IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Evolution Of Web-Based Steganography Techniques: Trends, Challenges And Future Directions

[1]Deepa S R[0000-0002-2071-9050],[2]Amita S,[3]Srushti Kumar, [4]Triya Hiremath

[1]Professor, [2]Student, [3]Student, [4]Student

[1]Department of CS&D,

[1]K.S. Institute of Technology, Bengaluru,India

Abstract: Steganography based on web technologies has improved in recent years from simple HTML and CSS manipulation to advanced techniques using artificial intelligence and advanced web APIs with cross-platform implementations. This review article analyses the progress, trends now, issues, and ways forward in web-based steganography. Classical steganography conceals data in images or sound, while web-based steganography extends this to web technologies. We review recent papers on methods such as HTML, CSS, JavaScript, HTTP headers, and web storage. Our research shows an increasing trend in web-based steganography applications of deep learning, especially those that utilize browser-native functionalities. Important research shortcomings are cross-browser compatibility, the absence of standardized metrics for evaluation, and few studies on steganalysis specific to the web. This review will be an asset to information security, data hiding, and web technology researchers and practitioners.

Index Terms - Web-Based Steganography, HTML Data Hiding, Web Page Steganography, Browser-Based Information Hiding, Network Security, Web Technology Encryption, Data Protection Strategies.

I. INTRODUCTION

Throughout history, many techniques were created in order to conceal information and have secure channels of communication. Through technologies and new ideas, today it has become possible to embed data in nearly any form of file, text, images, video, audio, or even the control flow charts of programs by altering their binary code.

Steganography, the science of concealing information in plain sight, is distinct from cryptography, which deals with encrypting information to render it unintelligible to unauthorized parties. Steganography has its roots in ancient history. Greek historian Herodotus recorded how Histaeus, a noble, tattooed a hidden message on a slave's scalp, which was not discovered until the hair grew back. During World War II, the Germans created the Microdot method, where data, especially photos, were reduced to the size of a very small dot and became close to undetectable. Presently, digital steganography uses different multimedia types and network-based channels of delivery to conceal data.

Whereas cryptography provides confidentiality by encrypting data, steganography hides its existence. Yet both are limited—if concealed information is in doubt, then steganography is defeated. Thus, steganography integrated with cryptography strengthens security, where it becomes more challenging to recognize and decode concealed messages.As deep learning (DL) increases and massive data is available, machine learning algorithms are being applied more and more to steganography. Methods based on deep learning, such as Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs), have proved very effective in hiding as well as revealing concealed messages. These make their way into the development of steganographic and steganalysis methods by enhancing security as well as detection rates.

This paper offers an exhaustive review of recent steganographic techniques, trends, and challenges. It further investigates publicly accessible datasets, typical assessment metrics, and a comparative study of numerous techniques.

