Implementasi Steganografi Teks Menggunakan Unispach dan Fuzzy

1st Aditya Aulia Rohman
Program Studi Informatika
Universitas Telkom, Kampus Surabaya
Surabaya, Indonesia
adityaaar@student.telkomuniversity.ac.id

2nd Rizky Fenaldo Maulana, S.Kom., M.Kom.
Program Studi Informatika
Universitas Telkom, Kampus Surabaya
Surabaya, Indonesia
rizkyfenaldo@telkomuniversity.ac.id

3rd Tanzilal Mustaqim, S.Kom., M.Kom.
Program Studi Informatika
Universitas Telkom, Kampus Surabaya
Surabaya, Indonesia
tanzilal@telkomuniversity.ac.id

***Abstrak* — Keamanan informasi menjadi semakin penting di era digital, terutama dalam pertukaran data teks melalui jaringan terbuka. Steganografi teks menawarkan solusi dengan menyembunyikan pesan rahasia ke dalam dokumen sehingga tidak mudah terdeteksi. Metode Unispach dikenal memiliki kapasitas penyimpanan tinggi, namun pola penyisipannya yang dapat diprediksi menurunkan tingkat keamanannya. Penelitian ini mengusulkan sistem steganografi teks yang menggabungkan metode Unispach dengan logika fuzzy Mamdani untuk meningkatkan kerahasiaan dan adaptivitas penyisipan. Sistem menganalisis dokumen Microsoft Word untuk menghitung kepadatan dan jarak antar whitespace, lalu menentukan lokasi penyisipan optimal berdasarkan nilai prioritas dari sistem fuzzy dengan membership function trapezoidal. Karakter Unicode tak terlihat disisipkan pada lokasi terpilih sesuai hasil analisis fuzzy. Pengujian dilakukan terhadap dokumen dengan berbagai panjang teks dan pesan, serta dibandingkan dengan metode Unispach murni. Hasil menunjukkan bahwa metode gabungan ini mampu meningkatkan ketahanan pesan hingga 93% pada skenario optimal, tanpa mengorbankan efisiensi waktu penyisipan maupun ekstraksi. Penelitian ini menunjukkan bahwa integrasi logika fuzzy dalam metode Unispach dapat meningkatkan keamanan steganografi teks melalui pendekatan adaptif terhadap struktur dokumen.**

***Kata kunci*— steganografi teks, unispach, logika fuzzy, unicode, keamanan informasi, whitespace**

I. PENDAHULUAN

Pada era digital, data dengan volume besar dibuat, dikomunikasikan, dan disimpan secara elektronik, mencakup informasi yang bersifat pribadi, rahasia perusahaan, hingga data yang berkaitan dengan keamanan nasional. Ketika data ditransmisikan melalui jaringan terbuka, risikonya meningkat karena akses jaringan dapat dilakukan oleh siapa saja tanpa otorisasi, sehingga informasi menjadi rentan terhadap penyadapan dan modifikasi [1], [2]. Dalam konteks ini, steganografi teks menjadi salah satu metode proteksi data yang efektif dengan cara menyisipkan pesan rahasia ke dalam dokumen sehingga tidak terdeteksi secara langsung oleh pihak ketiga.

Sejumlah penelitian telah mengembangkan metode steganografi berbasis karakter, seperti *bit-level embedding* dan *duality form of Bengali characters*. Namun, metode-metode tersebut memiliki keterbatasan dari sisi kapasitas penyimpanan pesan [1]. Teknik Unispach hadir sebagai solusi alternatif yang menawarkan kapasitas tinggi dengan memanfaatkan struktur *whitespace* dalam teks seperti antar-kalimat, antar-kata, akhir baris, dan antar-paragraf. Meskipun demikian, pola penyisipan Unispach masih bersifat deterministik dan dapat diprediksi [2], yang menurunkan tingkat keamanan sistem.

Untuk mengatasi hal tersebut, penelitian ini mengusulkan penggabungan metode Unispach dengan logika fuzzy sebagai pendekatan adaptif dalam menentukan lokasi penyisipan pesan. Logika fuzzy memiliki kemampuan untuk meniru pengambilan keputusan manusia melalui pendekatan berbasis derajat keanggotaan dan penalaran yang tidak biner [3]. Dengan menerapkan logika fuzzy Mamdani, sistem dapat menganalisis karakteristik *whitespace* seperti kepadatan dan jarak antar spasi, kemudian menentukan lokasi penyisipan yang lebih tersembunyi dan kompleks secara dinamis.

