SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

International Journal of Advanced Research in Computational Thinking and Data Science

Journal homepage:
https://semarakilmu.com.my/journals/index.php/ctds/index
ISSN: 3030-5225

International Journal of
ADVANCED RESEARCH IN COMPUTATIONAL THINKING AND DATA SCIENCE
ISSN 3030 5225

Exploring Steganographic Techniques for Enhanced Data Protection in Digital Files

Roshidi Din[1,*], Ahmad Hamid Shakir[2], Sarmad Hamzah Ali[3], Alaa Jabbar Qasim Almaliki[1], Sunariya Utama[1], Jabbar Qasim Almalik[4]

[1] School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah Darul Aman, Malaysia
[2] Al Muthanna University, College of Nursing, Samawah, Iraq
[3] Al Muthanna University, Computer Center Department, Samawah, Iraq
[4] Ashur University, Department of Medical Instrumentation Technique Engineering College, Baghdad, Iraq

ARTICLE INFO

Article history:
Received 15 February 2024
Received in revised form 20 March 2024
Accepted 24 March 2024
Available online 19 April 2024

Keywords:
Digital steganography; digital watermarks; integrity; covert communications; confidentiality

ABSTRACT

This article delves into the intricate field of digital steganography, a pivotal method for ensuring the confidentiality and integrity of hidden data within digital files. As digital communication continues to evolve, the necessity for robust security measures to protect sensitive information has never been more critical. This research primarily focuses on the exploration of steganographic techniques that not only safeguard the confidentiality of data but also maintain its integrity, thereby ensuring the data remains unchanged and secure from tampering. Additionally, the paper investigates the application of these methods in copyright protection and covert communications, highlighting their significance in the digital era. Through a comprehensive analysis of modern steganographic techniques, this study evaluates their advantages and disadvantages, along with their practical applicability in various information security tasks. The findings underscore the growing relevance of steganography in the face of increasing digital communication, offering insights into its role in military, diplomatic, and commercial domains. By examining digital watermarks and other steganographic tools, this work contributes to the ongoing discourse on digital privacy and security, presenting a nuanced understanding of how hidden data can be effectively embedded within digital files for protection against unauthorized access and use.

1. Introduction

Modern computer data processing technologies have significantly increased the level of information security due to the deep integration of cryptographic tools into information systems. As you know, in contrast to cryptographic information security [1,2], steganographic means first try to hide the very fact of the existence of confidential information. Steganographic methods that hide information in the streams of digitized signals and implemented based on computer technology and software are the subject study of digital steganography [3,4].

[*] *Corresponding author.*
E-mail address: roshidi@uum.edu.my

The relevance of the study of steganography is constantly growing because, with the spread of personal computers, and especially the Internet, the ability to transfer confidential information attracts the attention of a significant number of people. Most theoretical and practical research in the field of steganography is devoted to the development of new and improved existing methods of data concealment [6-8]. The purpose of this work is to study modern steganographic methods, analysis of their advantages and disadvantages, aspects of their practicality application.

