Jurnal Quancom
Vol.4, No.1, Juni 2026, pp. 41~46
e-ISSN: 2988-0998
P-ISSN: 2988-1005
DOI : https://doi.org/10.62375/hd0wxe73

Penerapan Steganografi Teks dan File pada Citra PNG dan BMP sebagai Perlindungan Informasi

Aldo Darel[1], Artha Sitorus[2], Laura Pasaribu[3]
[123]Sarjana Terapan Teknologi Rekayasa Perangkat Lunak, Institut Teknologi Del
darellaldo2004@gmail.com

Article Info

Article history:

Received 23 Mei 2026
Revised 11 Juni 2026
Accepted 22 Juni 2026

Keyword:

Steganografi, Least Significant Bit, Keamanan Informasi, PNG, BMP.

ABSTRACT

Information security is an urgent need in today's digital era, especially to protect confidential data from unauthorized access. This research proposes the application of steganography using the Least Significant Bit (LSB) method to hide text and files in PNG and BMP format images. This steganography technique aims to disguise the presence of confidential information, making it difficult to detect by third parties. The LSB method allows the insertion of information without significantly reducing the visual quality of the image. The developed application allows users to insert a secret message into an image and extract the information easily. Test results from five experimental scenarios show that the application achieved an 80% success rate (4 of 5 trials) in maintaining data confidentiality and integrity, successfully hiding and extracting various file formats such as .txt, .docx, and .pdf, with the only failure occurring when the embedded file size exceeded the host image's capacity. It is hoped that, by using this method, increasingly complex information security challenges can be overcome and provide additional protection to the copyright of digital products.

PENDAHULUAN

Keamanan informasi telah menjadi kebutuhan yang semakin mendesak di era digital saat ini, terutama dalam melindungi data rahasia dari akses pihak yang tidak berwenang. Dalam berbagai proses komunikasi digital, data yang dikirim sering kali berisiko mengalami kebocoran, manipulasi, atau bahkan penyadapan. Hal ini menjadi tantangan besar bagi organisasi maupun individu dalam menjaga kerahasiaan informasi yang bersifat sensitif.

Salah satu solusi untuk mengatasi permasalahan ini adalah dengan memanfaatkan teknik steganografi, sebuah metode penyembunyian pesan rahasia dalam media penampung seperti gambar, video, atau audio, tanpa menyebabkan perubahan mencolok pada media tersebut. Berbeda dengan enkripsi yang membuat data tidak dapat dibaca oleh pihak lain, steganografi bertujuan untuk menyembunyikan keberadaan pesan itu sendiri[1]**.** Dalam bukunya Schneider (1996) menjelaskan bahwa steganografi adalah ilmu yang mempelajari teknik penyembunyian pesan rahasia di dalam pesan lainnya sedemikian rupa sehingga orang lain tidak akan mengetahui bahwa terdapat pesan rahasia di dalamnya[2].

Dalam implementasi digital, steganografi memerlukan dua elemen penting, yaitu wadah penampung dan data rahasia yang akan disembunyikan. Media digital seperti citra, suara, teks, dan video sering kali dimanfaatkan sebagai wadah karena sifatnya yang fleksibel dan memungkinkan penyisipan pesan rahasia tanpa terdeteksi[3]. Teknik ini memberikan keuntungan tambahan, yakni menyamarkan eksistensi data rahasia, sehingga sulit dideteksi oleh pihak lain. Selain sebagai alat perlindungan informasi, steganografi juga dapat digunakan untuk melindungi hak cipta suatu produk, dengan memberikan lapisan perlindungan tambahan di mana keberadaan data itu sendiri tidak terlihat[4].

Salah satu teknik yang populer dalam steganografi adalah metode Least Significant Bit (LSB). Algoritma ini sederhana

namun efektif, dengan cara menggantikan bit paling tidak signifikan pada data media digital untuk menyisipkan pesan rahasia. Format gambar seperti PNG dan BMP sering menjadi pilihan utama karena struktur datanya mendukung penyisipan informasi tanpa menurunkan kualitas visual secara signifikan. Teknik ini juga memungkinkan pesan rahasia disisipkan dan diungkap kembali melalui proses ekstraksi yang mudah diimplementasikan[5][6].