Sejumlah studi sebelumnya telah menunjukkan bahwa kombinasi antara steganografi dan metode kecerdasan buatan seperti neural network dan logika fuzzy dapat meningkatkan keamanan dan ketahanan objek stego [3]. Oleh karena itu, penelitian ini bertujuan untuk merancang dan mengevaluasi sistem steganografi teks yang menggabungkan metode Unispach dan logika fuzzy, dengan fokus pada peningkatan kompleksitas pola penyisipan, kapasitas penyimpanan, serta ketahanan terhadap modifikasi dokumen. Penelitian ini dibatasi pada penyisipan pesan berbentuk teks dalam dokumen Microsoft Word (.docx) menggunakan karakter Unicode tak terlihat, dan tidak mencakup aspek enkripsi atau media lain selain teks.

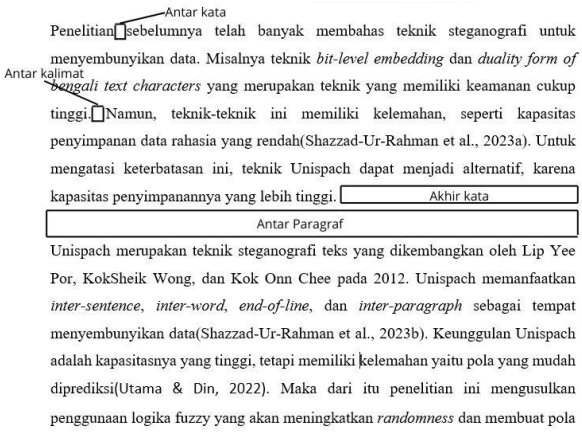
II. KAJIAN TEORI

A. Steganografi

Steganografi bisa didefinisikan sebagai seni dan ilmu menyembunyikan pesan rahasia di dalam cover object tanpa menimbulkan kecurigaan pihak penyerang. Cover object dapat berupa gambar, teks, video, audio, dll [4]. Steganografi teks merupakan sebuah metode steganografi yang menyembunyikan pesan rahasia berbentuk teks ke dalam teks lain (cover text) [5]. Tujuan utama steganografi adalah melindungi data rahasia dari pengguna yang seharusnya tidak punya akses. Hal ini membutuhkan dua komponen, yaitu data rahasia dan cover object untuk membuat objek stego [6]. Jadi cover object adalah media tempat menyembunyikan pesan rahasia yang belum 10 disisipi pesan rahasia tersebut, sedangkan objek stego adalah media yang sudah ada pesan rahasia di dalamnya. Pada penelitian ini cover object yang digunakan adalah file microsoft world.

B. Unispach

Unispach merupakan teknik steganografi teks yang memanfaatkan karakter Unicode Space tak terlihat untuk menyisipkan pesan rahasia ke dalam dokumen teks, khususnya file berformat Microsoft Word (.docx) [7]. Teknik ini menggunakan area whitespace sebagai lokasi penyisipan, mencakup empat jenis ruang antar: antar-kalimat (inter-sentence), antar-kata (inter-word), akhir baris (end-of-line), dan antar-paragraf (inter-paragraph). Gambar 1 menunjukan ilustrasi jenis ruang yang digunakan.



Gambar 1
Ilustrasi *whitespace*

Dari total 18 karakter *whitespace* yang tersedia dalam standar Unicode, Unispach secara selektif menggunakan 8 karakter yang tidak terlihat ketika fitur *show/hide* diaktifkan pada Microsoft Word. Namun, dalam penelitian ini hanya dipilih 4 karakter Unicode dengan lebar terkecil agar penyisipan lebih tersembunyi dan tidak memengaruhi tampilan dokumen secara signifikan, yaitu: *Hair Space*, *Six-Per-Em Space*, *Punctuation Space*, dan *Thin Space*.

Setiap karakter digunakan untuk menyandikan dua bit informasi biner. *Hair Space* merepresentasikan sekuen "00", *Six-Per-Em Space* untuk "01", *Punctuation Space* untuk "10", dan *Thin Space* untuk "11" [8]. Dengan demikian, pesan rahasia yang telah dikonversi ke dalam bentuk biner akan dibagi menjadi pasangan dua bit, yang kemudian diubah menjadi karakter Unicode tak terlihat. Karakter-karakter ini kemudian disisipkan ke lokasi *whitespace* dalam dokumen berdasarkan urutan penyisipan yang ditentukan oleh sistem.

