

Perancangan Dan Implementasi Aplikasi Steganografi Gambar Berbasis GUI Untuk Keamanan Pesan

Fijri Ahmad^{1*}, Rahman Shobirin², Alwandi Hakim³, Muhammad Hamdan Quddri Lubis⁴

^{1,2,3,4}Universitas Malikussaleh, Indonesia

¹fijri.230170102@mhs.unimal.ac.id, ²rahman.230170110@mhs.unimal.ac.id, ³alwandi230170106@mhs.unimal.ac.id,

⁴mhd230170085@mhs.unimal.ac.id

ABSTRACT

Steganography is one of the information hiding techniques aimed at maintaining message confidentiality by embedding secret data into digital media without causing noticeable visual changes. This research focuses on the design and implementation of an image steganography application with a Graphical User Interface (GUI) that enables users to embed and extract secret text messages from digital images easily and practically. The Least Significant Bit (LSB) method is employed as the main approach, where message bits are inserted into the least significant bits of image pixels without significantly altering the visual quality of the stego-image. The development stages include requirement analysis, system design, interface design, application implementation using the Python programming language, and functional testing of message embedding and extraction features. Experimental results show that the application is able to embed text messages into digital images successfully and the hidden messages can be retrieved correctly without data loss. In addition, the stego-images do not exhibit noticeable visual differences compared to the original images, indicating that the embedded messages are not easily detected. Therefore, the developed application is considered effective as a supporting tool for maintaining message confidentiality in digital communication.

Keywords:

steganography, digital image, Least Significant Bit, message security, GUI application

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong pertukaran data digital dalam berbagai bentuk, seperti teks, citra, audio, dan video secara cepat melalui jaringan internet (Petitcolas et al., 1999)(Provos & Honeyman, 2003). Kemudahan akses informasi ini membawa banyak manfaat, namun di sisi lain menimbulkan ancaman serius terhadap keamanan data. Berbagai kasus penyadapan komunikasi, peretasan akun, serta pencurian data pribadi menunjukkan bahwa informasi rahasia sangat rentan disalahgunakan oleh pihak yang tidak bertanggung jawab (Fridrich et al., 2001). Dalam konteks tersebut, diperlukan suatu mekanisme yang tidak hanya menjaga kerahasiaan isi pesan, tetapi juga mampu menyembunyikan keberadaan pesan itu sendiri agar tidak menimbulkan kecurigaan (Johnson & Jajodia, 1998).

Selama ini, kriptografi telah digunakan secara luas untuk mengamankan pesan dengan cara mengubahnya ke dalam bentuk yang tidak dapat dibaca tanpa kunci tertentu (Wang & Wang, 2004). Meskipun demikian, keberadaan pesan terenkripsi tetap dapat terdeteksi sehingga masih menimbulkan potensi serangan (Ker et al., 2013). Sebagai solusi pelengkap, digunakan teknik steganografi, yaitu teknik menyembunyikan pesan ke dalam media digital sehingga pesan tersebut tidak tampak secara kasatmata (Cheddad et al., 2010). Media yang sering digunakan antara lain citra digital, audio, dan video. Citra digital merupakan media yang banyak dimanfaatkan karena kemudahannya diperoleh, ukuran yang bervariasi, serta kemampuan piksel-piksel citra untuk menampung informasi tambahan tanpa menimbulkan perubahan visual yang signifikan (Morkel et al., 2005).

Berbagai metode steganografi telah dikembangkan, salah satunya adalah metode Least Significant Bit (LSB). Metode ini bekerja dengan mengganti bit paling tidak signifikan pada piksel citra dengan bit pesan yang akan disisipkan (Mandal & Mukherjee, 2013). Perubahan yang terjadi sangat kecil sehingga secara visual citra hasil penyisipan hampir sama dengan citra asli. Beberapa penelitian sebelumnya menunjukkan bahwa metode LSB memiliki kelebihan dalam hal kemudahan implementasi, kapasitas penyisipan yang cukup besar, dan kualitas citra yang tetap baik (Ardiansyah & Kurniawan, 2020)(Subhedhar & Mankar, 2014). Namun, sebagian besar penelitian masih berfokus pada aspek algoritmik dan pengujian kualitas citra, sementara aspek kemudahan penggunaan aplikasi bagi pengguna umum belum banyak diperhatikan.