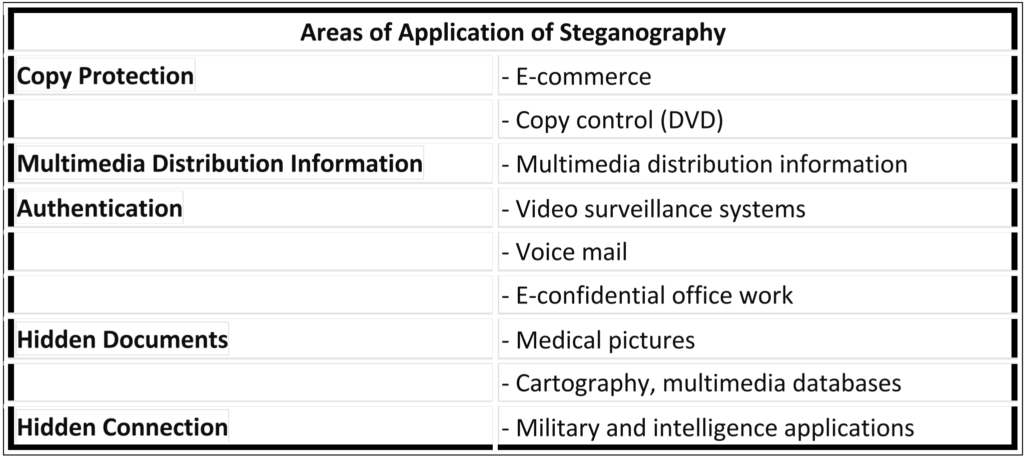
2. Steganography and Digital Watermarks

Digital steganography is a direction of classical steganography, which consists of the implementation of additional information in digital objects (containers), causing some distortion of these objects. This technology is designed to organize a secret relationship, which is a classic task of steganography, but recently it is also used for protecting intellectual property. One of the most effective technical means of protection multimedia information and is to embed in the protected object, invisible digital watermarks (IDW). Unlike ordinary paper watermarks, IDWs can be not only visible but also generally invisible. IDWs are analyzed by the special decoder, which decides on their correctness. IDWs may contain some code, owner information, or any other information [3-6]. The main difference between the problem of hidden data transmission and the problem of embedding the IDW is that in the first case the Unauthorized person must guess about the existence of the hidden message, while in the second case, its existence may not be hidden [7].

3. Application of Steganography Methods for Various Information Security Tasks

Traditionally, interest in steganographic methods has been manifested in the military and diplomatic circles, because until recently the term "steganography" meant only the covert transmission of information. Today, this technology is used in other areas of activity related to information security. Steganographic methods that allow hiding files of various formats, IP packet headers, text messages, and digital media data [8-10].

Table 1
Shows several problems that solve steganographic methods



Areas of Application of Steganography	
Copy Protection	- E-commerce
	- Copy control (DVD)
Multimedia Distribution Information	- Multimedia distribution information
Authentication	- Video surveillance systems
	- Voice mail
	- E-confidential office work
Hidden Documents	- Medical pictures
	- Cartography, multimedia databases
Hidden Connection	- Military and intelligence applications

Table 1 outlines a range of application areas where steganography, the practice of concealing information within another non-secret medium, can provide solutions to various challenges. The table is divided into distinct areas where steganographic techniques are commonly applied, demonstrating the technique's versatility.

- **Copy Protection:** In the domain of e-commerce and digital media, steganography helps protect copyrights by embedding unique information within digital products, like e-books or music files. This can prevent unauthorized copying or distribution. For instance, a steganographic method might hide data within the tracks of a DVD that identifies the original purchaser or source, thus discouraging piracy and aiding in tracking down pirated copies.
- **Multimedia Distribution Information:** Steganography can embed information into multimedia content distributed via platforms such as video-on-demand services. This embedded information can serve as digital watermarks to track distribution, verify authenticity, or manage digital rights, ensuring content producers receive due credit and compensation.
- **Authentication:** In surveillance systems, voice mail, and e-confidential office work, steganography adds an additional layer of security. It can embed authentication codes or watermarks within audio, video, or document files, which can verify the source and integrity of the data, ensuring that it has not been tampered with during transmission or storage.
- **Hidden Documents:** In medical imaging, steganography can conceal patient data within the image itself, ensuring privacy and confidentiality while maintaining quick access to vital information. Similarly, cartographic data and multimedia databases can employ steganography to hide sensitive information within maps or media files, protecting against unauthorized access or manipulation.
- **Hidden Connection:** Military and intelligence applications frequently use steganography for covert communications. Messages hidden within innocuous-looking documents or images can be transmitted without drawing attention, allowing for the secure exchange of sensitive information even when a communication channel is being monitored.

