Algoritma Steganografi untuk Pengamanan Data Teks ke dalam Citra Digital Menggunakan XOR Sederhana

Muchamad Kurniawan[1], Siti Agustini[2]

[1,2]Jurusan Sistem Komputer, Fakultas Teknologi Informasi, Institut Teknologi Adhi Tama Surabaya
Email: [1]sitiagustini@itats.ac.id, [2]muchamad.kurniawan@itats.ac.id

Abstract. *Confidentiality of data or information is very important to be guarded from someone who is not entitled to the data. One solution to data security is by steganography. Steganography is the science of inserting confidential information into other messages. In this study, the concept of steganography uses text messages hidden into a digital image. The image used is an image in grayscale form. The study was conducted 5 times with different text message sizes. As a result, the steganography system works well where all text messages can be encrypted and decrypted again. Running time will be higher when the size of the text message gets bigger and so does the entropy value so that the security level of the steganography process is higher.*
Keywords: *Steganografi, XOR, running time, entropy.*

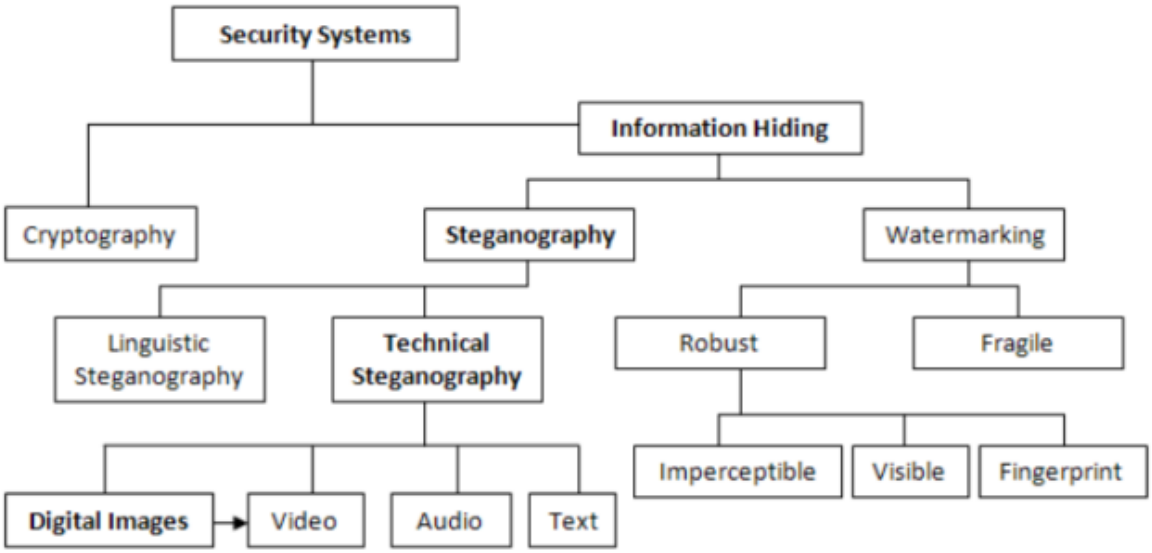
Abstrak. *Kerahasiaan data atau informasi merupakan hal yang sangat penting untuk dijaga dari seseorang yang tidak berhak atas data tersebut. Salah satu solusi untuk pengamann data adalah dengan steganografi. Steganografi merupakan ilmu untuk penyisipan informasi rahasia ke dalam pesan yang lain. Pada penelitian ini, konsep steganografi menggunakan pesan teks yang disembunyikan ke dalam suatu citra digital. Citra yang digunakan adalah citra dalam bentuk grayscale. Penelitian dilakukan sebanyak 5 kali dengan ukuran pesan teks yang berbeda-beda. Hasilnya, system steganografi berjalan dengan baik dimana semua pesan teks dapat dienkripsi dan didekripsi kembali. Running time akan semakin tinggi ketika ukuran pesan teks semakin besar dan begitu juga dengan nilai entropy sehingga tingkat keamanan dari proses steganografi ini semakin tinggi.*
Kata Kunci: *Steganografi, XOR, running time, entropy.*

