Penyisipan Pesan Pada Media Teks Menggunakan 2-Wrap Lenght dan Karakter Non-Breaking Space

Muhammad Ikhsan Thohir [a,1,*], Alun Sujjada [b,2], Zaenal Alamsyah [c,3], Reni Andian [c,4]

[a,b,c] Teknik Informatika, Universitas Nusa Putra, Cibolang, Sukabumi, 431555, Indonesia
[1] ikhsan.thohir@nusaputra.ac.id*; [2] alun.sujjada@nusaputra.ac.id; [3] zaenal.alamsyah@nusaputra.ac.id, [4] reni.andian_ti18@nusaputra.ac.id
* Penulis Korespondensi

ABSTRAK

Steganografi merupakan teknik penyembunyian pesan yang dianggap rahasia ke dalam file lain dengan cara menyamarkan isi pesan. Proses steganografi membutuhkan pesan dan cover. Cover adalah media yang digunakan untuk penyisipan atau penyembunyian pesan. Penelitian ini,menggunaan metode 2-wrap length untuk menentukan file teks yang akan disisipkan pesan. Metode ini didasari oleh konsep seperti file teks akan dikonversi ke bilangan ASCII untuk diubah menjadi bilangan biner. Proses selanjutnya yaitu menambahkan karakter nonbreaking space untuk membuat file baru yang secara kasat mata akan tampak mirip dengan file aslinya.

KATA KUNCI
2-wrap lenght
Karakter *non braking space*
Penyisipan pesan teks
Steganografi

ABSTRACT

Steganography is a technique for hiding messages that are considered confidential in other files by disguising the contents of the message. The steganography process requires a message and a cover. Cover is the media used for inserting or hiding messages. In this study, the 2-wrap length method is used to determine the text file where the message will be inserted. This method is based on the concept that a text file is converted to an ASCII number to be converted into a binary number. The next process is to add non-breaking space characters to create a new file that looks similar to the original file by naked eye.

KEYWORD
2-wrap lenght
Non braking space character
Teks Message Insertion
Steganography

This is an open-access article under the CC–BY-SA license

1. Pendahuluan

Seiring berkembangnya zaman kemajuan teknologi begitu pesat memepengaruhi berbagai bidang kehidupan terutama media informasi.Pengiriman data melalui internet sudah menjadi kebutuhan karena sifatnya yang efektif, efisien dan mudah, namun harus diperhatikan juga aspek keamanan data pada saat pengiriman terutama data rahasia. Pesatnya kemajuan teknologi tersebut membuat berkembangnya kejahatan sistem informasi. Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat 88.414.296 serangan siber telah terjadi sejak 1 Januari hingga 12 April 2020. Pada bulan Januari terpantau 25.224.811 serangan dan kemudian pada bulan Februari terekam 29.188.645 serangan lalu kemudian pada bulan Maret terjadi 26.423.989 serangan dan sampai dengan 12 April 2020 telah tercatat 7.576.851 serangan. Puncak jumlah serangan terjadi pada tanggal 12 Maret 2020 yang mencapai 3.344.470 serangan dan setelah itu jumlah serangan mengalami penurunan yang cukup signifikan saat diberlakukannya kebijakan work from home (WFH) di berbagai tempat. Namun demikian selama WFH berlangsung telah terjadi serangan siber yang memanfaatkan isu terkait dengan

Jurnal Restikom : Riset Teknik Informatika dan Komputer
Vol. 4., No. 1, April 2022, pp. 28-35