II. LITERATURE REVIEW

2.1 Image Steganography

1. *Steganography on JPEG Images: Issues and Challenges – Kumar, R. et al. (2024):* Reviewed the inherent limitations and challenges in applying steganography on JPEG images, especially due to lossy compression artifacts and format-specific constraints, highlighting the trade-offs between capacity, robustness, and imperceptibility in real-world scenarios [1].
2. *Review of recent advances in image steganography: Akshaya Kumar et al. (10 November 2022):* The work suggested an extensive review of recent advances in image steganography, such as spatial domain manipulation, encryption-based approaches, and deep approaches, and evaluated how different types of images influence different steganographic approaches [2].
3. *Robust Image Steganography – Jinyuan Tao et al. (2019):* Proposed robustness-focused methods for image steganography, utilizing distortion functions and optimization frameworks to improve resistance against image processing and steganalysis, especially in low redundancy scenarios [3].
4. *Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends – Inas J. Kadhim et al. (2019):* Provided a detailed survey of image steganography methods, evaluations, and challenges, comparing spatial, transform, and hybrid domain approaches while identifying open issues and future research directions [4].
5. *Steganography and Classification of Image Steganography Techniques – Sumeet Kaur et al. (2014):* Classified various image steganography techniques into distinct categories based on algorithmic principles, offering a structured overview to aid the selection and development of suitable methods for diverse applications [5].
6. *Image Steganalysis Based on Pretrained Convolutional Neural Networks – Taha Ahmed et al. (2022):* Demonstrated the effectiveness of transfer learning using pretrained CNNs for identifying steganographic patterns in digital images, emphasizing minimal training data requirements for high accuracy [6].
7. *Edge Adaptive Image Steganography Based on LSB Matching Revisited – Weiqi Luo et al. (2010):* Introduced an edge-adaptive method leveraging LSB matching to increase embedding efficiency and security by focusing on image regions less susceptible to visual distortions [7].
8. *Hiding Data in Images Using Steganography techniques with compression algorithms – Osama F. Abdel Wahab et al. (2019):* Employed compression techniques along with traditional steganography to enhance data concealment efficiency and payload optimization while preserving image quality [8].
9. *Research on image compression technology based on Huffman coding – Shuyun Yuan et al. (2019):* Explored Huffman coding for image compression, emphasizing its potential integration with steganographic techniques for space-efficient data hiding applications [9].
10. *An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection – Marwa M. Emam et al. (2016):* Proposed an LSB-based steganography method that introduces random pixel selection to increase unpredictability and reduce steganalysis vulnerability [10].
11. *An image steganography approach based on k-least significant bits (k-LSB) – O. Elharrouss et al. (2020):* Explored a k-LSB embedding approach, balancing between higher data hiding capacity and imperceptibility, with experiments validating its efficiency over traditional single-bit LSB [11].
12. *A Survey on Digital Image Steganography – Zaid Y. Al-Omari et al.(2015):* Presented a broad review of digital image steganography, discussing fundamental principles, classification, and performance metrics to guide future design choices [12].
13. *A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method – S. Rahman et al. (2022):* Introduced an improved LSB substitution technique that optimizes data embedding efficiency while maintaining high image quality and imperceptibility, with experimental validation demonstrating robustness against statistical and visual steganalysis methods [13].

2.2 Hybrid Cryptography-Steganography Techniques

1. *Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques: Osama F. Abdel Wahab et al. (2021):* Demonstrated enhanced protection of information through hybrid techniques combining RSA cryptography and compression steganography, highlighting hybrid security aspects above single-technique approaches [14].

2. *Handbook of Applied Cryptography – A. Menezes et al.(2018):* Offered foundational and in-depth coverage of cryptographic principles including symmetric/asymmetric encryption, hash functions, and key management, serving as a critical reference for designing secure cryptographic systems in steganographic applications [15].
3. *How to Pretrain for Steganalysis – Jan Butora et al. (2021):* Investigated the use of self-supervised and contrastive learning strategies for pretraining deep learning models, significantly enhancing steganalysis accuracy in detecting hidden content [16].
4. *An improved Security and Message Capacity Using AES and Huffman Coding on image steganography – C. A. Sari et al. (2019):* Combined AES encryption with Huffman-based compression and LSB steganography to boost payload capacity and security, demonstrating superior performance compared to traditional LSB schemes [17].

2.3 Webometric and Text Steganography

1. *Text steganography in webometrics: ShabnamRahberYaghobi et al. (2021):* Investigated webometric text steganography, highlighting implications toward web communication media adaptations [18].
2. *Hiding in the Plain Text: A Critical Analysis of Whitespace Steganography – Chunduru et al. (2021):* Critically analyzed the potential and limitations of whitespace-based text steganography, evaluating its stealthiness, efficiency, and application scope in plaintext mediums [19].