These examples highlight the broad utility of steganography as a tool for enhancing security and privacy across various fields. By embedding data within digital media, steganography offers a way to protect intellectual property, ensure the authenticity and integrity of information, maintain individual privacy, and secure sensitive communications. Its use ranges from commercial applications to critical national defense operations, making it a versatile and invaluable technique in the digital age. The effectiveness of steganography lies in its ability to be undetectable under normal conditions, thus allowing information to be hidden in plain sight. When implemented correctly, it makes the detection and extraction of the hidden information extremely difficult without the proper tools or keys, providing a form of security that complements traditional cryptographic methods.

Furthermore, steganography has evolved with technological advancements. Modern steganographic techniques can handle larger amounts of hidden data with more sophisticated embedding algorithms that make detection by steganalysis (the process of detecting steganography) more challenging. This evolution ensures that as digital media becomes more complex and widespread, steganography remains a critical tool for secure and private information handling in various applications. One of the problems associated with steganography is the variety of requirements for the system depending on the tasks it must solve. For example, the relationship between degrees the security of the size of the secret messages will vary depending on the purpose of the stego system [11,12]. To protect copyright, it is important that the watermark be stable before deleting or distorting, but the amount of information it contains may be small. For covert communication, on the other hand, the amount of information transmitted is much higher. Less resistance to container modifications becomes important, it must be sufficient to read hidden information. In Fig. 1 shows the relationship between the degree of security of the size of secret message [13-16].

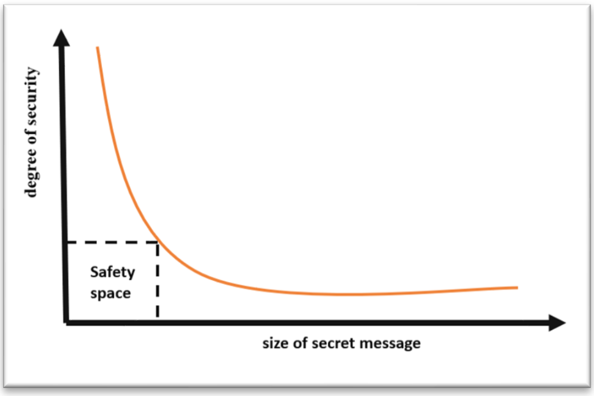


Fig. 1. The relationship between the degree of security of the size of secret message

In figure 1 The graph provided represents the relationship between the size of a secret message and the degree of security offered by steganography, which is the practice of hiding messages within other non-secret, seemingly innocuous messages, or media.

The y-axis, labeled "degree of security," indicates the level of protection against detection and/or deciphering of the hidden message. The x-axis represents the "size of secret message," showing that as the size of the embedded message increases, the degree of security typically decreases.

The curve begins high on the y-axis, suggesting that smaller messages enjoy a higher degree of security. This is likely because smaller messages are easier to hide and cause fewer anomalies in the carrier medium, making them less detectable by steganalysis tools. As the size of the secret message increases (moving to the right along the x-axis), the curve sharply declines and then gradually flattens out. This indicates a rapid decrease in security for an initial increase in message size, after which the decrease in security becomes more gradual. The point at which the curve begins to flatten marks the threshold beyond which increases in the message size do not significantly compromise the security. The "Safety space" delineated by the dashed line suggests an optimal range within which the size of the secret message is both practical and secure. Beyond this safety space, the risk of detection or deciphering increases, potentially compromising the hidden message.

This relationship is critical in steganography, as it illustrates the trade-off between capacity (how much information you can hide) and stealth (how well you can hide it). The graph serves as a guideline for practitioners of steganography to determine the safe limits for embedding secret messages without raising suspicion or making it too easy for the message to be uncovered through steganalysis.

4. Analysis of Existing Steganographic Methods

Elements of the visual environment (digital images and video) are characterized by significant redundancy of various nature:

- **code redundancy,** refers to the surplus coding information present in an image, which goes beyond what is necessary for image reconstruction. In digital images, this redundancy comes from the representation of each pixel with a set number of bits, regardless of whether all those bits are needed to describe the color or intensity accurately. Some pixels could be represented with fewer bits without significant loss of quality, due to the limited sensitivity of the human eye to certain colors or changes in luminance. By exploiting code redundancy, steganography can replace these surplus bits with hidden information, essentially embedding data in places where it will not affect the perceived image quality [3,4,17-19].