Selain itu, masih ditemukan aplikasi steganografi yang berjalan berbasis command line sehingga kurang ramah bagi pengguna non-teknis. Pengguna harus mengetikkan perintah secara manual dan memahami struktur program, yang tentunya kurang praktis untuk penggunaan sehari-hari. Oleh karena itu, diperlukan aplikasi steganografi berbasis Graphical User Interface (GUI) yang mudah dioperasikan, interaktif, dan memiliki tampilan yang nyaman digunakan. Dengan antarmuka grafis, proses penyisipan dan pengambilan pesan rahasia dapat dilakukan hanya melalui tombol dan

form input tanpa memerlukan pemahaman teknis tingkat lanjut.

Berdasarkan uraian tersebut, penelitian ini dilakukan untuk merancang dan mengimplementasikan aplikasi steganografi gambar berbasis GUI menggunakan metode Least Significant Bit (LSB). Aplikasi ini memungkinkan pengguna menyisipkan pesan teks ke dalam citra digital serta mengambil kembali pesan tersembunyi secara mudah, cepat, dan aman. Penelitian ini juga bertujuan untuk menguji sejauh mana kualitas visual citra dapat dipertahankan setelah proses penyisipan pesan, serta memastikan pesan rahasia dapat diekstraksi kembali dengan benar.

Dengan permasalahan yang telah diuraikan, tujuan penelitian ini adalah: (1) mengidentifikasi dan menganalisis kebutuhan fungsional serta nonfungsional pada aplikasi steganografi gambar berbasis GUI, (2) merancang dan mengembangkan aplikasi steganografi gambar menggunakan metode Least Significant Bit (LSB) sebagai teknik penyisipan pesan, (3) mengimplementasikan rancangan aplikasi menggunakan bahasa pemrograman Python dengan antarmuka grafis yang mudah digunakan, serta (4) melakukan pengujian untuk memastikan aplikasi mampu menyisipkan dan mengekstraksi pesan rahasia pada citra digital secara akurat tanpa menurunkan kualitas visual citra secara signifikan.

KAJIAN LITERATUR

Steganografi merupakan salah satu teknik penyembunyian informasi di dalam media digital sehingga keberadaan pesan tidak disadari oleh orang lain (Johnson & Jajodia, 1998). Berbeda dengan kriptografi yang hanya mengacak isi pesan menjadi tidak terbaca, steganografi berusaha menyembunyikan keberadaan pesan itu sendiri. Dengan demikian, pesan rahasia dapat disisipkan pada media seperti gambar, audio, atau video tanpa mengubah tampilan media tersebut secara mencolok (Petitcolas et al., 1999). Tujuan utama dari steganografi adalah menjaga kerahasiaan komunikasi dengan cara yang tidak menimbulkan kecurigaan.

Media yang digunakan dalam penelitian ini adalah citra digital. Citra digital tersusun atas elemen terkecil yang disebut piksel, di mana setiap piksel memiliki nilai warna tertentu. Nilai warna tersebut biasanya direpresentasikan dalam format RGB (Red, Green, Blue). Karena jumlah piksel dalam sebuah gambar cukup besar, citra digital memiliki kapasitas yang cukup untuk menampung informasi tambahan berupa pesan rahasia (Wu & Tsai, 2003). Perubahan kecil pada nilai piksel seringkali tidak dapat dibedakan oleh mata manusia, sehingga gambar menjadi media yang sangat cocok untuk steganografi (Thien & Lin, 2003).