2.4 Web-Based Steganography

1. *Web-Based Data Concealment: A Hybrid Approach that Combines Steganography and Visual Cryptography: SeniruEdiriweera et al. (2023):* Suggested a hybrid approach that combines steganography and visual cryptography for web-based scenarios, demonstrating multi-perspective data safeguarding methods [20].
2. *A Dynamic Steganography method for Web Images with Average Run-Length-Coding: Jin Liu et al. (2021):* Demonstrated dynamic steganography for web images using Average Run-Length-Coding to address modern content delivery challenges [21].
3. *Steganography using HTML Web Pages as Carrier: A Survey: Ishita Bajaj et al. (2019):* Listed HTML web pages as steganographic carriers and investigated their usage and shortcomings in covert communication [22].
4. *A Time-Based Dynamic Operation Model for Webpage Steganography Methods: S. Yuk et al. (2020):* Introduced adaptive and context-aware webpage steganography using time-based dynamic operations [23].
5. *HTML5 Zero Configuration Covert Channels: Security Threats and Challenges: Jason Farina et al. (2015):* Embraced security vulnerabilities of HTML5 covert channels, revealing the vulnerabilities of modern web technologies [24].
6. *Information Hiding in CSS: A Secure Scheme Text-Steganography using Public Key Cryptosystem: Herman Kabetta et al. (2012):* Formulated CSS-based steganography with public key cryptosystems, laying the groundwork for style-based methods [25].

2.5 Detection and Security Mechanisms

1. *Hiding in Plain Site: Detecting JavaScript Obfuscation through Concealed Browser API Usage: ShaownSarker et al. (2020):* Explored JavaScript obfuscation detection via camouflaged browser API usage, contributing to steganography-detection studies [26].

2.6 Database and Content Protection

1. *STEGANODB-A Secure Database through Steganography: Rejani et al. (2013):* Employed steganography for protecting databases, embedding sensitive information into innocuous database structures [27].
2. *Web Content Signing using Service Workers: Thomas Sutter et al. (2021):* Examined service workers in web content signing, enhancing data integrity via advanced verification processes [28].

2.7 Comprehensive Reviews

1. *A Brief Review on Various Aspects of Steganography Followed by Cryptographic Analysis: A. Agarwal, Sandeep Malik (2022):* Provided steganographic and cryptographic approach critical analysis, emphasizing finer data security aspect [29].
2. *Deep Learning Applied to Steganalysis of Digital Images: A Systematic Review: T.-S. Reinel, R.-P. Raúl, and I. Gustavo (2019):* Provided a comprehensive review of deep learning techniques in the domain of

image steganalysis, evaluating various architectures like CNNs and RNNs, their effectiveness in detecting steganographic content, and outlining future research directions in automated steganalysis [30].

III. THEORETICAL BACKGROUND

3.1 Introduction to Web-Based Steganography

Steganography, being a combination of the Greek words "steganos" (covered) and "graphein" (writing), is the science and art of concealing information within apparently innocent carriers in such a manner that the fact that the information exists at all may not be discoverable by unprivileged observers. While classical steganography has largely concerned digital media files like images, sound, and video, web-based steganography applies these principles to the dynamic and sophisticated World Wide Web platform. Web-based steganography is a reference to methods that use web technologies, protocols, and platforms as carriers for hidden information to support covert communication using websites, web applications, and related web resources. While the web keeps expanding as a main source of information exchange and communication, web-based steganography methods have also increased in intellectual level and variation in use.

3.2 Significance of Research in Web-Based Steganography

Web steganography has double functions in computer security: providing legitimate covert communications while possibly offering malicious activities such as malware delivery and information piracy. Its utility arises from global web access with the ability to evade conventional security measures. Privacy groups find such methods useful to maintain confidentiality if encryption is limited. With mounting digital surveillance, steganography employing ordinary web traffic becomes a resource for those who value their privacy, censorship-beleaguered journalists, and whistleblowers. The continuously changing web technology environment poses ever-evolving research contexts where there is an ongoing need to develop detection tools and countermeasures.

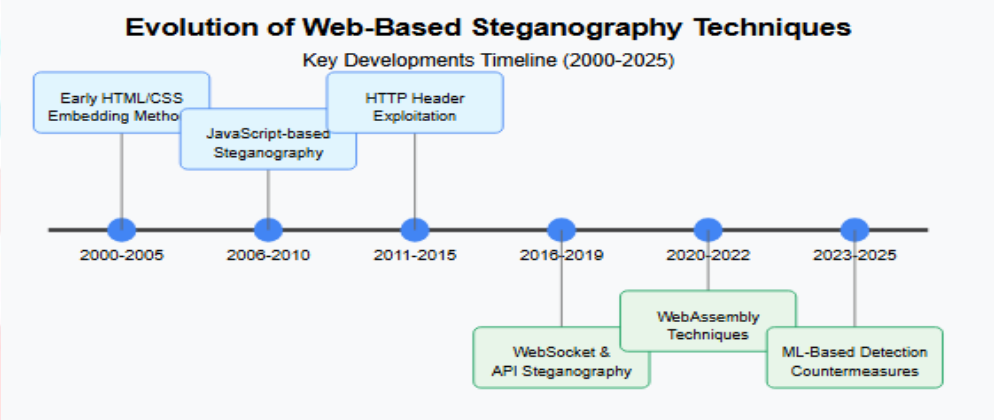

Figure 3.1: Evolution of web-based Steganography Techniques.

