KAJIAN DAN PENERAPAN PENGGABUNGAN STEGANOGRAPI DAN KRYPTOGRAPI PADA GAMBAR DAN TEKS

PUJI ASTUTI
SAPUTRA DWI NURCAHYA
Program studi Teknik Informatika, Fakultas Teknik, Matematika, dan IPA
Universitas Indraprasta

Abstrak. Keamanan data dalam proses penukaran data informasi dalam sebuah jaringan komunikasi sangat penting untuk diperhatikan seiring dengan kerahasian data. Steganografi merupakan teknik dan seni menyembunyikan informasi dan data digital dibalik informasi digital lain, sehingga informasi digital yang sesungguhnya tidak kelihatan 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. Cryptography adalah sebuah kumpulan teknik yang digunakan untuk mengubah informasi/pesan (plaintext) kedalam sebuah teks rahasia (ciphertext) yang kemudian bisa diubah kembali ke format semula. Pada saat membuat steganografi text pada media gambar menjadi lebih kuat dan aman. Implementasi yang digunakan adalah mengenkripsi pesan text terlebih dahulu dengan sebuah kata kunci menggunakan algoritma kriptografi Informasi yang terenkripsi tersebut kemudian dimasukkan pada pixel yang ditentukan berdasarkan tingkat kerapatan data.

Kata kunci: keamanan, steganografi, kriptografi, teks dan gambar

Abstract. Data security in the data exchange process information in a communication network is very important to note as data.Steganografi confidentiality and art techniques and digital data information hiding behind other digital information, so that information does not seem real digital steganography is commonly used text information hiding the media image. However, the method often used is simple enough so that third parties can still get the information hidden. Cryptography is a collection of techniques that are used to modify the information/message (plaintext) into a secret text (ciphertext) which can then be converted back to its original format. At the time of making the text steganography media image becomes stronger and safer. Implementation that is used to encrypt text messages in advance with a keyword using cryptographic algorithms that encrypted information is then entered on the pixel density is determined by data.

Keywords: security, steganography, cryptography, text and images

PENDAHULUAN

Steganografi merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni menyembunyikan sesuatu informasi. Steganografi dapat digolongkan sebagai salah satu bagian dari ilmu komunikasi. Kata steganografi berasal dari bahasa Yunani yang berarti "tulisan tersembunyi"[5]. Pada era informasi digital, steganografi merupakan teknik dan seni menyembunyikan informasi dan data digital dibalik informasi digital lain, sehingga informasi digital yang sesungguhnya tidak kelihatan.

Secara teori, semua file umum yang ada di dalam komputer dapat digunakan sebagai media, seperti file gambar berformat JPG, GIF, BMP, atau di dalam musik MP3, atau bahkan di dalam sebuah film dengan format WAV atau AVI. Semua dapat dijadikan tempat bersembunyi, asalkan file tersebut memiliki bit-bit data redundan yang dapat

dimodifikasi. Setelah dimodifikasi file media tersebut tidak akan banyak terganggu fungsinya dan kualitasnya tidak akan jauh berbeda dengan aslinya.

Data yang dikirim hasil enkripsi disembunyikan dalam *cover carrier* agar dapat meningkatkan keamanan pada saat transmisi. Banyak metoda steganografi yang melekatkan sejumlah besar informasi rahasia di dalam *pixel* pada *cover image.* Karena perasaan manusia yang tidak sempurna dalam hal visualisasi, keberadaan informasi rahasia yang ditempelkan tersebut dapat saja tidak terlihat. Tetapi informasi rahasia tersebut mungkin saja ditemukan, jika belum ditempatkan secara baik.

"Crypto" berarti "secret" (rahasia) dan "graphy" berarti "writing" (tulisan). Cryptography adalah sebuah kumpulan teknik yang digunakan untuk mengubah informasi/pesan (plaintext) kedalam sebuah teks rahasia (ciphertext) yang kemudian bisa diubah kembali ke format semula. Pelaku atau praktisi kriptografi disebut cryptographers. Sebuah algoritma kriptografik (cryptographic algorithm), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi.