C. Fuzzy

Logika fuzzy adalah pendekatan logika yang memungkinkan penalaran dengan nilai kebenaran yang bersifat kontinu antara 0 dan 1, berbeda dengan logika biner yang terbatas pada nilai absolut true dan false. Diperkenalkan pertama kali oleh Lotfi Zadeh pada tahun 1975, logika fuzzy digunakan untuk memodelkan ketidakpastian dan kompleksitas dalam pengambilan keputusan yang menyerupai cara berpikir manusia [9]. Kemampuan ini membuat logika fuzzy relevan untuk digunakan dalam sistem yang memerlukan seleksi lokasi penyisipan pesan secara adaptif, seperti dalam steganografi teks.

Dalam merancang sistem berbasis logika fuzzy, salah satu komponen penting adalah *membership function*, yaitu fungsi yang memetakan *input* numerik ke dalam nilai keanggotaan fuzzy. Penelitian ini menggunakan *trapezoidal membership function* karena fleksibilitasnya dalam membentuk representasi linguistik seperti rendah, sedang, dan tinggi. Fungsi ini didefinisikan dengan empat parameter: a, b, c, dan d, yang menentukan awal dan akhir dari sisi luar serta bagian datar pusat fungsi trapezoid [10].

Fuzzy Inference System (FIS) tipe Mamdani yang digunakan dalam penelitian ini terdiri dari empat komponen utama, yaitu fuzzifikasi, yaitu konversi *input* numerik ke dalam derajat keanggotaan fuzzy, basis aturan fuzzy, yang terdiri dari aturan IF-THEN berbasis logika linguistik, mesin penalaran, yang mengevaluasi aturan dan menghasilkan *output* fuzzy, dan defuzzifikasi, yaitu proses mengubah nilai fuzzy menjadi nilai *crisp* yang dapat diinterpretasikan dan diaplikasikan secara numerik.

Pada penelitian ini, sistem fuzzy digunakan untuk menentukan urutan lokasi penyisipan pesan yang optimal berdasarkan dua variabel utama, yaitu kepadatan *whitespace* dan jarak antar *whitespace*. Kepadatan *whitespace* dihitung sebagai rasio jumlah spasi terhadap total karakter dalam satuan teks, sedangkan jarak antar *whitespace* merupakan jumlah karakter di antara dua spasi. Masing-masing variabel memiliki tiga kategori keanggotaan, yaitu rendah, sedang, dan tinggi. *Output* dari sistem fuzzy adalah nilai prioritas yang menentukan seberapa cocok suatu lokasi dijadikan tempat penyisipan karakter Unicode. Sebanyak sembilan aturan fuzzy dirancang berdasarkan kombinasi dari dua variabel *input* tersebut. Tabel 1 menunjukkan aturan fuzzy yang digunakan dalam sistem.

Tabel 1
Aturan Fuzzy

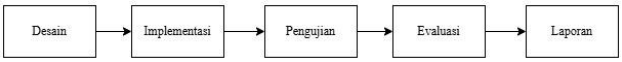
No	Kepadatan WS	Jarak Antar WS	Prioritas
1	Tinggi	Panjang	Tinggi
2	Tinggi	Sedang	Tinggi
3	Tinggi	Pendek	Sedang
4	Sedang	Panjang	Tinggi
5	Sedang	Sedang	Sedang
6	Sedang	Pendek	Rendah
7	Rendah	Panjang	Sedang
8	Rendah	Sedang	Rendah
9	Rendah	Pendek	Rendah

*WS = *Whitespace*

III. METODE

Gambar 2 menunjukkan alur penelitian yang menggambarkan tahapan-tahapan yang dilalui dalam proses

penelitian. Dimulai dengan tahap desain sistem yang melibatkan perancangan arsitektur steganografi teks yang menggabungkan metode Unispach dengan logika fuzzy Mamdani. Setelah itu, dilanjutkan dengan tahap implementasi yang mencakup pengembangan sistem menggunakan bahasa pemrograman Python. Kemudian dilakukan tahap pengujian untuk mengevaluasi kinerja sistem berdasarkan parameter kapasitas, kecepatan, dan ketahanan. Hasil pengujian kemudian dianalisis pada tahap evaluasi untuk menilai efektivitas metode yang dikembangkan dibandingkan dengan metode Unispach murni.



