Jurnal Teknologi Informatika dan Komputer Atma Luhur
Vol 1. September 2014
ISSN: 2406-7962

KRIPTOGRAFI DES DAN STEGANOGRAFI PADA DOKUMEN DAN CITRA DIGITAL MENGGUNAKAN METODE LSB

Burham Isnanto [1)], Ari Amir [2)]

[1)] Kepala Akreditasi, Dosen Teknik Informatika STMIK Atma Luhur Pangkalpinang
[2)] Kepala Laboratorium, Dosen Teknik Informatika STMIK Atma Luhur Pangkalpinang
Burham@Atmaluhur.ac.id [1)], Arie_a3@Atmaluhur.ac.id [2)]

ABSTRAK

Steganografi adalah metode untuk menyembunyikan informasi pada sebuah media, bisa berupa media gambar, suara ataupun video. Steganografi yang umum digunakan adalah penyembunyian informasi text pada media gambar. Namun metode yang sering digunakan masih cukup sederhana sehingga pihak ketiga masih bisa mendapatkan informasi yang disembunyikan. Metode yang digunakan dalam penelitian ini adalah menggunakan studi pemahaman sistem, studi literatur dan metode perancangan sistem menggunakan UML dengan pemrograman berorientasi objek. Aplikasi dibuat dengan menggunakan metode LSB dan menggunakan pemrograman VB6 sebagai implementasinya dengan tujuan yaitu membangun suatu aplikasi untuk mengamankan suatu data informasi dengan pemanfaatan teknik steganografi. Hasil penelitian berupa sebuah aplikasi steganografi yang dilengkapi dengan fungsi kriptografi DES pada saat penyisipan data yang berfungsi sebagai kode pembangkit dan mengenskripsi data agar keamanan suatu data dalam file lebih terjaga dan terlindungi dari pihak yang tidak berhak mengetahui data tersebut.

Kata kunci: Kriptografi, Steganografi,, LSB, Dokumen, Citra digital

ABSTRACT

Steganography is a method to hide information on a medium, can be a media images, sound or video. Steganography commonly used as the concealment of information text to the image. However, the method often used is quite simple so that third parties can still get hidden information. The method used in this research is system understanding study, literature and system design methods using UML and object-oriented programming. Applications created using LSB method and using VB6 programming as its implementation with the aim of making an application to secure an information data with the use of steganography techniques. The results of research in the form of a steganography application that comes with DES cryptographic function when the insertion of data that serves as a code generator and encrypt the data so that the security of the data in the file is preserved and protected from unauthorized parties know that data.

Keywords: Cryptography, Steganography,, LSB, documents, digital images

I PENDAHULUAN

Akibat penggunaan komputer di berbagai bidang penting yang membutuhkan tingkat privasi tinggi karena mengandung informasi rahasia sehingga menjadikan hampir semua kegiatan kita hasilnya akan disimpan dalam bentuk file digital Sebagian besar data yang tersimpan mencakup rahasia dari apa yang sudah kita kerjakan dan menyimpan informasi yang tidak semua orang berhak untuk mengetahuinya sehingga menyebabkan keamanan suatu data menjadi prioritas yang sangat penting. Kriptografi adalah metode pengolahan informasi dengan algoritma tertentu sehingga menjadi samar dan sulit dimengerti maknanya (Kurniawan, 2004). Untuk menghindari permasalahan tersebut maka lahirlah steganografi, yaitu metode menyembunyikan informasi pada sebuah media, bisa berupa media gambar, suara ataupun video (Barata, 2007). Pada penerapannya seringkali kriptografi dan steganografi diterapkan secara bersamaan untuk menjamin keamanan pesan rahasianya.

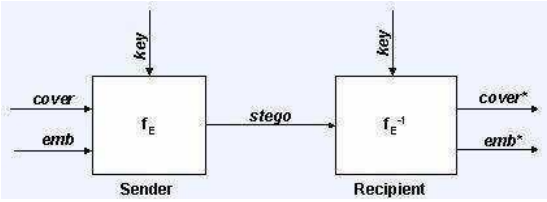
1.1 Tujuan

Tujuan dari tugas ini adalah membuat suatu program berbasis pengolahan citra yang dapat digunakan untuk melakukan steganografi data rahasia berupa gambar atau dokumen bereksteksi rft pada media penampung citra digital, serta untuk mengetahui kinerja program tersebut dan keandalannya terhadap berbagai operasi manipulasi data.