- **interpixel redundancy,** arises because adjacent pixels in an image often share similar or correlated color and intensity values. This spatial correlation leads to repetitive information across the image. Steganographic techniques can utilize these correlations by altering pixel values in a way that maintains their correlation with neighbors. Consequently, even though the actual pixel values are changed to encode secret data, the visual similarity between adjacent pixels is preserved, making the alterations imperceptible [2, 20-24].
- **Psychovisual dependence** stems from the human visual system's limitations. Our eyes are not equally sensitive to all visual stimuli; for example, they are more sensitive to luminance changes than to color changes. Moreover, the eye's ability to discern detail is not uniform across the visual field and diminishes in the periphery. Steganography can leverage this by embedding information in areas of the image less likely to be noticed by the human eye, such as in complex textures or in color variations that are less perceptible. The embedded data is placed where it is least likely to be detected visually, taking advantage of the psychovisual properties of human perception[25-29].

Therefore, much of the research in the field of steganography is devoted to methods of concealment confidential messages and digital watermarks (CEI) in still images. Now there are a large number of methods of hiding information and CEV in graphic files. Replacement methods in the spatial domain. A classic example is the method of replacing the younger one’s bit (LSB-method), which is because the lower bits of graphic, audio and video formats carry little information and their change has little effect on the quality of the transmitted image or sound. This makes it possible to use them to encrypt confidential information [30].

The main advantage of this method is the simplicity of implementation and the possibility of secret transfer large amount of information. However, due to the introduction of additional information is distorted the statistical characteristics of the container file and the hidden message are easy to detect by using statistical attacks such as estimating entropy and correlation coefficients. To reduce compromising features, require correction of statistical characteristics[31-36]. The disadvantage of this method is also its sensitivity to digital processing operations: compression, application of filtering, color conversion, geometric transformations, additional noise and format change container.

In methods operating in the frequency domain, the data is hidden in the frequency coefficients presentation of the container. For this purpose, transformations which are used in modern lossy compression algorithms (discrete cosine transforming the JPEG standard and wavelet conversion - in JPEG2000). Hiding information can to be carried out both in the initial image, and simultaneously with implementation of compression of the image of the container [37-39].

It is important that there are stego systems that take into account the peculiarities of the compression algorithm insensitive to further compression of the container. They also provide greater resistance to geometric transformations and transmission channel detection (compared to the LSB method), because there is the ability to vary a wide range of compressed image quality, making it is impossible to determine the origin of distortion [40].

Broadband methods. The essence of these methods is to expand the frequency band of the signal to spectrum width much larger than necessary to transmit real information. For There are two ways to expand the range: the method of direct expansion of the spectrum, using pseudo - random sequence, and the method of abrupt frequency readjustment. At this useful information is distributed over the entire range, so when the signal is lost in some frequency bands in other bands there is enough information to restore it.

The principle of operation of broadband methods is related to the problems solved by stego systems:

try to "dissolve" the secret message in the container and make it impossible detection [41]. Because the signal is distributed across the spectrum, it is difficult to isolate. This is essential the advantage of these methods, as well as resistance to accidental and intentional distortions. That's why they are used in communication technology to ensure high noise immunity and complexity of the process interception and detection. Instead, the disadvantage is the possibility of stego analysis due to digital processing using noise-cancelling filters[8-12, 30, 37-40, 42-46]. Statistical methods hide information by changing some statistics image properties. For example, the idea of the Patchwork algorithm is based on the assumption that pixel values are independent and evenly distributed. This generates a secret key for initialization of the pseudo-random number generator, which indicate the place in the image where watermark bits are entered. To do this, in accordance with the key, select n pairs of pixels (ai, bi) in which the brightness value changes as follows:

$$\bar{a} = ai + 1\,, \bar{b} = bi + 1 \tag{1}$$

When selecting a watermark, the amount is calculated:

$$Sn = \sum_{i=1}^{n} (\,\overline{ai} - \overline{bi}) \tag{2}$$

If Sn is significantly different from zero. Present the method provides high resistance to digital processing operations, and the difficulty of detection hidden data without the corresponding secret key. Thus, the results of the study show that the reliability of replacement methods in spatial area depends on the level of frequency distortion of the container. However, they are providing high speed and a significant amount of embedded data, so it is advisable to use when sending hidden messages. Methods operating in the frequency domain are available more resistant to distortion and digital processing operations but can hide less amount of data [47-55]. The presence of a secret key in broadband and statistical methods that use pseudo-random encoding, increases their reliability. And the distribution of hidden bits on throughout the container causes high resistance to accidental and intentional distortions that is taken into account when building a CEC.

5. Conclusion

In conclusion, the exploration of steganographic techniques presented in this paper illuminates the increasingly crucial role of data protection in the digital domain. As the sphere of digital communication expands, so too does the necessity for stringent security measures to shield sensitive information from unauthorized access and manipulation. This study delves into the intricate mechanics of digital steganography, highlighting its profound significance in maintaining the confidentiality and integrity of information. Steganography by its very nature, is designed to cloak the presence of confidential data, offering a covert channel within various digital mediums. This research has comprehensively analyzed contemporary steganographic methods, scrutinizing their strengths and weaknesses, and assessing their practical utility across a myriad of information security tasks. It is evident from the findings that steganography has evolved to become an indispensable tool in the arsenal against digital threats, finding its place in military, diplomatic, and commercial realms alike.

Through the application of sophisticated embedding algorithms, modern steganography can accommodate larger payloads of concealed data, while simultaneously challenging detection techniques known as steganalysis. The integration of these advanced methods underscores a key advantage of steganography: its ability to adapt and remain effective amid the complexities of modern digital media. Moreover, this paper has also highlighted the diversity of steganographic applications, ranging from copyright protection to covert operations, underscoring its adaptability and broad relevance. The balance between the size of the hidden message and the degree of security is a nuanced aspect of steganography that has been explored. The research identifies a "safety space" where the embedded message remains both practical and secure. This trade-off is central to the design of effective steganographic systems, where the objective is to maximize the capacity of the hidden information while minimizing its visibility and susceptibility to detection. The discussion within this paper also considers the implications of steganographic methods in various scenarios, such as the stability requirements of watermarks for copyright protection versus the larger information quantities needed for covert communication. This dichotomy emphasizes the need for bespoke steganographic strategies tailored to specific use cases. In light of the aforementioned considerations, it is clear that steganographic techniques play a pivotal role in fortifying digital privacy and security. The ongoing evolution of these techniques, alongside a nuanced understanding of their application, ensures that steganography remains a formidable, albeit invisible, guardian of information in an era where data breaches and cyber threats are omnipresent. As the landscape of digital communication continues to shift, the adaptability and ingenuity of steganographic practices will remain at the forefront of safeguarding information integrity and confidentiality.

References

[1] Qasim, Alaa Jabbar, Roshidi Din, and Farah Qasim Ahmed Alyousuf. "Review on techniques and file formats of image compression." *Bulletin of Electrical Engineering and Informatics* 9, no. 2 (2020): 602-610.

[2] Qasim, Alaa Jabbar, and Farah Qasim Ahmed Alyousuf. "History of image digital formats using in information technology." *QALAAI ZANIST JOURNAL* 6, no. 2 (2021): 1098-1112.

[3] Din, Roshidi, Massudi Mahmuddin, and Alaa Jabbar Qasim. "Review on steganography methods in multi-media domain." *International Journal of Engineering & Technology* 8, no. 1.7 (2019): 288-292.

[4] Din, Roshidi, and Alaa Jabbar Qasim. "Steganography analysis techniques applied to audio and image files." *Bulletin of Electrical Engineering and Informatics* 8, no. 4 (2019): 1297-1302.

