

Implementasi Steganografi Zero-Width Character pada Social Media

Dimas Bagoes Hendrianto^{1,2}

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

¹13522112@std.stei.itb.ac.id, ²dimasbagoes1954@gmail.com

Abstrak—Steganografi merupakan teknik penyembunyian informasi dengan cara menyisipkan pesan rahasia ke dalam media pembawa sehingga keberadaan pesan tersebut tidak mudah terdeteksi. Salah satu pendekatan steganografi teks yang berkembang adalah penggunaan *Zero-Width Character* (ZWC), yaitu karakter Unicode yang tidak memiliki representasi visual namun tetap diproses oleh sistem teks. Penelitian ini membahas implementasi steganografi berbasis *Zero-Width Character* pada media sosial sebagai sarana penyembunyian pesan rahasia dalam teks yang terlihat normal bagi pengguna umum. Metode yang diusulkan bekerja dengan mengonversi pesan rahasia menjadi representasi biner, kemudian memetakan bit-bit tersebut ke dalam karakter *Zero-Width* tertentu yang disisipkan pada teks pembawa. Proses ekstraksi dilakukan dengan mendeteksi dan mengonversi kembali karakter *Zero-Width* yang tersembunyi menjadi pesan asli. Hasil implementasi menunjukkan bahwa teknik ini mampu menyembunyikan informasi tanpa mengubah tampilan visual teks pada media sosial, sehingga sulit dideteksi secara kasat mata. Penelitian ini diharapkan dapat memberikan gambaran mengenai potensi dan keterbatasan steganografi teks berbasis *Unicode* dalam lingkungan media sosial modern.

Kata Kunci—media sosial, steganografi, teks, unicode, zero-width character

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong meningkatnya penggunaan media sosial sebagai sarana utama dalam pertukaran informasi berbasis teks. Platform media sosial tidak hanya digunakan untuk komunikasi sehari-hari, tetapi juga untuk berbagi opini, data, dan berbagai bentuk informasi digital lainnya. Namun, keterbukaan media sosial juga menimbulkan berbagai permasalahan, terutama terkait dengan keamanan informasi, privasi pengguna, serta potensi penyalahgunaan data.

Salah satu pendekatan yang dapat digunakan untuk melindungi informasi adalah steganografi. Steganografi merupakan teknik penyembunyian pesan rahasia di dalam media pembawa sehingga keberadaan pesan tersebut tidak dapat dikenali secara langsung. Berbeda dengan kriptografi yang berfokus pada penyamaran isi pesan, steganografi menekankan pada penyamaran keberadaan pesan itu sendiri. Dengan demikian, steganografi dapat menjadi solusi alternatif dalam menjaga kerahasiaan

komunikasi di lingkungan digital yang terbuka.

Pada steganografi berbasis teks, tantangan utama terletak pada keterbatasan kapasitas media pembawa serta tingginya kemungkinan perubahan format teks akibat proses normalisasi oleh sistem. Salah satu teknik yang berkembang untuk mengatasi keterbatasan tersebut adalah pemanfaatan *Zero-Width Character* (ZWC). *Zero-Width Character* merupakan karakter Unicode yang tidak memiliki lebar visual dan tidak memengaruhi tampilan teks, namun tetap dikenali oleh sistem pemrosesan teks. Karakter ini memungkinkan penyisipan informasi tambahan tanpa mengubah bentuk visual teks yang ditampilkan kepada pengguna.

Media sosial menjadi media yang menarik untuk penerapan steganografi berbasis *Zero-Width Character* karena sebagian besar platform mendukung Unicode dan memungkinkan pertukaran teks secara bebas. Dengan memanfaatkan karakter *Zero-Width*, pesan rahasia dapat disisipkan ke dalam teks seperti caption, komentar, atau pesan singkat tanpa menimbulkan kecurigaan. Namun demikian, setiap platform media sosial memiliki kebijakan dan mekanisme pemrosesan teks yang berbeda, sehingga berpotensi memengaruhi keberhasilan penyisipan dan ekstraksi pesan steganografi.

Berdasarkan latar belakang tersebut, diperlukan kajian mengenai implementasi steganografi *Zero-Width Character* pada media sosial, termasuk mekanisme penyisipan, proses ekstraksi, serta potensi dan keterbatasannya dalam lingkungan media sosial modern.