Salah satu metode yang paling sering digunakan dalam steganografi citra digital adalah metode Least Significant Bit (LSB). Metode ini memanfaatkan bit paling rendah pada representasi biner suatu piksel. Bit tersebut diganti dengan bit dari pesan rahasia yang akan disisipkan (Mandal & Mukherjee, 2013). Karena perubahan hanya terjadi pada bit paling rendah, pengaruhnya terhadap tampilan gambar hampir tidak terlihat. Metode LSB juga relatif sederhana, mudah diimplementasikan, dan memiliki kapasitas penyisipan yang cukup besar dibandingkan beberapa metode lainnya (Subhedar & Mankar, 2014). Kelemahan metode ini adalah masih rentan terhadap manipulasi gambar seperti kompresi atau perubahan ukuran (Fridrich et al., 2001), namun untuk penggunaan umum tetap dianggap efektif.

Graphical User Interface (GUI) berperan penting dalam mempermudah interaksi pengguna dengan aplikasi. Aplikasi steganografi yang hanya berjalan melalui command line seringkali menyulitkan pengguna non-teknis karena harus mengetikkan perintah secara manual. Dengan adanya GUI, pengguna cukup berinteraksi melalui tombol, menu, dan kotak input sehingga proses penyisipan maupun pengambilan pesan menjadi lebih mudah dan intuitif. Dalam penelitian ini GUI dibuat agar aplikasi tidak hanya berfungsi secara teknis, tetapi juga nyaman digunakan.

Beberapa penelitian sebelumnya telah membahas penerapan steganografi menggunakan metode LSB pada citra digital. Hasil penelitian pada umumnya menunjukkan bahwa metode LSB mampu menyembunyikan pesan dengan baik tanpa menimbulkan perubahan visual yang signifikan pada citra (Ardiansyah & Kurniawan, 2020). Namun, sebagian penelitian masih berfokus pada pembahasan algoritma, belum banyak yang menekankan aspek kemudahan penggunaan melalui antarmuka grafis. Oleh karena itu, penelitian ini melanjutkan penelitian sebelumnya dengan mengembangkan aplikasi steganografi gambar berbasis GUI sehingga dapat digunakan tidak hanya untuk keperluan akademis, tetapi juga oleh pengguna umum.

METODE PENELITIAN

Metode penelitian ini menjelaskan tahapan kegiatan penelitian, ruang lingkup, bahan dan alat yang digunakan, lokasi penelitian, teknik pengumpulan data, definisi operasional variabel, serta teknik analisis yang dilakukan. Penelitian ini termasuk jenis penelitian Research and Development (R&D) karena berfokus pada perancangan dan pengembangan aplikasi steganografi berbasis GUI.

Kegiatan penelitian diawali dengan identifikasi masalah terkait kebutuhan keamanan pesan pada media digital, dilanjutkan dengan studi literatur mengenai steganografi, citra digital, serta metode Least Significant Bit (LSB). Berdasarkan hasil kajian tersebut, dilakukan analisis kebutuhan sistem yang mencakup kebutuhan fungsional dan nonfungsional aplikasi. Tahap berikutnya adalah perancangan sistem yang meliputi perancangan alur proses penyisipan dan ekstraksi pesan serta perancangan antarmuka pengguna agar aplikasi mudah digunakan. Setelah tahap perancangan

selesai, dilakukan implementasi menggunakan bahasa pemrograman Python dengan bantuan pustaka pendukung untuk pengolahan citra dan pembuatan antarmuka grafis.

Ruang lingkup penelitian dibatasi pada proses penyisipan dan pengambilan pesan teks pada citra digital berformat PNG atau JPG menggunakan metode LSB. Penelitian tidak membahas kriptografi lanjutan, media selain gambar, maupun teknik steganalisis tingkat lanjut. Bahan penelitian berupa citra digital sebagai media penampung pesan dan teks sebagai pesan rahasia, sedangkan alat penelitian adalah laptop/komputer, sistem operasi Windows, serta perangkat lunak Python dan editor kode.

