# KEAMANAN DOKUMEN TEKS DIGITAL MENGGUNAKAN PENDEKATAN ALGORITMA *LINE-SHIFT CODING*

**AWAN SURYANADA**
**10100254**

**JURUSAN TEKNIK INFORMATIKA**
**FAKULTAS TEKNIK DAN ILMU KOMPUTER**
**UNIVERSITAS KOMPUTER INDONESIA**
**BANDUNG**
**2004**

# KEAMANAN DOKUMEN TEKS DIGITAL MENGGUNAKAN PENDEKATAN ALGORITMA *LINE-SHIFT CODING*

**A. Suryanada[1], M.P. Siallagan[1], N. Juhana[1]**
[1]Jurusan Teknik Informatika, F.T. Universitas Komputer Indonesia
Jl. Dipatiukur No. 112-114 Bandung 40132

**ABSTRAKSI**

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya dilakukan melalui jaringan public (internet), apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isinya oleh pihak-pihak yang tidak berhak.

Salah satu cara yang digunakan untuk pengamanan data adalah dengan menggunakan enkripsi dilakukan dengan menyandikan isi informasi (*plaintext*) tersebut menjadi isi yang tidak dipahami, dan untuk memperoleh kembali informasi yang asli, dilakukan proses deskripsi, disertai dengan menggunakan kunci yang benar. Namun sejalan dengan perkembangan ilmu penyandian, usaha untuk memperoleh kunci tersebut bisa dilakukan siapa saja. Untuk mengatasinya yaitu dengan menyisipkan informasi kedalam dokumen menggunakan pendekatan algoritma *line-shift coding*, yang kemudian informasi tersebut dapat dideteksi kembali.

Kata kunci : Enkripsi, deskripsi, penyisipan, deteksi, *line-shift coding.*

## 1. PENDAHULUAN

Perkembangan teknologi multimedia dewasa ini telah menyebabkan media digital menjadi kata yang populer. Salah satu bentuk perkembangan dalam media digital yaitu dokumen elektronik (dokumen teks digital). Dimana dokumen merupakan representasi riwayat organisasi secara eksplisit. Dokumen dalam bentuk elektronik memudahkan untuk dilakukan pembukaan serta penelusuran isi dari riwayat dokumen tersebut yang sebelumnya susah untuk dilakukan pada dokumen dalam bentuk kertas. Penggunaan dokumen digital ini akan memberikan kemudahan dalam penyebaran pada jaringan internet, dan kemurahan dalam penduplikasian (penyalinan) serta penyimpanannya untuk digunakan dikemudian hari. Kemudahan-kemudahan tersebut akhirnya dipergunakan secara negatif oleh pihak-pihak tertentu tanpa memperhatikan aspek hak cipta dari dokumen tersebut. Perlindungan hak cipta terhadap dokumen digital memang sudah lama menjadi perhatian.

Ketika sebuah pesan, file, dokumen berupa informasi dirasa sensitive atau nilai dari informasi tersebut menjadi sangat penting bagi user yaitu orang yang paling berhak menggunakan informasi tersebut. Informasi itu harus dirahasiakan dan perlu mendapat perlindungan. Keamanan data harus terjamin sehingga tidak sembarang orang yang bisa membukanya.

Kriptografi adalah salah satu teknik yang dapat digunakan untuk mengacak teks sehingga tidak seorangpun dapat mengetahui, kecuali ia mengetahui kode yang digunakan.

Dalam bentuk digital, penyebaran dokumen teks secara tidak sah dapat dilakukan dengan lebih mudah. Karena dengan kemajuan komunikasi data yang semakin baik, penduplikasian dan penyebaran dokumen teks akan semakin lebih cepat dan murah dibandingkan dengan dokumen berupa kertas. Berbeda dengan hasil duplikasi dokumen teks berupa kertas, hasil duplikasi pada dokumen teks digital tidak akan berbeda dengan dokumen aslinya. Oleh karena itu untuk menghindari publikasi dan distribusi dokumen teks secara tidak sah, adalah dengan menggunakan pendekatan teknik kriptografi yaitu dengan pengacakan teks pada dokumen aslinya.