Python adalah salah satu bahasa pemrograman yang populer karena sintaksnya yang sederhana dan mudah dipahami. Sebagai bahasa yang ditulis secara dinamis dan bersifat terinterpretasi, Python dapat menjalankan kode secara langsung tanpa memerlukan proses kompilasi terpisah. Keunggulan utama Python adalah keterbacaannya, sehingga memudahkan pengembang untuk memahami dan menggunakan kode. Kemudahan belajar ini membuat Python menjadi pilihan yang tepat bagi pemula maupun profesional. Berkat fleksibilitasnya, Python banyak digunakan di berbagai bidang, seperti pengembangan web, analisis data, hingga kecerdasan buatan[7].

Penelitian ini bertujuan untuk mengembangkan aplikasi steganografi berbasis metode LSB pada media gambar berformat PNG dan BMP dengan menggunakan Bahasa pemrograman Python. Aplikasi ini dirancang untuk memungkinkan pengguna menyisipkan pesan rahasia ke dalam gambar secara aman tanpa mengurangi kualitas visual media tersebut, serta memberikan kemampuan untuk mengekstraksi kembali pesan yang telah disisipkan dengan akurat.

Melalui jurnal ini, diharapkan para peneliti, pengembang, dan praktisi di bidang keamanan informasi dapat meningkatkan pemahaman mereka mengenai steganografi gambar dengan pendekatan metode LSB serta mengaplikasikannya menggunakan bahasa pemrograman Python[8].

METODE

Teknik Steganografi dengan menggunakan metode Least Significant Bit (LSB) adalah teknik dengan pendekatan yang melakukan penyisipan informasi didalam suatu citra digital[9]. Untuk mencapai hasil yang diinginkan dalam penelitian ini, diperlukan kerangka penelitian yang sistematis. Kerangka ini dirancang untuk memastikan bahwa setiap tahapan dilakukan secara terstruktur dan terorganisir guna mendukung pencapaian tujuan penelitian secara optimal. Dalam bagian metodologi ini, akan dijelaskan tahapan-tahapan yang dilakukan dalam pengembangan aplikasi, mulai dari perancangan aplikasi, implementasi algoritma untuk penyisipan dan ekstraksi pesan, hingga teknologi yang digunakan untuk membangun aplikasi tersebut[10].

A. Gambaran Umum Aplikasi

Implementasi digital untuk menyembunyikan teks dan file dokumen ke dalam gambar berformat PNG dan BMP menggunakan metode LSB dalam penelitian ini mencakup dua kategori utama yaitu proses penyembunyian teks dan file dokumen dan proses ekstraksi teks dan file dokumen. Pada proses penyembunyian, terdapat fitur untuk memasukkan teks atau file dokumen ke dalam gambar dengan format .txt, .docx, .pdf. Gambar yang telah disisipkan ini menjadi keluaran aplikasi dan dapat disimpan ke komputer. Sementara itu, pada proses ekstraksi, pengguna dapat mengambil teks atau file dokumen rahasia yang disisipkan dalam gambar tersebut. Hasil ekstraksi akan berupa file dengan ekstensi .txt, .docx, atau .pdf, sesuai dengan jenis file yang disembunyikan[11].