II. TEORI DASAR

A. Steganografi

Steganografi merupakan teknik sekaligus seni penyembunyian pesan rahasia ke dalam suatu media pembawa (*cover media*) sehingga keberadaan pesan tersebut tidak dapat dideteksi secara kasat mata. Tujuan utama steganografi bukan untuk menyamarkan isi pesan, melainkan untuk menyamarkan keberadaan pesan itu sendiri. Dengan demikian, pihak yang tidak berwenang tidak menyadari bahwa di dalam media tersebut terdapat informasi tersembunyi^[1].

Secara umum, sistem steganografi terdiri dari tiga komponen utama, yaitu *cover object*, *secret message*,

dan *stego object*. *Cover object* merupakan media pembawa yang digunakan untuk menyisipkan pesan, seperti teks, citra, audio, atau video. *Secret message* adalah pesan rahasia yang akan disembunyikan, sedangkan *stego object* merupakan hasil akhir setelah proses penyisipan pesan ke dalam media pembawa [1].

Berdasarkan jenis media pembawanya, steganografi dapat diklasifikasikan menjadi beberapa kategori, antara lain steganografi citra, steganografi audio, steganografi video, dan steganografi teks. Steganografi citra merupakan jenis yang paling banyak dikembangkan karena citra digital memiliki redundansi data yang cukup besar. Namun demikian, steganografi teks memiliki karakteristik tersendiri yang menjadi tantangan karena keterbatasan redundansi dan tingginya sensitivitas terhadap perubahan karakter [1].

Dalam steganografi teks, penyisipan pesan seringkali dilakukan dengan memanfaatkan karakteristik tertentu dari teks, seperti spasi, format huruf, struktur kalimat, atau karakter khusus. Salah satu pendekatan modern dalam steganografi teks adalah pemanfaatan karakter *Unicode* yang tidak terlihat secara visual, seperti *Zero-Width Character*. Pendekatan ini memungkinkan penyisipan informasi tanpa mengubah tampilan teks secara visual, sehingga tingkat keterdeteksian menjadi sangat rendah.

Keberhasilan suatu metode steganografi umumnya diukur berdasarkan tiga kriteria utama, yaitu kapasitas (*capacity*), ketahanan (*robustness*), dan ketakterdeteksian (*imperceptibility*). Kapasitas menunjukkan jumlah data yang dapat disisipkan ke dalam media pembawa. Ketahanan berkaitan dengan kemampuan pesan tersembunyi untuk tetap dapat diekstraksi meskipun media pembawa mengalami perubahan atau pemrosesan ulang. Sementara itu, ketakterdeteksian mengacu pada sejauh mana keberadaan pesan tersembunyi sulit dibedakan dari media asli [1].

Selain steganografi, terdapat pula bidang kajian yang disebut steganalisis. Layaknya kriptanalisis dalam konteks kriptografi, steganalisis bertujuan untuk mendeteksi apakah suatu media mengandung pesan tersembunyi atau tidak. Keberadaan steganalisis menuntut metode steganografi untuk terus dikembangkan agar semakin sulit dideteksi oleh analisis visual maupun statistik [3].

B. *Unicode* dan *Zero-Width Character*

Unicode merupakan standar pengkodean karakter universal yang dirancang untuk merepresentasikan teks dari berbagai bahasa dan sistem penulisan di dunia secara konsisten. Standar ini memungkinkan berbagai platform dan sistem operasi untuk memproses teks multibahasa dalam satu representasi karakter yang sama [4]. *Unicode* tidak hanya

mencakup karakter yang terlihat secara visual atau kasat mata, tetapi juga karakter kontrol dan karakter khusus yang memiliki fungsi tertentu dalam pemrosesan teks.

Salah satu kelompok karakter khusus dalam *Unicode* adalah *Zero-Width Character*. *Zero-Width Character* merupakan karakter yang tidak memiliki lebar visual dan tidak memengaruhi tampilan teks ketika dirender, namun tetap diproses oleh sistem sebagai bagian dari string teks [4]. Contoh *Zero-Width Character* yang umum digunakan antara lain *Zero Width Space* (U+200B), *Zero Width Non-Joiner* (U+200C), *Zero Width Joiner* (U+200D), dan *Word Joiner* (U+2060).