Gambar 2
Alur Penelitian

A. Perancangan Sistem Penyisipan Pesan

Proses penyisipan pesan rahasia dimulai dengan konversi pesan teks menjadi representasi biner menggunakan standar ASCII. Setiap karakter dikonversi menjadi 8-bit biner, kemudian dipasangkan menjadi kelompok 2-bit untuk dikodekan menggunakan empat karakter Unicode tak terlihat*:* *Hair Space* (00), *Six-Per-Em Space* (01), *Punctuation Space* (10), dan *Thin Space* (11).

Sistem kemudian menganalisis dokumen Microsoft Word (.docx) untuk mengidentifikasi lokasi *whitespace* potensial sebagai tempat penyisipan. Setiap lokasi dievaluasi berdasarkan dua parameter utama: kepadatan *whitespace* yang dihitung sebagai rasio jumlah spasi terhadap total karakter dalam unit teks, dan jarak antar *whitespace* yang merepresentasikan jumlah karakter di antara dua spasi berurutan.

Logika fuzzy Mamdani diimplementasikan dengan *membership function trapezoidal* untuk kedua variabel *input*. Kepadatan *whitespace* dikategorikan menjadi rendah (0-0.3), sedang (0.2-0.7), dan tinggi (0.6-1.0), sedangkan jarak antar *whitespace* diklasifikasikan sebagai pendek (0-4 karakter), sedang (3-7 karakter), dan panjang (6-10 karakter). Sistem fuzzy menggunakan sembilan aturan inferensi untuk menghasilkan nilai prioritas yang menentukan urutan lokasi penyisipan optimal.

B. Perancangan Sistem Ekstraksi Pesan

Proses ekstraksi melibatkan identifikasi dan ekstraksi karakter Unicode tak terlihat dari dokumen stego, kemudian konversi balik ke representasi biner dan diubah menjadi pesan teks asli. Sistem membaca dokumen secara berurutan untuk menemukan keempat jenis karakter Unicode yang digunakan, mengkonversinya kembali ke pasangan 2-bit sesuai dengan pemetaan Unispach, dan merekonstruksi pesan rahasia melalui konversi biner ke ASCII.

C. Skenario Pengujian dan Evaluasi

Evaluasi sistem dilakukan berdasarkan tiga parameter utama: kapasitas penyisipan, kecepatan proses, dan ketahanan terhadap modifikasi. Kapasitas diukur berdasarkan jumlah maksimum pesan yang dapat disisipkan sesuai dengan ketersediaan *whitespace* dalam dokumen. Kecepatan penyisipan dan ekstraksi dihitung menggunakan persamaan (1) dan (2):

$$KP = WSP - WMP \quad (1)$$

$$KE = WSE - WME \quad (2)$$

Dimana KP adalah kecepatan penyisipan, WSP adalah waktu selesai penyisipan, WMP adalah waktu mulai penyisipan, KE adalah kecepatan ekstraksi, WSE adalah waktu selesai ekstraksi, dan WME adalah waktu mulai ekstraksi.

Ketahanan sistem dievaluasi melalui pengujian modifikasi dokumen dengan menghapus 10 *whitespace* secara acak, kemudian mengukur akurasi bit (BA) menggunakan persamaan (3):

$$BA = \frac{Jumlah\ Bit\ yang\ Benar}{Jumlah\ Bit\ yang\ Disisipkan} \times 100\% \quad (3)$$

Pengujian dilakukan menggunakan tiga dokumen Microsoft Word dengan variasi ukuran (1000, 3000, dan 5000 karakter) dan tiga pesan rahasia dengan panjang berbeda (11, 100, dan 200 karakter). Setiap kombinasi dokumen dan pesan diuji untuk menganalisis performa sistem pada berbagai skenario beban kerja. Hasil pengujian dibandingkan dengan implementasi metode Unispach murni sebagai *baseline* untuk mengevaluasi peningkatan kinerja yang dicapai melalui integrasi logika fuzzy.

IV. HASIL DAN PEMBAHASAN

A. Implementasi Sistem

Sistem steganografi teks yang dikembangkan dalam penelitian ini terdiri dari tiga komponen utama, yaitu modul penyisipan pesan, modul ekstraksi pesan, dan antarmuka berbasis web. Seluruh proses dirancang untuk memanfaatkan keunggulan metode Unispach dalam kapasitas penyembunyian serta logika fuzzy dalam menentukan lokasi optimal penyisipan, sekaligus menghadirkan antarmuka yang sederhana untuk penggunaan praktis.