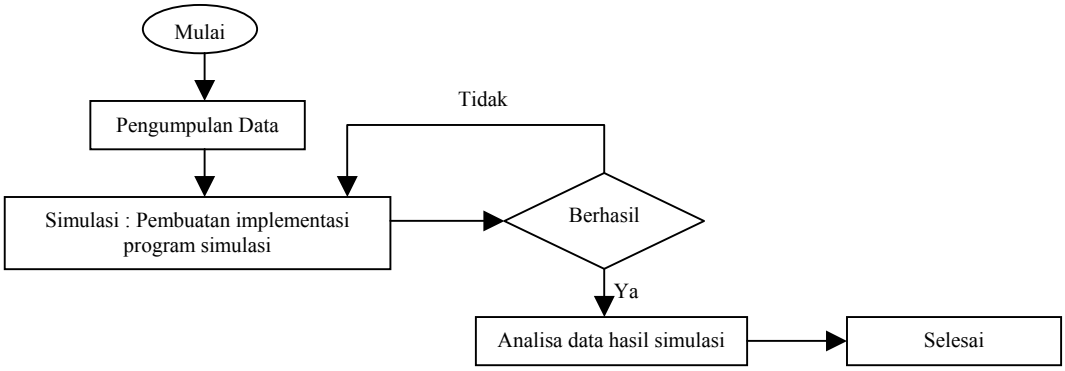
## 2. METODOLOGI

Penelitian dilakukan di Universitas Komputer Indonesia (UNIKOM) terhitung Maret 2004 sampai Juli 2004. Metodologi yang digunakan dalam implementasi program simulasi untuk penyusunan tugas akhir ini adalah sebagai berikut :

a. Studi kepustakaan, yaitu mengumpulkan literatur bacaan-bacaan berupa jurnal, textbook, artikel-artikel yang berhubungan dengan permasalahan yang diambil, karena pada dasarnya data-data yang penulis peroleh dan penulis angkat sebagai bahan penulisan berasal dari studi pustaka yang telah ada.
b. Mengadakan survei terhadap data yang telah ada, penulis bertugas menggali teori-teori yang telah berkembang dalam bidang ilmu yang berkepentingan, mencari metode-metode serta teknik penelitian, baik dalam megumpulkan data atau dalam menganalisa data, yang telah pernah digunakan oleh peneliti-peneliti terdahulu.
c. Konsep penyelesaian permasalahan dalam perlindungan hak cipta atas dokumen teks digital yaitu dengan melakukan perancang sebuah program simulasi implementasi teknik-teknik yang digunakan untuk menjaga keamanan terhadap dokumen teks digital.

Peralatan yang digunakan adalah 1 buah PC dengan spesifikasi sebaga berikut : AMD Athlon 900 Mhz, 20 GB, RAM 128 MB, Microsoft Windows 98 SE, Delphi 6.0, Microsoft Word 2000, Notepad.

Gambar dibawah ini menunjukan tahapan penelitian yang dilakukan :




Gambar 1. Tahapan Penelitian

## 3. HASIL PERCOBAAN/SIMULASI

Dalam implementasinya kita harus mengetahui cara kerja dan tujuan dari keamanan data itu sendiri. Dalam penelitian ini yang akan dilakukan adalah mencoba menyisipkan suatu informasi kedalam file teks berformat (*.txt) dengan menggunakan pendekatan metode *line-shift coding*.

Dalam pendekatan *line-shift coding,* penyisipan dilakukan dengan menggeser baris teks secara tegak lurus keatas atau kebawah pada dokumen teks. Dengan merandom baris mana yang akan digeser maka kita akan mudah menemukan baris yang dikodekan.

Ada empat proses yang dilakukan dalam percobaan kali ini yaitu : proses penyisipan, proses pendeteksian, proses enkripsi dan proses deskripsi.

a. Proses penyisipan

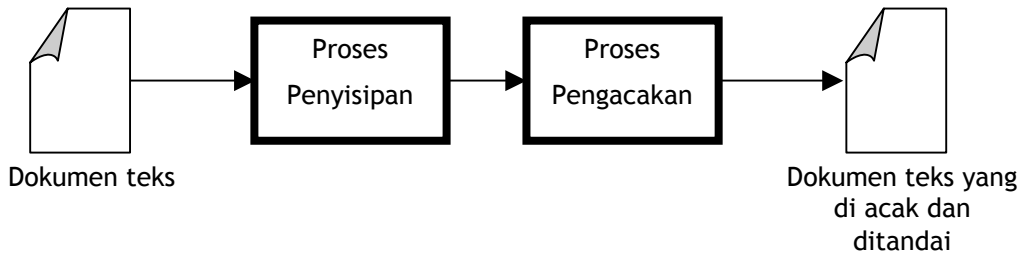
   Proses-proses yang dilakukan dalam penyisipan adalah :

   1). Input file
   2). Scanning file teks
   3). Tentukan informasi yang akan disisipkan
   4). Deteksi jumlah baris
   5). Random baris yang akan disisipkan
   6). Menyisipkan informasi, geser baris
   7). Simpan file

b. Proses Pendeteksian
   1. Input file
   2. Scanning file teks
   3. Deteksi mulai dari baris pertama sampai baris ke-N
   4. Jika ada sisipan maka tampilkan
   5. Selesai.