Karakter-karakter tersebut pada awalnya dirancang untuk mendukung tata letak dan penyambungan huruf pada bahasa tertentu, seperti bahasa Arab dan bahasa dengan sistem ligatur. Namun, sifatnya yang tidak terlihat secara visual menjadikan *Zero-Width Character* sangat potensial untuk dimanfaatkan dalam steganografi teks. Dengan memanfaatkan *Zero-Width Character*, informasi rahasia dapat disisipkan tanpa mengubah tampilan visual teks, sehingga sulit dideteksi oleh pengguna biasa maupun pengamat kasat mata.

C. Steganografi Teks pada Media Sosial

Steganografi teks pada media sosial memanfaatkan teks yang dipublikasikan pada platform daring sebagai media pembawa pesan tersembunyi. Media sosial mendukung pertukaran teks berbasis *Unicode* dan memungkinkan pengguna untuk mempublikasikan konten dalam jumlah besar, sehingga menyediakan lingkungan yang sesuai untuk penerapan steganografi teks [5].

Pemanfaatan *Zero-Width Character* pada media sosial memungkinkan penyisipan pesan rahasia pada teks seperti caption, komentar, atau pesan langsung tanpa mengubah tampilan visualnya. Pesan tersembunyi tetap dapat dibawa dan disebarkan selama teks tersebut tidak mengalami proses normalisasi atau penghapusan karakter khusus. Dengan demikian, media sosial dapat berfungsi sebagai saluran komunikasi tersembunyi yang tidak mencolok.

Namun demikian, penerapan steganografi teks pada media sosial memiliki keterbatasan. Beberapa platform menerapkan mekanisme pemrosesan teks seperti normalisasi *Unicode*, penyaringan karakter tertentu, atau pemangkasan karakter yang dianggap tidak relevan. Proses ini berpotensi menghapus atau merusak karakter *Zero-Width* sehingga pesan tersembunyi tidak dapat diekstraksi kembali. Oleh karena itu, pengujian terhadap perilaku masing-masing platform media sosial menjadi aspek penting dalam implementasi steganografi *Zero-Width Character*.

D. Steganalisis sebagai Ancaman Steganografi

Steganalisis merupakan bidang kajian yang bertujuan untuk mendeteksi keberadaan pesan tersembunyi dalam suatu media. Berbeda dengan kriptanalisis yang berfokus pada pemecahan isi pesan terenkripsi, steganalisis berfokus pada identifikasi apakah suatu media mengandung pesan rahasia atau tidak [3].

Secara umum, steganalisis dapat diklasifikasikan menjadi dua pendekatan utama, yaitu *targeted steganalysis* dan *blind steganalysis*. *Targeted steganalysis* dirancang untuk mendeteksi metode steganografi tertentu, sedangkan *blind steganalysis* tidak bergantung pada algoritma penyisipan tertentu dan umumnya memanfaatkan analisis statistik serta pembelajaran mesin [3].

Keberadaan teknik steganalisis mendorong pengembangan metode steganografi yang semakin halus dan sulit terdeteksi. Steganografi berbasis *Zero-Width Character* memiliki keunggulan dalam hal ketakterlihatan secara visual, namun tetap berpotensi terdeteksi melalui analisis karakter *Unicode* atau inspeksi struktur teks secara mendalam. Oleh karena itu, pemahaman terhadap steganalisis menjadi penting dalam merancang sistem steganografi teks yang lebih aman dan efektif [6].

E. Representasi Biner dan Proses Encoding Pesan

Dalam steganografi digital, pesan rahasia umumnya direpresentasikan dalam bentuk biner sebelum dilakukan proses penyisipan. Representasi biner diperlukan karena sebagian besar teknik steganografi bekerja pada level bit untuk mempermudah pemetaan antara pesan rahasia dan media pembawa. Teks, gambar, maupun data digital lainnya pada dasarnya dapat direpresentasikan sebagai deretan bit melalui proses pengkodean tertentu [1].

Pada steganografi teks berbasis *Zero-Width Character*, pesan rahasia terlebih dahulu dikonversi ke dalam kode biner menggunakan standar pengkodean karakter seperti ASCII atau UTF-8. Setiap bit atau kelompok bit kemudian dipetakan ke karakter *Zero-Width* tertentu. Sebagai contoh, satu jenis *Zero-Width Character* dapat merepresentasikan bit '0', sedangkan karakter *Zero-Width* lainnya merepresentasikan bit '1'.