Pada proses penyisipan pesan, langkah pertama dimulai dengan konversi pesan rahasia ke dalam representasi biner 8-bit. Setiap dua bit dari hasil konversi ini kemudian diterjemahkan menjadi karakter Unicode tak terlihat menggunakan aturan Unispach. Karakter yang digunakan adalah *Hair Space*, *Six-per-em Space*, *Punctuation Space*, dan *Thin Space* yang masing-masing mewakili sekuen biner “00”, “01”, “10”, dan “11”.

Setelah dikonversi, sistem menganalisis dokumen Microsoft Word yang akan digunakan sebagai media penyisipan (*cover object*). Unit teks seperti kalimat, akhir baris (*end-of-line*), dan antar-paragraf diidentifikasi, lalu dihitung dua parameter penting: kepadatan *whitespace* dan jarak antar *whitespace*. Kedua parameter ini diproses dalam sistem fuzzy bertipe Mamdani untuk menentukan nilai prioritas penyisipan pada setiap unit teks. Lokasi dengan nilai prioritas tertinggi dipilih hingga kapasitas ruang mencukupi untuk menampung seluruh pesan. Karakter Unicode tak terlihat kemudian disisipkan ke lokasi terpilih, dengan menjaga urutan logis berdasarkan letak kemunculan dalam dokumen.

Pada proses ekstraksi pesan, sistem membalik seluruh langkah penyisipan. Pertama, seluruh karakter Unicode tak terlihat yang telah disisipkan dalam dokumen dibaca dan dikumpulkan. Karakter-karakter ini dikonversi kembali ke bit menggunakan pemetaan sebaliknya, lalu digabung menjadi rangkaian bit. Setiap 8-bit dari rangkaian tersebut diubah menjadi karakter ASCII untuk membentuk kembali pesan

asli. Keakuratan proses ekstraksi ini menjadi indikator keberhasilan utama sistem.

Untuk mendukung penggunaan praktis oleh pengguna non-teknis, sistem steganografi ini juga diimplementasikan dalam bentuk *website*. Terdapat dua halaman utama: halaman penyisipan dan halaman ekstraksi. Pada halaman penyisipan, pengguna dapat memilih *file* dokumen .docx, memasukkan pesan rahasia, lalu menekan tombol *Embed Secret Message* untuk memulai proses penyisipan. Halaman ekstraksi memungkinkan pengguna untuk mengunggah dokumen stego dan menampilkan kembali pesan rahasia yang tersembunyi setelah menekan tombol *Extract Hidden Message*. Antarmuka dirancang sederhana, intuitif, dan mendukung perpindahan cepat antar fitur melalui tombol navigasi di bagian atas.

B. Hasil Pengujian dan Evaluasi

Pengujian sistem dilakukan untuk mengevaluasi kinerja metode steganografi teks yang dikembangkan dengan mengukur tiga parameter utama: kapasitas penyisipan, kecepatan proses (penyisipan dan ekstraksi), serta ketahanan terhadap modifikasi. Dua metode dibandingkan: metode gabungan Unispach dan logika fuzzy, serta metode Unispach murni sebagai pembanding.

Pada pengujian menggunakan kombinasi Unispach dan logika fuzzy, hasil ditampilkan dalam Tabel 1. Tiga dokumen dengan panjang teks berbeda (1000, 3000, dan 5000 karakter) digunakan sebagai media uji, dan masing-masing diuji dengan tiga panjang pesan rahasia (11, 100, dan 200 karakter). Hasil pengujian menunjukkan bahwa sistem mampu menyesuaikan lokasi penyisipan berdasarkan prioritas fuzzy, dengan waktu penyisipan dan ekstraksi yang tetap relatif cepat meskipun ukuran pesan meningkat.

Tabel 2
Hasil Pengujian Metode Unispach dan Fuzzy

Nama *file*	**Panjang *Cover Text* (Karakter)**	**Kapasitas (Unicode)**	**Panjang Pesan rahasia (Karakter)**	**Waktu Penyisipan (ms)**	**Waktu Ekstraksi (ms)**	**Ketahanan**
cover_1	1000	433	11	137	9	85%
			100	136	9	64%
			200	138	11	43%
cover_2	3000	1076	11	206	10	90%
			100	209	10	65%
			200	210	11	57%
cover_3	5000	1731	11	335	14	93%
			100	337	11	81%
			200	333	14	63%

Ketahanan sistem terhadap perubahan juga tergolong tinggi pada pesan pendek, namun cenderung meningkat seiring bertambahnya ukuran dokumen dan panjang pesan rahasia yang disisipkan. Hal ini terjadi karena dokumen yang lebih panjang memiliki lebih banyak *whitespace*, memungkinkan distribusi karakter tak terlihat yang lebih merata. Ketahanan cenderung lebih tinggi pada pesan pendek dan dokumen besar karena penyisipan menjadi tersebar dan menyatu dengan struktur teks. Logika fuzzy terbukti membantu sistem dalam memilih lokasi yang optimal dan tersembunyi, sehingga meningkatkan resistensi terhadap perubahan seperti penghapusan atau pengeditan ringan.

