

Steganografi Linguistik pada Teks Bahasa Indonesia

Christine Hutabarat- NIM 13520005
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail : 13520005@std.stei.itb.ac.id

Abstrak— Steganografi linguistik adalah bidang yang memanfaatkan bahasa manusia untuk menyembunyikan pesan rahasia dalam teks sehari-hari, sehingga keberadaan pesan tersebut tidak dicurigai. Dalam makalah ini, telah dieksplorasi penggunaan *masked language model* (MLM) untuk steganografi pada teks bahasa Indonesia. MLM, seperti BERT, dilatih untuk memprediksi kata yang hilang berdasarkan konteks sekitarnya, memberikan kemampuan untuk menyisipkan pesan rahasia secara alami dalam teks. Dilakukan juga penyesuaian sistem steganografi sederhana yang menggunakan BERT untuk menyisipkan pesan biner ke dalam teks bahasa Indonesia. Sistem ini mengubah kata-kata tertentu menjadi sinonimnya yang diprediksi oleh model, berdasarkan skor prediksi yang melewati ambang batas tertentu. Penelitian ini menguji efektivitas metode ini dengan mempertimbangkan kealamian teks dan kapasitas penyisipan. Hasil penelitian menunjukkan bahwa pendekatan ini dapat menyembunyikan pesan dengan baik dalam teks bahasa Indonesia, meskipun diperlukan teks yang panjang dan ambang batas skor prediksi yang rendah untuk menyisipkan pesan yang besar. Dibahas juga tantangan dan peluang dalam pengoptimalan teknik ini, termasuk pengembangan model bahasa khusus dan strategi pembagian pesan. Makalah ini diharapkan dapat memberikan kontribusi dalam bidang keamanan informasi dan komunikasi rahasia, serta membuka arah baru untuk penelitian steganografi linguistik di masa depan.

Kata kunci—steganografi linguistik; bahasa Indonesia

I. PENDAHULUAN

Steganografi linguistik adalah ilmu menyembunyikan pesan rahasia di dalam bahasa manusia sehari-hari. Dalam era digital yang semakin maju, steganografi telah berkembang dan memanfaatkan banyak carrier seperti gambar, video, maupun audio digital yang dapat digunakan sebagai media penyembunyian pesan. Namun, selain media-media tersebut, bahasa merupakan salah satu alternatif penyembunyian pesan yang sangat menarik dan efektif. Bahasa manusia memiliki keragaman aksen, dialek, dan tata bahasa yang berbeda-beda di setiap wilayah, sehingga memberikan tantangan tersendiri dalam mendeteksi adanya pesan tersembunyi.

Hal ini menyebabkan sulitnya melakukan steganalisis pada bahasa, karena tidak mudah menemukan keanehan terutama pada bahasa sehari-hari yang selalu berubah dan berkembang. Bahasa Indonesia, dengan kekayaan kosakata dan nuansa yang dimilikinya, menjadi salah satu bahasa yang potensial untuk diterapkan steganografi linguistik. Dalam bahasa Indonesia,

pesan tersembunyi dapat disisipkan melalui berbagai cara, seperti penggunaan sinonim, variasi struktur kalimat, serta penggunaan idiom dan ungkapan khas. Keunikan ini membuat steganografi linguistik pada teks bahasa Indonesia menjadi topik yang menarik untuk dikaji lebih dalam.

Makalah ini akan membahas salah satu metode steganografi sederhana yang digunakan dalam steganografi linguistik pada teks bahasa Indonesia, mengeksplorasi teknik penyisipan pesan dan ekstraksi pesan, serta menganalisis efektivitas dan tantangan yang dihadapi dalam mendeteksi pesan tersembunyi. Melalui pemahaman yang lebih mendalam tentang steganografi linguistik, diharapkan dapat ditemukan cara-cara baru yang lebih aman dan efisien dalam melindungi informasi rahasia, sekaligus memperkaya wawasan tentang penggunaan bahasa sebagai alat komunikasi yang tidak hanya terbatas pada fungsi sehari-hari, tetapi juga sebagai sarana untuk keamanan informasi.