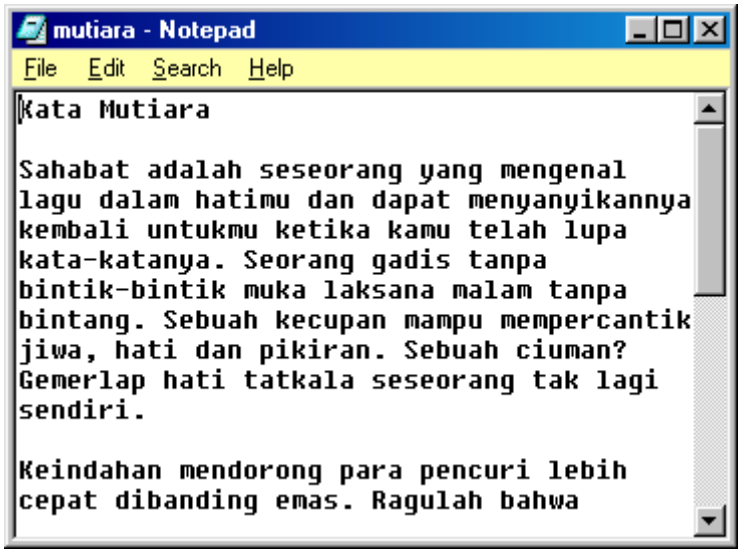
c. Proses Enkripsi
   Algoritma enkripsi yang digunakan adalah *shift cipher* dimana nilai karakter akan digeser.
   1. Merubah karakter kedalam bentuk ascii
   2. Tambah dengan sepuluh (*ciphertext* = nilai ascii + 10)
   3. Hasil dirubah dalam bentuk karakter kembali

d. Proses Deskripsi
   Algoritma deskripsi merupakan kebalikan dari enkripsi.
   1. Merubah karakter kedalam bentuk ascii
   2. Kurangi dengan sepuluh (*plaintext* = nilai ascii - 10)
   3. Hasil dirubah kedalam bentuk karakter




Gambar 2. Proses yang terjadi

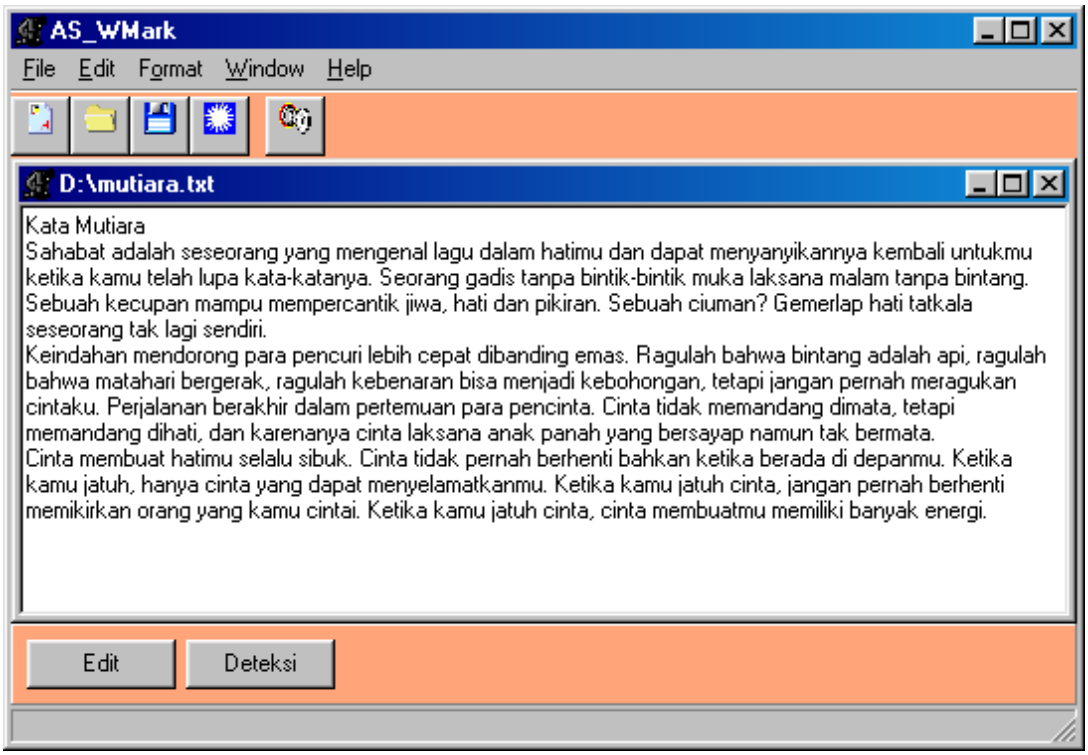
Untuk lebih jelasnya kita akan mencoba menyisipkan informasi kedalam dokumen yang bernama mutiara.txt dengan ukuran 1.01 KB.




