Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Feb 2025, VIII (1): 534 – 542 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

TINJAUAN ONTOLOGI, EPISTEMOLOGI, DAN AKSIOLOGI DALAM BIDANG ILMU STEGANOGRAFI

Frainskoy Rio Naibaho
Universitas Sumatera Utara, Medan
e-mail: frainskoyrio@students.usu.ac.id

Abstract: *Steganography is a field of science that studies the technique of hiding information in digital media to protect data from third-party detection ketiga (Atawneh et al., 2013; Michaylov & Sarmah, 2024; Sitompul et al., 2018). This article reviews steganography through three philosophical perspectives: ontology, epistemology, and axiology. Ontologically, steganography explains the existence of hidden information in host media and its interactions. Epistemology plays a role in the process of developing and validating knowledge related to hiding and detection techniques. Meanwhile, axiology highlights the ethical benefits and risks, including the use to protect privacy and the potential for misuse in cybercrime. Steganography, with this comprehensive understanding, plays an important role in data security and information technology.*

Keywords: *Steganography, Ontology, Epistemology, and Axiology*

Abstrak: Steganografi adalah bidang ilmu yang mempelajari teknik penyembunyian informasi di dalam media digital untuk melindungi data dari deteksi pihak ketiga (Atawneh et al., 2013; Michaylov & Sarmah, 2024; Sitompul et al., 2018). Artikel ini meninjau steganografi melalui tiga perspektif filosofis: ontologi, epistemologi, dan aksiologi. Secara ontologis, steganografi menjelaskan keberadaan informasi tersembunyi dalam media host dan interaksinya. Epistemologi berperan dalam proses pengembangan dan validasi pengetahuan terkait teknik penyembunyian dan deteksi. Sementara itu, aksiologi menyoroti manfaat dan risiko etis, termasuk penggunaan untuk melindungi privasi dan potensi penyalahgunaan dalam kejahatan siber. Steganografi, dengan pemahaman komprehensif ini, berperan penting dalam keamanan data dan teknologi informasi.

Kata kunci: Steganografi, Ontologi, Epistemologi, dan Aksiologi

PENDAHULUAN

Steganografi, yang berasal dari bahasa Yunani "steganos" (tertutup) dan "grapho" (menulis) (Atawneh et al., 2013; Dutta et al., 2020; Kaur Brar & Sharma, 2018; Majeed et al., 2021; Ratan & Veni Madhavan, 2002; A. Singh & Singh, 2013; N. Singh & Todwal, 2018; Sitompul et al., 2018), merupakan teknik yang digunakan untuk menyembunyikan informasi di dalam media digital, seperti gambar, audio, dan video, dengan tujuan agar keberadaan informasi tersebut tidak terdeteksi (Atawneh et al., 2013; Kaur Brar & Sharma, 2018; Majeed et al., 2021; A. Singh & Singh, 2013; N. Singh & Todwal, 2018; Sitompul et al., 2018). Dalam dunia yang semakin terhubung secara digital, di mana data menjadi aset yang sangat berharga, pentingnya steganografi dalam konteks keamanan data semakin meningkat (Atawneh et al., 2013; Mukherjee & Sanyal, 2017; Mythreyi & Vaidehi, 2007; Saad Ahmed et al., 2021; Sathisha et al., 2011; Sitompul et al., 2018). Teknik ini berfungsi untuk melindungi informasi sensitif dari potensi ancaman, seperti pencurian data, penyadapan, dan serangan siber, yang dapat merugikan individu maupun organisasi (Bonavoglia, 2022; Dehshibi et al., 2018; Karampidis et al., 2018; Klubsuwan & Mungsing, 2009; Pal

& Madhavan, 2002; Rao & Pandit, 2007; Rushdi & Ba-rukab, 2005; Sairam & Boopathybagan, 2019; S. Singh & Singh, 2014; Sitompul et al., 2018).