II. TEORI DASAR

A. Steganografi Linguistik

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia sedemikian sehingga keberadaan pesan tersebut tidak dicurigai [1]. Tujuan utama dari steganografi adalah untuk menghindari kecurigaan akan adanya pesan dari pihak ketiga. Terdapat banyak bentuk yang dapat dimanfaatkan untuk steganografi, seperti gambar digital, audio digital, hingga teks. Bahasa manusia adalah salah satu bentuk yang dinilai tepat untuk tujuan ini karena bahasa manusia lazim digunakan dan tidak mencurigakan [2].

Steganografi linguistik, khususnya, adalah cabang steganografi yang memanfaatkan bahasa sebagai media penyembunyian pesan. Terdapat tiga jenis utama steganografi linguistik yang menggunakan format teks: berbasis modifikasi, seleksi, dan pembangkitan kata [3]. Steganografi berbasis modifikasi menyembunyikan pesan tersembunyi dengan cara mengubah konten dari teks asli. Salah satu contoh sederhana dari metode ini adalah dengan mengubah beberapa kata dalam sebuah kalimat dengan sinonimnya. Misalnya, dalam kalimat “Saya ingin pergi ke pasar,” kata “pergi” dapat diubah menjadi sinonimnya, “berangkat,” sehingga dihasilkan *stegotext* “Saya ingin berangkat ke pasar.” Teknik ini memanfaatkan keragaman bahasa untuk menyamarkan pesan tanpa mengubah makna keseluruhan kalimat secara drastis.

Steganografi berbasis seleksi, di sisi lain, memanfaatkan korpus teks yang ada untuk memilih teks berdasarkan kata kunci dan label tertentu. Teknik ini memilih teks yang sudah ada yang mengandung kata kunci tertentu yang berkaitan dengan pesan yang ingin disembunyikan. Hal ini memungkinkan penyisipan pesan tanpa perlu mengubah teks asli secara signifikan, sehingga mengurangi risiko terdeteksinya pesan rahasia.

Sementara itu, steganografi berbasis pembangkitan kata umumnya menggunakan teknik *natural language processing* (NLP) untuk menyembunyikan pesan rahasia. Metode ini lebih kompleks dan melibatkan penggunaan algoritma NLP untuk menghasilkan teks yang secara alami menyisipkan pesan tersembunyi. Algoritma ini dapat membangkitkan teks yang koheren dan semantik yang sesuai dengan konteks asli, sehingga sangat sulit untuk mendeteksi adanya pesan tersembunyi tanpa mengetahui algoritma yang digunakan.

Ketiga jenis steganografi linguistik ini memiliki keunggulan dan tantangan masing-masing dalam hal keamanan dan deteksi. Steganografi berbasis modifikasi sederhana dan mudah diimplementasikan, namun rentan terhadap analisis linguistik yang mendalam. Steganografi berbasis seleksi menawarkan keamanan yang lebih tinggi karena teks asli tidak banyak berubah, tetapi memerlukan korpus teks yang besar dan relevan. Sedangkan steganografi berbasis pembangkitan kata menawarkan keamanan tertinggi dengan teks yang dihasilkan secara dinamis, namun memerlukan teknologi NLP yang canggih dan sumber daya komputasi yang besar.

B. Masked Language Model (MLM)

Masked language model adalah sebuah model bahasa yang dilatih untuk melakukan prediksi pada kata yang hilang berdasarkan konteks yang diberikan kata-kata di sekitarnya [4]. Kata yang ingin diprediksi ditandai dengan label seperti [MASK]. Sebagai contoh, jika diberikan kalimat “saya ingin [MASK] ke pasar”, maka salah satu kandidat kata yang sesuai untuk melengkapi kalimat tersebut adalah “pergi”. Salah satu contoh *masked language model* yang mutakhir adalah BERT (Bidirectional Encoder Representations from Transformers) [5].