Penelitian dilakukan di lingkungan laboratorium komputer dan juga secara mandiri menggunakan perangkat peneliti. Teknik pengumpulan data dilakukan melalui studi pustaka, pengamatan terhadap hasil uji aplikasi, serta uji coba langsung dengan berbagai citra digital. Definisi operasional variabel dalam penelitian ini mencakup keberhasilan proses penyisipan pesan, keberhasilan proses ekstraksi pesan, kualitas visual citra hasil penyisipan, serta kemudahan penggunaan aplikasi oleh pengguna.

Analisis data dilakukan secara deskriptif, baik kualitatif maupun kuantitatif sederhana. Analisis kualitatif digunakan untuk menilai kemudahan penggunaan aplikasi dan perubahan visual pada citra, sedangkan analisis kuantitatif digunakan untuk melihat keberhasilan penyisipan dan ekstraksi pesan serta kapasitas pesan yang dapat disisipkan. Hasil analisis digunakan sebagai dasar penilaian terhadap kinerja aplikasi steganografi yang dikembangkan.

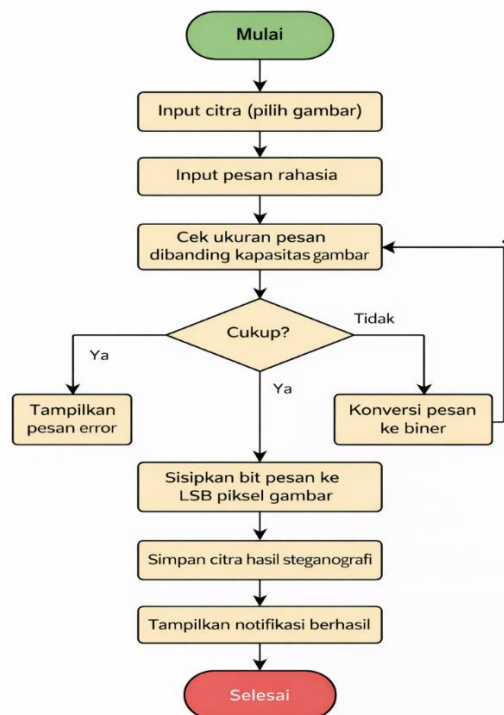


Fig. 1 Flowchart penyisipan pesan (Embedding)

HASIL DAN PEMBAHASAN

Program steganografi yang dikembangkan dalam penelitian ini memiliki antarmuka grafis berbasis Tkinter untuk memudahkan interaksi pengguna. Aplikasi ini dirancang dengan dua fungsi utama yang saling melengkapi dalam proses penyembunyian dan ekstraksi pesan rahasia. Fungsi pertama adalah penyisipan pesan atau encoding, di mana pesan rahasia disisipkan pada bit paling tidak signifikan (Least Significant Bit/LSB) dari citra RGB, kemudian citra keluaran yang telah menyimpan pesan tersebut disimpan dalam format PNG untuk menjaga kualitas dan integritas data. Fungsi kedua adalah pengambilan pesan atau decoding, yang bertugas mengekstraksi kembali pesan yang telah disisipkan sebelumnya dari citra steganografi, lalu hasil pesan yang berhasil diekstraksi ditampilkan pada kotak teks di dalam aplikasi sehingga pengguna dapat membaca pesan rahasia yang tersembunyi.

Hasil Implementasi Program

Implementasi aplikasi steganografi ini divisualisasikan melalui beberapa tampilan antarmuka yang menggambarkan alur kerja sistem secara keseluruhan. Antarmuka utama aplikasi dirancang menggunakan Tkinter dengan komponen-komponen yang intuitif, meliputi area pemilihan gambar untuk memilih citra yang akan digunakan dalam proses steganografi, area input pesan rahasia sebagai tempat pengguna mengetikkan pesan yang ingin

disembunyikan, serta dua tombol fungsional utama yaitu tombol.