Proses encoding dilakukan dengan menyisipkan karakter *Zero-Width* di antara karakter teks normal, seperti di antara huruf atau kata. Karena karakter *Zero-Width* tidak memiliki representasi visual yang terlihat kasat mata, penyisipan ini tidak mengubah tampilan teks yang dihasilkan. Pada sisi penerima, proses decoding dilakukan dengan mengekstraksi karakter *Zero-Width* dari teks, kemudian mengonversinya kembali ke bentuk biner dan selanjutnya ke pesan asli.

F. Karakteristik dan Kriteria Evaluasi Steganografi Teks

Evaluasi terhadap metode steganografi diperlukan untuk menilai efektivitas dan keamanannya. Secara umum, terdapat beberapa kriteria utama yang digunakan untuk mengevaluasi sistem steganografi, yaitu kapasitas (*capacity*), ketakterdeteksian (*imperceptibility*), dan ketahanan (*robustness*) [1].

Kapasitas menunjukkan jumlah maksimum data rahasia yang dapat disisipkan ke dalam media pembawa tanpa menimbulkan perubahan yang mencolok. Pada steganografi teks berbasis *Zero-Width Character*, kapasitas relatif terbatas karena jumlah karakter *Zero-Width* yang dapat disisipkan harus disesuaikan dengan panjang teks pembawa.

Ketakterdeteksian mengacu pada sejauh mana keberadaan pesan tersembunyi sulit dikenali, baik secara visual maupun melalui analisis statistik. Metode berbasis *Zero-Width Character* memiliki tingkat ketakterdeteksian visual yang sangat tinggi karena tidak memengaruhi tampilan teks. Namun, metode ini tetap berpotensi terdeteksi melalui analisis karakter *Unicode* secara mendalam [3].

Ketahanan berkaitan dengan kemampuan pesan tersembunyi untuk bertahan terhadap perubahan atau pemrosesan ulang media pembawa. Dalam konteks media sosial, ketahanan dipengaruhi oleh kebijakan platform, seperti normalisasi *Unicode* atau penghapusan karakter tertentu. Oleh karena itu, aspek ketahanan menjadi faktor penting dalam implementasi steganografi *Zero-Width Character* pada media sosial [5].

III. ANALISIS PERMASALAHAN DAN DESAIN

A. Analisis Permasalahan

Perkembangan media sosial sebagai sarana komunikasi digital telah meningkatkan kebutuhan akan mekanisme pengamanan informasi, khususnya dalam konteks kerahasiaan komunikasi. Meskipun teknik kriptografi mampu melindungi isi pesan, keberadaan pesan terenkripsi itu sendiri masih dapat menimbulkan kecurigaan. Oleh karena itu, diperlukan pendekatan lain yang mampu menyembunyikan keberadaan pesan agar komunikasi dapat berlangsung secara terselubung.

Steganografi teks menjadi salah satu solusi untuk permasalahan tersebut karena memungkinkan penyisipan pesan rahasia ke dalam teks yang tampak normal. Namun, steganografi teks memiliki keterbatasan utama berupa rendahnya redundansi data pada teks, sehingga kapasitas penyisipan menjadi terbatas dan mudah terpengaruh oleh perubahan kecil pada media pembawa. Metode konvensional seperti manipulasi spasi atau perubahan format teks sering kali dapat terdeteksi secara visual atau dihapus oleh sistem pemrosesan teks.

Pemanfaatan karakter *Unicode*, khususnya *Zero-Width Character*, menawarkan solusi terhadap permasalahan ketakterlihatan dalam steganografi teks. Karakter *Zero-Width* tidak memiliki representasi visual namun tetap diproses sebagai bagian dari teks, sehingga memungkinkan penyisipan informasi tanpa mengubah tampilan teks. Meskipun demikian, penggunaan *Zero-Width Character* juga menghadapi tantangan, seperti kemungkinan terhapus akibat normalisasi *Unicode* atau kebijakan pemrosesan teks pada platform media sosial tertentu.

B. Kebutuhan Sistem

Berdasarkan analisis permasalahan tersebut, sistem steganografi yang dirancang harus memenuhi beberapa kebutuhan sebagai berikut:

1. Sistem mampu menyisipkan pesan rahasia ke dalam teks tanpa mengubah tampilan visual teks.
2. Sistem memanfaatkan karakter *Unicode* yang tidak terlihat untuk meningkatkan ketakterdeteksian.
3. Sistem dapat dijalankan secara mandiri tanpa bergantung pada platform media sosial tertentu.
4. Sistem mampu menerima masukan langsung dari pengguna melalui antarmuka terminal.