II TINJAUAN TEORI

2.1 Steganografi

Menurut Barata Simon (Barata, 2007) steganografi adalah ilmu dan seni dari menulis pesan rahasia di dalam sebuah media sedemikian rupa sehingga keberadaan pesan tidak disadari oleh indera manusia. (Abbas, 2010) Dengan menggunakan steganografi, sebuah pesan rahasia dapat disembunyikan di dalam sebuah informasi yang tidak mencurigakan dan mengirimkannya tanpa ada seorang pun yang mengetahui keberadaan pesan rahasia tersebut.



Gambar 1 Gambaran Umum Steganografi

2.2 Perbedaan Steganografi dan Kriptografi

Beberapa perbedaan kriptografi dan steganografi diungkapkan oleh Andi Kristanto (Kristanto, 2004) Steganografi dan kriptografi sangat erat kaitannya namun keduanya merupakan hal yang berbeda. Kriptografi mengacaukan pesan sehingga pesan tersebut tidak dapat dimengerti sedangkan steganografi menyembunyikan pesan sedemikian rupa sehingga tidak ada pihak yang mengetahui keberadaan pesan tersebut. Dalam beberapa situasi, mengirimkan sebuah pesan yang telah dienkripsi akan menimbulkan kecurigaan sedangkan sebuah pesan rahasia yang tidak tampak tentunya tidak akan dicurigai. Kedua teknik ini dapat digabungkan untuk menghasilkan perlindungan yang lebih baik terhadap sebuah pesan, yaitu ketika steganografi gagal dan pesan dapat terlihat, pesan tersebut masih tidak dapat diartikan karena telah dienkripsi menggunakan teknik – teknik kriptografi.

Namun, terdapat sebuah persamaan di antara kriptografi dan steganografi, (Katzenbeisser, 2000) yaitu kualitas kriptografi bergantung pada sebuah kunci, demikian pula dengan steganografi. Menemukan pesan rahasia baik yang disembunyikan melalui steganografi ataupun dienkripsi menggunakan kriptografi hanya mungkin terjadi jika mengetahui kunci yang tepat.

2.3 Metode Steganografi LSB

Menurut Yudhi Andrian (Andrian, 2013) Ketika sebuah *file* dibuat, biasanya terdapat beberapa *byte* di dalam *file* yang tidak benar – benar dibutuhkan atau tidak penting. Area dari *byte* tersebut dapat diganti dengan informasi yang akan disembunyikan dan tidak

akan merusak *file*. Hal ini memungkinkan seseorang untuk menyembunyikan informasi di dalam *file* dan yakin bahwa tidak ada seorang pun yang akan mengetahui perubahan di dalam *file*.

Metode LSB bekerja dengan baik pada *file* gambar yang memiliki resolusi tinggi dan memiliki warna yang beragam, dan pada *file* audio yang memiliki suara yang beragam dan memiliki bit *rate* yang tinggi. Metode LSB biasanya tidak mengubah ukuran *file*, namun hal ini juga tergantung padaukuran informasi yang akan disimpan ke dalam *file*.

Untuk memperkuat teknik penyembunyian data, bit – bit data rahasia tidak digunakan mengganti *byte* yang berurutan namun dipilih susunan *byte* yang acak. Misalnya jika terdapat 50 *byte* dan 6 bit data yang akan disembunyikan maka *byte* yang diganti bit LSB-nya dipilih secara acak, misalkan *byte* nomor 36, 5, 21, 10, 18, 49. (Bruice, 2007)

III METODE PENELITIAN

Penelitian dilakukan dengan mengikuti metodologi sebagai berikut :