Sebagai pembanding, metode Unispach murni diuji dengan skenario yang sama. Hasil pengujian disajikan pada Tabel 2. Meskipun proses penyisipan dan ekstraksi berjalan lebih cepat karena tidak melalui tahap evaluasi fuzzy, ketahanan sistem lebih rendah, terutama saat menangani pesan panjang. Hal ini disebabkan tidak adanya analisis struktur teks dalam penentuan lokasi penyisipan, sehingga posisi penyisipan menjadi kurang tersembunyi dan lebih mudah terdampak oleh modifikasi dokumen.

Tabel 3
Hasil Pengujian Metode Unispach

Nama *file*	**Panjang *Cover Text* (Karakter)**	**Kapasitas (Unicode)**	**Panjang Pesan rahasia (Karakter)**	**Waktu Penyisipan (ms)**	**Waktu Ekstraksi (ms)**	**Ketahanan**
cover_1	1000	433	11	42	11	65%
			100	48	10	52%
			200	51	10	56%
cover_2	3000	1076	11	45	11	75%
			100	55	10	58%
			200	75	10	58%
cover_3	5000	1731	11	50	10	95%
			100	64	11	60%
			200	80	11	62%

Pola peningkatan ketahanan tetap terlihat pada pesan sedang dan dokumen besar, namun secara umum sistem tanpa fuzzy lebih rendah ketahanannya. Perbandingan ini memperlihatkan bahwa komponen fuzzy berperan penting dalam meningkatkan ketahanan sistem.

Untuk menggambarkan dampak pada struktur dari proses penyisipan terhadap, Gambar 1 dan Gambar 2 memperlihatkan perbandingan antara *file* asli dan *file* stego setelah disisipkan pesan rahasia menggunakan metode Unispach dan fuzzy. *File* stego menunjukkan perubahan yang signifikan pada tata letak: kalimat-kalimat berpindah baris, terjadi pemenggalan kata secara tidak wajar, serta jarak antarbaris mengalami pergeseran. Perubahan ini terutama terjadi pada bagian akhir paragraf dan menjadikan dokumen terlihat tidak rapi secara visual.

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old. Richard McClintock a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage and going through the cites of the word in classical literature, discovered the undoubtable source.

Gambar 3
File Asli

Lorem Ipsum is simply dummy text of the printing and typesetting industry.
Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown pr
inter took a galley of type and scrambled it to make a type specimen book.
It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentiall
y unchanged.
It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, a
nd more recently with desktop publishing software like Aldus PageMaker including versions of Lorem I
psum.

Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old. Richard McClintock a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage and going through the cites of the word in classical literature, discovered the undoubtable source.

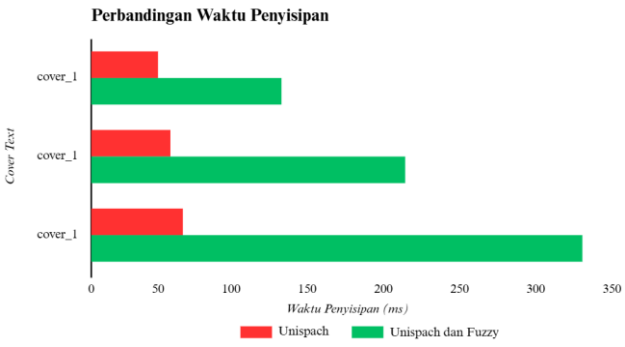
Gambar 4
File Stego

Penyebab utama dari distorsi ini adalah karakter Unicode tak terlihat seperti *Hair Space* dan *Thin Space* yang memengaruhi proses *rendering* oleh Microsoft Word. Meskipun tidak terlihat secara kasat mata, karakter-karakter ini memiliki lebar tertentu yang diinterpretasikan sebagai spasi tambahan, sehingga mengganggu format teks asli.