C. Desain Sistem

Desain sistem steganografi *Zero-Width Character* dibagi menjadi dua modul utama, yaitu modul *encoding* dan modul *decoding*. Pemisahan modul ini bertujuan untuk mensimulasikan penggunaan sistem dalam kondisi nyata, di mana pengirim dan penerima pesan berada pada sisi yang berbeda.

Modul *encoding* bertugas menerima teks pembawa dan pesan rahasia dari pengguna. Pesan rahasia kemudian dikonversi ke dalam representasi biner menggunakan pengkodean UTF-8. Setiap bit biner dipetakan ke karakter *Zero-Width* tertentu dan disisipkan ke dalam teks pembawa.

Modul *decoding* bertugas menerima teks stego yang mengandung karakter *Zero-Width*. Sistem melakukan pemindaian terhadap teks untuk mendeteksi karakter *Zero-Width* yang telah disisipkan. Karakter tersebut kemudian dikonversi kembali ke bentuk biner dan direkonstruksi menjadi teks asli.

D. Desain Antarmuka

Antarmuka sistem dirancang berbasis terminal untuk menjaga kesederhanaan dan fokus pada fungsi utama sistem. Modul *encoding* dan *decoding* masing-masing dijalankan melalui file Python terpisah, yaitu *encode.py* dan *decode.py*. Pengguna berinteraksi dengan sistem melalui

perintah terminal dan memasukkan teks pembawa, pesan rahasia, serta teks stego secara langsung.

Pendekatan berbasis terminal ini dipilih karena mudah diimplementasikan, portabel, dan memungkinkan sistem dijalankan di berbagai lingkungan tanpa memerlukan dependensi tambahan.

IV. IMPLEMENTASI

A. Gambaran Umum Sistem

Implementasi steganografi *Zero-Width Character* pada media sosial dilakukan dengan membangun sistem yang mampu menyisipkan dan mengekstraksi pesan rahasia dalam teks tanpa mengubah tampilan visual teks tersebut. Sistem ini dirancang agar pesan rahasia dapat dikirimkan melalui platform media sosial dalam bentuk teks yang terlihat normal bagi pengguna umum.

Secara umum, sistem terdiri dari dua proses utama, yaitu proses penyisipan pesan atau *embedding* dan proses ekstraksi pesan atau *extraction*. Proses penyisipan bertujuan untuk menyisipkan pesan rahasia ke dalam teks pembawa menggunakan karakter *Zero-Width*, sedangkan proses ekstraksi bertujuan untuk mengembalikan pesan rahasia dari teks yang telah disisipi.

B. Arsitektur Komponen

Arsitektur sistem steganografi *Zero-Width Character* terdiri dari beberapa komponen utama sebagai berikut:

1. Input Pesan Rahasia

Pesan rahasia berupa teks yang akan disembunyikan. Pesan ini dapat berupa kata, kalimat, atau informasi lain yang dikirimkan secara tersembunyi.

2. Teks Pembawa (*Cover Text*)

Teks pembawa merupakan teks normal yang akan dipublikasikan pada media sosial, seperti *caption* atau komentar.

3. Modul Encoding

Bertugas mengonversi pesan rahasia ke dalam bentuk biner dan memetakan setiap bit ke karakter *Zero-Width* tertentu.

4. Teks Stego (*Stego Text*)

Teks *output* atau hasil penyisipan karakter *Zero-Width* yang secara visual identik dengan teks pembawa.

5. Modul Decoding

Bertugas mendeteksi dan mengekstraksi karakter *Zero-Width* dari teks stego untuk mengembalikan pesan rahasia.

C. Proses Encoding

Proses *encoding* merupakan tahap penyisipan pesan rahasia ke dalam teks pembawa. Tahapan *encoding* yang diimplementasikan pada sistem ini adalah sebagai berikut:

1. Konversi Pesan ke Biner

```
Fungsi text_to_binary  
def text_to_binary(text):  
    return ''.join(format(byte, '08b') for byte in text.encode('utf-8'))
```

Gambar 4.1. Implementasi Fungsi text_to_binary
Sumber: Dokumentasi Pribadi

Pesan rahasia dikonversi ke dalam representasi biner menggunakan pengkodean karakter UTF-8. Setiap karakter diubah menjadi deretan bit.