Dalam konteks keamanan data, steganografi berperan penting sebagai lapisan perlindungan tambahan yang dapat digunakan bersamaan dengan teknik kriptografi (Fyffe et al., 2019; Mahajan, 2014; Michaylov & Sarmah, 2024; Sairam & Boopathybagan, 2019; Sirisha et al., 2018; Sitompul et al., 2018; Srinivasan et al., 2017; Wijaya et al., 2018). Dengan menyembunyikan data di dalam media yang tampaknya tidak berbahaya, steganografi membuat pengintaian lebih sulit dilakukan (Dutta et al., 2020; Fyffe et al., 2019; Klubsuwan & Mungsing, 2009; Mahajan, 2014). Hal ini sangat penting dalam transaksi digital, di mana keamanan informasi pribadi dan finansial menjadi prioritas utama. Dalam beberapa studi, ditemukan bahwa penggabungan steganografi dengan enkripsi dapat meningkatkan keamanan data secara signifikan, terutama dalam mencegah akses illegal (Atawneh et al., 2013; Dutta et al., 2020; Kaur Brar & Sharma, 2018; Klubsuwan & Mungsing, 2009; Majeed et al., 2021; Ratan & Veni Madhavan, 2002; A. Singh & Singh, 2013; N. Singh & Todwal, 2018; Sitompul et al., 2018).

Selanjutnya, aspek keamanan komputer juga tidak bisa diabaikan. Sistem komputer rentan terhadap berbagai serangan, termasuk malware dan teknik pemrograman jahat yang mencoba mengeksploitasi kelemahan dalam perangkat lunak (Bonavoglia, 2022; Dehshibi et al., 2018; S. Singh & Singh, 2014). Dalam konteks ini, steganografi dapat digunakan untuk menyimpan informasi terkait serangan atau aktivitas mencurigakan tanpa menarik perhatian, sehingga meningkatkan ketahanan sistem terhadap deteksi (Jeevitha & Amutha Prabha, 2018; M et al., 2019).

Di era digital saat ini, seiting dengan maraknya ancaman terhadap privasi dan keamanan data. Teknik steganografi menjadi salah satu solusi yang paling relevan. Dengan menggunakan berbagai media seperti gambar, audio, dan video, steganografi berupaya melindungi informasi sensitif dari akses yang illegal (Atawneh et al., 2013; Bonavoglia, 2022; Dehshibi et al., 2018; M et al., 2019). Steganografi menjadikan metode yang tidak kalah penting dalam keamanan data atau informasi.

Steganografi penting karena metode ini merupakan cara untuk menyembunyikan informasi sensitif di dalam media lain, sehingga mencegah akses yang illegal (Atawneh et al., 2013; Karampidis et al., 2018; Mythreyi & Vaidehi, 2007; Sitompul et al., 2018). Hal ini dapat meningkatkan keamanan data, terutama dalam konteks transaksi digital dan komunikasi pribadi. Karena dalam metode steganografi data disembunyikan pada file stego, yang dapat menyulitkan pendeteksian oleh pihak ketiga (Atawneh et al., 2013; Dutta et al., 2020; Jeevitha & Amutha Prabha, 2018; Karampidis et al., 2018; Kaur Brar & Sharma, 2018; Nasution et al., 2021; Pal & Madhavan, 2002; A. Singh & Singh, 2013; N. Singh & Todwal, 2018). Selain itu, steganografi juga membantu melindungi privasi individu dan organisasi dari serangan siber dan penyadapan. Dengan kombinasi teknik ini bersama kriptografi, steganografi menciptakan lapisan perlindungan tambahan yang memperkuat sistem keamanan secara keseluruhan (Mahajan, 2014; Pal & Madhavan, 2002; Po-Hsian, 2010; Wijaya et al., 2018).