3.3 Historical Evolution of Web-Based Steganography

The history of web steganography has paralleled web technology advancements. Older methods (1990s-2000s) employed straightforward HTML alterations such as whitespace adjustment, concealed comments, and color-conformant text, with limited capacity and weak concealment. As technology improved, techniques utilized image steganography in web contexts. Figure 3.1 shows the timeline of evolution of Web-based Steganography techniques.

New techniques developed with CSS to hide information through style attribute manipulation. HTML5 significantly increased the scope with new APIs (Canvas, Web Storage, WebRTC, Service Workers) that provided new covert channels. Modern web steganography now goes beyond browsers to servers, network protocols, and cross-origin communication, making it a rich environment of information hiding methodologies.

IV. METHODOLOGY

4.1 Web-Based Image Steganography

Image steganography is the core aspect of web-based information hiding, owing to the ubiquity of images on the web and their high data hiding capacity. Figure 4.1 dhows the specific and major categories of Web-based Steganography. Recent trends have moved away from mere Least Significant Bit (LSB) substitution methods towards more sophisticated techniques that maintain image quality while improving detection resistance. The increasing use of adaptive embedding algorithms, which examine image characteristics to determine optimal locations for data embedding that reduce visual distortions. This trend is

of special interest to web applications as user interaction is directly impacted by image quality. There has also been significant growth in the use of deep learning methods in image steganography, particularly the employment of Generative Adversarial Networks (GANs) in the generation of cover images specifically designed for steganographic use. Such methods are especially beneficial in online platforms, as images are subject to a range of transformations—resizing, compression, and format conversion—during the transmission and display process.

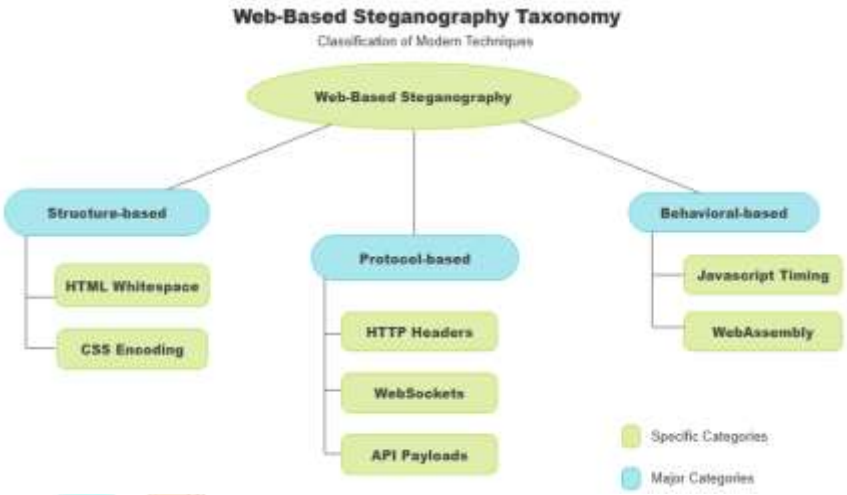

Figure 4.1: Web-based Steganography Modern Techniques

4.2 Steganography Using CSS and HTML

CSS enables strong steganographic possibilities by the slight manipulation of properties such as color values, coordinates, and transformations that are imperceivable to the naked eye but effective enough for embedding data. For instance, altering a color from #3A7CB9 to #3A7CB8 is visually indistinguishable yet can be used to encode data. HTML structure also allows for steganography by means of attribute ordering, identical tag structures, and optional element manipulation. HTML5's custom data attributes (data-*) are especially good carriers because they don't impact rendering while leaving legitimate-looking containers for concealed data that can pass casual inspection.