Bagaimana mengkaji dan penggabungan steganografy dan cryptograpy pada gambar dan teks ?

TINJAUAN PUSTAKA

Kriptografi

Kriptografi (cryptography) berasal dari bahasa Yunani: "cryptos" artinya "secret" (rahasia), sedangkan "graphein" artinya "writing" (tulisan). Jadi, kriptografi berarti "secret writing" (tulisan rahasia). Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat di mengerti lagi maknanya[1].

Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekedar privacy, tetapi juga untuk tujuan data integrity, authentication, dan non-repudiation (Munir Rinaldi, 2006: 2).

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana[3].

Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi antara lain:

1. Kriptografi dapat memenuhi kebutuhan umum suatu transaksi:
   a. Kerahasiaan (*confidentiality*) dijamin dengan melakukan enkripsi (penyandian).
   b. Keutuhan (*integrity*) atas data-data pembayaran dilakukan dengan fungsi *hash* satu arah.
   c. Jaminan atas identitas dan keabsahan (*authenticity*) pihak-pihak yang melakukan transaksi dilakukan dengan menggunakan *password* atau sertifikat digital. Sedangkan keotentikan data transaksi dapat dilakukan dengan tanda tangan digital.
   d. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (*non-repudiation*) dengan memanfaatkan tanda tangan digital dan sertifikat digital.

2. Karakteristik cryptosytem yang baik sebagai berikut:
   a. Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.

b. Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.
c. Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
d. Cryptosystem yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya

Steganografi

Pengertian Steganografi

Steganografi berasal dari bahasa Yunani yang artinya untuk tulisan yang disembunyikan. Steganografi merupakan prosespenyembunyian data rahasia ke dalam data lainnya. Data yang menjadi media erupakan data yang umum dikirimkan, bisa berupa teks, gambar, audio, maupun video. Data yang dijadikan media untuk menyembunyikan pesan disebut *cover medium*. *Cover medium* yang telah tambahkan pesan rahasia dengan steganografi disebut stego data. Pada keadaan yang ideal, siapapun yang melakukan *scan* terhadap data tersebut tidak akan mengetahui bahwa data tersebut mengandung data lain yang rahasia sehingga pengambilan data hanya dapat dilakukan oleh penerima yang berhak.

Penerapan Steganografi

Steganografi modern bertujuan untuk mempertahankan keberadaan pesan rahasia tidak terdeteksi, tetapi sistem stenografi seringkali meninggalkan jejak yang bisa dideteksi pada *cover medium*. Karena itu digunakan tambahan informasi rahasia pada steganografi modern yang disebut sebagai kunci. . *Skema Steganografi* Steganografi modern diharapkan hanya bisa terdeteksi apabila kunci rahasia tersebut diketahui. Dalam steganografi, untuk mempertahankan agar tetap tidak terdeteksi, *cover medium* asli yang belum dilapisi pesan rahasia harus dijaga kerahasiaannya. Apabila *cover medium* yang asli pernah diperlihatkan kepada orang lain, *cover medium* yang asli tersebut bisa dibandingkan dengan *cover medium* yang telah menjadi *stego data* dan perbedaannya akan terlihat. Pada gambar *cover image* yang telah dilapisi data rahasia akan berubah warnanya walaupun tidak selalu terlihat jelas. Pada steganografi digital modern, data dimasukkan ke dalam data redundan (data yang tersedia tetapi seringkali tidak diperlukan), seperti *field* pada protocol komunikasi, gambar grafik, dan sebagainya.