Dalam rangka memahami sepenuhnya peran steganografi dalam keamanan informasi, perlu dilakukan analisis melalui tiga pilar filosofis—ontologi, epistemologi, dan aksiologi. Pendekatan ini tidak dapat membantu dalam pengembangan teknik-teknik steganografi yang lebih efektif tetapi juga memastikan bahwa praktik-praktik tersebut dilakukan dengan mempertimbangkan nilai-nilai etis dan tanggung jawab sosial (Nasution et al., 2022), (Nasution et al., 2019; Yasin et al., 2018). Ontologi membantu untuk

memahami realitas yang tersembunyi dalam teknik steganografi, termasuk entitas dan hubungan yang ada di dalamnya. Epistemologi berperan dalam pengembangan dan validasi pengetahuan tentang teknik-teknik yang digunakan, memastikan bahwa solusi yang diterapkan mampu menghadapi tantangan keamanan yang terus berkembang. Sementara itu, aksiologi mengingatkan kita pada nilai-nilai etis yang harus dipertimbangkan dalam penggunaan steganografi, terutama ketika menyangkut privasi individu dan potensi penyalahgunaan untuk tujuan jahat.

Melalui tinjauan ini, diharapkan dapat memberikan wawasan yang lebih komprehensif mengenai peran steganografi dalam keamanan data dan bagaimana pendekatan filosofis dapat membantu dalam pengembangan teknik yang lebih aman dan bertanggung jawab.

METODE

Ontologi Dalam Steganografi

Ontologi dalam konteks steganografi mengacu pada pemahaman mengenai hakikat keberadaan dan realitas dari objek tersembunyi dalam media digital. Hal ini melibatkan pertanyaan mendalam seperti: Apa yang dimaksud dengan informasi tersembunyi? dan Bagaimana data tersembunyi itu berinteraksi dengan media pembawanya (host media)? Pendekatan ontologis membantu menjelaskan keberadaan entitas tersembunyi (Nasution et al., 2019; Yasin et al., 2018), misalnya, pesan rahasia yang disisipkan di dalam gambar atau audio yang tidak tampak secara eksplisit namun tetap ada sebagai bagian integral dari media tersebut.

Media Host dan Data Tersembunyi

Dalam steganografi, media host seperti gambar, video, atau audio berfungsi sebagai "kulit luar" yang menyembunyikan informasi (Nasution et al., 2019; Sitompul et al., 2018). Konsep ini mengacu pada realitas tersembunyi. Walaupun data rahasia tidak terlihat, namum data tersebut tetap ada secara fungsional dan dapat diakses oleh pihak yang mengetahui teknik decoding yang benar (Dehshibi et al., 2018; Jeevan & Krishnakumar, 2019). Ini merupakan perbedaan mendasar antara steganografi dengan kriptografi. Adapun tujuan utamanya adalah bukan hanya melindungi isi informasi, tetapi juga menyembunyikan fakta bahwa informasi itu ada. Banyak cara yang telah dilakukan, seperti penyisipan pesan pada LSB dengan mengacak posisi penyispan (Sitompul et al., 2018). Sebelum dilakukan penyisipan pesan rahasia, pesan tersebut dienkripsi dengan metode kriptogrgapi (Mahajan, 2014; Sitompul et al., 2018). Dalam penelitian (Jeevitha & Amutha Prabha, 2018), menyisipkan pesan pada tepi media host. Penelitian lain menunjukkan dalam satu piksel pesan rahasia akan disisipkan ke dalam delapan sub-piksel pseudo heksagonal(Jeevan & Krishnakumar, 2019).

Interaksi antara Entitas dan Keamanan Data

Pemahaman ontologis dalam steganografi penting untuk mengevaluasi risiko keamanan data. Teknologi ini memungkinkan entitas tersembunyi berinteraksi dengan lingkungan tanpa disadari, yang dapat digunakan untuk meningkatkan keamanan atau justru untuk tujuan berbahaya, seperti penyelundupan informasi rahasia. Sebagai contoh, serangan malware berbasis steganografi dapat menyembunyikan kode berbahaya dalam gambar yang dikirim melalui email, membuatnya sulit dideteksi oleh sistem keamanan konvensional (Jeevitha & Amutha Prabha, 2018; Sathisha et al., 2011).