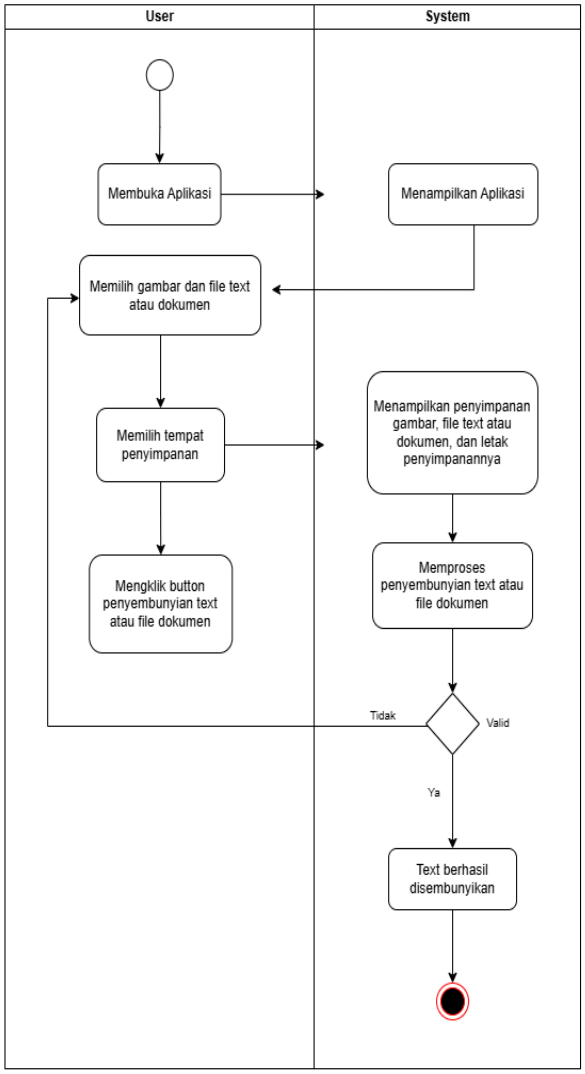
B. Analisa Kebutuhan

Pembuatan aplikasi Implementasi digital untuk menyembunyikan teks dan file dokumen ke dalam gambar berformat PNG dan BMP menggunakan metode LSB dalam penelitian ini membutuhkan perangkat keras dan perangkat lunak[12]. Adapun perangkat keras dan perangkat lunak yang dibutuhkan. Spesifikasi perangkat keras Processor Intel Core i5-1135G7, Processor (2.40GHz, 2419Mhz), RAM 8GB. Spesifikasi perangkat lunak Operating System Windows 11, visual studio code, menggunakan bahasa Python versi 3.11.5

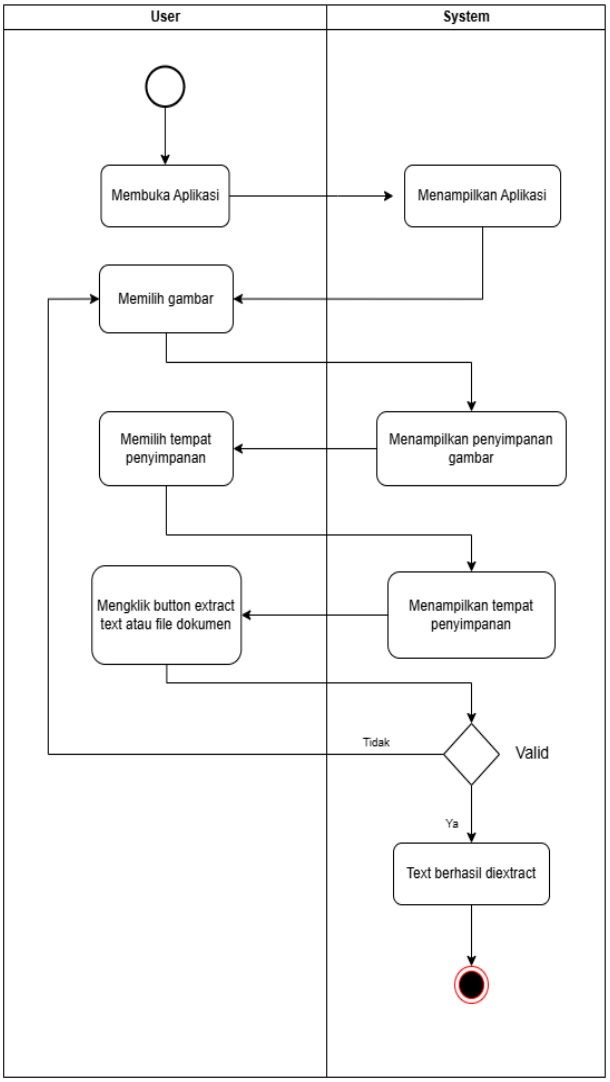
C. Alur Kerja Aplikasi

Alur kerja aplikasi untuk implementasi digital dalam menyembunyikan teks dan file dokumen ke dalam gambar berformat PNG dan BMP menggunakan metode LSB dapat digambarkan menggunakan diagram UML. Diagram UML yang digunakan yakni activity diagram untuk proses penyembunyian menggambarkan langkah- langkah penyembunyian teks berupa .txt dan file dokumen ke dalam gambar dan untuk proses ekstraksi menggambarkan langkah-langkah ekstraksi teks berupa .txt dan file dokumen dari gambar. Activity diagram penyembunyian ditunjukkan oleh Gambar 1. Activity diagram ekstraksi ditunjukkan oleh Gambar 2[13].