3.1 Pemahaman Sistem dan Studi literature

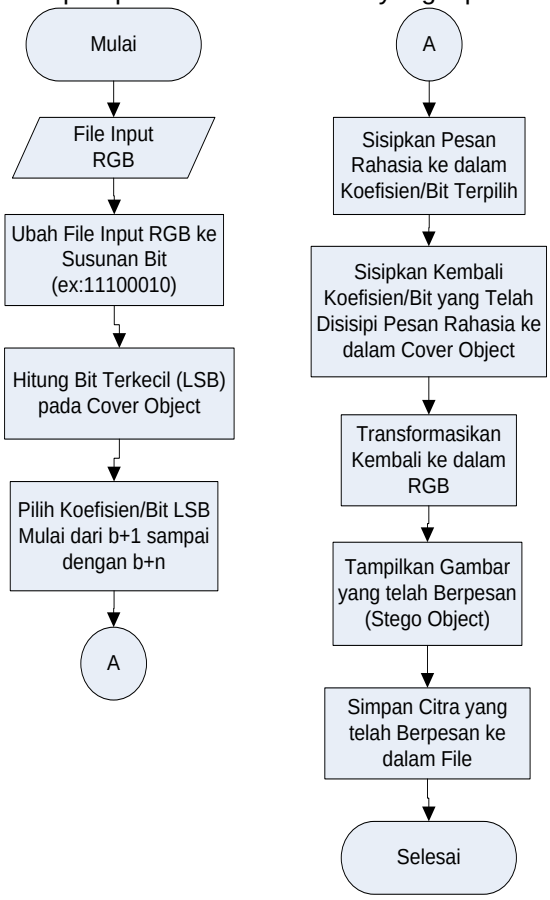
Pada tahap ini akan dipelajari sejumlah literatur mengenai konsep dan teknologi yang akan digunakan untuk perancangan sistem. Mencari dan mempelajari bahan literatur mengenai konsep dasar *Steganography*.

3.2 Analisis dan perancangan sistem

Tahap ini meliputi perancangan sistem dengan menggunakan studi literatur dan mempelajari konsep teknologi dari *software* yang ada. Tahap ini merupakan tahap yang paling penting dimana bentuk awal aplikasi yang akan diimplementasikan didefinisikan. Pada tahapan ini dilakukan desain model data, desain proses-proses yang ada, dan desain antar muka aplikasi.

Program dibuat menjadi 2 bagian utama, yaitu bagian *Encoder* dan bagian *Decoder*. Bagian *Encoder* digunakan untuk melakukan proses penyembunyian atau penyisipan data rahasia ke dalam data penampung, sedangkan bagian *Decoder* digunakan untuk melakukan proses pengambilan atau pengungkapan data rahasia yang tersembunyi atau tersisip di dalam data penampung.

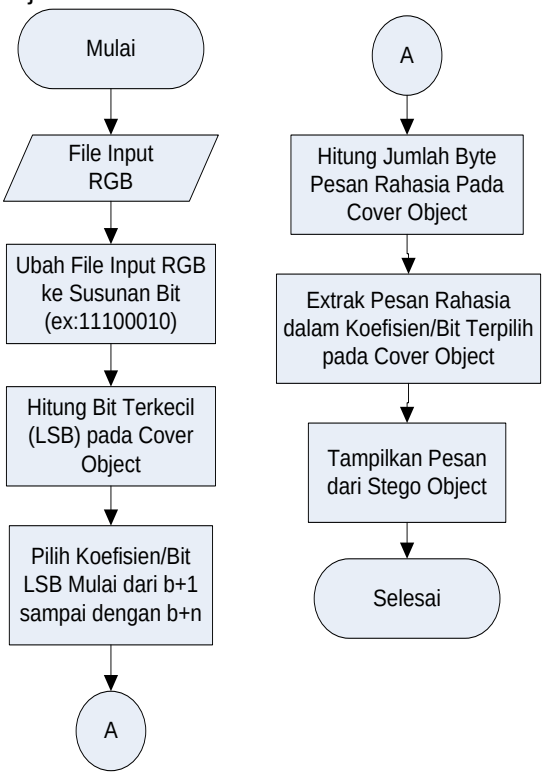
Pada proses penyisipan pesan (embedding message) dimulai dengan memilih gambar yang akan dijadikan cover object untuk menyisipkan dan menyembunyikan pesan ke dalam gambar kemudian menentukan key file yang akan digunakan sebagai password dalam proses extract dan menuliskan isi pesan text yang akan disisipkan kedalam gambar. Sedangkan pada proses pendeteksian pesan (extraction message) dimulai dengan memilih file gambar atau covert object yang akan akan di extract dan memasukan key file, yang hasil y ekstraksi pesannya dapat disimpan pada satu file tertentu yang dipilih.