Ontologi sebagai Dasar Desain Teknik Steganografi

Pemikiran ontologis juga berperan dalam mengembangkan metode baru. Peneliti perlu memahami cara entitas tersembunyi berintegrasi dengan media dan bagaimana informasi tersebut dapat

dideteksi atau dilindungi (Atawneh et al., 2013; Dutta et al., 2020). Misalnya, dalam teknik Least Significant Bit (LSB), perubahan kecil pada bit terakhir dari piksel gambar dapat menyimpan pesan rahasia tanpa mempengaruhi kualitas gambar secara signifikan(Jeevitha & Amutha Prabha, 2018; Kaur Brar & Sharma, 2018; A. Singh & Singh, 2013; N. Singh & Todwal, 2018). Dengan memahami hakikat keberadaan informasi di tingkat bit, peneliti dapat merancang algoritma yang semakin sulit dideteksi.

Implikasi Ontologi untuk Data Informatika

Secara lebih luas, pemahaman ontologi membantu mengidentifikasi potensi kerentanan dan peluang dalam sistem keamanan data atau informasi. Dengan memetakan berbagai realitas tersembunyi di dunia digital, steganografi dapat berfungsi sebagai alat pertahanan maupun ancaman, tergantung siapa yang menggunakannya. Misalnya, teknik ini dapat melindungi komunikasi rahasia di bidang militer atau bisnis, tetapi juga dapat disalahgunakan untuk menyelundupkan informasi oleh pelaku kriminal.

Ontologi dalam steganografi menyoroti hakikat realitas tersembunyi dan interaksinya dengan media digital. Dengan memahami keberadaan informasi tersembunyi dan bagaimana terintegrasi atau disembunyikan, para peneliti dan praktisi keamanan data, dapat lebih siap dalam menghadapi tantangan keamanan yang terus berkembang. Ontologi tidak hanya berperan dalam memahami teknik dasar, tetapi juga membantu merumuskan kebijakan dan sistem pertahanan yang lebih baik untuk melindungi privasi dan keamanan data atau informasi dengan penyembunyian pesan.

Epistemologi Dalam Steganografi

Epistemologi dalam konteks steganografi berfokus pada cara memperoleh, memvalidasi, dan mengembangkan pengetahuan tentang teknik penyembunyian informasi. Ini mencakup metode ilmiah, algoritma, dan teknik yang digunakan untuk menciptakan dan mendeteksi steganografi. Pemahaman epistemologis diperlukan untuk memastikan bahwa pengetahuan tentang steganografi dapat diterapkan dengan efektif sekaligus beradaptasi dengan tantangan dan ancaman baru di bidang keamanan informasi.

Proses Pembentukan Pengetahuan dalam Steganografi

Pengetahuan dalam steganografi berkembang melalui eksperimen dan penelitian dalam bidang kriptografi, ilmu komputer (Jeevitha & Amutha Prabha, 2018; Nasution et al., 2019), dan matematika terapan. Peneliti mempelajari teknik seperti Least Significant Bit (LSB) (A. Singh & Singh, 2013; N. Singh & Todwal, 2018; Sitompul et al., 2018), transformasi domain frekuensi (misalnya, Discrete Cosine Transform atau DCT) (Jeevitha & Amutha Prabha, 2018; Sathisha et al., 2011), dan teknik berbasis deep learning (Dutta et al., 2020). Pengetahuan ini kemudian divalidasi melalui eksperimen untuk memastikan bahwa informasi yang disembunyikan sulit dideteksi, sekaligus tetap mempertahankan kualitas media host (Fyffe et al., 2019; Mukherjee & Sanyal, 2017; Saad Ahmed et al., 2021; A. Singh & Singh, 2013). Epistemologi dalam steganografi juga menekankan kolaborasi ilmiah melalui publikasi, terutama dalam komunitas keamanan informasi (Rushdi & Ba-rukab, 2005; Venukumar & Pathari, 2016; Wijaya et al., 2018). Perkembangan algoritma dan metode baru sering kali didasarkan pada riset-riset sebelumnya, sehingga menciptakan basis pengetahuan kumulatif yang baru (Pal & Madhavan, 2002; Po-Hsian, 2010; Rao & Pandit, 2007; Ratan & Veni Madhavan, 2002).