Covid-19. Jenis serangan yang paling banyak adalah trojan activitysebanyak 56% dan kemudian disusul dengan aktifitas information gathering (pengumpulan informasi) sebanyak 43% dari total keseluruhan serangan, sedangkan1% sisanya merupakan web application attack. (Badan Siber Dan Sandi Negara Republik Indonesia) Dengan berbagai teknik banyak yang mencoba untuk mengakses informasi yang bukan haknya untuk melindungi data yang dikirim, dengan demikian banyak dikembangkan berbagai teknik untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak, salah satunya adalah teknik steganografi. Menurut Munir (2009), steganografi adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) dengan sedemikian sehingga keberadaan (eksistensi) pesan yang tidak terdeteksi oleh indera manusia. Steganografi memiliki beberapa metode diantaranya*: Least Significan Bit Insertion (LSB), Algorithms and Transformation, Redundant Pattern Encoding, dan Spread Spectrum method.* Dalam Buku Histories of Herodatus steganografi sudah digunakan sejak 2.500 tahun yang lalu untuk kepentingan politik, militer, diplomatik, juga untuk kepentingan pribadi sebagai alat komunikasi.Catatan pertama tentang steganografi ditulis oleh Herodotus, yaitu seorang sejarawan Yunani. Herodatus mengirim pesan rahasia dengan menggunakan kepala budak atau prajurit sebagai media. Caranya dengan menuliskan pesan di atas kepala budak yang telah dibotaki, ketika rambut budak telah tumbuh, budak tersebut diutus untuk membawa pesan rahasia di balik rambutnya. Di era modern, teknik steganografi menjadi populer setelah kasus pemboman gedung WTC pada 11 September 2001 di Amerika Serikat. Pada saat itu, teroris menyembunyikan pesan-pesan kegiatan terornya dalam berbagai media yang dapat dijadikan penampung untuk menyembunyikan file seperti pada image, audio dan video. Penelitian-penelitian sebelumnya terkait pengamanan informasi sudah banyak dilakukan.Mulyanto menyisipan pesan teks pada citra menggunakan metode LSB dan 2-Wrap Length,untuk meningkatkan kemampuan LSB dalam menyisipkan pesan, ditambahkan algoritma peletakan pada bagian mana dari citra pesan akan disisipkan. Semakin acak posisi pesan maka semakin tidak mudah terbaca informasi yang dirahasiakan pada pesan teserbut. Metode 2 wrap-length digunakan untuk menentukan posisi piksel yang akan disisipkan pesan.Ulil Amri mengimplementasikan steganografi teks menggunakan metode pencocokan LSB dan Karakter Non-Breaking Space sebagai penanda pesan.Pesan teks disisipkan dengan cara menyisipkan file pesan ke dalam file teks dengan format (.txt atau .docx) dengan metode pencocokan LSB (Least Significant Bit) dan penanda pesan.Pandikumar dan Gebreslassie menggunakan metode LSB dengan teknik peletakan acak pada tepi citra. Pesan yang akan disisipkan diacak terlebih dahulu dengan menggunakan teknik kriptografi Advanced Encryption Standard (AES) untuk memberikan keamanan yang
lebih. Pada penelitian ini,peneliti mengusulkan penggunaan metode 2-wrap length untuk menentukan file teks yang akan disisipkan pesan.Metode ini didasari oleh konsep seperti file teks akan dikonversi ke bilangan ASCII untuk diubah menjadi bilangan biner. Proses selanjutnya yaitu menambahkan karakter non-breaking space untuk membuat file baru yang secara kasat mata akan tampak mirip dengan file aslinya.

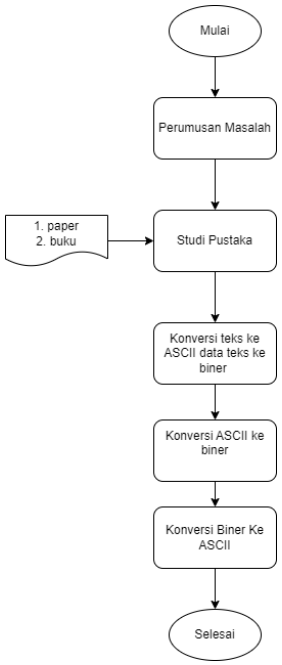
2. Tinjauan Pustaka

Steganografi "*steganography"* adalah ilmu, teknik atau seni menyembunyikan pesan rahasia "*hiding message"* atau tulisan rahasia "*covered writing*" sehingga keberadaan pesan tidak terdeteksi orang lain kecuali pengirim dan penerima pesan tersebut.Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana disinilah fungsi dari teknik steganografi yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas [1]. Pada penelitian sebelumnya teknik 2-wrap length digunakan untuk menentukan posisi penyisipan pesan teks ke dalam citra untuk menghasilkan penyisipan yang lebih acak sehingga isi pesan tidak mudah diketahui [2]. Penelitian sebelumnya juga menyebutkan Penyisipan pesan teks adalah metode yang paling banyak digunakan dalam steganografi [3]. ASCII (*American Standard Code for Information Interchange*) adalah standar