4.3 JavaScript-Based Steganography

JavaScript has revolutionized web-based steganography by making dynamic and adaptive hiding of information possible. Scientists have investigated embedding data via code structure, naming conventions, and execution patterns without compromising functionality. In addition to static properties, runtime behaviors such as timing variability and memory access further contribute to concealment. Browser APIs, particularly the Canvas API, provide pixel-level manipulation akin to classical image steganography. Moreover, WebAssembly offers new opportunities for covert data embedding owing to its binary form and optimized execution.

4.4 HTTP Header Steganography

The application of communication-level steganography using HTTP headers is a fresh trend in the area of web-based information hiding methods. There works that show that even in deeply controlled deep packet inspection-based environments, there is typically an inability to detect anomalies in header structure, sequence, or rate, as long as these changes adhere to protocol specifications. This approach is of specific interest because it operates at the protocol layer rather than the content layer, and therefore its performance even when web content is encrypted through HTTPS. Modern implementations increasingly leverage temporal patterns across a series of requests to achieve greater capacity while, at the same time, reducing detectability, effectively diffusing the steganographic signature across a session rather than focusing it in individual transactions.

4.5 Web Storage Steganography

The emergence of client-side storage technologies like local Storage, Session Storage, IndexedDB, and the Cache API has brought new opportunities for web-based steganography. The StegoBrowser implementation showed how random patterns of data storage can hide information in data belonging to seemingly legitimate applications, using methods that rely on key naming schemes, value encoding schemes, and storage timing to encode additional information beyond what is stored. Cross-origin features that are a part of some of the storage mechanisms provide especially interesting opportunities for steganography because they

could provide covert communication between otherwise unrelated websites—a feature that has important implications for security research and possible malicious exploitation.

V. CHALLENGES IN WEB-BASED STEGANOGRAPHY

5.1 Detection and Steganalysis

The biggest challenge to web-based steganography is the development of effective detection methods (steganalysis) that are specifically designed for web environments. Unlike traditional media steganography, where files can be analysed in isolation, web-based methods must contend with the dynamic, interconnected nature of online content and the sheer diversity of technologies involved. Researchers have taken significant steps in this direction with their WebStegNet framework, which employs deep learning methods to identify steganographic content in several web components at once. Their research also identified the challenges of maintaining detection capability across a range of browsers, device types, and network environments—factors that can have a significant impact on web content rendering and processing. Statistical analysis methods that are effective for static media files are ineffective when applied to web components due to the inherent volatility of web content and the complex interactions between web page components.

5.2 Capacity Limitations

The achievement of a high data hiding capacity, with the maintenance of undetectability, is a key issue in the area of web-based steganography. While some carriers, likeimages, have the potential to hide large amounts of information, many web-specific techniques—ranging from CSS manipulation to changes in HTML structure—have severely limited capacity. This limitation necessitates that practical applications must withstand difficult trade-offs in the amount of information concealed versus detection risk. Recent researchers have addressed this problem by using adversarial machine learning techniques that actively optimize embedding patterns in response to the unique characteristics of each carrier element, thereby achieving impressive capacity gains without compromising security against existing detection methods. Nevertheless, their solution also acknowledged that scalability of capacity is still an issue for web-based techniques, particularly for time-critical communications that cannot be split across sessions or pages.

5.3 Robustness against Web Transformations

Web steganography is severely challenged by content changes that take place during transmission, processing, and rendering, with CDNs, proxy servers, caching systems, and optimization software frequently modifying web resources in a manner that can destroy concealed information. Normal web development techniques such as JavaScript minification, CSS optimization, image transcoding, and HTML restructuring directly threaten steganographic applications, requiring creative countermeasures. One potential solution is to intercept and alter content at the browser level once all server-side and network-level modifications have been made, essentially fixing robustness problems by operating on the final rendered content; however, this solution necessitates advanced client-side implementation via browser extensions, restricting its use for users who cannot or will not install extra software and introducing a basic trade-off between steganographic robustness and usability.