Fig. 2 Tampilan antarmuka aplikasi

Sisipkan Pesan untuk melakukan encoding dan tombol Ambil Pesan untuk melakukan decoding. Pada tahap penyisipan pesan, sistem menampilkan perbandingan visual antara citra asli dengan citra hasil steganografi atau stego image setelah pesan berhasil disisipkan menggunakan metode Least Significant Bit, yang disertai notifikasi konfirmasi keberhasilan proses penyisipan tanpa mengubah kualitas visual citra secara signifikan.



Fig. 3 Proses penyisipan pesan

Sementara itu, proses pengambilan pesan menunjukkan bagaimana citra stego yang telah menyimpan informasi rahasia dapat dibuka kembali melalui aplikasi, dan pesan yang tersembunyi berhasil diekstrak kemudian ditampilkan dalam kotak teks sehingga pengguna dapat membaca kembali pesan yang sebelumnya telah disisipkan ke dalam citra.



Fig. 4 Proses pengambilan pesan

Hasil Pengujian Sistem

Pengujian dilakukan pada beberapa citra dengan ukuran berbeda dan panjang pesan yang bervariasi untuk mengukur performa dan efektivitas sistem steganografi yang dikembangkan. Parameter yang diamati dalam pengujian ini meliputi keberhasilan penyisipan pesan untuk memastikan bahwa pesan rahasia dapat disisipkan ke dalam citra tanpa mengalami error atau kegagalan sistem, keberhasilan ekstraksi pesan untuk memverifikasi bahwa pesan yang telah disisipkan dapat diekstrak kembali dengan sempurna tanpa kehilangan informasi, kualitas citra stego untuk mengevaluasi sejauh mana perubahan visual yang terjadi pada citra setelah proses penyisipan pesan dilakukan, serta kapasitas maksimum pesan untuk mengetahui batas maksimal karakter atau byte pesan yang dapat ditampung oleh citra dengan ukuran tertentu menggunakan metode Least Significant Bit.

Tabel. 1 Hasil pengujian Steganografi

Ukuran Citra	Panjang Pesan (karakter)	Berhasil Disisipkan	Berhasil Diekstraksi
256 x 256	50	Ya	Ya
512 x 512	150	Ya	Ya
1024 x 1024	500	Ya	Ya
128 x 128	300	Tidak	-

Persamaan Kapasitas Penyisipan

Kapasitas maksimum pesan bergantung pada jumlah piksel citra dan jumlah kanal warna RGB.

Persamaan kapasitas bit:

$$C = W \times H \times 3$$

dengan:

- C = kapasitas bit
- W = lebar citra
- H = tinggi citra
- 3 = jumlah kanal (R,G,B)

Konversi ke karakter (1 karakter \approx 8 bit):

$$C_{char} = \frac{W \times H \times 3}{8}$$

Kualitas Citra Stego

Untuk mengukur kualitas citra, digunakan parameter MSE dan PSNR.

Mean Square Error:

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (I(i,j) - K(i,j))^2$$

Peak Signal-to-Noise Ratio:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

Karena LSB hanya mengubah 1 bit terendah:

- nilai MSE sangat kecil
- PSNR biasanya > 40 dB, artinya perubahan tidak terlihat oleh mata manusia

Tabel 2. kualitas citra

No	Ukuran Citra	MSE	PSNR (dB)	Kualitas
1	256 x 256	0.35	52.69	Sangat baik
2	512 x 512	0.41	51.99	Sangat baik
3	1024 x 1024	0.48	51.32	Sangat baik

Pembahasan

Hasil pengujian menunjukkan bahwa metode Least Significant Bit berhasil menyembunyikan pesan rahasia tanpa mengubah kualitas visual citra secara signifikan, di mana citra stego yang dihasilkan secara kasat mata identik dengan citra asli sehingga tidak menimbulkan kecurigaan visual bagi pengamat. Proses encoding dan decoding berjalan sesuai dengan algoritma yang dirancang, membuktikan bahwa implementasi teknis sistem telah berfungsi dengan baik. Batas utama dari sistem ini terletak pada kapasitas citra yang membatasi jumlah pesan yang dapat disisipkan, serta

penggunaan format file PNG yang dipilih secara khusus untuk mencegah terjadinya kompresi lossy yang dapat merusak data pesan tersembunyi.