yang berlaku di seluruh dunia untuk kode berupa angka yang merepresentasikan karakter-karakter, baik huruf, angka, maupun simbol yang digunakan oleh komputer. Terdapat 128 karakter standar ASCII yang masing-masing direpresentasikan oleh tujuh digit bilangan biner mulai dari 0000000 hingga 1111111.Fungsi Kode ASCII adalah sebagai karakter kode dari user atau admin dalam menjalankan perintah dan akan ditranslasikan agar komputer memahami kode dari user karena komputer hanya membaca angka binner [4]. Kemudian, pada penelitian sebelumnya menyebutkan Penggunaan karakter non-breaking space mengakibatkan perubahan terhadap tampilan dari isi file stego, tetapi tidak mengakibatkan perubahan karakter, makna kata atau informasi yang ada [5].

3. Metodologi Penelitian

Pada tahapan ini merupakan metodologi penelitian peneliti, metode kuantitatif digunakan pada penelitian ini untuk meneliti sampel konversi teks , ASCII dan biner. Berikut flowchart metodologi penelitian.



Gambar 1. Flowchart Metodologi Penelitian

3.1 Perumusan Masalah

Untuk menentukan steganografi dengan metode penyisipan teks dapat bekerja dengan baik untuk penyandian data, dimana masih sedikit penelitian yang menggunakan metode ini untuk bisa menentukan metode mana yang terbaik yang digunakan untuk steganografi.

3.2 Studi Pustaka

Untuk memperkuat akar masalah dan solusi dibutuhkan studi pustaka yang cukup untuk menentukan permasalahan yang ada. Studi pustaka yang menjadi acuan antara lain paper jurnal dari penelitian sebelumnya.

ISSN 2686-4797
Jurnal Restikom : Riset Teknik Informatika dan Komputer
Vol. 4., No. 1, April 2022, pp. 28-35

3.3 Konvesi teks ke ASCII data teks ke biner

Pesan teks yang akan disisipkan dikonversi terlebih dahulu kedalam bilangan ASCII. Fungsi dari kode ASCII ialah untuk mewakili karakter-karakter angka maupun huruf didalam komputer, sebagai contoh dapat kita lihat pada karakter 1, 2, 3, A, B, C, dan sebagainya. menjadi bilangan biner dengan pengkodean ASCII. Terdapat 128 karakter standar ASCII yang masing-masing direpresentasikan oleh tujuh digit bilangan biner mulai dari 0000000 hingga 1111111. Berikut adalah tabel bilangan ASCII :

Char	ASCII Code	Binary	Char	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	R	082	01010010
s	115	01110011	S	083	01010011
t	116	01110100	T	084	01010100
u	117	01110101	U	085	01010101
v	118	01110110	V	086	01010110
w	119	01110111	W	087	01010111
x	120	01111000	X	088	01011000
y	121	01111001	Y	089	01011001
z	122	01111010	Z	090	01011010

Gambar I. Tabel Bilangan ASCII

Sebagai contoh, karakter teks "HAI" dikonversikan menjadi bilangan ASCII, sehingga diperoleh hasil seperti di bawah ini :

Tabel 1. Tabel Konversi teks ke ASCII

Karakter	Kode ASCII
H	48
A	41
I	49

3.4 Konvesi ASCII ke Biner

Proses selanjutnya yaitu kode ASCII yang kemudian akan dikonfersi ke bilangan biner sehingga terbentuk bit-bit yang terdiri dari bit '0' dan bit '1'. Bit inilah yang akan dikirimkan dan pada penerima akan dikodekan kembali. Kemudian bit-bit tadi yang dikirimkan dan akan dikodekan kembalikedalam teks aslinya. Proses inilah yang dinamakan decoding. Misalnya kita ingin mengirimkan pesan "lidya". Maka setiap huruf yaitu l,i,d,y,a akan dikodekan menjadi biner.
Kode ASCII untuk setiap huruf :
l = 108 = 0110 1100 (yang dikirim pertama)
i = 105 = 0110 1001
d = 100 = 0110 0100
y = 121 = 0111 1001
a = 97 = 0110 0001 (yang dikirim terakhir)
Kemudian bit-bit tadi yang dikirimkan dan akan dikodekan kembali kedalam teks aslinya. Asumsikan pengiriman tanpa gangguan. Maka, pada penerima akan diterima kode

Kode bit

01101101 01101001 01110010 01101001 01101011

Kemudian kode-kode bit itu akan diterjemahkan dengan memisah menjadi 8 bit.

