DOI: 10.54254/2755-2721/94/2024MELB0059

Advanced Reversible Data Hiding Techniques in JPEG Images: Methods, Applications, and Future Perspectives

Xinyi Li

School of Computer Engineering and Science, Shanghai University, Shanghai, China

1599616830@shu.edu.cn

Abstract. This paper provides an extensive review of recent advancements in reversible information hiding methods tailored for JPEG images, a predominant compression standard crucial for data security and digital copyright protection. It starts by outlining fundamental concepts related to JPEG image structure and reversible data hiding techniques. The analysis then delves into three primary methods: modifications to JPEG quantization tables, adjustments in Huffman tables, and corrections of Discrete Cosine Transform (DCT) coefficients, detailing how each technique contributes to effective and secure data embedding. Furthermore, the exploration of potential applications in critical areas highlights the versatile utility of these techniques in safeguarding digital content. Concluding with a discussion on future research directions, this paper emphasizes the significant potential for growth in this field, particularly in enhancing security measures and improving efficiency. Such advancements promise to extend the applicability of reversible data hiding, ensuring robust copyright protection and information security in the digital age.

Keywords: Reversible data hiding, quantization table modification, dct coefficient correction.

1. Introduction

The rapid development of information technology, particularly with the expansion of the Internet and mobile communications, has catalyzed an unprecedented increase in digital information flows. While these advancements have brought significant convenience to daily life, they have also introduced serious security challenges, such as online fraud, hacker attacks, and the misuse of stolen digital data. In this context, Reversible Data Hiding (RDH), first introduced by Barton in 1997, has emerged as a crucial technique for data protection, copyright management, and privacy preservation. RDH enables the embedding of additional information within an image without degrading its original quality, ensuring both the retrievability of the hidden data and the full recovery of the original image [1, 2].

Despite its benefits, RDH faces significant challenges, particularly when applied to JPEG images—a format widely used due to its efficient compression but inherently complex in terms of compression mechanisms and data structure. This complexity poses heightened demands on RDH techniques, requiring them to balance the high capacity and confidentiality of embedded information with the maintenance of visual quality. The intricate nature of JPEG's structure complicates the application of RDH, necessitating sophisticated algorithms to effectively manage the embedding and extraction processes without compromising the integrity of the original image.

This Article's Contribution: Focusing on the JPEG format, this paper explores RDH techniques specifically designed for these images. It discusses the advantages and disadvantages of various RDH methods, highlighting their suitability for different application scenarios. This analysis encompasses modifications to JPEG quantization tables, adjustments in Huffman tables, and the correction of Discrete Cosine Transform (DCT) coefficients, detailing how each approach impacts the overall efficacy of data hiding. By examining current challenges and outlining potential future developments, the paper aims to advance the field of RDH, pushing for innovations that enhance security and efficiency in managing digital content across highly compressed image formats.

2. Reversible Data Hiding Techniques and Evaluation Criteria in JPEG Images

The JPEG standard is extensively employed digital image compression standard specially designed for compressing static images. It defines a lossy compression method that sacrifices some original image data to reduce file size [3]. Because of the difference of human vision, the eye is not very sensitive to high-frequency information within images, which contains the compressible content, often referren to as redundant data. Therefore, a key characteristic of JPEG compression lies in its ability to effectively balance the compression ratio with the quality of the resulting image. By adjusting the quantization parameters, it is possible to achieve a high compression ratio while still keeping adequate quality of images [4].

2.1. JPEG image compression techniques

Figure 1 provides an illustration of the workflow involved in the JPEG image compression algorithm. The first step is converting the colour mode to the YCrCb color space. The first step is to separate important information from unimportant information and YCbCr is suitable for this task. For the human eye, variations in brightness within an image are more easily detected, which can be attributed to the structure of the eye. There are two kinds of photoreceptor cells in the retina: rod cells, which are sensitive to changes in brightness, and cone cells, which handle color perception. Since rod cells far outnumber cone cells, we are more sensitive to details in brightness. The next step involves image segmentation. For a specified uncompressed image of dimensions MxN, the image is partitioned into 8x8 pixel sub-blocks to facilitate block processing. A Discrete Cosine Transform (DCT) is subsequently applied to each sub-block. In the resulting array after the DCT transformation, the first value represents the direct component, referred to as the DC coefficient, whereas the remaining values are categorized as AC coefficients [5]. By using a quantization table, the data is then quantized, resulting in a quantized DCT spare matrix of the same size. After performing entropy coding on the resulting sparse matrix, the compressed data segment in the JPEG bitstream is obtained. Because the entropy coding process is lossless, the modified sparse matrix can be entirely decoded from the bitstream. This characteristic makes the quantized DCT coefficients an ideal embedding domain for RDH methods [6].