1. Pendahuluan

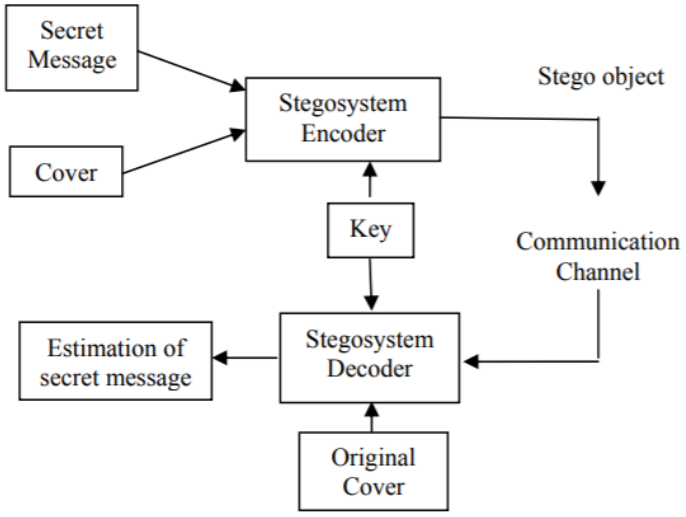
Pada sistem keamanan jaringan, steganografi merupakan cabang ilmu dari penyisipan informasi. Steganografi adalah cabang ilmu yang dikembangkan untuk pengamanan informasi. Steganografi mempelajari bagaimana suatu informasi rahasia tidak dapat diketahui orang yang tidak berhak dengan cara menyisipkan atau menyembunyikan pesan rahasia tersebut ke dalam pesan yang lain. Perkembangan penyisipan informasi dapat dilihat pada Gambar 1. Steganografi terbagi dalam 2 kategori yaitu Technical Steganography dan Linguistic Steganografi. Media Technical Steganografi meliputi citra digital, video, audio, dan teks. Format gambar yang digunakan dalam penyisipan citra digital diantaranya adalah Graphics Interchange Format (GIF), Joint Photograpic Expert Group (JPEG), dan Portable Network Graphisc (PNG). Selain itu, format citra Bitmap (BMP) juga dapat digunakan sebagai cover citra penyisipan data.

Blok diagram sistem steganografi secara keseluruhan dapat dilihat pada gambar 2. Pada gambar 2 menjelaskan input dari Stegosystem adalah teks rahasia dan cover yaitu citra yang digunakan untuk menyembunyikan teks. Selain itu juga terdapat sebuah key yang dimasukkan ke dalam stegosystem encoder sehingga menghasilkan stego object. Stego object ini dikirimkan melalui kanal komunikasi menuju ke penerima. Pada saat di penerima, stego object yang didapat diekstraksi dengan stegosystem decoder. Hasil dari stegosystem adalah original cover atau citra sebagai media penyisipan dan estimasi pesan rahasia.

ISSN: 2579-566X (Online)
ISSN: 2477-5274 (Print)



Gambar 1. Fokus disiplin ilmu penyisipan informasi (Chedad et al, 2010)



Gambar 2. Skema Sistem Steganografy (Kamaldeep et. al, 2017)

Komunikasi melalui internet yang terus berkembang membuat pesan yang dikirim rentan terhadap pencurian data terhadap orang yang tidak berhak atas data tersebut. Sehingga diperlukan suatu metode agar pesan dapat sampai ke penerima dengan aman tanpa adanya pencurian data atau perubahan data. Salah satu solusinya adalah dengan Steganografi. Metode Steganografi yang diterapkan pada penelitian ini menggunakan metode operasi XOR sederhana dengan enkripsi 16 bit setiap pixel citra dan karakter dari pesan rahasia.

2. Penelitian Terkait

Pengembangan teknik steganografi telah dikembangkan dalam beberapa tahun terakhir. (Husein et. al, 2018) menggunakan teknik mapping untuk penyisipan teks ke dalam *gray image*. Peneliti menggunakan ASCII Mapping Technique (ATM) untuk menciptakan encoded table dengan memetakan pesan teks dan menyesuaikan beberapa bit dengan citra yang digunakan. Hasil dari penelitian ini menunjukkan bahwa teknik ini memberikan komputasi yang rendah sehingga memberikan performa yang efektif untuk banyak aplikasi.

(Bhattacharyya et. al., 2013) juga melakukan penelitian dengan menerapkan metode ASCII Mapping Technology (ATM) sebagai metode steganografi teks. Namun berbeda dengan penelitian Husein, penelitian ini juga menerapkan teknik quantum logic untuk meningkatkan level keamanan. Nilai Shannon entropy dan correlation-coefficient menunjukkan bahwa Stego teks dihasilkan dengan degradasi nol atau minimum menggunakan metode ATM ini.

Penelitian yang lain telah dilakukan oleh Vipul. Pada penelitian ini diusulkan teknik baru untuk penyimpanan informasi di dalam sebuah citra. Untuk memaksimalkan kapasitas penyimpanan, peneliti menggunakan algoritma kompresi data yang turut digunakan. Algoritma kompresi mengharuskan program bekerja pada range antara 1 bit sampai 8 bit per pixel ratio. Dengan menerapkan algoritma kompresi data ini, peneliti telah mengembangkna aplikasi yang membantu pengguna untuk efisiensi penyisipan data (Vipul, 2013).