2. Pemetaan Bit ke Zero-Width Character

```
ZWC_ZERO = '\u200b' # bit 0  
ZWC_ONE = '\u200c' # bit 1
```

Gambar 4.2. Pemetaan Bit ke Zero-Width Character
Sumber: Dokumentasi Pribadi

Pada implementasi ini digunakan dua jenis Zero-Width Character, yaitu:

- Zero Width Space (U+200B) untuk merepresentasikan bit 0
- Zero Width Non-Joiner (U+200C) untuk merepresentasikan bit 1

3. Penyisipan ke Teks Pembawa

```
Fungsi encode_message  
def encode_message(cover_text, secret_message):  
    binary_message = text_to_binary(secret_message)  
  
    zwc_sequence = ''  
    for bit in binary_message:  
        zwc_sequence += ZWC_ZERO if bit == '0' else ZWC_ONE  
  
    return cover_text + zwc_sequence
```

Gambar 4.3. Implementasi Fungsi encode_message
Sumber: Dokumentasi Pribadi

Karakter Zero-Width disisipkan di antara karakter teks pembawa, misalnya setelah setiap karakter atau setiap kata. Pola penyisipan ini ditentukan agar tidak mudah terdeteksi dan tetap konsisten saat proses decoding.

4. Pembentukan Teks Stego

Hasil dari proses penyisipan adalah teks stego yang secara visual tidak berbeda dari teks pembawa, namun mengandung pesan rahasia di dalamnya.

D. Proses Decoding

Proses decoding merupakan kebalikan dari proses encoding dan bertujuan untuk mengekstraksi pesan rahasia dari teks stego. Tahapan decoding meliputi:

1. Identifikasi Karakter Zero-Width

Sistem membaca teks stego dan mendeteksi keberadaan karakter Zero-Width yang digunakan dalam proses encoding.

2. Konversi Zero-Width ke Biner

```
Fungsi binary_to_text  
def binary_to_text(binary):  
    bytes_list = [binary[i:i+8] for i in range(0, len(binary), 8)]  
    byte_array = bytearray(int(b, 2) for b in bytes_list)  
    return byte_array.decode('utf-8', errors='ignore')
```

Gambar 4.4. Implementasi Fungsi binary_to_text
Sumber: Dokumentasi Pribadi

Setiap karakter Zero-Width yang terdeteksi dikonversi kembali ke bit biner sesuai dengan pemetaan yang telah ditentukan.

3. Rekonstruksi Pesan Rahasia

```
Fungsi decode_message  
def decode_message(stego_text):  
    binary_message = ''  
  
    for char in stego_text:  
        if char == ZWC_ZERO:  
            binary_message += '0'  
        elif char == ZWC_ONE:  
            binary_message += '1'  
  
    decoded_text = binary_to_text(binary_message)  
  
    return decoded_text
```

Gambar 4.5. Implementasi Fungsi decode_message
Sumber: Dokumentasi Pribadi

Deretan bit biner dikelompokkan kembali menjadi byte, kemudian dikonversi ke karakter teks menggunakan pengkodean UTF-8 sehingga diperoleh pesan rahasia asli.

E. Implementasi pada Media Sosial

Teks stego yang dihasilkan kemudian diuji dengan cara dipublikasikan pada platform media sosial berbasis teks. Implementasi difokuskan pada pengiriman pesan melalui caption atau komentar. Selama platform media sosial tidak melakukan penghapusan atau normalisasi karakter Zero-Width, pesan rahasia dapat diekstraksi kembali secara utuh.

Pada implementasi ini, sistem tidak memerlukan modifikasi khusus pada platform media sosial, karena seluruh proses penyisipan dan ekstraksi dilakukan pada sisi pengguna. Hal ini menjadikan metode steganografi Zero-Width Character fleksibel dan dapat diterapkan pada berbagai platform media sosial yang mendukung Unicode.

F. Batasan Implementasi

Implementasi sistem ini memiliki beberapa batasan, antara lain:

1. Kapasitas penyisipan bergantung pada panjang teks pembawa.
2. Karakter Zero-Width berpotensi dihapus oleh proses normalisasi teks pada platform tertentu.
3. Sistem belum dilengkapi dengan mekanisme enkripsi tambahan pada pesan rahasia.