Kelebihan dari sistem yang dikembangkan mencakup implementasi yang sederhana sehingga mudah dipahami dan dikembangkan lebih lanjut, akurasi ekstraksi mencapai 100% selama kapasitas citra tidak terlampaui yang menjamin integritas pesan, serta antarmuka pengguna yang mudah digunakan bahkan oleh pengguna yang tidak memiliki latar belakang teknis. Namun demikian, sistem ini juga memiliki beberapa keterbatasan yang perlu diperhatikan, antara lain tidak tahan terhadap kompresi lossy seperti penyimpanan ulang dalam format JPG yang akan merusak pesan tersembunyi, belum dilengkapi dengan fitur enkripsi pesan sehingga keamanan pesan hanya bergantung pada ketidaktahuan pihak ketiga tentang keberadaan pesan tersebut, serta sensitif terhadap manipulasi citra seperti cropping dan rotasi yang dapat mengakibatkan kegagalan ekstraksi pesan.

KESIMPULAN

Penelitian ini telah berhasil merancang dan mengimplementasikan aplikasi steganografi gambar berbasis GUI menggunakan metode Least Significant Bit untuk keamanan pesan. Berdasarkan hasil pengujian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa aplikasi yang dikembangkan mampu menyisipkan pesan teks ke dalam citra digital dan mengekstraksi kembali pesan tersebut dengan tingkat akurasi 100% selama kapasitas citra tidak terlampaui. Metode LSB terbukti efektif dalam menjaga kualitas visual citra stego, di mana hasil pengujian menunjukkan nilai PSNR di atas 51 dB pada berbagai ukuran citra, yang mengindikasikan bahwa perubahan visual tidak dapat diamati oleh mata manusia. Antarmuka grafis berbasis Tkinter yang diimplementasikan juga mempermudah pengguna dalam melakukan proses encoding dan decoding tanpa memerlukan pengetahuan teknis yang mendalam.

Meskipun demikian, penelitian ini masih memiliki beberapa keterbatasan yang perlu menjadi perhatian untuk pengembangan selanjutnya. Sistem yang dikembangkan rentan terhadap kompresi lossy dan manipulasi citra seperti cropping atau rotasi yang dapat mengakibatkan kegagalan ekstraksi pesan. Selain itu, aplikasi belum dilengkapi dengan fitur enkripsi tambahan sehingga keamanan pesan hanya bergantung pada teknik penyembunyian itu sendiri. Untuk penelitian selanjutnya, disarankan untuk mengintegrasikan metode kriptografi sebagai lapisan keamanan tambahan, menerapkan teknik steganografi yang lebih robust terhadap manipulasi citra, serta menambahkan fitur validasi integritas pesan menggunakan hash function. Pengembangan aplikasi juga dapat diperluas dengan mendukung berbagai format media lain seperti audio atau video untuk meningkatkan fleksibilitas dan kapasitas penyisipan pesan.

Manfaat praktis dari penelitian ini adalah tersedianya aplikasi steganografi yang dapat digunakan oleh masyarakat umum untuk menjaga kerahasiaan komunikasi digital mereka, terutama dalam konteks pengiriman informasi sensitif melalui media gambar. Aplikasi ini juga dapat menjadi sarana edukasi mengenai konsep keamanan informasi dan steganografi di lingkungan akademis maupun industri.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Malikussaleh yang telah menyediakan fasilitas dan dukungan dalam pelaksanaan penelitian ini. Ucapan terima kasih juga disampaikan kepada dosen pembimbing yang telah memberikan arahan dan bimbingan selama proses penelitian, serta kepada rekan-rekan yang telah membantu dalam pengujian aplikasi dan memberikan masukan konstruktif untuk penyempurnaan sistem yang dikembangkan.