[5] QASSIM, ALAA JABBAR, and Y. Sudhakar. "Information Security with Image through Reversible Room by using Advanced Encryption Standard and Least Significant Bit Algorithm." *International Journal of Advances in Computer Science and Technology* 4, no. 4 (2015): 93-97.

[6] Din, Roshidi, Osman Ghazali, and Alaa Jabbar Qasim. "Analytical review on graphical formats used in image steganographic compression." *Indonesian Journal of Electrical Engineering and Computer Science* 12, no. 2 (2018): 441-446.

[7] Alyousuf, Farah Qasim Ahmed, Roshidi Din, and Alaa Jabbar Qasim. "Analysis review on spatial and transform domain technique in digital steganography." *Bulletin of Electrical Engineering and Informatics* 9, no. 2 (2020): 573-581.

[8] Alaa Jabbar Qasim, D., Roshidi, *Capacity Performance of LSB Method On Multi-Layer Images in Steganography* International Journal of Engineering and Techniques, 2022. **8**(5): p. 118 -121

[9] Atiyah, Abbas Gatea, NimetAllah Nasser Faris, Gadaf Rexhepi, and Alaa Jabbar Qasim. "Integrating Ideal Characteristics of Chat-GPT Mechanisms into the Metaverse: Knowledge, Transparency, and Ethics." In *International Multi-Disciplinary Conference-Integrated Sciences and Technologies*, pp. 131-141. Cham: Springer Nature Switzerland, 2023.

[10] Din, Roshidi, and Sunariya Utama. "The Design Review of Feature-based Method in Embedding the Hidden Message in Text as the Implementation of Steganography." *Borneo International Journal eISSN 2636-9826* 6, no. 3 (2023): 88-95.

[11] Din, Roshidi. "Comparison Of Steganographic Techniques of Spatial Domain and Frequency Domain in Digital Images." *Borneo International Journal eISSN 2636-9826* 6, no. 3 (2023): 109-118.

[12] Utama, Sunariya, and Roshidi Din. "Performance Review of Feature-Based Method in Implementation Text Steganography Approach." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 28, no. 2 (2022): 325-333.

[13] Westfeld, Andreas, and Andreas Pfitzmann. "Attacks on steganographic systems: Breaking the steganographic utilities EzStego, Jsteg, Steganos, and S-Tools-and some lessons learned." In *International workshop on information hiding*, pp. 61-76. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999.

[14] Bosch, Karl, Karl Bosch, Karl Bosch, Karl Bosch, and Germany Mathematician. *Elementare Einführung in die Wahrscheinlichkeitsrechnung*. Vol. 6. Vieweg, 2006.

[15] Anderson, Ross, ed. "Information hiding: First international workshop cambridge, uk, may 30–june 1, 1996 proceedings." In *International Workshop on Information Hiding 1*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996.

[16] Razali, Nazim, Aida Mustapha, Sunariya Utama, and Roshidi Din. "A review on football match outcome prediction using bayesian networks." In *Journal of Physics: Conference Series*, vol. 1020, no. 1, p. 012004. IOP Publishing, 2018.

[17] Taouil, Youssef, and El Bachir Ameur. "Steganographic Scheme Based on Message-Cover matching." *International Journal of Electrical & Computer Engineering (2088-8708)* 8, no. 5 (2018).

[18] Tao, Jinyuan, Sheng Li, Xinpeng Zhang, and Zichi Wang. "Towards robust image steganography." *IEEE Transactions on Circuits and Systems for Video Technology* 29, no. 2 (2018): 594-600.

[19] ALabaichi, Ashwak, Maisa'A. Abid Ali K. Al-Dabbas, and Adnan Salih. "Image steganography using least significant bit and secret map techniques." *International journal of electrical & computer engineering (2088-8708)* 10, no. 1 (2020).