C. Pembahasan

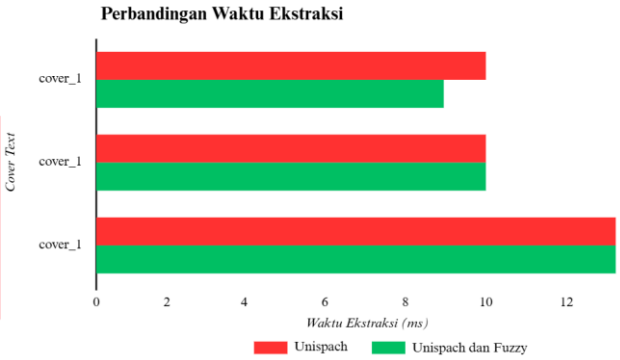
Hasil pengujian menunjukkan bahwa sistem mampu menyisipkan pesan rahasia ke dalam dokumen Microsoft Word (.docx) menggunakan karakter Unicode tak terlihat seperti *Hair Space*, *Six-Per-Em Space*, *Punctuation Space*, dan *Thin Space*. Lokasi penyisipan ditentukan secara adaptif berdasarkan dua parameter utama: kepadatan *whitespace* dan jarak antar *whitespace* yang diproses melalui sistem fuzzy Mamdani untuk menghasilkan nilai prioritas tiap kalimat dan *End of Line*nya (EOL).

Perbandingan performa metode Unispach murni dengan metode gabungan Unispach dan fuzzy divisualisasikan melalui tiga *bar chart*: Gambar 5 (waktu penyisipan), Gambar 6 (waktu ekstraksi), dan Gambar 7 (ketahanan pesan).



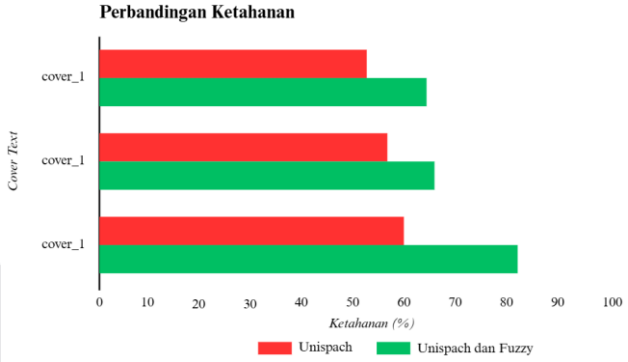
Gambar 5
Bar Chart Perbandingan Waktu Penyisipan

Grafik pada Gambar 5 menunjukkan bahwa metode Unispach dan fuzzy membutuhkan waktu penyisipan yang lebih tinggi dibandingkan metode Unispach murni. Hal ini disebabkan oleh proses tambahan berupa perhitungan kepadatan dan jarak antar *whitespace*, serta penilaian prioritas menggunakan fuzzy. Misalnya, pada *file cover_3*, metode dengan fuzzy mencatat waktu 337 ms, sedangkan metode murni hanya sekitar 64 ms. Penambahan waktu ini merupakan konsekuensi dari proses evaluasi yang lebih kompleks, namun berkontribusi terhadap pemilihan lokasi penyisipan yang lebih aman.



Gambar 6
Bar Chart Perbandingan Waktu Ekstraksi

Sebaliknya, pada Gambar 6 terlihat bahwa waktu ekstraksi antara kedua metode relatif sebanding dan tetap berada di kisaran 9–11 ms. Hal ini menunjukkan bahwa penggunaan logika fuzzy hanya berdampak pada tahap penyisipan, sementara ekstraksi tetap ringan dan cepat.



Gambar 7
Bar Chart Perbandingan Ketahanan

Gambar 7 memperlihatkan perbedaan dari segi ketahanan terhadap modifikasi. Metode Unispach dan fuzzy secara konsisten mencatat nilai ketahanan yang lebih tinggi dibandingkan metode murni. Sebagai contoh, pada *file cover_3*, ketahanan mencapai 81% untuk metode fuzzy, dibandingkan dengan 60% untuk metode Unispach saja. Peningkatan ini menunjukkan bahwa pemilihan lokasi berbasis fuzzy menghasilkan pola penyisipan yang lebih tersembunyi dan tidak mudah terganggu oleh modifikasi dokumen seperti penghapusan *whitespace*.

Secara keseluruhan, kombinasi Unispach dan fuzzy memang memerlukan waktu penyisipan yang lebih lama, tetapi memberikan peningkatan ketahanan sistem tanpa mengorbankan waktu ekstraksi. Dengan demikian, pendekatan ini sangat cocok untuk skenario yang

mengutamakan keamanan dan keandalan dibandingkan kecepatan penyisipan.

