**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI**

**INSTITUT TEKNLOGI SEPULUH NOPEMBER**

**USULAN TUGAS AKHIR**

# IDENTITAS PENGUSUL

**NAMA : Ubaldias Arinarindra**

**NRP : 5110100022**

**DOSEN WALI : Dr.Nanik Suciati,S.Kom.,M.Kom.**

**DOSEN PEMBIMBING : 1. Tohari Ahmad, S.Kom., MIT., Ph.D.  
 2. Hudan Studiawan, S.Kom., M.Kom.**

# JUDUL TUGAS AKHIR

“Pengembangan Teknik Steganografi Berbasis Teks Terkompresi pada *Email*”

# LATAR BELAKANG

Sesuai dengan perkembangan jaman kerahasiaan data menjadi salah satu aspek penting dalam komunikasi antara dua belah pihak atau lebih. Banyak cara untuk merahasiakan data yang akan kita kirim, bisa dengan memberi *password*, kriptografi, memecah data menjadi beberapa bagian maupun dengan menyisipkan data pada sebuah wadah atau disebut steganografi. Salah satu cara yang mulai banyak dikembangkan untuk mengamankan data adalah dengan menggunakan steganografi atau penyembunyian data. Saat ini dalam dunia digital, teknik steganografi banyak digunakan untuk menyembunyikan informasi rahasia dengan berbagai maksud. Salah satu tujuan steganografi adalah untuk mengirimkan pesan rahasia melalui jaringan tanpa menimbulkan kecurigaan. Di samping itu steganografi juga dapat digunakan untuk melakukan autentikasi terhadap suatu hasil karya sebagaimana pemanfaatan *watermarking*.

Steganografi memerlukan setidaknya dua properti. Properti pertama adalah wadah penampung (*cover*) dan yang kedua adalah data atau pesan yang disembunyikan. Untuk meningkatkan tingkat keamanan data yang disimpan, dapat dilakukan dengan menambahkan *property* kunci (*key*) rahasia. Berkas hasil dari proses steganografi sering disebut berkas stego atau stego objek.

Saat ini surat elektronik merupakan salah satu media penyampaian pesan yang sangat sering digunakan oleh masyarakat umum. Pentingnya menjaga rahasia yang akan dikirim melalui surat elektronik sudah layaknya kita pikirkan. Oleh sebab itu steganografi menjadi salah satu solusi dalam penyelesaian kerahasiaan data pada surat elektronik. Pada surat elektronik pun sering terdapat banyak orang-orang yang promosi suatu barang melalui *email* yang tidak kita inginkan. Pesan-pesan tersebut sering disebut *spam.* Oleh sebab itu teknik steganografi pada surat elektronik yang mampu menyembunyikan pesan dalam bentuk *spam* layak untuk dikembangkan dan dipelajari karena bilamana terdapat orang yang berniat jahat untuk membajak atau mengintai pesan yang kita terima, maka mereka hanya akan melihat pesan tersebut sebagai *spam*.

# RUMUSAN MASALAH

Rumusan masalah yang diangkat dalam Tugas Akhir ini adalah:

1. Bagaimana cara menyisipkan teks dalam *stego cover*?
2. Bagaimana cara menyamarkan *stego cover* sehingga tidak mudah dikenali oleh pihak-pihak lain yang tidak memiliki kepentingan pada proses komunikasi?
3. Bagaimana cara membangkitkan *stego key* sesuai dengan masukan teks yang akan disisipkan.

# BATASAN MASALAH

Beberapa batasan masalah yang menjadi batas pada Tugas Akhir ini adalah:

1. Aplikasi yang akan dibangun tidak akan mengurusi mekanisme pengiriman surat elektronik.
2. Bahasa pemrograman yang akan digunakan untuk membangun aplikasi adalah Java.
3. Kompresi pada teks yang akan disisipkan menggunakan metode Huffman.