BERT telah menunjukkan kinerja yang luar biasa dalam berbagai tugas pemrosesan bahasa alami (NLP) karena kemampuannya memahami konteks kata dalam kalimat secara dua arah. Penelitian yang dilakukan pada [6] menghasilkan sebuah sistem steganografi sederhana untuk bahasa Inggris yang memanfaatkan model BERT. Sistem tersebut menerima masukan *cover text* dalam bentuk *string* dan pesan rahasia dalam bentuk biner. Berdasarkan interval yang telah ditentukan, dilakukan *masking* pada setiap karakter yang bukan merupakan kata henti (*stopword*), tanda baca, angka, atau subkata non-inisial pada interval tersebut.

Untuk setiap *mask* kemudian dicari kandidat kata pengganti yang sesuai dengan konteks yang diberikan. Setiap kandidat kata pengganti kemudian diuji dan disaring berdasarkan skor prediksi yang melebihi ambang batas yang sudah ditentukan. Kata pengganti yang akhirnya dipilih merupakan kata pengganti pada daftar kandidat dengan indeks sesuai dengan

pesan rahasia. Berdasarkan algoritma tersebut, baik pengirim maupun penerima pesan harus memiliki dua variabel rahasia, yaitu interval dan nilai ambang batas skor prediksi.

Selain itu, penggunaan *masked language model* dalam steganografi menawarkan beberapa keunggulan. Pertama, kemampuan model untuk memahami dan memprediksi kata-kata dalam konteksnya memungkinkan penyisipan pesan yang lebih alami dan sulit dideteksi. Kedua, fleksibilitas dalam pemilihan kandidat kata pengganti memberikan variasi yang cukup besar, sehingga meningkatkan kerahasiaan dan keamanan pesan yang disembunyikan.

Penelitian lebih lanjut menunjukkan bahwa penggunaan BERT untuk steganografi dapat ditingkatkan dengan mengoptimalkan parameter model dan menyesuaikannya dengan karakteristik bahasa target. Selain itu, pengembangan model serupa untuk bahasa selain Inggris, seperti bahasa Indonesia, membutuhkan penyesuaian pada korpus data pelatihan dan teknik *masking* yang sesuai dengan struktur dan kaidah bahasa tersebut.

III. IMPLEMENTASI DAN ALGORITMA

Pada makalah ini, dilakukan adaptasi dari penelitian yang dilakukan oleh [6] agar bisa digunakan untuk steganografi teks bahasa Indonesia. Untuk itu, diperlukan beberapa perubahan. Perubahan pertama yang dilakukan terletak pada pemilihan model bahasa. Program steganografi sebelumnya menggunakan *BERT base model* [5]. Dengan banyaknya ketersediaan model BERT pada daftar model, dipilih salah satu model BERT untuk bahasa Indonesia [7]. Model ini berisi model yang sudah dilatih dengan menggunakan teks dari Wikipedia bahasa Indonesia sebesar 522MB. Terdapat 32000 kosakata yang terdapat pada *dataset*.

Selain mengubah model, dilakukan juga perubahan pada kata henti. Kata henti untuk bahasa Indonesia diambil dari pustaka *nlc* yang terdapat pada Python.

Adapun berikut merupakan langkah-langkah dari algoritma:

1. Masukan berupa *cover text* dan pesan rahasia biner diterima.

<p><i>Cover text:</i> Bunga yang kamu beli kemarin itu sangat indah namun saat ini sudah layu.</p> <p>Pesan rahasia: 1011</p>

2. Dilakukan *preprocessing* dengan mengubah semua huruf pada kalimat menjadi huruf kecil dan *masking* berdasarkan interval. Dimisalkan interval $i = 3$

bunga yang kamu [MASK] kemarin itu sangat indah namun saat ini sudah layu.

3. Dicari kandidat kata pengganti dengan misalkan skor minimal s 0.01 dan berdasarkan model BERT didapatkan enam belas kandidat yaitu 'mekar', 'lihat', 'tanam', 'kenal', 'beli', 'bunga', 'lakukan', 'temui', 'suka',

'sayang', 'jual', 'terima', 'cinta', 'simpan', 'alami', dan 'makan'.