Gambar 2. Diagram Alir Proses Enkripsi

Selanjutnya adalah setelah memilih koefisien atau bit-bit terpilih maka proses berikutnya adalah menyisipkan pesan rahasia ke dalamnya koefisien atau bit-bit tersebut sehingga akan dihasilkan koefisien atau bit-bit

yang baru yang telah mengandung pesan, dan menyisipkannya kembali ke dalam cover-object, yang kemudian koefisien tersebut selanjutnya akan di transformasikan kembali kedalam nilai RGB yang baru lalu ditampilkan dalam gambar baru yang telah disisipkan pesan atau stego-object kemudian menyimpan citra yang telah berpesan ke dalam cover-object.



Gambar 3. Diagram Alir Proses Dekripsi

IV PEMBAHASAN

4.1 Desain Antarmuka

Pada saat pertama kali menjalankan aplikasi ini, user diminta untuk memasukkan dulu pasword untuk menjalankan aplikasinya.

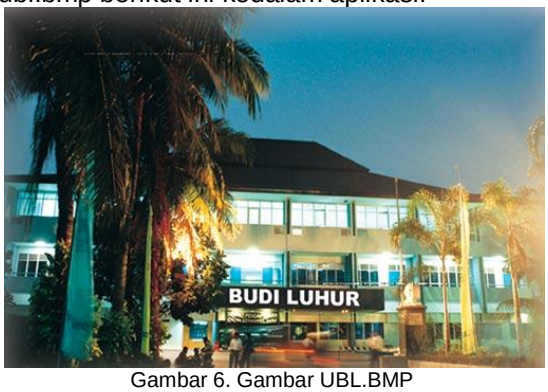
Gambar 4. Gambar Antarmuka Pasword Aplikasi

Hal ini dikarenakan agar hanya orang yang berhak memakai aplikasi ini saja yang boleh menggunakannya.

Gambar 5. Antarmuka Program Steganografi

4.2. Eksekusi Program Enkripsi

Sebelum kita memasukkan pesan rahasia yang akan dikirimkan, terlebih dahulu kita memasukkan gambar yang akan dipakai sebagai inang (induk) dari pesan rahasianya. File gambar bisa berupa format bmp, jpg atau gif.
Misalnya disini kami akan memakai gambar ubl.bmp berikut ini kedalam aplikasi:

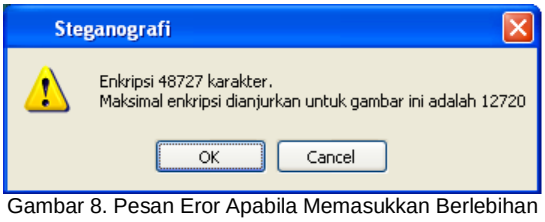


Gambar 6. Gambar UBL.BMP

Setelah dimasukkan kedalam aplikasi maka akan menjadi :

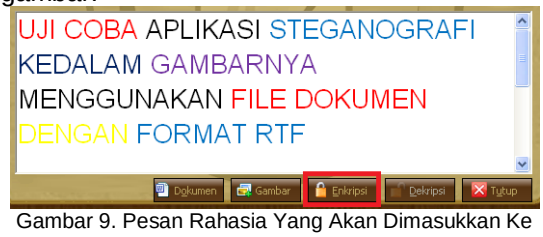
Gambar 7. Gambar Steganografi Setelah Dimasukkan Gambar

Langkah selanjutnya adalah memasukkan file dokumen atau file gambar yang merupakan pesan rahasia yang akan diberikan. Ukuran gambar rahasia harus lebih kecil dari gambar induk nya. Demikian juga pesan rahasia dokumen yang dimasukkan bisa berupa grafik, tabel, ataupun teks berwarna yang apabila dijumlahkan jumlah karakternya tidak melebihi jumlah karakter dari gambar induk nya. Apabila jumlah karakter dari pesan rahasia yang dimasukkan kedalam gambar ternyata lebih besar dari kapasitas gambar induknya maka akan muncul pesan sebagai berikut:



Gambar 8. Pesan Eror Apabila Memasukkan Berlebihan Karakter Rahasia

Apabila ukuran dari pesan rahasia yang kita masukkan memenuhi besaran dari gambar induknya maka akan langsung dilakukan proses penyisipan pesan rahasia ke dalam gambar.