[20] Abikoye, Oluwakemi Christiana, and Roseline Oluwaseun Ogundokun. "Efficiency of LSB steganography on medical information." *International Journal of Electrical and Computer Engineering (IJECE)* 11, no. 5 (2021): 4157-4164.

[21] Al-Smadi, Ahmad Mohamad, Ahmad Al-Smadi, Roba Mahmoud Ali Aloglah, Nisrein Abu-Darwish, and Ahed Abugabah. "Files cryptography based on one-time pad algorithm." *International Journal of Electrical and Computer Engineering (IJECE)* 11 (2021).

[22] Khudher, I.M.J.E.-E.J.o.E.T., *LSB Steganography Strengthen Footprint Biometric Template.* 2021. **1**(9): p. 109.

[23] Madhi, Hadi Hussein, Mustafa Sahib Shareef, Seham Ahmed Hashem, and Abdallah Waleed Ali. "Pixel steganography method for grayscale image steganography on colour images." *Periodicals of Engineering and Natural Sciences* 9, no. 3 (2021): 615-624.

[24] Vijay, K., K. S. Jayareka, G. Kirubasri, and Priya Vijay. "Enhancing the Security of Data Using Digital Stemage Technique." *Annals of the Romanian Society for Cell Biology* 25, no. 6 (2021): 9138-9143.

[25] Samagh, R. and S. Rani, *Data Hiding using Image Steganography.* 2015.

[26] Sidhik, Siraj, S. K. Sudheer, and VP Mahadhevan Pillai. "Performance and analysis of high capacity steganography of color images involving wavelet transform." *Optik* 126, no. 23 (2015): 3755-3760.

[27] Swetha, V., V. Prajith, and V. Kshema. "Data hiding using video steganography-a survey." *International Journal of Science, Engineering and Computer Technology* 5, no. 6 (2015): 206.

[28] AlKorbi, Hamad, Ali AlAtaby, Majid AlTaee, and Waleed AlNuaimy. "Highly efficient image steganography using Haar DWT for hiding miscellaneous data." *Jordanian Journal of Computers and Information Technology* 2, no. 1 2016): 17-17.

[29] Kavitha, P. "A survey on lossless and lossy data compression methods." *International Journal of Computer Science & Engineering Technology* 7, no. 03 (2016): 110-114.

[30] Din, Roshidi, Massudi Mahmuddin, and Alaa Jabbar Qasim. "Review on steganography methods in multi-media domain." *International Journal of Engineering & Technology* 8, no. 1.7 (2019): 288-292.

[31] Mainberger, Markus, Christian Schmaltz, Matthias Berg, Joachim Weickert, and Michael Backes. "Diffusion-based image compression in steganography." In *Advances in Visual Computing: 8th International Symposium, ISVC 2012, Rethymnon, Crete, Greece, July 16-18, 2012, Revised Selected Papers, Part II 8*, pp. 219-228. Springer Berlin Heidelberg, 2012.

[32] Mansour, Romany F., Waleed F. Awwad, and Amal A. Mohammed. "A robust method to detect hidden data from digital images." (2012).

[33] Marimuthu, M., R. Muthaiah, and P. Swaminathan. "School of Computing, SASTRA University,Thanjavur,Tamilnadu, India." *Research Journal of Applied Sciences, Engineering and Technology* 4, no. 24 (2012): 5381-5386.

[34] Nosrati, Masoud, Ronak Karimi, and Mehdi Hariri. "Reversible data hiding: principles, techniques, and recent studies." *World Applied Programming* 2, no. 5 (2012): 349-353.

[35] Nosrati, Masoud, Ronak Karimi, and Mehdi Hariri. "Audio steganography: a survey on recent approaches." *world applied programming* 2, no. 3 (2012): 202-205.

[36] Patel, Hardik, and Preeti Dave. "Steganography technique based on DCT coefficients." *International Journal of Engineering Research and Applications* 2, no. 1 (2012): 713-717.