Pengetahuan Eksplisit dan Pengetahuan Implisit dalam Steganografi Pengetahuan Eksplisit

Pengetahuan ini tersedia secara publik, seperti algoritma dan kode yang diterbitkan dalam artikel ilmiah atau

jurnal. Misalnya, algoritma LSB (Jeevan & Krishnakumar, 2019; Mythreyi & Vaidehi, 2007; S. Singh & Singh, 2014; Sitompul et al., 2018), Most Significant Bit (MSB), metode hybrid (Saad Ahmed et al., 2021), deteksi tepi, pengacakan, transformasi diskrit (Kaur Brar & Sharma, 2018; N. Singh & Todwal, 2018), dan histogram dapat dipelajari dan digunakan oleh siapa saja dengan mengakses artikel ilmiah yang telah terpublikasi.

Pengetahuan Implisit

Hal ini melibatkan keterampilan praktis dan pemahaman intuitif yang tidak selalu terdokumentasi, seperti pengalaman mendeteksi steganografi secara manual atau menggunakan teknik heuristic (Bonavoglia, 2022). Keahlian ini sering kali menjadi milik profesional keamanan dan peneliti yang berpengalaman (Fyffe et al., 2019; Karampidis et al., 2018; M et al., 2019).

HASIL DAN PEMBAHASAN

Validasi Pengetahuan dan Pengujian Algoritma

Pengujian dan validasi algoritma menjadi aspek penting dalam epistemologi steganografi. Validasi ini dilakukan dengan mengukur rasio keberhasilan penyembunyian informasi dengan menggunakan pengujian, Peak Signal to Noise Ratio (PSNR) (Michaylov & Sarmah, 2024; Sairam & Boopathybagan, 2019), Mean Square Error (MSE) (Michaylov & Sarmah, 2024; Sirisha et al., 2018), Mean Absolute Error (MAE), atau Histogram Similarity (HS) (Ratan & Veni Madhavan, 2002; Sitompul et al., 2018), kualitas media host, dan kemampuan metode untuk menghindari deteksi. Pengetahuan ini berkembang melalui eksperimen berulang dan analisis statistik, yang membantu memperbaiki algoritma atau mengembangkan metode baru.

Selain itu, proses validasi juga mencakup pengujian terhadap serangan deteksi (steganalysis), yaitu upaya pihak ketiga untuk mengidentifikasi informasi tersembunyi. Setiap kali sebuah algoritma berhasil dipecahkan, maka peneliti mendapatkan pengetahuan baru yang dapat diterapkan untuk menciptakan metode yang lebih aman lagi.

Epistemologi dan Tantangan Teknologi Baru

Seiring berkembangnya teknologi, tantangan baru dalam steganografi juga muncul. Penggunaan machine learning dan deep learning untuk mendeteksi informasi tersembunyi telah menciptakan persaingan dalam pengembang teknik steganografi dan steganalysis. Oleh karena itu, epistemologi steganografi berfokus pada bagaimana pengetahuan dapat berkembang secara dinamis untuk menghadapi ancaman dan menciptakan solusi baru.

Epistemologi dalam steganografi tidak hanya berfokus pada bagaimana teknik-teknik penyembunyian informasi ditemukan dan dikembangkan, tetapi juga berfokus pada proses pengujian dan validasi pengetahuan tersebut. Hal ini berperan penting dalam memastikan bahwa metode steganografi mampu mengimbangi perkembangan ancaman dalam dunia keamanan data. Dengan memahami epistemologi, peneliti dan praktisi dapat berinovasi dan mengembangkan sistem keamanan yang lebih andal dan adaptif.

Aksiologi Dalam Steganografi

Aksiologi dalam steganografi berkaitan dengan nilai-nilai etis, manfaat, dan dampak sosial dari penerapan teknik penyembunyian pesan. Hal ini mencakup pertanyaan tentang bagaimana steganografi digunakan; apakah untuk tujuan baik atau buruk; dan konsekuensi moral dari penggunaannya.