File Gambar

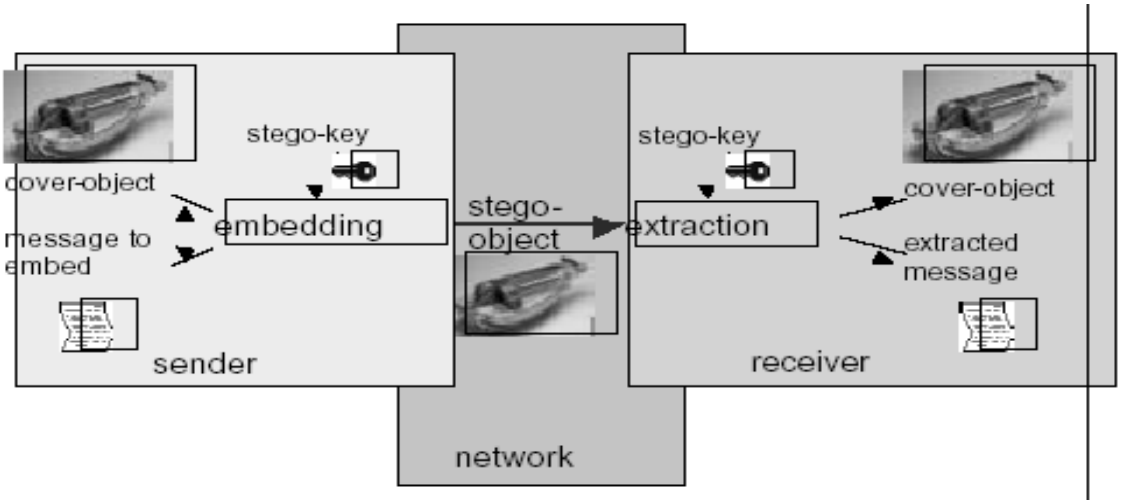
Pada komputer, suatu gambar adalah suatu array dari bilangan yang merepresentasikan intensitas terang pada point yang bervariasi (pixel). Pixel ini menghasilkan *raster data* gambar. Suatu ukuran gambar yang umum adalah 640 x 480 pixel dan 256 warna (atau 8 bit per pixel). Suatu gambar akan berisi kira-kira 300 kilobit data.

Gambar digital disimpan juga secara khusus di dalam file 24-bit atau 8-bit. Gambar 24-bit menyediakan lebih banyak ruang untuk menyembunyikan informasi; bagaimanapun, itu dapat sungguh besar (dengan perkecualian gambar JPEG). Semua variasi warna untuk pixel yang diperoleh dari tiga warna dasar: merah, hijau dan biru. Setiap warna dasar direpresentasikan dengan 1 byte; gambar 24-bit menggunakan 3 byte per pixel untuk merepresentasikan suatu nilai warna. 3 byte ini dapat direpresentasikan sebagai nilai hexadecimal, decimal, dan biner.

METODE

Metode penelitian yang digunakan untuk menyelesaikan tugas ini ada beberapa hal, diantaranya:

1. Studi pustaka meliputi:
   a. Pencarian berbagai referensi yang ada diperpustakaan atau di media maya (internet) yang ada sangkut pautnya dengan tugas ini.
   b. Pendalami materi tentang *steganography*, teknik penyembunyian dan pengungkapan data serta semua hal yang berhubungan dengan tugas ini.
2. Merancang sistem aplikasi: merupakan tahap pembuatan aplikasi *steganography*
3. Pengujian sistem aplikasi: merupakan tahap pengujian aplikasi yang telah dibuat berjalan sesuai dengan yang diinginkan atau tidak.
4. Penyusunan laporan:
   Membuat laporan terhadap keseluruhan kegiatan pembuatan tugas yang menjelaskan secara detail tentang tahaptahap penyususnan tugas sini.



Gambar 1. Proses dalam steganografi

PEMBAHASAN

Steganografi yang dibahas di sini adalah penyembunyian data di dalam citra digital. Meskipun demikian, penyembunyian data dapat juga dilakukan pada wadah berupa suara digital, teks, ataupun video. Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah:

a. Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.
b. Data yang disembunyikan harus mampu bertahan terhadap manipulasi yang dilakukan pada citra penampung. Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak.
c. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*).