5.4 Browser Compatibility

The heterogeneity of rendering engines and web browsers presents particular difficulties to web-based steganography. Methods that work perfectly in one browser completely fail in another due to differences in rendering algorithms, JavaScript engines, CSS interpretation, or supported features. This problem is particularly important for steganographic systems that rely on correct visual rendering or exact timing behaviors, since these factors have considerable differences between browsers. Existing research has grown more interested in finding browser-agnostic methods or developing adaptive methods that modify their embedding strategies based on the detected browser environment. However, in real-world implementations, many functional steganographic systems are designed for particular browsers or browser families primarily, thus accepting the limitation of lower coverage in favor of higher reliability within their target environments.

V. CONCLUSION AND FUTURE SCOPE

Web-based steganography has progressed from basic techniques to advanced methods based on contemporary web technologies and machine learning. While capacity and hiding have improved, countermeasures are behind attackers. The discipline does not have standardized metrics, thorough cross-browser testing, or investigation of emerging technologies such as WebAssembly. Priorities for future research must include the formulation of standardized evaluation frameworks for dealing with web-related

issues, leveraging technologies such as WebAssembly and WebGPU for hardware acceleration, introducing blockchain-based integrity checks and zero-knowledge proofs, developing browser-native steganography APIs, and improving counter-steganography tools such as real-time examination systems. Academic-industry collaboration is crucial to advance the field ethically and avoid misuse.

REFERENCES

[1] Akshaya Kumar, Rajneesh Rani, and Samayveer Singh, "A survey of recent advances in image steganography," Security and Privacy, vol. 6, 2022, doi: 10.1002/spy2.281.

[2] Kumar, R., Bansal, S. and Bansal, R.K., 2024, December. Steganography on JPEG Images: Issues and Challenges. In 2024 International Conference on Communication, Control, and Intelligent Systems (CCIS) (pp. 1-5). IEEE.

[3] Jinyuan Tao, Sheng Li, Xinpeng Zhang, and Zichi Wang, "Towards Robust Image Steganography," IEEE Transactions on Circuits and Systems for Video Technology, 2019, doi: 10.1109/tcsvt.2018.2881118.

[4] Inas Jawad Kadhim, PrashanPremaratne, Peter James Vial, and Brendan Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," Neurocomputing, vol. 335, 2019, doi: 10.1016/j.neucom.2018.06.075.

[5]Sumeet Kaur, S. Bansal, and R. Bansal, "Steganography and classification of image steganography techniques," 2014 International Conference on Computing for Sustainable Global Development (INDIACom), 2014, doi: 10.1109/indiacom.2014.6828087.

[6] Taha Ahmed, B. TareqHammad and N. Jamil, "Image Steganalysis based on Pretrained Convolutional Neural Networks," 2022 IEEE 18th International Colloquium on Signal Processing & Applications (CSPA), Selangor, Malaysia, 2022, pp. 283-286, doi: 10.1109/CSPA55076.2022.9782061.

[7] Weiqi Luo, Fangjun Huang, and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," IEEE Transactions on Information Forensics and Security, vol. 5, 2010, doi: 10.1109/tifs.2010.2041812.

[8] Osama F. Abdel Wahab, A. Hussein, H. Hamed, H. Kelash, A. Khalaf, and Hanafy M. Ali, "Hiding data in images using steganography techniques with compression algorithms," TELKOMNIKA (Telecommunication Computing Electronics and Control), 2019, doi: 10.12928/telkomnika.v17i3.12230.

[9] Shuyun Yuan, and Jianbo Hu, "Research on image compression technology based on Huffman coding," Journal of Visual Communication and Image Representation, vol. 59, 2019, doi: 10.1016/j.jvcir.2018.12.043.

[10]Marwa M. Emam, A. A. Aly, and F. Omara, "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection,", 2016, doi: 10.14569/ijacsa.2016.070350.

[11]O. Elharrouss, N. Almaadeed and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2020, pp. 131-135, doi: 10.1109/ICIoT48696.2020.9089566.

[12]Zaid Y. Al-Omari, and Ahmad T. Al-Taani, "A Survey on Digital Image Steganography," International Conference on Industrial Technology, 2015, doi: 10.15849/icit.2015.0016.