Diagram aktivitas adalah representasi yang menggambarkan berbagai proses yang berlangsung dalam sebuah sistem. Diagram ini berkaitan dengan diagram use case sebelumnya, yang mencakup proses pengkodean watermark dan penghapusan watermark[14]. Berikut adalah diagram aktivitas dari sistem yang telah dikembangkan:



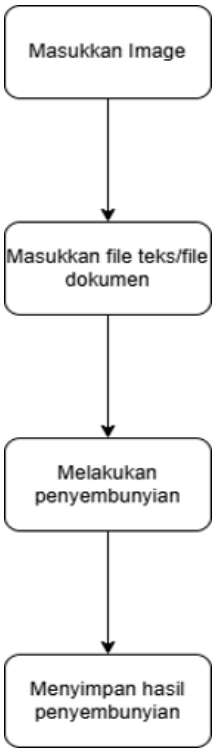
Gambar 1. Activity diagram penyembunyian



Gambar 2. Activity diagram ekstraksi

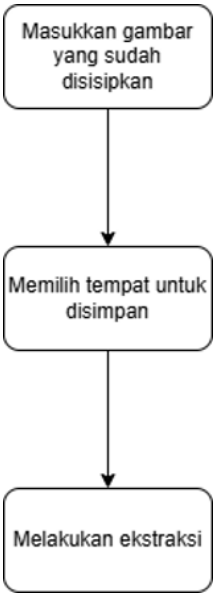
D. Prosedur Penggunaan Aplikasi

Penggunaan aplikasi ini meliputi 2 tahap yaitu menyembunyikan teks .txt dan file dokumen dan ekstraksi teks .txt dan file dokumen. Prosedur untuk menyembunyikan teks .txt dan file dokumen digambarkan dalam bentuk *flowchart* yang ditunjukkan pada Gambar 3. *Flowchart* yang dibuat dalam aplikasi ini adalah untuk menunjukkan representasi alur dan urutan dalam suatu prosedur penyelesaian masalah[15].



Gambar 3. Prosedur untuk Menyembunyikan Gambar

Selanjutnya prosedur ekstraksi gambar dalam aplikasi ini dapat dilihat pada flowchart yang ditunjukkan oleh



Gambar 4. Prosedur untuk Mengekstraksi Gambar

E. Perancangan Tampilan Aplikasi

Perancangan perangkat lunak adalah sebuah proses bertahap yang bertujuan untuk merancang pembuatan program, mencakup struktur data, arsitektur perangkat lunak, representasi antarmuka, serta prosedur pengkodean. Tahapan ini mengubah kebutuhan yang telah diidentifikasi menjadi representasi desain yang dapat diimplementasikan menjadi sebuah program. Rancangan halaman ini dapat dilihat pada gambar 5[16].

Gambar 5. Tampilan aplikasi

HASIL DAN PEMBAHASAN

A. Uji Coba Aplikasi

Dalam uji coba aplikasi terdapat 3 macam uji coba, yaitu uji coba penyisipan terhadap teks berupa .txt, penyembunyian terhadap file dokumen, penyembunyian teks berupa .txt dan file dokumen dengan ukuran yang berbeda-beda. Hasil uji coba terhadap penyembunyian terhadap teks berupa .txt dapat dilihat pada tabel 1. Hasil uji coba terhadap penyembunyian terhadap file dokumen dapat dilihat pada tabel 2. Hasil uji coba terhadap penyembunyian teks berupa .txt dan file dokumen dengan ukuran yang berbeda-beda dapat dilihat pada tabel 3.

TABEL I
HASIL UJI COBA PENYEMBUNYIAN TEKS

No	Host Image	Text .txt	Hasil Penyembunyian	Hasil Ekstraksi
1	hkbp.bmp(225x225)(6kb)	Kepal.txt(1kb)	BerhasilCoba1.png(225x225)(41,1kb)	BerhasilEkstak1.txt(1kb)
2	hkbp.bmp(225x225)(6kb)	Kepal.txt(11 kb)	Berhasil Coba2.png (225x225) (41,7 kb)	Berhasil Ekstrak2.txt(1kb)

TABEL II
HASIL UJI COBA PENYEMBUNYIAN FILE

No	Host Image	Text .txt	Hasil Penyembunyian	Hasil Ekstraksi
1	hkbp.bmp(225x225)(6kb)	Article_Printed_Submission.docx(56kb)	Tidak Berhasil	-
2	Contoh1.png(646x961)(59kb)	Article_Printed_Submission.docx(56kb)	BerhasilCoba3.png(646x961)(461kb)	Berhasil Ekstrak 3.docx(190kb)
3	Semangat.png(1080x1080)(518kb)	quality-costing-technique.pdf(354kb)	BerhasilCoba4.png(1080x1080)(1,12mb)	-