# TUJUAN PEMBUATAN TUGAS AKHIR

Tujuan dari pembuatan Tugas Akhir ini adalah:

1. Pengembangan teknik steganografi berbasis teks pada media surat elektronik.
2. Memanfaatkan sisi negatif dari *spam* yang sering dianggap sebagai sampah surat elektronik sebagai *stego cover.*
3. Mengurangi resiko terjadinya penyadapan pada media surat elektronik.

# MANFAAT TUGAS AKHIR

Hasil dari Tugas Akhir ini diharapkan dapat memberi manfaat pada bidang teknologi informasi dalam bidang keamanan data dengan cara mengembangkan sebuah metode steganografi baru pada media surat elektronik dengan cara menyamarkan *stego cover* sebagai *spam* yang sering diabaikan pada umumnya karena dianggap sebagai sampah surat elektronik.

# TINJAUAN PUSTAKA

Pada bagian ini akan dijelaskan beberapa tinjauan pustaka yang akan dipakai dalam Tugas Akhir ini. Tinjauan pustaka dapat berasal dari buku, artikel ilmiah (paper), internet, dan sebagainya.

## 8.1. Steganografi

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. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Kata "steganografi" berasal dari bahasa Yunani *steganos*, yang artinya “tersembunyi atau terselubung”, dan *graphein*, “menulis”.

Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Steganografi dapat diklasifikasikan ke dalam kategori berikut: substitusi sinonim, transformasi sintaksis, kesalahan penulisan, dan transformasi semantik. Kelebihan steganografi jika dibandingkan dengan kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.

## 8.2. *Email*

*Email* atau surat elektronik adalah sebuah surat bertipe digital yang dikirimkan melalui jaringan komputer [1]. *Email* sendiri dapat digunakan dengan fasilitas internet. Karena *email* menggunakan jaringan internet, maka proses pengirimannya pun tergolong lebih cepat dan mudah, tidak seperti surat biasa yang menggunakan kertas dan harus ditaruh di kantor pos, lalu kita harus menunggu berhari-hari agar surat kita sampai tujuan. *Email* tidaklah terhambat oleh batasan jarak dan waktu seperti halnya surat biasa. Saat *email* terkirim di jaringan internet, dan langsung menyampaikan pesan kepada penerima dari pengirim dalam waktu yang sangat cepat. Agar penerima dapat membaca atau mendapatkan pesan yang dikirimkan kepadanya penerima hanya perlu untuk memiliki koneksi internet pula dan masuk ke situs-situs yang menyediakan layanan *email*.

*Email* sendiri secara garis besar dapat dibedakan menjadi 2 yaitu:

1. *Email* berbasis SMTP/POP
2. *Email* berbasis web

## 8.3. *Spam*

Spam adalah *Email* yang tidak diminta oleh pengguna (*unsolicited email*) yang dikirim ke banyak orang. Contoh email yang berisi *spam* adalah iklan, undian, informasi palsu, *phising*, penipuan dan lain sebagainya [2]. Para pelaku *spam* biasanya disebut *spammer*, dan bentuk *spam* disebut *spamming. Spam* sama halnya seperti *email* pada umumnya, yang membedakan *spam* dan *email* biasa hanyalah konteks yang terdapat pada isi *email*. *Spam* dikirimkan dengan biaya operasional yang sangat rendah karena *spam* tidak memerlukan sarana *mailing list* untuk mencapai para pelanggan yang diinginkan. Karena hambatan masuk yang sangat rendah, maka banyak *spammer* yang muncul dan banyak pesan tidak diminta masuk pada *email* kita dengan jumlah yang sangat banyak. *Spam* sering mengganggu penerimanya dan terkadang menipu penerimanya. Oleh sebab itu, *spam* dianggap sebagai sampah *email*. Berita *spam* termasuk dalam kegiatan melanggar hukum dan merupakan perbuatan pidana yang dapat terkena undang-undang internet.