[37] Din, Roshidi, Rosmadi Bakar, Sunariya Utama, Jamaluddin Jasmis, and Shamsul Jamel Elias. "The evaluation performance of letter-based technique on text steganography system." *Bulletin of Electrical Engineering and Informatics* 8, no. 1 (2019): 291-297.

[38] Alyousuf, Farah Qasim Ahmed, Roshidi Din, and Alaa Jabbar Qasim. "Analysis review on spatial and transform domain technique in digital steganography." *Bulletin of Electrical Engineering and Informatics* 9, no. 2 (2020): 573-581.

[39] Din, R., et al., *Analysis Review on Image Compression Domain.* International Journal of Engineering Technology, 2019. **8**(1.7): p. 293-296.

[40] Qasim, Alaa Jabbar, Roshidi Din, and Farah Qasim Ahmed Alyousuf. "Review on techniques and file formats of image compression." *Bulletin of Electrical Engineering and Informatics* 9, no. 2 (2020): 602-610.

[41] Kuhn, Markus G., and Ross J. Anderson. "Soft tempest: Hidden data transmission using electromagnetic emanations." In *Information Hiding: Second International Workshop, IH'98 Portland, Oregon, USA, April 14–17, 1998 Proceedings 2*, pp. 124-142. Springer Berlin Heidelberg, 1998.

[42] Din, R., O. Ghazali, and A.J. Qasim, *Analytical review on graphical formats used in image steganographic compression.* ndones. J. Electr. Eng. Comput. Sci, 2017. **5**(3): p. 401-408.

[43] Din, Roshidi, Osman Ghazali, and Alaa Jabbar Qasim. "Analytical review on graphical formats used in image steganographic compression." *Indonesian Journal of Electrical Engineering and Computer Science* 12, no. 2 (2018): 441-446.

[44] Qasim, Alaa Jabbar, and Farah Qasim Ahmed Alyousuf. "History of image digital formats using in information technology." *QALAAI ZANIST JOURNAL* 6, no. 2 (2021): 1098-1112.

[45] Din, Roshidi, and Alaa Jabbar Qasim. "Steganography analysis techniques applied to audio and image files." *Bulletin of Electrical Engineering and Informatics* 8, no. 4 (2019): 1297-1302.

[46] Din, Roshidi. "Comparative Analysis of Methods for Digital Steganography in Images." *Borneo International Journal eISSN 2636-9826* 6, no. 3 (2023): 119-127.

[47] Bendale, D.R. and M.R. Chinchore, *Advanced Encryption then Compression System for Grayscale Images and Color Images.*

[48] Fang, Wen-Pinn. "A Data Hiding Method which the Secret Image Exist After Cropping Style Image Resizing." *J. Inf. Hiding Multim. Signal Process.* 6, no. 2 (2015): 365-370.

[49] Kahn D. (1996) The history of steganography. In: Anderson R. (eds) Information Hiding. IH 1996. Lecture Notes in Computer Science, v.S., Berlin, Heidelberg.

[50] R Rastogi, Somya, and Achala Shakya. "An Analysis of Recently Used Steganography Techniques on Images." *International Journal of Computer Science Trends and Technology (IJCST)* 3, no. 5 (2015).

[51] Sawant, A., V. Darji, and A. Shetty, *Data Hiding in Encrypted Images.*

[52] Staff, D., *Reference guide: Graphics Technical Options and Decisions.* p. http://www.devx.com/projectcool/Article/19997.

[53] Sujith, T., *Data Concealing in Encrypted Images Using Reversible Data Hiding (RDH) Technique.* INTERNATIONAL JOURNAL OF COMPUTER TRENDS & TECHNOLOGY. **1**(6): p. 192-198.

[54] Suparna, C.P., *Data Hiding In Encrypted Images.*

[55] Zhang, Chun-Yu, Wenxiang Zhang, and Shaowei Weng. "Comparison of two kinds of image scrambling methods based on LSB steganalysis." *J. Inf. Hiding Multim. Signal Process.* 6, no. 4 (2015): 666-673.