Teknik Penyembunyian Data

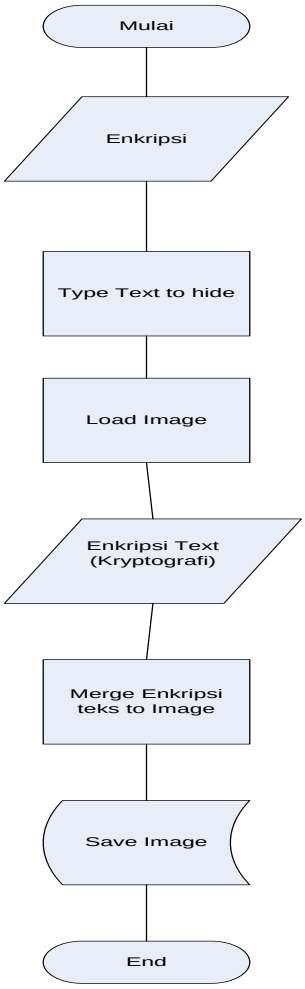
Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia. Salah satu metode penyembunyian data dengan menggunakan Steganografi.

Teknik Pengungkapan Data

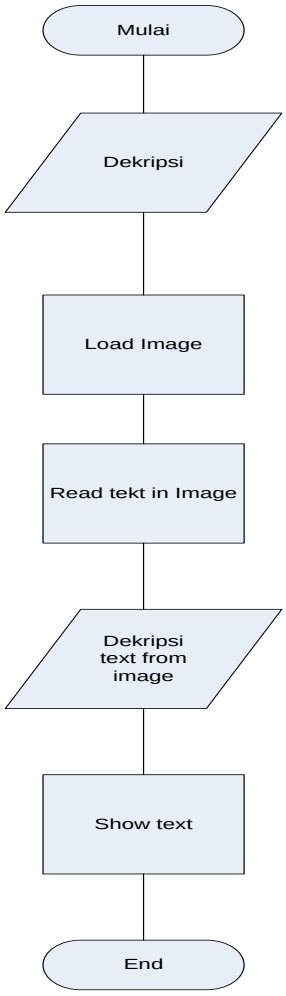
Data yang disembunyikan di dalam citra dapat dibaca kembali dengan cara pengungkapan (*reveal* atau *extraction*). Posisi *byte* yang menyimpan bit data dapat diketahui dari bilangan acak yang dibangkitkan oleh *PRNG*. Karena algoritma kriptografi yang digunakan menggunakan kunci pada proses enkripsi, maka kunci yang sama digunakan untuk membangkitkan bilangan acak. Bilangan acak yang dihasilkan sama dengan bilangan acak yang dipakai pada waktu penyembunyian data. Dengan demikian, bit-bit data rahasia yang bertaburan di dalam citra dapat dikumpulkan kembali.

Flow chart

Penggambaran sistem dituangkan melalui flow chart yang menggambarkan prosedur, adapun flow chart tersebut dapat di lihat pada gambar 2. dan gambar 3. di bawah ini:



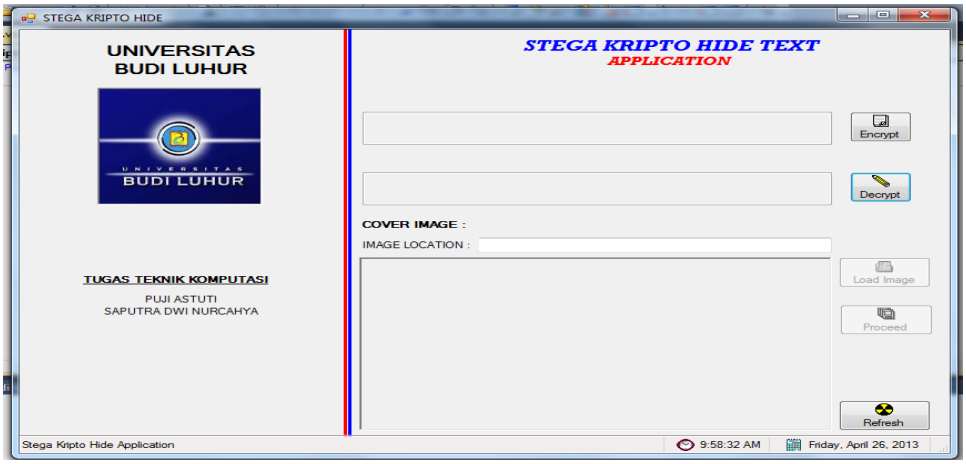
Gambar 2. Proses Enkripsi



Gambar 3. Proses Dekripsi

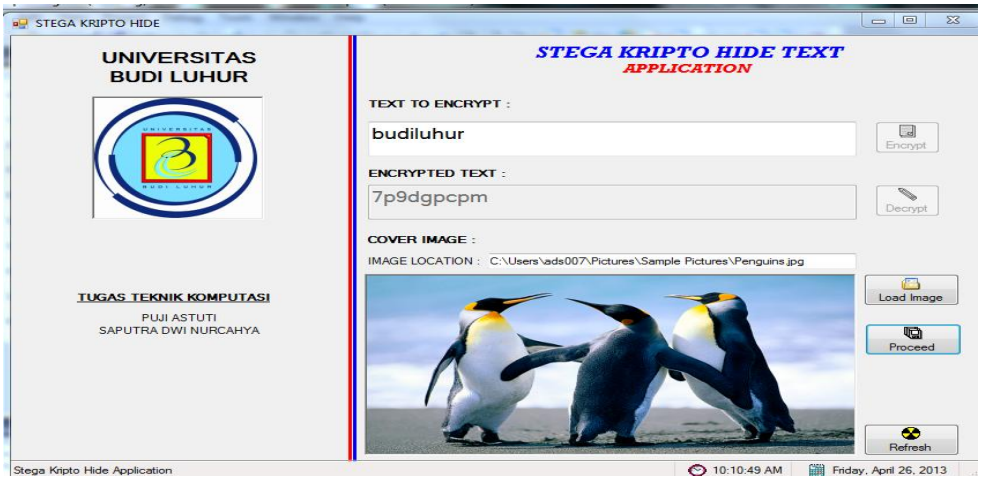
Penyisipan Pesan ke dalam *Image*

Dengan menggunakan bahasa pemrograman visual basic, fungsi yang akan digunakan untuk *encoding* atau menyisipkan pesan ke dalam *image*:



Gambar 4. Tampilan Awal Program

Pada Gambar 4. terdapat tombol-tombol seperti Encrypt untuk menulis pesan yang akan disampaikan, tombol Descrypt menampilkan hasil yang sudah di proses, tombol load image untuk mengambil gambar yang berguna untuk hide pesan yang dikirim, tombol proceed berguna untuk memproses teks yang encrypt dan tombol refresh.