V. KESIMPULAN

Penelitian ini berhasil mengimplementasikan sistem steganografi teks berbasis kombinasi metode Unispach dan logika fuzzy. Sistem yang dikembangkan mampu mengonversi pesan teks menjadi karakter Unicode tak terlihat, kemudian menganalisis struktur dokumen untuk menghitung kepadatan dan jarak antar *whitespace*. Nilai-nilai tersebut digunakan sebagai *input* ke dalam sistem fuzzy Mamdani yang menghasilkan skor prioritas untuk setiap unit teks. Skor prioritas ini menentukan lokasi penyisipan secara adaptif, sehingga menghasilkan pola penyisipan yang lebih kompleks dan tidak mudah diprediksi.

Hasil pengujian menunjukkan bahwa sistem memiliki performa yang baik antara kapasitas, ketahanan, dan kecepatan. Pada dokumen dengan 5.000 karakter, sistem mampu menyisipkan hingga 1.731 karakter tak terlihat setara dengan metode Unispach murni namun dengan ketahanan yang lebih tinggi, yaitu mencapai 81% pada skenario optimal, dibandingkan 60% pada metode murni. Meskipun waktu penyisipan sedikit lebih lama akibat proses fuzzy, waktu ekstraksi tetap sama dan berada di bawah 12 milidetik. Dengan demikian, sistem ini tidak hanya mampu menyembunyikan pesan secara efektif, tetapi juga lebih tahan terhadap modifikasi dokumen.

REFERENSI

[1] M. Shazzad-Ur-Rahman, M. S. Kaiser, M. B. Alam, and S. N. Nova, “A Data Hiding Technique Combining Steganography and Cryptography for Secured Communication,” in *2023 International Conference on Information and Communication Technology for Sustainable Development, ICICT4SD 2023 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 432–437. doi: 10.1109/ICICT4SD59951.2023.10303563.

[2] S. Utama and R. Din, “Performance Review of Feature-Based Method in Implementation Text Steganography Approach,” *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 28, no. 2, pp. 325–333, Oct. 2022, doi: 10.37934/araset.28.2.325333.

[3] S. Dhawan *et al.*, “Secure and resilient improved image steganography using hybrid fuzzy neural network with fuzzy logic,” *Journal of Safety Science and Resilience*, vol. 5, no. 1, pp. 91–101, Mar. 2024, doi: 10.1016/j.jnlssr.2023.12.003.

[4] R. Thabit, N. I. Udzir, S. M. Yasin, A. Asmawi, and A. A. A. Gutub, “CSNTSteg: Color Spacing Normalization Text Steganography Model to Improve Capacity and Invisibility of Hidden Data,” *IEEE Access*, vol. 10, pp. 65439–65458, 2022, doi: 10.1109/ACCESS.2022.3182712.

[5] F. R. Shareef Taka, “Journal of Information Hiding and Multimedia Signal Processing Text Steganography based on Noorani and Darkness,” *Ubiquitous International*, vol. 12, no. 3, 2021.

[6] R. H. Ali and J. M. Kadhim, “Text-based Steganography using Huffman Compression and AES Encryption Algorithm,” *Iraqi Journal of Science*, vol. 62, no. 11, pp. 4110–4120, Nov. 2021, doi: 10.24996/ijs.2021.62.11.31.

[7] R. Adinugraha, T. W. Purboyo, and R. E. Saputra, “A PROPOSED MODIFIED TEXT STEGANOGRAPHY TECHNIQUE USING UNISPACH WITH XOR ENCRYPTION AND SHIFT CIPHER,” vol. 15, no. 8, 2020, [Online]. Available: www.arpnjournals.com

[8] L. Y. Por, K. Wong, and K. O. Chee, “UniSpaCh: A text-based data hiding method using Unicode space characters,” *Journal of Systems and Software*, vol. 85, no. 5, pp. 1075–1082, 2012, doi: 10.1016/j.jss.2011.12.023.

[9] H. H. Tang and N. S. Ahmad, “Fuzzy logic approach for controlling uncertain and nonlinear systems: a comprehensive review of applications and advances,” 2024, *Taylor and Francis Ltd.* doi: 10.1080/21642583.2024.2394429.

[10] R. Saatchi, “Fuzzy Logic Concepts, Developments and Implementation,” *Information (Switzerland)*, vol. 15, no. 10, Oct. 2024, doi: 10.3390/info15100656.