Gambar 2. Dokumen teks mutiara.txt

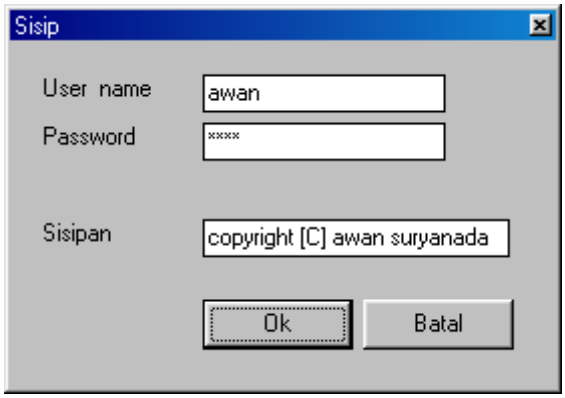
Langkah-langkah yang dilakukan :

1. Input dokumen teks




Gambar 3. Dokumen mutiara.txt dalam program simulasi

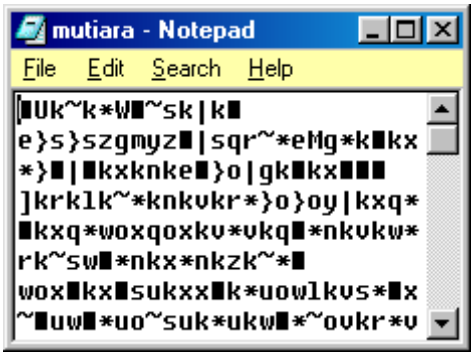
2. Tuliskan informasi yang akan disisipkan




Gambar 4. Informasi sisipan

3. Tekan OK dan simpan

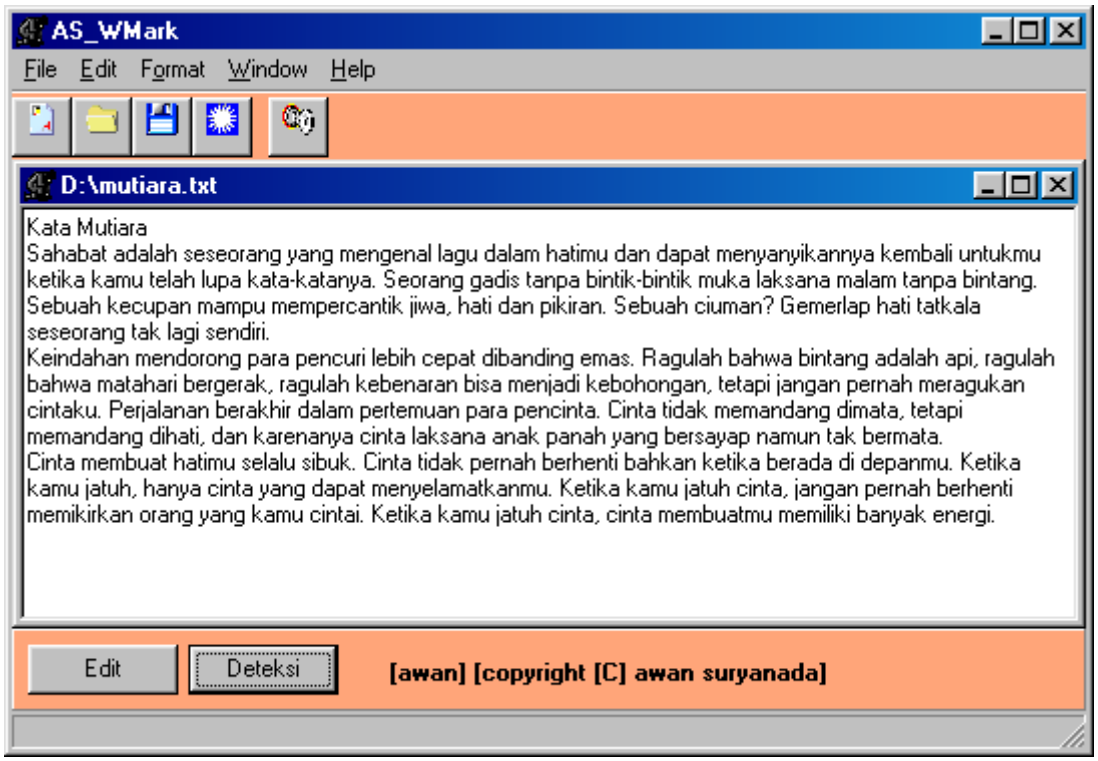
Dengan melakukan proses tersebut diatas maka kita sudah melakukan proses penyisipan informasi kepemilikan, sehingga kita dapat membuktikan bahwa dokumen tersebut adalah milik kita. Dokumen mutiara.txt hasil tersebut tidak akan bisa dibaca disembarang *software* pembaca dokumen teks, seperti notepad, Microsoft *word* dan sebagainya. Sehingga dengan demikian akan membantu / menjaga keamanan di dalam penyalinan dokumen yang tidak sah.