TABEL III
HASIL UJI COBA PENYEMBUNYIAN TEKS & FILE DENGAN UKURAN BERBEDA

No	Host Image	Text .txt	Hasil Penyembunyian	Hasil Ekstraksi
1	hkbp.bmp(225x225)(6kb)	Article_Printed_Submission.docx(56kb)	Tidak Berhasil	-
2	Contoh1.png(646x961)(59kb)	Article_Printed_Submission.docx(56kb)	BerhasilCoba3.png(646x961)(461kb)	Berhasil Ekstrak 3.docx(190kb)
3	Semangat.png(1080x1080)(518kb)	quality-costing-technique.pdf(354kb)	BerhasilCoba4.png(1080x1080)(1,12mb)	-
4	hkbp.bmp(225x225)(6kb)	Kepal.txt(1kb)	BerhasilCoba1.png(225x225)(41,1kb)	BerhasilEkstak1.txt(1kb)
5	hkbp.bmp(225x225)(6kb)	Kepal.txt(11kb)	BerhasilCoba2.png(225x225)(41,7kb)	BerhasilEkstrak2.txt(1kb)

B. Tahapan Prosedur

Langkah-langkah dalam prosedur untuk menyembunyikan teks .txt dan file dokumen adalah sebagai berikut:

1. Masukkan Host Image
   Masukkan gambar yang akan digunakan sebagai media penampung dengan memilihnya melalui tombol browse yang tersedia pada aplikasi.
2. Masukkan file teks/file dokumen
   Pilih file teks atau dokumen yang akan disisipkan ke dalam host image. Pastikan ukuran teks atau file dokumen yang akan disembunyikan lebih kecil dari ukuran gambar yang digunakan sebagai host image.
3. Melakukan Penyembunyian
   Setelah memasukkan teks atau file dokumen, klik tombol sembunyikan teks atau sembunyikan file. Teks atau file dokumen serta gambar yang telah dipilih akan diproses menggunakan metode LSB. Proses ini menghasilkan gambar yang telah berisi teks atau file dokumen yang disisipkan.
4. Menyimpan Hasil Penyembunyian
   Gambar yang telah disisipkan dapat disimpan dengan memilih tombol *browse* pada aplikasi.

Langkah-langkah dalam prosedur untuk mengekstraksi gambar adalah sebagai berikut:

1. Masukkan gambar yang ingin diekstraksi dengan memilihnya melalui tombol *browse* pada aplikasi.
2. Memilih tempat untuk disimpan.
   Pilih lokasi di komputer untuk menyimpan hasil ekstraksi dengan menggunakan tombol.
3. Melakukan Ekstraksi
   Selanjutnya, gambar akan diekstraksi dengan memilih tombol Ekstrak Teks atau Ekstrak File.

SIMPULAN

Kesimpulannya, implementasi steganografi menggunakan metode *Least Significant Bit* (LSB) berhasil menyembunyikan teks .txt dan file dokumen dalam gambar dengan baik. Dengan antarmuka grafis berbasis Tkinter, pengguna dapat dengan mudah memilih gambar (format BMP atau PNG), menyembunyikan file dokumen atau teks .txt, serta mengekstrak data yang disembunyikan. Perbedaan antara format BMP dan PNG sangat penting dalam konteks steganografi. BMP lebih ideal karena tidak menggunakan kompresi sehingga data yang disisipkan tetap utuh tanpa distorsi, sedangkan PNG meskipun menghasilkan ukuran file lebih kecil melalui kompresi *lossless*, dapat mempengaruhi keutuhan bit yang disembunyikan. Penelitian ini membuka peluang untuk pengembangan lebih lanjut dengan mengeksplorasi teknik steganografi lain yang lebih efisien dan aman dalam menyembunyikan data.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada Bapak Rudy Chandra, S.Kom., M.Kom**.** selaku dosen pembimbing yang telah memberikan bimbingan, arahan, serta masukan yang sangat berarti dalam proses penyusunan penelitian ini. Peneliti juga menyampaikan apresiasi kepada rekan peneliti dan seluruh pihak yang telah memberikan dukungan serta kontribusi, baik secara langsung maupun tidak langsung, sehingga penelitian ini dapat diselesaikan dengan baik. Semoga hasil penelitian ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan.