(Deepika,2017) membuat penelitian untuk penyisipan teks ke dalam data menggunakan metode LSB (Least Significant Bit). Hasil penelitian menunjukkan bahwa nilai PSNR berada di angka 49.32 dan akurasi sebesar 94%. (Kukapali) membuat penelitian mengenai Pixel Indicator Method (PIM). Tekniknya adalah dengan menggunakan 3 MSB terakhir dari setiap pixel. Pada penelitian ini digunakan algoritma Blowfish untuk proses enkripsi. Peneliti mengklaim bahwa dengan perbedaan warna pada citra akan memperkuat system steganografi sehingga susah untuk dipecahkan.

(Kamaldeep,2017) memberikan konsep steganografi menggunakan 2 bit LSB dan operasi XOR. Peneliti menerapkan operasi XOR pada data ke 8 dan ke 1, data ke 7 dan ke 2. Setelah itu didapat 2 bit. Bit yang telah didapat menggantikan posisi LSB. Penelitian dilakukan dengan beberapa citra yang berbeda. Hasil observasi terhadap penelitian ini menunjukkan bahwa metode ini menunjukkan hasil yang bagus dengan nilai PSNR dan MSE. MEtode ini juga menunjukkan peningkatan kapasitas pesan.

3. Metode Penelitian

Pada penelitian ini, digunakan pesan rahasia berupa teks dalam bentuk txt. Sedangkan cover image memiliki format atau ekstensi PNG. Citra yang digunakan dikonversi ke dalam bentuk gray scale. Metode pada penelitian ini adalah membagi karakter setiap karakter menjadi 16 bit dari pesan teks dan juga membagi tiap pixel ke dalam 16 bit. Kemudian, setiap pixel dan karakter dilakukan operasi XOR. Proses ini berulang sampai karakter terakhir. Proses enkripsi ini menghasilkan citra yang berisi teks pesan rahasia. Pada proses dekripsi, citra asli dan citra yang telah terenkrip dibagi dalam 16 bit. Kemudian, setiap bagian dari citra asli dan citra yang telah terenkrip dilakukan operasi XOR. Sehingga didapat pesan rahasia dan citra asli lagi.

1. Pseudocode

Algoritma yang digunakan pada penelitian ini dapat dilihat pada pseudocode di bawah :

- Proses penyisipan data ke dalam citra grayscale (enkripsi)

```
1. Membaca teks pesan rahasia dan citra grayscale.
2. loop while(urutan karakter <= total karakter)
   {
      karakter = konversi ke 16 bit integer (karakter)
      pixel = konversi ke 16 bit integer (pixel)
      pixel_terenkripsi= (pixel) bitwise_xor (karakter)
      pixel = pixel selanjutnya
      karakter = karakter selanjutnya
      urutan karakter = urutan karakter + 1
    }
3. pixel terenkripsi = pixel citra asli
```

ISSN: 2579-566X (Online)
ISSN: 2477-5274 (Print)

- Proses ekstraksi data dari citra grayscale (dekripsi)

```
1. Membaca citra asli dan citra terenkripsi
2. loop while( urutan pixel <= total pixel)
   {
      pixel asli=konversi ke 16 bit integer (pixel asli)
      pixel_terenkripsi=konversi ke 16 bit integer (pixel_terenkripsi)
      a= (pixel asli) bitwise_xor (pixel_terenkripsi)
          if a=0 then break else decrypted_text=a

      pixel asli=next pixel asli
      pixel_terenkrip=next pixel_terenkrip.
}
```

2. Parameter Kualitas Hasil Steganografi

a. Running time

Running time merupakan waktu yang dibutuhkan untuk sebuah proses steganografi dari awal sampai akhir.

b. Entropy

Entropy merupakan sebuah konsep yang random dimana terdapat kemungkinan yang tidak pasti. Entropy juga menyataka jumlah informasi dalam suatu pesan. Entropy digunakan untuk menghitung jumlah bit rata-rata yang digunakan untuk pengkodean. Nilai entropy dapat dihitung dengan persamaan :

$$\boldsymbol{H = -\sum_{k=0}^{n} P(k) log_2(P(k))}$$

Dimana :

H : entropy

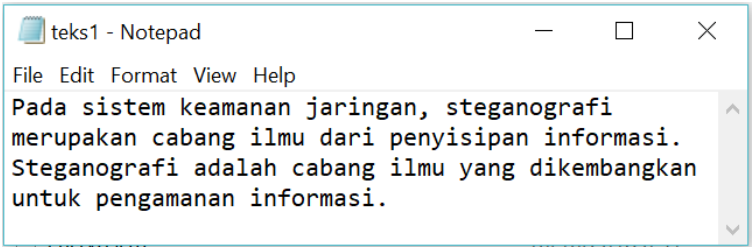
n : jumlah symbol yang berbeda di dalam pesan

