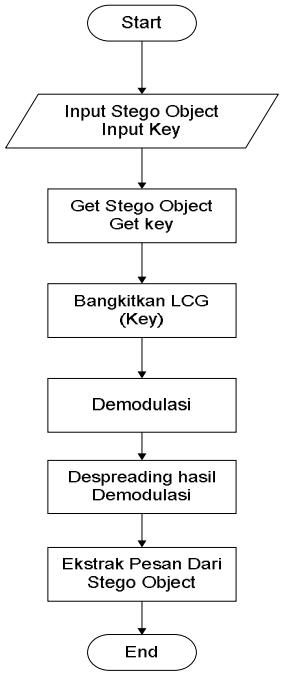
Pada Proses Embedding ini dimana cover image yang digunakan adalah dengan format JPG atau PNG. Untuk proses penyisipan sebuah pesan kedalam cover image, yaitu dengan cara memilih dahulu cover image serta sudah ditentukan pesan yang akan disisipkan. Kemudian dilakukan beberapa proses seperti pembangkitan bilangan acak dengan menggunakan algoritma LCG (*Linear Congruential Generator*), proses spreading atau penyebaran dan proses modulasi untuk pengacakan antara pesan dan kata kunci yang didapatkan dari pembangkitan bilangan acak. Untuk lebih Jelasnya proses embedding dapat dilihat didalam flowchart pada Gambar 4.



p-ISSN: 1978-5232
e-ISSN: xxxx-xxxx

b. Proses Extraction

Dalam proses extraction atau ekstraksi ini proses yang dilakukan hampir sama halnya dengan proses embedding atau penyisipan tetapi ada beberapa perbedaan. Dalam proses ini terlebih dahulu dipilih stego object yaitu image yang sudah disisipi sebuah pesan. Kemudian melakukan beberapa proses ekstraksi diantaranya proses demodulasi dimana proses ini melibatkan bilangan acak yang telah dibangkitkan dari kata kunci yang digunakan dan proses despreading untuk mendapatkan bit-bit dari pesan sehingga menghasilkan deret bilangan biner yang nantinya berfungsi agar pesan yang telah disisipkan kedalam stego object dapat diekstraksi dan dapat dibaca. Untuk lebih jelasnya proses ekstraksi dapat dilihat didalam flowchart pada Gambar 5.



Gambar 5. Flowchart Proses Ekstraksi Pesan

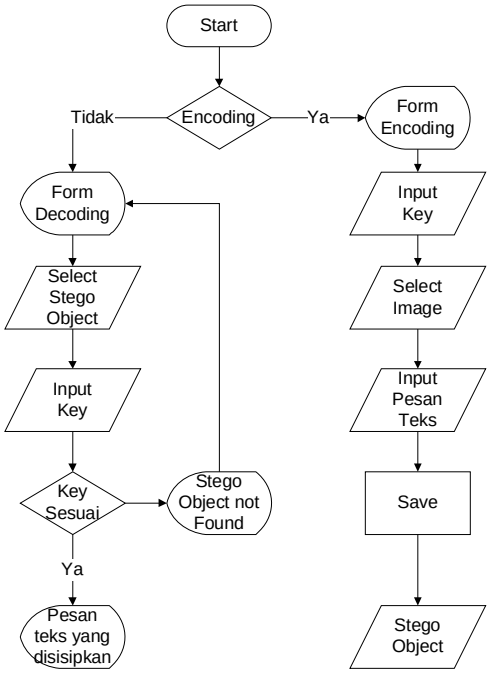
p-ISSN: 1978-5232
e-ISSN: xxxx-xxxx

IV. IMPLEMENTASI SISTEM

Di dalam implementasi sistem akan diperlihatkan tampilan antarmuka dan proses encode dan decode dari aplikasi ini serta flowchart implementasi pada android.

A. Flowchart Implementasi Pada Android

Berikut ini pada gambar 6 merupakan flowchart implementasi pada android.