V. PENGUJIAN

Pengujian dilakukan untuk mengevaluasi kinerja sistem steganografi *Zero-Width Character* yang telah diimplementasikan. Tujuan utama pengujian adalah untuk memastikan bahwa sistem mampu menyisipkan dan mengekstraksi pesan rahasia dengan benar tanpa mengubah tampilan visual teks pembawa. Selain itu, pengujian bertujuan untuk menilai ketahanan sistem terhadap proses penyalinan teks serta kompatibilitasnya dengan lingkungan media sosial.

A. Pengujian Sistem Dasar

Dilakukan untuk memastikan proses encoding dan decoding berjalan dengan benar.

```
PS C:\Dimas\Sem 7\Kriptografi\Makalah\Steganografi-ZWC> python encode.py
=== ENCODING STEGANOGRAFI ZERO-WIDTH CHARACTER ===
Masukkan cover text:
> Sekarang jam setengah sebelas

Masukkan pesan rahasia:
> X1xiX1xiX1xi

=== TEKS STEGO (SALIN UNTUK MEDIA SOSIAL) ===
Sekarang jam setengah sebelas
```

Gambar 5.1. Pengujian Dasar Encoding

Sumber: Dokumentasi Pribadi

```
PS C:\Dimas\Sem 7\Kriptografi\Makalah\Steganografi-ZWC> python decode.py
=== DECODING STEGANOGRAFI ZERO-WIDTH CHARACTER ===
Masukkan teks stego:
> Sekarang jam setengah sebelas

=== PESAN RAHASIA ===
X1xiX1xiX1xi
```

Gambar 5.2. Pengujian Dasar Decoding

Sumber: Dokumentasi Pribadi

B. Pengujian Kapasitas

Dilakukan untuk mengukur kapasitas atau ukuran pesan rahasia yang bisa disisipkan menjadi teks stego.

Tabel 5.1. Pengujian Kapasitas

Sumber: Dokumentasi Pribadi

No	Cover Message	Secret Message	Hasil Decoding	len(secret message)
1	test			4
2	test	a	a	12

3	test	aa	aa	20
4	test	aaa	aaa	28
5	test	aaaa	aaaa	36
6	test	aaaaa	aaaaa	44
7	test	aaaaaa	aaaaaa	52
8	test	aaaaaaa	aaaaaaa	60
9	test	aaaaaaaa	aaaaaaaa	68
10	test	aaaaaaaaa	aaaaaaaaa	76

C. Pengujian Media Sosial

Dilakukan untuk mengetahui apakah platform media social yang umum digunakan bisa digunakan untuk menyembunyikan pesan melalui teks stego dan pesan rahasia di dalamnya bisa diperoleh oleh orang lain juga. Pengujian menggunakan *cover message* yaitu “hallo” dan *secret message* yaitu “test”.

Tabel 5.2. Pengujian Media Sosial

Sumber: Dokumentasi Pribadi

No	Platform	Hasil Decoding	len(secret message)	Keutuhan
1	Whatsapp		5	Hilang
2	Instagram		5	Hilang
3	Youtube		6	Hilang
4	Line	test	37	Utuh
5	Discord	test	37	Utuh
6	TikTok		5	Hilang

VI. KESIMPULAN

Berdasarkan pengujian yang telah dilakukan, dapat disimpulkan bahwa metode steganografi teks berbasis *Zero-Width Character* mampu menyisipkan dan mengekstraksi pesan rahasia dengan baik pada lingkungan yang tidak melakukan normalisasi atau penghapusan karakter *Unicode* tertentu. Hasil pengujian kapasitas menunjukkan bahwa panjang pesan rahasia berbanding lurus dengan panjang internal teks stego. Setiap penambahan satu karakter pada pesan rahasia menyebabkan peningkatan panjang representasi tersembunyi, namun tidak mengubah tampilan visual teks stego secara kasat mata.

Pengujian kapasitas juga menunjukkan bahwa sistem mampu mengekstraksi pesan rahasia secara utuh selama teks stego tidak mengalami perubahan. Seluruh pengujian dengan variasi panjang pesan rahasia berhasil didekodekan dengan benar, yang menandakan bahwa mekanisme *encoding* dan *decoding*.