4. Dihitung kapasitas dari kandidat, yaitu panjang bit dari jumlah kandidat dikurangi dengan satu sehingga didapatkan

$$\text{kapasitas} = \text{len}(10000 - 1)$$

$$\text{kapasitas} = \text{len}(1111) = 4$$

5. Karena kandidat memiliki kapasitas sebesar 4 bit, maka seluruh bit pada pesan rahasia dapat direpresentasikan dalam satu kata ganti. Nilai dari pesan rahasia adalah 11, sehingga dipilih kata ganti pada indeks ke-11 dari daftar kandidat.
6. Dipilih kata 'terima' untuk mengisi *mask* sehingga didapatkan *stegotext*

bunga yang kamu terima kemarin itu sangat indah namun saat ini sudah layu.

lain, perusahaan yang menaungi [MASK] itu sebetulnya sudah sejak 2021 melakukan phk secara bertahap.

Adapun pesan rahasia yang disisipkan adalah dengan panjang 31 bit.

10110010110001010100101110000001

Tabel 1 menunjukkan kapasitas yang dimiliki oleh teks menurut model BERT dengan variasi skor prediksi minimal. Nilai skor prediksi minimal yang mampu menampung seluruh pesan sebesar 0.000001 dengan kapasitas 32 bit. Dengan nilai ini, didapatkan *stegotext* berikut.

ristadi menjelaskan pabrik tersebut kapasitas jumlah karyawan yang mencapai anggota ribu orang. di provinsi lain, perusahaan yang menaungi product itu sebetulnya sudah sejak 2021 melakukan phk secara bertahap.

Tabel 1 Kapasitas dari variasi minimal skor prediksi untuk *cover text 1*

Skor prediksi minimal	Total kapasitas
0.01	3
0.005	6
0.001	9
0.0005	12
0.000001	32

Dilakukan juga eksperimen pada sebuah teks berita yang memiliki nama entitas. Skema eksperimen dan pesan rahasia sama dengan eksperimen teks sebelumnya. *Cover text* menghasilkan lima kata yang dapat dijadikan *carrier* pesan rahasia.

Cover text 2:

Sebagai komitmen pada literasi, Prastowo mengaku tidak mengkomersialkan digitalisasi itu dan semata untuk pendidikan publik. Dia juga memohon maaf kepada LP3ES karena tidak tahu bahwa isi buku itu ternyata sudah diterbitkan ulang sebagai bagian buku Karya Lengkap Bung Hatta (2018).

Masked text:

sebagai komitmen pada [MASK], prastowo mengaku tidak mengkomersialkan digitalisasi itu dan semata untuk pendidikan [MASK]. dia juga memohon maaf kepada lp3es karena tidak tahu bahwa [MASK] buku itu ternyata sudah diterbitkan [MASK] sebagai bagian buku karya [MASK] bung hatta (2018).

Kapasitas dari *cover text 2* berdasarkan skor prediksi minimal ditunjukkan pada Tabel 2. Nilai skor prediksi minimal yang mampu menampung seluruh besar adalah sebesar 0.0001 dengan kapasitas 38 bit. Nilai skor prediksi minimal tersebut menghasilkan *stegotext* seperti sebagai berikut.

Sementara itu, untuk mengekstrak pesan rahasia dari *stegotext*, dilakukan langkah-langkah berikut.

1. Masukkan berupa *stegotext* dan rahasia bersama berupa nilai *i* dan *s* adalah 3 dan 0.01 secara berurutan.

Stegotext:
bunga yang kamu terima kemarin itu sangat indah namun saat ini sudah layu.

2. Lakukan *masking* berdasarkan interval *i*.

bunga yang kamu [MASK] kemarin itu sangat indah namun saat ini sudah layu.

3. Cari kandidat kata pengganti berdasarkan model yang sudah disepakati bersama yaitu model BERT. Didapatkan kandidat adalah 'mekar', 'lihat', 'tanam', 'kenal', 'beli', 'bunga', 'lakukan', 'temui', 'suka', 'sayang', 'jual', 'terima', 'cinta', 'simpan', 'alami', dan 'makan'.
4. Diketahui bahwa kata yang digunakan adalah "terima" yang berada pada indeks ke-11. Representasi angka 11 dalam bentuk biner adalah 1011. Maka pesan rahasia didapatkan.