Gambar 9. Pesan Rahasia Yang Akan Dimasukkan Ke Gambar

Langkah selanjutnya adalah pencet tombol enkripsi makan akan dilakukan proses penyisipan file dari pesan rahasia nya kedalam gambar seperti berikut ini:

Gambar 10. Proses Penyisipan Pesan Rahasia Ke Gambar

Proses penyisipan pesan rahasia ke dalam gambar ditandai dengan adanya penyisipan titi titik kecil ke dalam gambar yang disebelah kanan. Semua karakter pesan rahasia akan disisipkan secara acak. Proses persentase penyisipan bisa dilihat dari gambar loading nya. Pada saat proses loading sudah mencapai 100% akan ditampilkan pesan bahwa proses penyisipan sudah selesai.

Setelah proses penyisipan pesan rahasia ke gambarnya selesai maka anda bisa pencet OK agar proses pengembalian gambar semula bisa terlihat.

Gambar 11 Proses Pengembalian Ke Gambar Asli

Gambar 12. Proses Pengembalian Gambar Asli Selesai

Langkah selanjutnya adalah aplikasi steganografi akan menyimpan file baru yang sudah disisipi dengan pesan rahasia kedalam sebuah gambar dengan nama file sesuai nama

file gambar awal dengan akhiran _pesan.bmp. Dalam contoh ini file gambar tersebut menjadi UBL_PESAN.BMP

Gambar 13. Tampilan Gambar Awal Dan Akhir Setelah Penyisipan

Dari tampilan gambar terlihat bahwa hampir tidak bisa dilihat perbedaan dari gambar aslinya dengan gambar setelah dilakukan penyisipan pesan rahasia. Hal tersebut sangat menguntungkan bagi kita sebagai pengguna aplikasi karena hal tersebut otomatis tidak akan menimbulkan kecurigaan bagi pihak ketiga yang tidak berhak mengetahui isi pesan rahasia tersebut.

4.3. Eksekusi Program Deskripsi

Pada proses decode ini kita akan melihat proses penguraian dari gambar yang sudah berisi pesan rahasia agak kita bisa mengetahui pesan rahasia apa yang disisipkan ke gambar.
Langkah pertama adalah kita ambil dulu gambar yang sudah ada pesan rahasianya yaitu UBL_PESAN.BMP

Gambar 14. UBL_PESAN.BMP

Sehingga tampilan awal dari proses deskripsi adalah sebagai berikut:

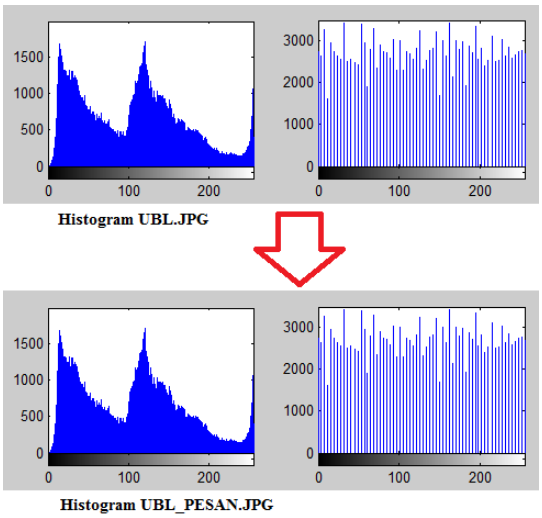
Gambar 15. Gambar Awal Proses Deskripsi

Langkah selanjutnya adalah pencet deskripsi sehingga nantinya aplikasi akan langsung melakukan pembacaan dari gambar yang sudah berisi pesan rahasia. Hasil pembacaan akan ditampilkan didalam kotak yang ada ditengah antarmuka. Untuk proses deskripsi ini memang tidak memerlukan memasukkan pasowrd hal itu dikarenakan pada saat pembuatan aplikasi ini sudah dipakai algoritma yang tidak memungkinkan bagi orang lain untuk bisa membuka pesan rahasianya apabila menggunakan aplikasi yang laen selain aplikasi yang sudah kami buat. Tampilan akhirnya setelah dilakukan proses deskripsi adalah sebagai berikut:

Gambar 16 Gambar Akhir Proses Deskripsi

4.4 Analisa Akhir

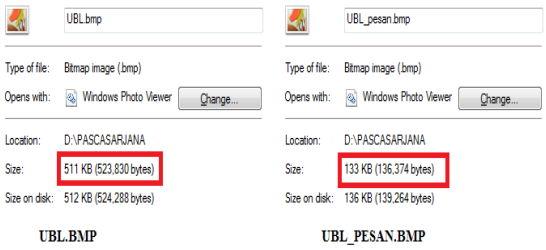
Analisa yang pertama kita lakukan dengan cara melihat histogram dari gambar sebelum dan sesudah penyisipan gambar. Proses mengubah gambar menjadi histogram dilakukan dengan menggunakan program Matlab dengan script:



Gambar 17 Perbandingan Histogram

Dari gambar histogram kedua gambar diatas terlihat bahwa hampir tidak ada perbedaan antara histogram gambar awal UBL.JPG dengan histogram dari gambar yang sudah disisipi dengan pesan rahasia UBL_PESAN.JPG.
Hal itu lebih menguntungkan bagi kita karena untuk kebanyakan steganografi yang lain akan terlihat perbedaan yang sangat mencolok dari histogram gambar sebelum dan sesudah penyisipan pesan. Dengan perbedaan yang sangat tidak terlihat ini lebih membuat kesulitan bagi pihak ketiga untuk bisa mengetahui bahwa ada pesan rahasia yang tersembunyi didalam gambar tersebut.

Analisa yang kedua dilakukan dengan melihat ukuran dari file sebelum dan sesudah dilakukan proses penyisipan pesan sebagai berikut:



Gambar 18 Perbandingan Ukuran File

Dari gambar diatas terlihat bahwa ukuran gambar sebelum dan sesudah dilakukan penyisipan mengalami perubahan. Bentuk ukuran dari file yang sudah dilakukan penyisipan menjadi lebih kecil daripada file gambar aslinya.

V KESIMPULAN

Berdasarkan hasil analisa diketahui bahwa aplikasi steganografi yang telah dihasilkan dari implementasi algoritma LSB (*Least Significant Bit*) dapat digunakan dengan sangat baik untuk menyembunyikan pesan rahasia berupa dokumen maupun gambar ke dalam sebuah gambar sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut karena perbedaan dari gambar asli dan gambar yang disisipi pesan rahasia sangat tipis. Pada proses ekstraksi, pesan atau informasi yang disisispkan pada file citra uji dalam aplikasi steganografi ini, dapat diperoleh kembali secara utuh atau dengan kata lain pesan yang disisipkan sebelum proses penyisipan dan setelah proses ekstraksi sama tanpa ada perubahan.

Hasil pengujian dengan histogram menunjukkan bahwa gambar asli dan gambar sesudah ada penyisipan pesan tidak mengalami perubahan yang signifikan. Dari segi warna pembentuknya benar benar tidak terlihat adanya perbedaan. Dengan demikian pesan yang disisipkan kedalam gambar tidak akan menimbulkan kecurigaaan dan menjaga keamanan pesan yang disisipkan dalam file citra digital tersebut. Bisa dkatakan bahwa kualitas gambar sebelum dan sesudah dilakukan penyisipan tidak mengalami perubahan.

Pada pengujian perbandingan ukuran gambar sebelum dan sesudah adanya penyisipan menunjukkan bahwa apabila diantara banyak gambar asli, disisipkan pesan rahasia dengan ukuran yang sama akan menghasilkan gambar dengan ukuran yang sama pula. Banyaknya karakter pesan rahasia yang akan disisipkan pada gambar sangat dipengaruhi oleh besarnya file gambar induk nya. Semakin besar ukuran gambar induk nya maka semakin banyak pula pesan rahasia yang bisa dimasukkan ke dalam gambar tersebut.

VI DAFTAR PUSTAKA

Abbas, Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt (2010), Digital image steganography: Survey and analysis of current methods Signal

Andrian, Yudhi. (2013), Modifikasi Metode Least Significant Bit (LSB) Pada Steganografi Citra Digital, UMI: Medan

Barata, Simon. (2007), Studi Steganografi Dalam File MP3, Makalah Prodi TI, Dep TI: ITB

Bruice, Schneier. (2007), Applied Cryptography Protocols, Algorithm and Source Code in C. Second edition. Wiley India edition.

Katzenbeisser, F.A.P. Petitcolas. (2000), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA

Kristanto, Andi. (2004). Memahami Model Enkripsi Dan Keamanan Data" Andi Offset: Yogyakarta

Kurniawan, Yusuf. (2004). Kriptografi: Keamanan Internet dan Jaringan Komunikasi. Penerbit Informatika Bandung: Yogyakarta