Manfaat dan Nilai Positif Steganografi

Keamanan dan privasi membahas dalam steganografi membahas tentang steganografi dapat melindungi data sensitif, seperti komunikasi diplomatik,

intelijen militer, atau data transaksi keuangan. Selain keamanan dan privasi, aksiologi juga membahas kebebasan berbicara dan berekspresi dalam metode steganografi, dalam kondisi represif, steganografi memungkinkan peneliti dan praktisi berkomunikasi tanpa terdeteksi oleh otoritas.

Dampak Etis dan Penyalahgunaan

Namun, steganografi juga memiliki potensi disalahgunakan untuk tujuan berbahaya. Dampak etis dan penyalahgunaan steganografi dapat dibagi menjadi dua bagian, yaitu kejahatan siber dan penyalahgunaan data. Kejahatan siber mendeskripsikan pelaku kriminal yang dapat menyembunyikan perintah atau malware dalam media digital. Sedangkan penyelundupan data dapat dideskripsikan tentang informasi ilegal dapat dikirim melalui platform terbuka tanpa terdeteksi, seperti gambar atau video di media sosial.

Pertimbangan Etis dan Regulasi

Aksiologi menekankan pentingnya tanggung jawab dalam pengembangan dan penerapan teknik steganografi. Peneliti dan praktisi keamanan perlu mempertimbangkan apakah metode steganografi memperkuat perlindungan atau membuka peluang baru bagi kejahatan. Hal ini menimbulkan kebutuhan akan kebijakan dan regulasi yang jelas, guna memastikan bahwa steganografi digunakan untuk kepentingan masyarakat dan bukan untuk merugikan.

Aksiologi dalam steganografi mendorong para penliti dan praktisi untuk mempertimbangkan dampak etis dari teknologi ini, baik manfaat maupun risiko. untuk kebaikan publik yang dapat meminimalkan potensi penyalahgunaan.

SIMPULAN

Steganografi penting karena metode ini sangat efektif untuk menyembunyikan informasi sensitif dalam media yang tampaknya tidak mencurigakan. Dengan meningkatnya ancaman terhadap privasi dan keamanan data, mempelajari steganografi menjadi krusial dalam hal melindungi privasi karena membantu individu dan organisasi menjaga informasi pribadi agar tidak jatuh ke tangan yang salah; keamanan data karena menambahkan lapisan perlindungan pada data sensitif, terutama dalam transaksi digital; mencegah penyadapan karena mengurangi risiko deteksi dan penyadapan informasi oleh pihak ketiga. Dengan memahami steganografi, para profesional keamanan informasi dapat merancang sistem yang lebih robust dan efisien dalam melindungi data. Tinjauan ontologi, epistemologi, dan aksiologi memberikan kerangka filosofis yang komprehensif dalam memahami dan mengembangkan steganografi. Secara ontologis, steganografi mengkaji eksistensi informasi tersembunyi dan interaksinya dengan media digital, membentuk realitas ganda antara media host dan pesan rahasia. Epistemologi berperan dalam pengembangan dan validasi pengetahuan mengenai teknik penyembunyian dan deteksi pesan, memastikan metode yang digunakan mampu bertahan terhadap tantangan keamanan. Sedangkan perspektif aksiologi, steganografi memunculkan persoalan etis antara manfaatnya dalam melindungi privasi dan risikonya sebagai alat kejahatan siber, menuntut regulasi, pertanggungjawaban dan kebijakan yang jelas.