P(k) : probabilitas kejadian symbol k

4. Hasil dan Pembahasan

Pada penelitian ini telah dilakukan percobaan dengan 5 pesan teks yang berbeda ukurannya. File teks yang digunakan berukuran 1KB, 2KB, 3KB, 53KB, dan 100 KB. Setiap percobaan yang dilakukan diukur kualitas hasil steganografi berdasarkan parameter running time dan entropy. Berikut adalah contoh input sistem steganografi yang telah dibuat :

1. Pesan Teks dalam bentuk .txt



Gambar 3. Contoh pesan teks yang akan dienkripsi (teks1.txt)

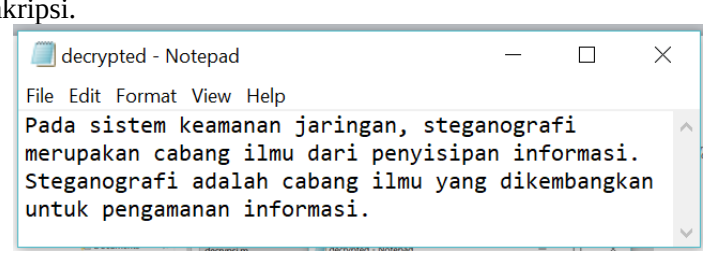
2. Citra digital dalam bentuk grayscale

Gambar 4. Citra digital asli sebagai cover image pesan teks

Hasil enkripsi dengan system steganografi dapat dilihat pada gambar 5

Gambar 5. Citra digital yang telah disisipkan teks1.txt

Hasil dekripsi dari citra digital yang telah dienkripsi bersama dengan teks dapat dilihat pada gambar 6. Gambar 6 adalah pesan teks yang disembunyikan pada citra digital. Isi pesan teks tersebut sama dengan teks saat dienkripsi.



Gambar 6. Pesan teks hasil dekripsi (decrypted.txt)

Untuk mengetahui kualitas dari sistem steganografi ini, maka diukur hasil enkripsi dengan 2 parameter yaitu running time dan entropy. Hasil selengkapnya dapat dilihat pada table 1. Dengan bertambahnya ukuran teks yang digunakan maka running time untuk enkripsi juga akan semakin lama.

ISSN: 2579-566X (Online)
ISSN: 2477-5274 (Print)

Parameter berikutnya yaitu entropy. Entropy merupakan perhitungan untuk memperkirakan panjang bit rata-rata untuk sebuah kode atau simbol pesan, sehingga semakin tinggi nilai entropy akan menghasilkan system yang semakin aman. Dari table 1 terlihat bahwa nilai entropy semakin besar seiring dengan bertambahnya ukuran teks. Hal ini menandakan semakin besar ukuran teks maka semakin banyak elemen/karakter/symbol yang disandikan sehingga menghasilkan nilai entropy yang semakin tinggi.

Tabel 1. Parameter Kualitas Hasil Steganografi

Ukuran Teks	Running time (detik)	Entropy
1 KB	0.0567	7.3057
2 KB	0.0582	7.3751
3 KB	0.0659	7.4203
53 KB	0.0762	7.6060
100 KB	0.0791	7.6060

5. Kesimpulan

Penelitian ini bertujuan untuk membangun sebuah system steganografi penyembunyian informasi berupa teks ke dalam sebuah citra digital grayscale. Penelitian dilakukan dengan 5 macam teks dengan ukuran yang berbeda. Hasil penelitian ini menunjukkan bahwa semakin besar ukuran teks maka semakin lama running time untuk proses enkripsi. Sedangkan nilai entropy semakin besar ketika ukuran teks bertambah besar sehingga meningkatkan keamanan dari teks yang disembunyikan.

Referensi

Bhattacharyya, S., P. Indu, and G. Sanyal,2013, Hiding Data in Text using ASCII Mapping Technology (AMT). International Journal of Computer Applications, 70(18).

Deepika dan Er. Jasdeep Singh Mann. 2017. Steganography System for Hiding Text and Images Using Improved LSB Method. International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 02.

Hussein L., Ahmed A., Sinan A., Salam dan Jasim H., 2018. Hiding text in gray image using mapping technique. IOP Conf. Series: Journal of Physics: Conf. Series 1003 (2018) 012032 doi :10.1088/1742-6596/1003/1/012032 J. Phys.: Conf. Ser. 1003 012032.

Joshi, K., Yadav, K., Chawla, G. 2017. An Enhanced Method for Data Hiding using 2-Bit XOR in Image Steganography. International Journal of Engineering and Technology (IJET).

Sharma, V. dan Kumar, S. 2013. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4.