[13]S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan and M. Zakarya, "A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method," in IEEE Access, vol. 10, pp. 124053-124075, 2022, doi: 10.1109/ACCESS.2022.3224745.

[14]Osama F. Abdel Wahab, Ashraf A. M. Khalaf, Aziza I. Hussein, and Hesham F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques," IEEE Access, vol. 9, 2021, doi: 10.1109/access.2021.3060317.

[15]Menezes, P. V. Oorschot, and S. Vanstone, "Handbook of Applied Cryptography,", 2018, doi: 10.1201/9781439821916.

[16]Jan Butora, YassineYousfi, and Jessica Fridrich. 2021. How to Pretrain for Steganalysis. In Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '21). Association for Computing Machinery, New York, NY, USA, 143–148. https://doi.org/10.1145/3437880.3460395.

[17]C. A. Sari, Giovani Ardiansyah, D. Setiadi, and E. H. Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography," TELKOMNIKA (Telecommunication Computing Electronics and Control), 2019, doi: 10.12928/telkomnika.v17i5.9570.

[18]ShabnamRahberYaghobi, and HediehSajedi, "Text steganography in webometrics," International journal of information technology, vol. 13, no. 2, 2021, doi: 10.1007/s41870-020-00572-z.

[19]Chunduru, Eswara Sai Prasad, and Nagendar Rao Koppolu. "Hiding in the Plain Text: A Critical Analysis of Whitespace Steganography." (2021).

[20]SeniruEdiriweera, B.A.S. Dilhara, and ChamaraDisanayake, "Web-Based Data Hiding: A Hybrid Approach Using Steganography and Visual Cryptography," International Conference on Soft Computing and Software Engineering, 2023, doi: 10.1109/scse59836.2023.10214994.

[21]Jin Liu, and Yiwen Zhang, "A Dynamic Steganography Method for Web Images with Average Run-Length-Coding,", 2021, doi: 10.30564/jcsr.v3i1.2735.

[22]Ishita Bajaj, and R. Aggarwal, "Steganography using HTML Web Pages as a Carrier: A Survey," SSRN Electronic Journal, 2019, doi: 10.2139/ssrn.3351033.

[23]S. Yuk, and Youngho Cho, "A Time-Based Dynamic Operation Model for Webpage Steganography Methods," Electronics, 2020, doi: 10.3390/electronics9122113.

[24]Jason Farina, Mark Scanlon, Stephen Kohlmann, Nhien-An Le Khac, and M-TaharKechadi, "HTML5 Zero Configuration Covert Channels: Security Risks and Challenges," arXiv: Cryptography and Security, 2015.

[25]Herman Kabetta, YudiDwiandiyanta, and Suyoto, "Information Hiding in CSS : A Secure Scheme Text-Steganography using Public Key Cryptosystem," ArXiv, 2012, doi: 10.2139/ssrn.3635340.

[26]ShaownSarker, Jordan Jueckstock, and A. Kapravelos, "Hiding in Plain Site: Detecting JavaScript Obfuscation through Concealed Browser API Usage," ACM/SIGCOMM Internet Measurement Conference, 2020, doi: 10.1145/3419394.3423616.

[27]Rejani, R., D. Murugan, and Deepu V. Krishnan. "STEGANODB-A Secure Database using Steganography." ICTACT Journal on Communication Technology 4, no. 3 (2013): 785-789.

[28]Thomas Sutter, Kevin Lapagna, P. Berlich, Marc Rennhard, and Fabio Germann, "Web Content Signing with Service Workers," ArXiv, vol. abs/2105.05551, 2021, doi: 10.21256/zhaw-22514.

[29]Agarwal, and Sandeep Malik, "A Brief Review on Various Aspects of Steganography Followed by Cryptographic Analysis," 2022 IEEE 7th International conference for Convergence in Technology (I2CT), 2022, doi: 10.1109/i2ct54291.2022.9825422.

[30]T. -S. Reinel, R. -P. Raúl and I. Gustavo, "Deep Learning Applied to Steganalysis of Digital Images: A Systematic Review," in IEEE Access, vol. 7, pp. 68970-68990, 2019, doi: 10.1109/ACCESS.2019.2918086.