Pada pengujian media sosial, diperoleh hasil yang berbeda-beda antar platform. Platform seperti WhatsApp, Instagram, YouTube, dan TikTok tidak mampu mempertahankan karakter *Zero-Width Character*, sehingga pesan rahasia tidak dapat diekstraksi kembali dan dinyatakan hilang. Hal ini menunjukkan bahwa platform-platform tersebut melakukan normalisasi atau penyaringan karakter *Unicode* tertentu pada teks yang dipublikasikan atau dikirimkan.

Sebaliknya, platform Line dan Discord mampu mempertahankan karakter *Zero-Width Character* secara utuh. Pada kedua platform tersebut, pesan rahasia berhasil diekstraksi kembali tanpa kehilangan data, yang ditunjukkan oleh hasil decoding yang sesuai dengan pesan asli. Temuan ini menunjukkan bahwa keberhasilan steganografi berbasis *Zero-Width Character* sangat bergantung pada kebijakan pemrosesan teks yang diterapkan oleh masing-masing platform media sosial.

Secara keseluruhan, hasil pengujian membuktikan bahwa steganografi *Zero-Width Character* efektif digunakan sebagai metode penyembunyian pesan rahasia pada media sosial tertentu, khususnya platform yang tidak melakukan normalisasi *Unicode* secara agresif. Namun, metode ini memiliki keterbatasan pada platform yang secara aktif memodifikasi atau menghapus karakter *Unicode* tidak terlihat, sehingga penerapannya perlu mempertimbangkan karakteristik dan kebijakan masing-masing media sosial.

VII. UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas limpahan berkat dan kemurahan-Nya makalah ini dapat diselesaikan dengan baik. Penulis menyampaikan penghargaan dan terima kasih yang sebesar-besarnya kepada Bapak Dr. Ir. Rinaldi, M.T., selaku dosen pengampu mata kuliah IF4020 Kriptografi, atas ilmu, bimbingan, serta arahan yang telah diberikan sehingga penulis memperoleh pemahaman yang mendalam dalam menyusun makalah ini. Ucapan terima kasih juga penulis sampaikan kepada kedua orang tua yang senantiasa memberikan doa, dukungan, dan motivasi, sehingga penulis dapat menyelesaikan tugas ini dengan penuh kesungguhan. Penulis berharap makalah ini dapat memberikan manfaat bagi pembaca serta menjadi kontribusi kecil dalam pengembangan ilmu pengetahuan, khususnya di bidang kriptografi.

VIII. LAMPIRAN

Penulis telah berhasil melakukan implementasi fisik sistem yang dirancang, disertai dengan pengujian secara menyeluruh. Hasil implementasi tersebut telah didokumentasikan dan diarsipkan dalam sebuah tautan yang dapat diakses secara publik. Untuk keperluan uji coba maupun pengembangan lebih lanjut, pembaca dapat mengakses repositori GitHub penulis pada alamat berikut:

<https://github.com/dimasb1954/Steganografi-ZWC.git>

REFERENSI

- [1] R. Munir, "Steganografi (Bagian 1)," 2025. <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2025-2026/08-Steganografi-Bagian1-2025.pdf> (diakses pada 23 Desember 2025).
- [2] R. Munir, "Metode BPCS Steganography (Bit-Plane Complexity Segmentation)," 2025.

<https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2025-2026/09-Steganografi-Bagian2-BPCS-2025.pdf> (diakses pada 23 Desember 2025).

- [3] R. Munir, "Steganalisis," 2025. <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2025-2026/10-Steganografi-Bagian3-2025.pdf> (diakses pada 23 Desember 2025).
- [4] The Unicode Consortium, "The Unicode Standard," 2023. <https://www.unicode.org/standard/standard.html> (diakses pada 23 Desember 2025).
- [5] A. M. Kaplan dan M. Haenlein, "Users of the World, Unite! The Challenges and Opportunities of Social Media," *Business Horizons*, 2010. <https://www.sciencedirect.com/science/article/pii/S0007681309001232> (diakses pada 23 Desember 2025).
- [6] N. Provos dan P. Honeyman, "Detecting Steganographic Content on the Internet," 2002. <https://www.ndss-symposium.org/ndss2002/detecting-steganographic-content-internet/> (diakses pada 23 Desember 2025).

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 25 Desember 2025



Dimas Bagoes Hendrianto
13522112