Gambar 6. *Flowchart* Implementasi Pada Android

1. Form Utama

Dalam tampilan awal atau tampilan utama disini terdapat 2 menu yaitu untuk melakukan proses encode dan melakukan proses decode. Apabila user ingin melakukan proses penyisipan pesan kedalam image maka dapat memilih menu encode image dan sebaliknya apabila user ingin melakukan ekstraksi pesan yang sudah disisipkan dalam image maka user dapat memilih menu decode image. Tampilan utama aplikasi dapat dilihat pada gambar 7

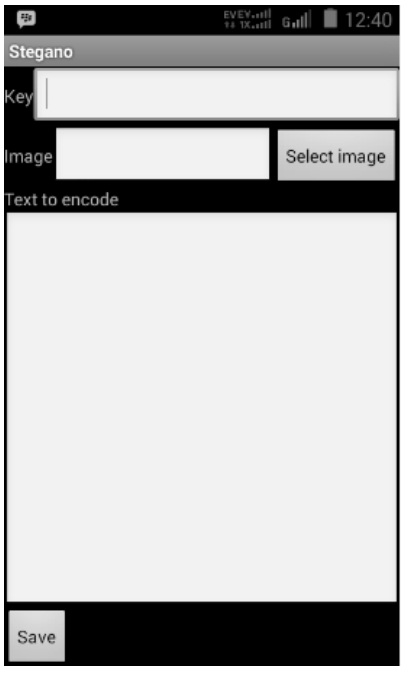
p-ISSN: 1978-5232
e-ISSN: xxxx-xxxx

2. Form Encode Image

Di dalam form encode image terdapat beberapa field yang nantinya akan digunakan sebagai proses encoding atau penyisipan pesan ke dalam image, field-field tersebut antara lain:

a. Field key
   Field key berfungsi sebagai kata kunci untuk melakukan encoding atau penyisipan pesan .
b. Field Image dan Select Image
   Berfungsi untuk menampilkan detail image yang akan disisipi pesan. Untuk select image berfungsi memilih image yang ada didalam memory yang akan dilakukan proses encoding.
c. Field text to encode
   Field ini berfungsi sebagai tempat untuk menuliskan sebuah text atau pesan yang akan disisipkan kedalam image yang sudah ditentukan.
d. Tombol save
   Berfungsi untuk eksekusi atau memproses encoding image dari beberapa field yang sudah diisi sebelumnya serta menyimpannya sebagai stego image atau image yang sudah disisipi sebuah pesan.

Tampilan dari form encode image dapat dilihat pada gambar 8

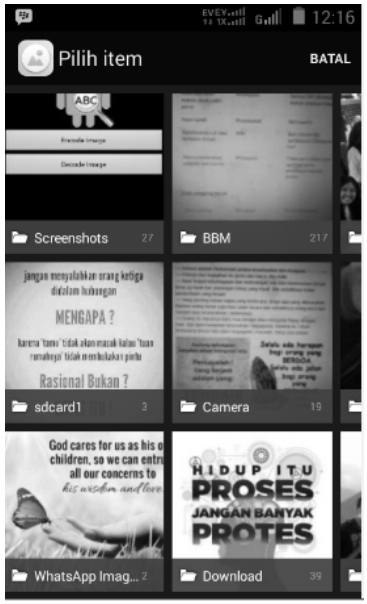


Gambar 8. Tampilan encode Image

p-ISSN: 1978-5232
e-ISSN: xxxx-xxxx

3. Form Decode Image

Di dalam decode image harus terlebih dahulu memilih image yang akan diekstraksi, sehingga ketika dipilih menu decode image maka akan muncul gallery yang berisi beberapa gambar atau image dalam mobile device. Stego image akan berada di dalam folder bernama sdcard1. Untuk lebih jelasnya dapat dilihat pada gambar 9