01100001 = 97 = a (yang diterima terakhir)

01111001 = 121 = y

01100100 = 100 = d

01101001 = 105 = i

01101100 = 108 = l (yang diterima pertama)

Maka diterjemahkan bahwa pesannya adalah kata "lidya"

3.5 Konversi Biner ke ASCII

Untuk melakukan konversi dari bilangan biner ke ASCII, dapat menggunakan tabel Biner - ASCII. Setiap 8 digit bilangan biner merupakan satu karakter ASCII.
Contoh 1:
Konversikan 01001000 01000101 01001100 01001100 01001111 ke ASCII.
Pisahkan bilangan biner per 8 digit.
01001000 01000101 01001100 01001100 01001111
1) 01001000 = H
2) 01000101 = E
3) 01001100 = L

4) 01001100 = L
5) 01001111 = O
Jadi, 0100100001000101010011000100110001001111 = HELLO

Untuk proses pengambilan pesan, maka dilakukan konversi data biner ke ASCII agar pesan mudah untuk dibaca.

4. Hasil dan Pembahasan

4.1. Hasil

Untuk membuahkan hasil yang maksimal sesuai dengan yang diharapkan, maka dibuat kembali alat konversi menggunakan visual basic, dan beberapa tool lainnya seperti text editor dan requirement software.

4.2. Pembahasan

4.2.1. Planning

Pada tahap ini penulis melakukan persiapan sehingga didapatkan aplikasi penunjang untuk perancangan program berikut, aplikasi yang dipakai yaitu visual Basic.Tidak hanya itu penulis juga mendapatkan berbagai file teks untuk bisa di uji coba pada program.

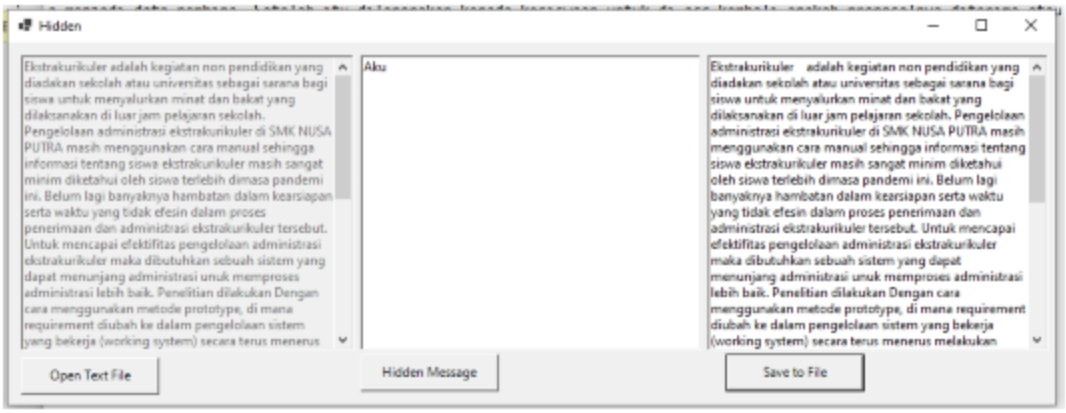
4.2.2. Analisis

Pada tahap ini penulis melakukan analisis dengan mengumpulkan berbagai bahan berupa file teks dengan ukuran 8 bit untuk 1 karakter.