## 8.4. Kompresi data

Kompresi data adalah sebuah cara untuk memadatkan data sehingga hanya memerlukan ruangan penyimpanan lebih kecil sehingga lebih efisien dalam menyimpannya atau mempersingkat waktu pertukaran data tersebut. Tujuan proses kompresi data adalah untuk mengurangi redundansi dari sebuah deskripsi data [3]. Pada umumnya, algoritma kompresi data dibedakan antara *lossless* atau *lossy*. Kompresi data *lossless* adalah transformasi dari representasi himpunan data asli sehingga memungkinkan untuk menghasilkan himpunan data yang sama seperti aslinya dengan melakukan proses dekompresi. Kompresi *lossless* digunakan saat berkas asli dan berkas hasil dekompresi harus sama persis (contoh penggunaan dalam kompresi berkas teks, kode yang *executable*, berkas dari pengolah kata, dan lain lain). Kompresi data *lossy* adalah transformasi dari representasi himpunan data asli yang tidak mungkin untuk menghasilkan kembali himpunan data yang sama persis dengan aslinya saat didekompresi, tetapi menghasilkan representasi data yang mendekati aslinya. Kompresi *lossy* digunakan di internet dan secara khusus pada media *streaming* dan aplikasi telepon.

## 8.5. Huffman Code

Huffman code atau disebut algoritma huffman merupakan salah satu teknik kompresi data menggunakan struktur data *binary tree*, hal ini dilakukan untuk mengurangi penggunaan *disk space* dan *network traffic.* Algoritma Huffman merupakan salah satu algoritma kompresi yang cukup terkenal dan populer.

Algoritma huffman ditemukan oleh David Huffman pada tahun 1952. Algoritma ini menggunakan pengkodean yang mirip dengan kode morse. Berdasarkan tipe kode, algoritma huffman termasuk mode statistik. Berdasarkan teknik pengkodeannya, termasuk *symbolwise*. Algoritma huffman merupakan salah satu algoritma untuk menkompres teks [4].

Langkah-langkah algoritma huffman sendiri yaitu pertama kita mendapatkan frekuensi dari setiap simbol dari data. Lalu urutkan simbol-simbol yang didapatkan sesuai dengan frekuensi keluar secara *descending.* Lalu kita menghitung probabilitas dari setiap simbol. Dan yang terakhir kita membentuk *binary tree* untuk menghasilkan *prefix code*.

# RINGKASAN ISI TUGAS AKHIR

Pada Tugas Akhir ini penulis mengusulkan metode steganografi berbasis teks terkompresi pada media surat elektronik dengan menyamarkan sebagai spam untuk menyimpan pesan rahasia. Berikut variabel yang akan digunakan dalam aplikasi yang akan dibangun:

* S = Pesan rahasia (*Secret massage*)
* T = Teks dasar (*Text base*)
* *Text* = Teks yang didapat dari teks dasar
* ΔD = Jarak relatif (*Relative distance)*
* A = Himpunan dari ekstensi alamat *email*
* D = Matriks jarak relatif (*Matrix of relative distance*)
* E = Matriks
* R = Matriks jarak relatif yang dibangun ulang (*Matrix of reconstructed relative distance*)
* K1 = Global *stego key*
* K2 = Himpunan dari alamat email yang dipilih dan dimodifikasi

Gambar 1 menjelaskan alur proses yang akan dijalankan pada aplikasi ini.

Langkah 2

T (Teks dasar)

Langkah 1

Bangun dan simpan ΔD pada setiap *Text* di T untuk membentuk D

S (Pesan Rahasia)

Petakan karakter dari S pada karakter *Text*, dan bangun ΔD

Apakah ada overflow di D?

e=0 , r=0

E = D \ 26

R = D mod 26

YA

Langkah 3

TIDAK

Temukan perulangan Ṝ terbanyak pada R dan dapatkan Ḕ pada E dan *Text* (T\*)pada T.