Gambar 5. File mutiara hasil dibaca dengan notepad

Dokumen teks hasil tersebut dapat dideteksi informasinya, sehingga meskipun sudah banyak penyalinan yang dilakukan, kita akan tetap dapat membuktikan dokumen tersebut milik kita. Berikut langkah-langkah yang dilakukan dalam proses deteksi :

1. Input dokumen teks
2. Deteksi (dengan menekan tombol Deteksi pada program simulasi)




Gambar 6. Proses deteksi

## 4. KESIMPULAN

Berdasarkan analisis hasil implementasi dan penelitian yang dilakukan dalam penyisipan informasi kepemilikan pada dokumen teks digital, beberapa hal yang dapat disimpulkan :

1. Penyadap akan sulit menemukan informasi pada dokumen teks yang dicurigainya, karena ia harus memecah sistem keamanan terhadap informasi yang disembunyikan tanpa mengetahui kunci yang digunakan.

2. Perbedaan dokumen teks asli dengan dokumen teks hasil, tidak akan terlihat jika dilihat dari tampilan pada program simulasi, namun akan terlihat jika dilihat dengan menggunakan notepad.
3. Ukuran dokumen teks hasil akan selalu lebih besar jika dibandingkan dengan dokumen teks asli. Ukuran tersebut akan tergantung dengan karakter informasi yang disisipkan.
4. Pemilik dokumen teks akan mampu mempertahankan hak kepemilikkannya karena informasi yang disisipkan, karena ia dapat mendeteksi informasi yang disisipkan.

## 5. DAFTAR PUSTAKA


1. N.F Maxemchuk and S. Low, *Marking Text Dokuments*. University of Melbourne Australia, hal 1-5 (1997).
2. J.T. Brassil, S. Low and N.F. Maxemchuk, *Copyright Protection for the Electronic Distribution of Text Documents*. Bell Labs Lucent Tech, Univercity of Melbourne, AT&T Labs, hal 1-5 (1999).
3. M.S. Widodo, Teknik Watermarking Pada Dokumen Teks Digital. Institut Teknologi Bandung, hal 1-19 (2003).
4. F. Hartung and M. Kutter, *Multimedia Watermarking Techniques*, University of Erlangen-Nuremberg Germany, University of Rhode Island, hal 1079-1084 (1999).
5. R.J. Anderson and F.A.P. Petitcolas, *Information Hiding An Annotated Bibliography*. University of Cambridge, hal 22-24 (1999).
6. A. Budiyono, Enkripsi Data Kunci Simetris Dengan Algoritma Kriptografi LOKI97, Institut Teknologi Bandung, hal 1-5 (2004).
7. Yulis, Keamanan Data Dengan Konsep Autheticity, hal 1-4 (2004).
8. K. Satrio, Mengenal Kriptografi, Neotek, hal 12-13 (2003).
9. T. Heriyanto, Pengenalan Kriptografi, hal 1-9 (1999).
10. I.M.A. Jaya, Penyandian Data Dengan Algoritma Kriptografi Neokeon, Institut Teknologi Bandung, hal 1-8 (2003).
11. R. Baharuddin, Pengenalan Kriptografi, www.komputer.com, hal 1-8 (2004).
12. D.R. Stinson, Cryptography : Theory and Practice, CRC Press, Boca Raton, (1995).
13. H.C.A.V. Tilborg, Fundamentals of Cryptology, Kluwer Academic Publishers, Boston, (2000).