4.2.3. Desain

4.2.3.1 Form penyisipan pesan teks

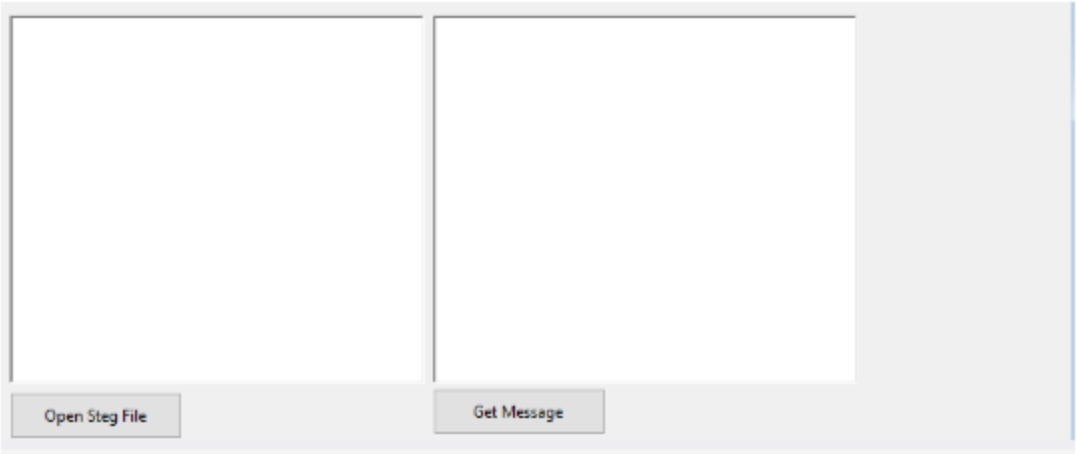
Program menyediakan satu tampilan dengan tiga menu untuk penyisipan pesan teks yaitu open file teks,hidden message, dan save to file.Langkah pertama dalam penyisipan teks ini yaitu open file teks yang akan disisipi pesan lalu masukan pesan rahasia yang ingin di sisipkan ke dalam pesan teks untuk selanjutnya disimpan.



Gambar 2. Form Penyisipan Pesan Teks

4.2.3.1 Form mendapatkan dan membuka pesan rahasia (private message)

Program menyediakan satu tampilan yang berisi menu open steg file dan get message untuk membuka dan mendapatkan pesan rahasia.



Gambar 3. Form Mendapatkan dan Membuka Pesan Rahasia

5. Kesimpulan

Seiring berkembangnya zaman kemajuan teknologi begitu pesat memepengaruhi berbagai bidang kehidupan terutama media informasi.Pengiriman data melalui internet sudah menjadi kebutuhan karena sifatnya yang efektif, efisien dan mudah.Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) dengan sedemikian sehingga keberadaan (eksistensi) pesan yang tidak terdeteksi oleh indera manusia. Pada penelitian ini,peneliti mengusulkan penggunaan metode 2-wrap length untuk menentukan file teks yang akan disisipkan pesan.Metode ini didasari oleh konsep seperti file teks akan dikonversi ke bilangan ASCII untuk diubah menjadi bilangan biner. Proses selanjutnya yaitu menambahkan karakter non-breaking space untuk membuat file baru yang secara kasat mata akan tampak mirip dengan file aslinya.

Daftar Pustaka

[1] Y. Aditya, A. Pratama, and A. Nurlifa, "Studi pustaka untuk steganografi dengan beberapa metode," *Semin. Nas. Apl. Teknol. Inf. 2010 (SNATI 2010)*, vol. 2010, no. Snati, pp. 32–35, 2010.

[2] M. Arief, Bramanto Wicaksono Putra, Royke Vincentius Febriana, "Penyisipan Pesan Teks pada Citra Menggunakan Metode LSB dan 2-Wrap Length," *Semin. Nas. APTIKOM*, pp. 536–543, 2019.

[3] S. Sembiring, "Menyisipkan Pesan Teks Pada Gambar Dengan Metode End of File," *Pelita Inform. Budi Darma*, vol. IV, pp. 45–51, 20AD.

[4] E. Handayani, W. L. Pratitis, A. Nur,) Syaifudin, A. Mashuri, and B. Nugroho, "Perancangan Aplikasi Kriptografi Berbasis Web Dengan Algoritma Double Caesar Cipher Menggunakan Tabel Ascii," *Semnasteknomedia Online*, vol. 5, no. 1, pp. 1-2–241, 2017, [Online]. Available: https://ojs.amikom.ac.id/index.php/semnasteknomedia/article/view/1628

ISSN 2686-4797
Jurnal Restikom : Riset Teknik Informatika dan Komputer
Vol. 4., No. 1, April 2022, pp. 28-35

[5] U. Amri, I. G. P. S. Wijaya, and F. Bimantoro, "Steganografi Menggunakan Metode Pencocokan LSB dan Karakter Non-Breaking Space Sebagai Penanda Pesan," *J. Comput. Sci. Informatics Eng.*, vol. 1, no. 1, p. 23, 2018, doi: 10.29303/jcosine.v1i1.18.