Langkah 4

Langkah 5

Kompresi Ṝ dengan Huffman coding

K1 (Alamat *Email*)

Langkah 6

Dapatkan 13 Alamat *Email* dengan *latin square*

Pisahkan Ṝ terkompresi menjadi kelompok 12-bit

G1 = 9bit awal

G2 = 3bit terakhir

K1(Alamat *Email*)

Ubah *x* dan *y* menjadi huruf dengan *latin square* dan *z* menjadi ekstensi *email* dengan A

x=[(G1)10]\26

y = (G1)10 mod 26

z=(G2)10

Langkah 7

Bangkitkan *stego cover* dengan T\* dan K2

Modifikasi alamat *email* membentuk K2 dengan Ḕ

A (indeks biner)

Langkah 9

Langkah 8

Gambar 1 Diagram Alur Dari Teknik Steganografi

(Diambil dari [5])

# METODOLOGI

## Penyusunan proposal tugas akhir

Tahap pertama untuk memulai pengerjaan tugas akhir yaitu penyusunan proposal. Pada proposal ini, penulis mengajukan gagasan mengenai steganografi berbasis teks terkompresi pada surat elektronik dengan menyamarkan sebagai *spam*.

## Studi literatur

Pada tahap ini dilakukan pencarian informasi dan studi literatur yang diperlukan. Informasi didapatkan dari buku dan materi-materi lain yang berhubungan dengan metode yang digunakan dalam pengerjaan Tugas Akhir ini dan juga didapat dari internet maupun buku acuan.

## Implementasi perangkat lunak

Implementasi merupakan tahap untuk membangun metode tersebut. Untuk mengimplementasikan metode tersebut digunakan kakas bantu yaitu NetBeans.

## Pengujian dan evaluasi

Pada tahap ini dilakukan pengujian dengan menggunakan beberapa macam teks untuk mencoba aplikasi apakah telah sesuai dengan rancangan dan desain metode yang dibuat, serta mencari ketidaksesuaian yang ada pada program untuk selanjutnya dilakukan perbaikan dan penyempurnaan. Pengujian akan dilakukan dengan cara mencoba apakah aplikasi dapat menyamarkan teks yang akan disisipkan sebagai *spam*. Dan untuk ekstraksi pesan rahasia yang telah disamarkan sebagai *spam* akan dibuat sebuah *plug-in* pada *web browser* untuk mengekstrak pesan yang diterima.

## Penyusunan Buku Tugas Akhir

Pada tahap ini dilakukan penyusunan laporan yang menjelaskan dasar teori dan metode yang digunakan dalam tugas akhir ini serta hasil dari implementasi aplikasi perangkat lunak yang telah dibuat. Sistematika penulisan buku tugas akhir secara garis besar antara lain:

1. Pendahuluan
   1. Latar Belakang
   2. Rumusan Masalah
   3. Batasan Tugas Akhir
   4. Tujuan
   5. Metodologi
   6. Sistematika Penulisan
2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Pengujian dan Evaluasi
5. Kesimpulan dan Saran
6. Daftar Pustaka

# JADWAL KEGIATAN

Berikut ini dipaparkan jadwal kegiatan pengerjaan tugas akhir

**Tabel 1 Jadwal Kegiatan Pengerjaan Tugas Akhir**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Tahapan | 2014 | | | | | | | | | | | | | | | | |
| Maret | | | | April | | | | Mei | | | | | Juni | | | |
| Penyusunan Proposal |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Studi Literatur |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Perancangan system |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Implementasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Pengujian dan evaluasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Penyusunan buku |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

# DAFTAR PUSTAKA

|  |  |
| --- | --- |
| [1] | “Pengertian dan Jenis Layanan Email,” [Online]. Availaible: http://www.artikeltik.com/pengertian-jenis-layanan-email.html [Accesed 25 March 2014] |
| [2] | “Pengertian E-Mail Spam dan Pencegahannya,” [Online]. Availaible: http://www.indosite.com/tutorials/pengertian-e-mail-spam-dan-pencegahannya/ [Accesed 25 March 2014] |
| [3] | Deskoy, A. (2009). Listega : list-based steganography metodology. *Int J Inf Secur, vol. VIII,*, 247-261. |
| [4] | “Algoritma Huffman,” [Online]. Availaible: http://www.metode-algoritma.com/2013/02/algoritma-huffman.html [Accesed 25 March 2014] |
| [5] | Satir, E.,& Isik, H. (2012). A Huffman compression based text steganography method. *Springer Science+Business Media, LLC*, 1-26. |