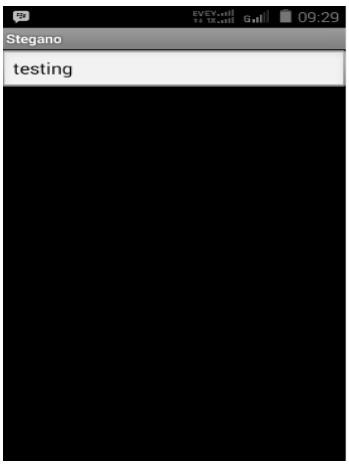
Gambar 9. Gallery Pada Mobile Device

Setelah memilih stego image yang berada di dalam folder sdcard1 maka akan muncul konfirmasi kata kunci yang digunakan. Kata kunci yang dimaksud disini sama persis ketika melakukan proses encode image. Lebih jelasnya dapat dilihat pada gambar 10

Gambar 10 Konfirmasi Kata Kunci

p-ISSN: 1978-5232
e-ISSN: xxxx-xxxx

Kata kunci harus sama seperti pada saat melakukan proses encode image, jika tidak maka stego image tidak dapat diekstraksi dan pesan yang disisipkan tidak akan bisa terbaca. Apabila kata kunci atau key sesuai maka stego image akan bisa diekstraksi dan pesan yang disisipkan akan bisa terbaca seperti pada gambar 11



Gambar 11 Pesan Yang Terbaca Setelah Ekstraksi

V. SIMPULAN DAN SARAN

A. Kesimpulan

Dari semua uraian yang sudah dibahas serta diterangkan maka dapat diambil kesimpulan sebagai berikut :

1. Pengamanan pesan teks ke dalam image dapat dilakukan dengan menggunakan teknik steganografi spread spectrum..
2. Steganografi dengan metode spread spectrum dapat diterapkan ke dalam image berformat JPG dan PNG.
3. Dalam proses pengujian yang dilakukan dengan beberapa image dengan ukuran yang berbeda-beda dapat disimpulkan bahwa jumlah maksimal karakter pesan yang dapat ditampung oleh sebuah image mengikuti ukuran image tersebut.
4. Berdasarkan proses pengujian yang dilakukan menggunakan 10 image dengan ukuran berbeda terdapat 1 dari 10 image tersebut yang mengalami perubahan bentuk image sehingga tingkat keberhasilan sistem mencapai 90%

2. Saran

Dari semua uraian yang sudah dibahas serta diterangkan maka berikut terdapat beberapa saran diantaranya :

1. Aplikasi Steganografi ini hanya berfungsi menyisipkan sebuah pesan ke dalam image dengan format JPG dan PNG saja, diharapkan aplikasi ini dapat menyisipkan sebuah pesan dengan tipe yang lain seperti audio (.mp3 .wav) gambar (bitmap, gif) atau file yang lainnya.

p-ISSN: 1978-5232
e-ISSN: xxxx-xxxx

2 Teknik yang digunakan adalah teknik steganografi spread spectrum maka tidak menutup kemungkinan untuk menggunakan teknik yang lebih baik di dalam kinerja dan kecepatan proses.
3. Dilihat dari hasil pengujian tingkat keberhasilan sistem masih sebesar 90 % dikarenakan terdapat 1 image dari 10 image yang diujikan mengalami perubahan bentuk setelah dilakukan penyisipan pesan. Diharapkan untuk penelitian-penelitian yang selanjutnya dapat menyempurnakan kekurangan ini.

VI. DAFTAR PUSTAKA

Ariyus. 2009. Keamanan Multimedia. Yogyakarta. Andi Publisher.

Kipper. 2004. Investigator's Guide to Steganography. Washington. Auerbach.

Miano, John. 1999. Compressed Image File Format JPEG, PNG, GIF, XBM, BMP. Addison Wesley Longman Inc.

Munir, Renaldi. 2004. Steganografi dan Watermarking. Bandung. Informatika.

Munir, Renaldi. 2006. Kriptografi, Steganografi dan Watermarking. Bandung. Informatika.

Safaat, Nazruddin. 2011. Pemrograman Aplikasi Mobile Smartphone dan Tablet PC berbasis Android.Bandung. Informatika.