DAFTAR PUSTAKA

Atawneh, S., Almomani, A., & Sumari, P. (2013). Steganography in digital images: Common approaches and tools. IETE Technical Review, 30(4), 344. https://doi.org/10.4103/0256-4602.116724

Bonavoglia, P. (2022). The ciphers of the Republic of Venice an overview. Cryptologia, 46(4), 323–346. https://doi.org/10.1080/01611194.2021.1901797

Dehshibi, M. M., Shanbehzadeh, J., &

Pedram, M. M. (2018). A robust image-based cryptology scheme based on cellular non-linear network and local image descriptors. International Journal of Parallel, Emergent and Distributed Systems, 35(5), 514–534. https://doi.org/10.1080/17445760.2018.1510929

Dutta, H., Das, R. K., Nandi, S., & Prasanna, S. R. M. (2020). An Overview of Digital Audio Steganography. IETE Technical Review, 37(6), 632–650. https://doi.org/10.1080/02564602.2019.1699454

Fyffe, B., Wang, Y., & Duncan, I. (2019). Human visual based perception of steganographic images. Journal of Cyber Security Technology, 3(2), 61–107. https://doi.org/10.1080/23742917.2019.1609393

Jeevan, K. M., & Krishnakumar, S. (2019). Image hiding technique using a pseudo hexagonal structure approach. International Journal of Computers and Applications, 41(5), 359–366. https://doi.org/10.1080/1206212X.2018.1438037

Jeevitha, S., & Amutha Prabha, N. (2018). A COMPREHENSIVE REVIEW ON STEGANOGRAPHIC TECHNIQUES AND IMPLEMENTATION. ARPN Journal of Engineering and Applied Sciences, 13(17). www.arpnjournals.com

Karampidis, K., Kavallieratou, E., & Papadourakis, G. (2018). A review of image steganalysis techniques for digital forensics. Journal of Information Security and Applications, 40, 217–235. https://doi.org/10.1016/j.jisa.2018.04.005

Kaur Brar, R., & Sharma, A. (2018). A Review on Steganography. International Journal of Computer and Information Technology, 7(1), 45–48. www.ijcit.com

Klubsuwan, K., & Mungsing, S. (2009). Digital data security and hiding on virtual reality video 3D GIS. International Journal of Management Science and Engineering Management, 4(3), 163–176. https://doi.org/10.1080/17509653.2009.10684575

M, H. F., I, E. H., & A, A. A. (2019). Internet of Things Applications and its Security. International Journal of Computer Applications, 182(41), 9–11. www.ijcaonline.org

Mahajan, P. (2014). Steganography: A Data Hiding Technique. International Journal of Advanced Research in Computer Science and Software Engineering, 4(11), 759–763. https://www.researchgate.net/publication/344412253

Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A Review on Text Steganography Techniques. Mathematics, 9(21), 2829. https://doi.org/10.3390/math9212829

Michaylov, K. D., & Sarmah, D. K. (2024). Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations. Journal of Cyber Security Technology, 1–27. https://doi.org/10.1080/23742917.2024.2304441

Mukherjee, S., & Sanyal, G. (2017). Enhanced Position Power First Mapping (PPFM) based image steganography. International Journal of Computers and Applications, 39(2), 59–68. https://doi.org/10.1080/1206212X.2016.1273624

Mythreyi, S., & Vaidehi, V. (2007). Gabor Transform based Image Steganography. IETE Journal of Research, 53(2), 103–112. https://doi.org/10.1080/03772063.2007.10876126

Nasution, M. K. M., Hidayat, R., & Syah, R. (2022). Computer Science. International Journal on Advanced Science, Engineering and Information Technology, 12(3), 1142.

https://doi.org/10.18517/ijaseit.12.3.14832

Nasution, M. K. M., Onrizal, & Aulia, I. (2019). Design of the research problem statement. Journal of Physics: Conference Series, 1235(1), 012115. https://doi.org/10.1088/1742-6596/1235/1/012115

Nasution, M. K. M., Sitompul, O. S., Elveny, M., & Syah, R. (2021). Data science: A Review towards the Big Data Problems. Journal of Physics: Conference Series, 1898(1), 012006. https://doi.org/10.1088/1742-6596/1898/1/012006

Pal, S. K., & Madhavan, C. E. V. (2002). Investigating Steganographic Communications. IETE Technical Review, 19(4), 207–212. https://doi.org/10.1080/02564602.2002.11417033