IV. EKSPERIMEN

Dilakukan eksperimen pada sebuah teks berita. Pada eksperimen akan dilakukan pengujian terhadap skor prediksi minimum dengan interval sebesar 3. Berikut merupakan *cover text* yang digunakan, diikuti dengan teks yang sudah dilakukan *masking*. *Cover text* menghasilkan empat kata yang dapat diubah dengan kata lainnya sebagai *carrier* pesan rahasia.

Cover text 1:

Ristadi menjelaskan pabrik tersebut memiliki jumlah karyawan yang mencapai puluhan ribu orang. Di sisi lain, perusahaan yang menaungi pabrik itu sebetulnya sudah sejak 2021 melakukan PHK secara bertahap.

Masked text:

ristadi menjelaskan pabrik tersebut [MASK] jumlah karyawan yang mencapai [MASK] ribu orang. di [MASK]

sebagai komitmen pada ip, prastowo mengaku tidak mengkomersialkan digitalisasi itu dan semata untuk pendidikan inti. dia juga memohon maaf kepada Ip3es karena tidak tahu bahwa tujuh buku itu ternyata sudah diterbitkan serentak sebagai bagian buku karya kader bung hatta (2018).

Tabel 2 Kapasitas dari variasi minimal skor prediksi untuk cover text 2

Skor prediksi minimal	Total kapasitas
0.01	13
0.005	16
0.001	27
0.0005	30
0.0001	38

Berdasarkan hasil eksperimen, diketahui bahwa untuk dapat menampung pesan rahasia sebesar 32 bit, dengan empat hingga lima kata yang menjadi *carrier*, diperlukan nilai minimal skor prediksi yang sangat kecil. Selain itu, karena penggunaan skor prediksi yang sangat rendah, kata ganti yang digunakan seringkali tidak sesuai dengan konteks aslinya, menghasilkan kalimat yang tidak alami atau bahkan terkesan tidak masuk akal. Sebagai contoh, pada *stegotext 2*, kata-kata pengganti yang dipilih oleh model tidak sesuai dengan struktur kalimat bahasa Indonesia yang benar, sehingga kalimat tersebut sulit dipahami oleh pembaca dan meningkatkan risiko deteksi steganografi.

V. KESIMPULAN DAN SARAN

Algoritma steganografi yang diajukan mampu menyisipkan pesan pada teks berbahasa Indonesia. Karena pesan rahasia yang diterima dalam bentuk bit, maka hampir seluruh format dokumen digital dapat disisipkan pada teks. Representasi biner dari sebuah dokumen memungkinkan fleksibilitas dalam menyembunyikan berbagai jenis informasi, mulai dari pesan teks sederhana hingga file kompleks seperti gambar, audio, dan video. Namun, tantangan utama dalam metode ini adalah ukuran dokumen yang direpresentasikan dalam bentuk biner sering kali sangat besar. Hal ini menyebabkan perlunya teks yang sangat panjang untuk menyembunyikan pesan tersebut secara efektif.

Selain itu, ketika ukuran pesan rahasia meningkat, kapasitas teks untuk menyisipkan bit-bit pesan harus diperhitungkan dengan cermat. Untuk mengatasi hal ini, ambang batas nilai skor prediksi perlu disesuaikan. Ambang batas yang cukup rendah memungkinkan lebih banyak kandidat kata pengganti yang bisa dipilih, sehingga meningkatkan kapasitas setiap mask untuk menyisipkan informasi. Dengan demikian, teks yang dihasilkan tidak hanya panjang, tetapi juga bervariasi secara linguistik, membantu menyamarkan pesan rahasia dengan lebih baik.

Namun, menurunkan ambang batas skor prediksi juga membawa risiko. Skor prediksi yang terlalu rendah dapat menyebabkan pemilihan kata pengganti yang kurang sesuai dengan konteks asli, yang bisa mengurangi kealamian teks dan

meningkatkan kemungkinan deteksi. Oleh karena itu, penting untuk menemukan keseimbangan yang tepat antara kapasitas penyisipan pesan dan kealamian teks.