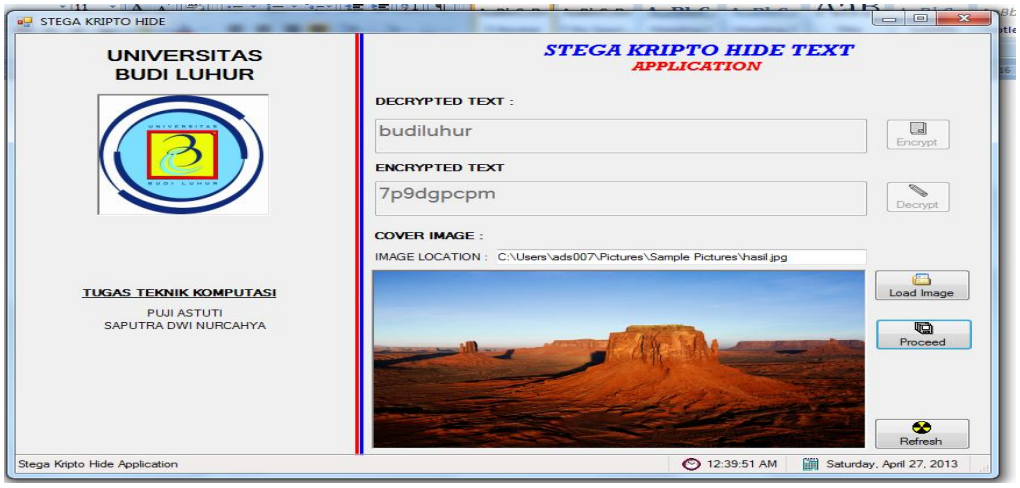


Gambar 5. Proses Kerja

Pada Gambar 5. menerangkan proses kerja, dimana langkah awal sebagai berikut: pertama clik tombol Encrypt dan tulis teks di kolom teks to Encrypt setelah itu clik tombol load image, untuk memilih gambar yang kita inginkan fungsinya untuk hide teks yang akan kita kirim. Setelah gambar kita pilih kemudian clik tombol proses, kemudian akan ada teks di kolom Encrypt to teks dan simpan gambar yang kita pilih.

Gambar 6. Melihat hasil gambar

Pada Gambar 6. menjelaskan bagaimana melihat teks yang telah di Encrypt, langkah pertama clik tombol load image dan pilih gambar yang sudah di Encrypt kemudian tekan tombol proses dan akam tampil seperti gambar 7. di bawah ini



Gambar 7. Hasil Akhir

PENUTUP

Kesimpulan yang bisa diambil oleh pembahasan diatas antara lain:

a. Dengan menggunakan steganografi menggunakan sebuah kombinasi dari bidang jenis teknik untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung berkas. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya.
b. Keamanan data sangat penting dalam proses yang dilakukan untuk mengamankan sebuah pesan (plaintext) menjadi pesan yang tersembunyi (ciphertext) sehingga tidak dapat dibaca oleh orang yang tidak berhak.

DAFTAR PUSTAKA

Andreas Westfeld, Andreas Pfitzmann. **Attacks on Steganographic Systems.** Dresden University of Technology, Department of Computer Science, D-01062 Dresden, Germany

Birgit Pfitzmann. 1996. **Information Hiding Terminology.** in Ross Anderson (Ed.): Information Hiding. First International Workshop, LNCS 1174, Springer-Verlag Berlin Heidelberg. pp. 347–350

FAP Petitcolas, RJ Anderson, MG Kuhn. **Attacks on Copyright Marking Systems.** http://www.cl.cam.ac.uk/~fapp2/papers

M. R. Nelson. **LZW Data Compression. Dr. Dobb's Journal.** Oktober 1989.

Neil F. Johnson, Sushil Jajodia. 1998. **Steganalysis of Images Created Using Current Steganography Software**, in David Aucsmith (Ed.): Information Hiding, LNCS 1525, Springer-Verlag Berlin Heidelberg. pp. 32–47

Robert Tinsley. 1996. **Steganography and JPEG Compression.** Final Year Project Report, University of Warwick.

http://mardian87.150m.com/STEGANOGRAFI.html

http://jre.elektro.unsyiah.ac.id/wp-content/uploads/2012/03/8_1_2_8_13.pdf

http://digilib.its.ac.id/public/ITS-Undergraduate-16398-5107100055-Paper.pdf

http://pustaka.unpad.ac.id/wpcontent/uploads/2009/06/kriptografi_dan_stenografi_menggunakan_algoritma_vigenere_dan_tea.pdf