Po-Hsian, H. (2010). A weight-based data hiding method for binary image using selective binary numeral system. Journal of Discrete Mathematical Sciences and Cryptography, 13(5), 429–444. https://doi.org/10.1080/09720529.2010.10698305

Rao, N. V., & Pandit, S. N. N. (2007). Multimedia Digital Rights Protection Using Watermarking Techniques. Information Systems Security, 16(2), 93–99. https://doi.org/10.1080/10658980701322528

Ratan, R., & Veni Madhavan, C. E. (2002). Steganography based Information Security. In IETE Technical Review (Vol. 19, Issue 4).

Rushdi, A. M., & Ba-rukab, O. M. (2005). Fault-tree modelling of computer system security. International Journal of Computer Mathematics, 82(7), 805–819. https://doi.org/10.1080/00207160412331336017

Saad Ahmed, S., Memon, M., Jaffari, R., & Jawaid, M. (2021). StegoBound: A Novel Image Steganography Technique Using Boundary-Based LSB Substitution. Journal of Hunan University Natural Sciences, 48(6), 153–163.

Sairam, T. D., & Boopathybagan, K. (2019). Computational intelligence-based steganalysis comparison for RCM-DWT and PVA-MOD methods. Automatika, 60(3), 285–293. https://doi.org/10.1080/00051144.2019.1579434

Sathisha, N., Kasukurthi Suresh, B., B, R. K., & Patnaik, L. M. (2011). EMBEDDING INFORMATION IN DCT COEFFICIENTS BASED ON AVERAGE COVARIANCE. International Journal of Engineering Science and Technology, 3(4), 3184–3194. https://www.researchgate.net/publication/266333755

Singh, A., & Singh, S. (2013). A Review on the Various Recent Steganography Techniques. IJCSN International Journal of Computer Science and Network, 2(6), 142–156. www.IJCSN.org

Singh, N., & Todwal, V. (2018). A Review of Steganography. International Journal of Innovative Science and Research Technology, 3(1), 723–728. www.ijisrt.com

Singh, S., & Singh, A. (2014). An Information Security Technique Using DES-RSA Hybrid and LSB. International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), 355(14), 187–192. https://www.researchgate.net/publication/278329872

Sirisha, B. L., Kumar, S. S., & Mohan, B. C. (2018). Secret image sharing using eigenvalues and eigenvectors. Journal of Information and Optimization Sciences, 39(4), 871–878. https://doi.org/10.1080/02522667.2017.1383659

Sitompul, O. S., Naibaho, F. R., Situmorang, Z., & Nababan, E. B. (2018). Steganography with Highly

Random Linear Congruential Generator for Security Enhancement. 2018 Third International Conference on Informatics and Computing (ICIC), 1–6. https://doi.org/10.1109/IAC.2018.8780445

Srinivasan, K., Gowthaman, T., & Kanakaraj, J. (2017). A novel copyright marking approach using steganography and robust RSA asymmetric-key cryptographic technique in audio files. Journal of Discrete Mathematical Sciences and Cryptography, 20(8), 1563–1571. https://doi.org/10.1080/09720529.2017.1402575

Venukumar, V., & Pathari, V. (2016). A survey of applications of threshold cryptography—proposed and practiced. Information Security Journal: A Global Perspective, 25(4–6), 180–190. https://doi.org/10.1080/19393555.2016.1251996

Wijaya, B. A., Nasution, M. K. M., & Zamzami, E. M. (2018). The steganographic video analysis uses combination of discrete cosine transform and discrete wavelet transform algorithms. Journal of Physics: Conference Series, 1116(2), 022046. https://doi.org/10.1088/1742-6596/1116/2/022046

Yasin, V., Zarlis, M., & Nasution, M. K. M. (2018). FILSAFAT LOGIKA DAN ONTOLOGI ILMU KOMPUTER. Journal of Information System, Applied, Management, Accounting and Research, 2(2), 68–75. http://journal.stmikjayakarta.ac.id/index.php/jisamar