DAFTAR PUSTAKA

[1] S. Watermarking and D. Steganografi, "Steganografi dan Watermarking Departemen Teknik Informatika Institut Teknologi Bandung," 2004.

[2] T. T. Nguyen and H. Lee, *High-speed low-complexity elliptic curve cryptographic processor*. 2016. doi: 10.1109/ISOCC.2015.7401749.

[3] [1] N. Nurmaesah, T. Lestari, and A. Retno Mariana, "Aplikasi Steganografi Untuk Menyisipkan Pesan Dalam Media Image," *Technol. Accept. Model*, vol. 8, no. 1, pp. 13–17, 2017.

[4] C. Jatmoko, L. B. Handoko, C. A. Sari, D. R. Ignatius, and M. Setiadi, "U Ji P Erforma P Enyisipan P Esan Dengan M Etode Lsb Dan Msb," vol. 14, no. 1, pp. 47–56, 2018.

[5] I. U. W. Mulyono, Y. Kusumawati, and N. K. Ningrum, "Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis Least Significant Bit Dalam Cipher," *J. Masy. Inform.*, vol. 14, no. 1, pp. 16–28, 2023, doi: 10.14710/jmasif.14.1.51484.

[6] Saifuddin, A. Rakhmadi Mido, and E. Ujianto, "Perancangan Aplikasi Steganografi Menggunakan Metode Discrete Cosine Transformation berbasis Android," *J. Ilm. Komput.* , vol. 16, no. 1, pp. 25–36, 2020.

[7] A. C. Darmawan, "Pengembanga Aplikasi Berbasis Web dengan Python Flask untuk Klasifikasi Data Menggunakan Metode Decision Tree C4.5," *J. Pendidikan Konseling*, vol. 4, no. 5, pp. 5351–5362, 2022.

[8] F. Rizki Permana, R. Fadillah Setiyanto, and A. Rafi Fauzi, "Image Steganography Dengan Menggunakan Metode LSB Pada Python," *J. Pendidik. Teknol.*, vol. 2, no. 1, pp. 1–7, 2023.

[9] A.W. Laksono, S. Suhada, and A. Zakaria, "Implementasi Metode Least Significant Bit (Lsb) Dalam Teknik Steganografi Pada Citra Digital Menggunakan Matlab," vol. 4, no. 1, 2024.

[10] C. Satriatama, M. Huda, and I. U. Nadhori, "Implementasi dan Analisa Teknik Steganografi Multi-carrier Pada File Multimedia,"

[11] S. R. Febriani and D. C. Irawati, "Implementasi Digital Watermarking Pada Citra Menggunakan Metode Least Significant Bit," *J. Inform. dan Komput.*, vol. 21, no. 3, pp. 8–18, 2016, [Online]. Available: https://ejournal.gunadarma.ac.id/index.php/infokom/article/download/1522/128

[12] P. D. S. Kunjung Wahyudi, "Aplikasi kriptografi untuk pertukaran pesan menggunakan teknik steganografi dan algoritma aes," *Pros. Semin. Nas. Teknoin*, no. January 2011, pp. 67–72, 2018.

[13] O. Soleh, F. Alfiah, and B. Yusuf, "Perancangan Aplikasi Steganografi Dengan Teknik LSB dan AlgoritmaRC4 & Base64 Encoding," *Technomedia J.*, vol. 3, no. 1, pp. 1–15, 2018, doi: 10.33050/tmj.v3i1.493.

[14] J. Beno, A. . Silen, and M. Yanti, "Hasil Uji Coba Penyembunyian teks dan file dokumen dengan ukuran yang berbeda-beda," *Braz Dent J.*, vol. 33, no. 1, pp. 1–12, 2022.

[15] U. Aplikasi, "Analisa Kualitas Citra pada Steganografi,"

[16] A. Tenggono, "Aplikasi Perlindungan Hak Cipta Digital dengan Kriptografi dan Stenografi," *Teknomatika*, vol. 06, no. 02, pp. 22– 32, 2016, [Online]. Available: http://ojs.palcomtech.com/index.php/teknomatika/article/view/4%0Ahttp://ojs.palcomtech.com/index.php/teknomatika/article/view/ 4/4