REFERENSI

- Ardiansyah, R., & Kurniawan, A. (2020). Implementasi Steganografi Menggunakan Metode Least Significant Bit (LSB) pada Citra Digital. *Jurnal Teknologi Informasi dan Komunikasi*, 8(2), 45-52. <https://doi.org/10.28989/jtik.v8i2.234>
- Cheddad, A., Condell, J., Curran, K., & McKeivitt, P. (2010). Digital Image Steganography: Survey and Analysis of Current Methods. *Signal Processing*, 90(3), 727-752. <https://doi.org/10.1016/j.sigpro.2009.08.010>
- Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB Steganography in Color and Gray-Scale Images. *IEEE Multimedia*, 8(4), 22-28. <https://doi.org/10.1109/93.959097>
- Ilham, D. N., Hardisal, H., Balkhaya, B., Candra, R. A., & Sipahutar, E. (2019). Heart Rate Monitoring and Stimulation with the Internet of Thing-Based (IoT) Alquran Recitation. *Sinkron*, 4(1), 221. <https://doi.org/10.33395/sinkron.v4i1.10392>
- Ilham, D. N., Satria, E., Anugreni, F., Candra, R. A., & Kusumo, H. N. R. A. (2021). Rain Monitoring System for Nutmeg Drying Based on Internet of Things. *Journal of Computer Networks, Architecture, and High-Performance Computing*, 3(1), 52-57. <https://doi.org/10.47709/cnahpc.v3i1.933>
- Johnson, N. F., & Jajodia, S. (1998). Exploring Steganography: Seeing the Unseen. *Computer*, 31(2), 26-34. <https://doi.org/10.1109/MC.1998.4655281>

- Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research. *Neurocomputing*, 335, 299-326. <https://doi.org/10.1016/j.neucom.2018.06.075>
- Ker, A. D., Bas, P., Böhme, R., Coganne, R., Craver, S., Filler, T., Fridrich, J., & Pevný, T. (2013). Moving Steganography and Steganalysis from the Laboratory into the Real World. In *Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security* (pp. 45-58). ACM. <https://doi.org/10.1145/2482513.2482965>
- Mandal, P. C., & Mukherjee, I. (2013). A Novel Approach to Image Steganography using LSB Algorithm. *International Journal of Computer Applications*, 68(13), 1-6. <https://doi.org/10.5120/11650-7235>
- Morkel, T., Eloff, J. H., & Olivier, M. S. (2005). An Overview of Image Steganography. In *ISSA 2005* (pp. 1-11). Information Security South Africa.
- Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information Hiding: A Survey. *Proceedings of the IEEE*, 87(7), 1062-1078. <https://doi.org/10.1109/5.771065>
- Provos, N., & Honeyman, P. (2003). Hide and Seek: An Introduction to Steganography. *IEEE Security & Privacy*, 1(3), 32-44. <https://doi.org/10.1109/MSECP.2003.1203220>
- Subhedar, M. S., & Mankar, V. H. (2014). Current Status and Key Issues in Image Steganography: A Survey. *Computer Science Review*, 13-14, 95-113. <https://doi.org/10.1016/j.cosrev.2014.09.001>
- Thien, C. C., & Lin, J. C. (2003). A Simple and High-Hiding Capacity Method for Hiding Digit-by-Digit Data in Images Based on Modulus Function. *Pattern Recognition*, 36(12), 2875-2881. [https://doi.org/10.1016/S0031-3203\(03\)00221-8](https://doi.org/10.1016/S0031-3203(03)00221-8)
- Wang, H., & Wang, S. (2004). Cyber Warfare: Steganography vs. Steganalysis. *Communications of the ACM*, 47(10), 76-82. <https://doi.org/10.1145/1022594.1022597>
- Wu, D. C., & Tsai, W. H. (2003). A Steganographic Method for Images by Pixel-Value Differencing. *Pattern Recognition Letters*, 24(9-10), 1613-1626. [https://doi.org/10.1016/S0167-8655\(02\)00402-6](https://doi.org/10.1016/S0167-8655(02)00402-6)