Sistem steganografi pada teks berbahasa Indonesia dapat ditingkatkan dengan memperhatikan aspek tata bahasa secara lebih mendalam dan memilih kata-kata yang lebih mudah untuk diganti, seperti predikat dan objek dalam kalimat. Kata-kata yang mengandung nama orang, nama entitas, atau judul sebaiknya tidak diubah, karena perubahan pada kata-kata tersebut dapat mengganggu makna dan konteks kalimat secara keseluruhan. Dengan pendekatan ini, penggunaan interval untuk menentukan kata-kata yang akan diubah dapat dihindari, sehingga mengurangi risiko perubahan kata-kata yang merujuk pada entitas spesifik.

Pendekatan ini memungkinkan sistem untuk tetap mempertahankan kealamian dan kejelasan teks, menghindari kesalahan dalam penggantian kata-kata penting. Selain itu, diperlukan eksperimen lebih lanjut untuk menentukan nilai skor prediksi yang tepat untuk teks bahasa Indonesia. Hal ini penting agar teks yang dihasilkan tidak hanya mampu menampung pesan rahasia dengan baik tetapi juga tetap alami dan koheren. Eksperimen ini juga harus mencakup penentuan panjang teks yang optimal untuk dapat menampung seluruh pesan rahasia tanpa mengorbankan kualitas dan keterbacaan teks.

Di masa depan, penelitian harus mencakup evaluasi yang lebih komprehensif, termasuk penilaian oleh manusia untuk menilai kealamian dari stegotext yang dihasilkan. Evaluasi oleh penutur asli bahasa Indonesia sangat penting untuk memastikan bahwa teks yang dihasilkan tidak hanya memenuhi kriteria teknis tetapi juga terasa alami dan mudah dipahami oleh pembaca. Dengan demikian, diharapkan sistem steganografi linguistik yang lebih efektif dan efisien dapat dikembangkan, meningkatkan keamanan dan keandalan dalam menyembunyikan pesan rahasia dalam teks bahasa Indonesia. Selain itu, diharapkan bahwa steganalisis dari steganografi linguistik pada bahasa Indonesia juga dapat dilakukan.

REFERENSI

- [1] Rinaldi Munir, "Steganografi (Bagian 1)." Diakses: 6 Juni 2024. [Daring]. Tersedia pada: <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/07-Steganografi-Bagian1-2024.pdf>
- [2] Z. M. Ziegler, Y. Deng, dan A. M. Rush, "Neural Linguistic Steganography," Sep 2019, [Daring]. Tersedia pada: <http://arxiv.org/abs/1909.01496>
- [3] L. Xiang, R. Wang, dan Z. Yang, "Generative Linguistic Steganography: A Comprehensive Review," *KSII Transactions on Internet and Information Systems*, vol. 16, no. 3, Mar 2022, doi: 10.3837/tiis.2022.03.013.
- [4] "Masked Language Model in BERT - Scaler Topics." Diakses: 12 Juni 2024. [Daring]. Tersedia pada: <https://www.scaler.com/topics/nlp/masked-language-model-explained/>
- [5] J. Devlin, M.-W. Chang, K. Lee, dan K. Toutanova, "BERT: Pre-training of Deep Bidirectional

Transformers for Language Understanding,” dalam *Proceedings of the 2019 Conference of the North*, Stroudsburg, PA, USA: Association for Computational Linguistics, 2019, hlm. 4171–4186. doi: 10.18653/v1/N19-1423.

- [6] H. Ueoka, Y. Murawaki, dan S. Kurohashi, “Frustratingly Easy Edit-based Linguistic Steganography with a Masked Language Model,” Apr 2021, [Daring]. Tersedia pada: <http://arxiv.org/abs/2104.09833>
- [7] “cahya/bert-base-indonesian-522M · Hugging Face.” Diakses: 12 Juni 2024. [Daring]. Tersedia pada: <https://huggingface.co/cahya/bert-base-indonesian-522M>

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, 12 Juni 2024

Ttd

Christine Hutabarat 13520005