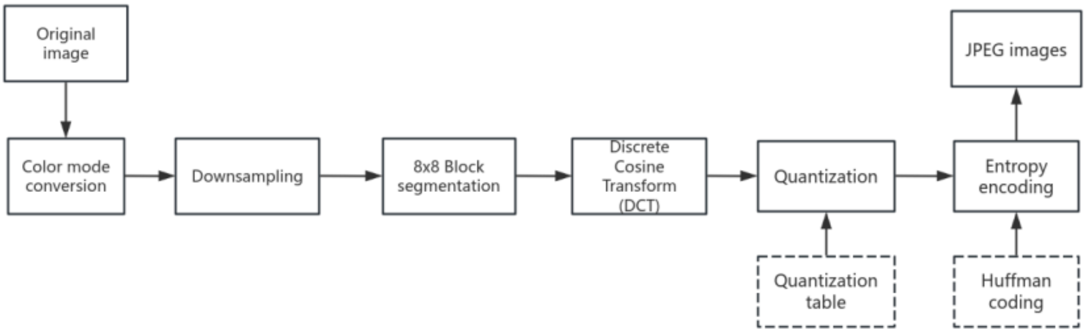

Figure 1. JPEG image compression process (Photo credit: Original).

2.2. Concepts and models

Reversible data hiding, commonly referred to as lossless data hiding, represents a significant branch of information hiding [7]. It features characteristics such as invisibility, imperceptibility, robustness, stability, and security in the hidden information [8]. The model of this technique is illustrated in Figure 2 and Figure 3. The encrypted information, combined with the key, is hidden within the carrier information through a reversible embedding algorithm, resulting in the stego information. During the extraction process, the recipient uses the extraction algorithm to separate the original carrier information and the key, thereby retrieving the original information prior to encryption.

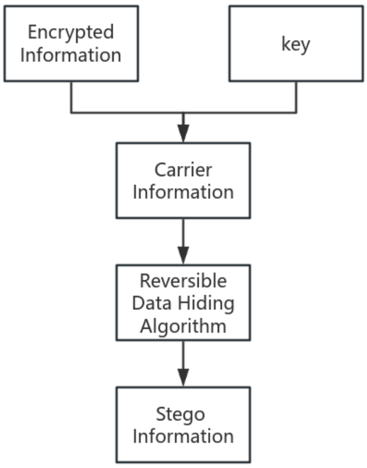

Figure 2. Embedding Process (Photo credit: Original).

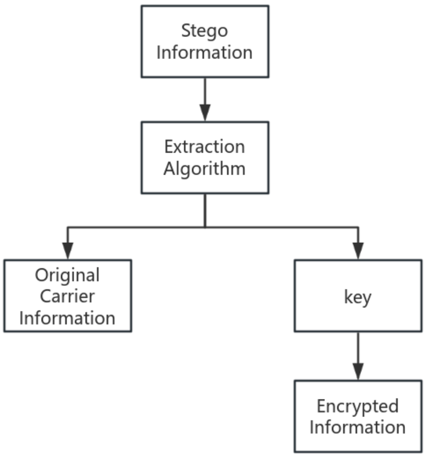

Figure 3. Extraction Process (Photo credit: Original).

2.3. Evaluation metrics

In JPEG reversible data hiding technology, evaluation metrics provide objective references and analyses by comparing the effectiveness of different methods. These metrics are utilized to assess the specific effectiveness of various algorithms, primarily focusing on the following aspects: embedding capacity, image quality, security, and robustness.

2.3.1. Embedding capacity. Embedding capacity serves as a critical metric for evaluating the effectiveness of reversible information hiding technology. This term refers to the highest capacity of information that can be embedded in an image without significantly degrading its quality. The higher embedding capacity means that more information can be hidden in the image, which can protect the digital image to a greater extent, which plays a very important role in digital rights protection, watermark identification, and privacy information storage. However, expanding the embedding capacity without restrictions will inevitably compromise image quality. Consequently, it becomes imperative to impose limits on the size of the embedding capacity in practical applications, ensuring that a balance is maintained in accordance with the specific requirements of each use case.

2.3.2. Image quality. The image quality evaluation index assesses how the visual impact of the modified image compares to that of the original, following the embedding of information. The quality of an image directly impacts its applications in various scenarios. Common methods for evaluating image quality include Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM).PSNR assesses quality by calculating the error between the image after information embedding and the original image; the higher the PSNR value, the better the visual quality of the image. The calculation of Peak Signal-to-Noise Ratio (PSNR) relies on the Mean Squared Error (MSE), which quantifies the mean value of the squared discrepancies between two images. The formula for PSNR is as follows.

$$\mathrm{PSNR} = 10 * \log_{10}(\frac{MAX_I^2}{MSE}) = 20 * log_{10}(\frac{MAX_I}{\sqrt{MSE}}) \quad (1)$$

In this context, MAX denotes the highest pixel value that an image can possess. If the image is 8-bit, the MAX value is typically 255. The formula for calculating the Mean Squared Error (MSE) is as follows.

$$\mathrm{MSE} = \frac{1}{\mathrm{mn}} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \| I(i,j) - K(i,j) \|^2 \quad (2)$$

In this context, I (i, j) and K (i, j) represent the pixel values. These values are found at the position (i, j) in the original and processed images, respectively. Meanwhile, m and n signify the total number of rows and columns in the image.

SSIM focuses more on the structural information of an image, such as brightness, contrast, and texture, providing a better reflection of human visual perception. Therefore, a higher SSIM value shows that the embedded image is more visually similar to the original image. This means that the two images look more alike to the human eye [9].

2.3.3. Security. Security refers to the concealment of the embedded information and the ability to prevent unauthorized third parties from detecting, extracting, or tampering with the hidden information. To make concealed information difficult to detect and decipher, researchers frequently employ advanced embedding algorithms or encryption techniques. These approaches enhance the security of the hidden data, ensuring that unauthorized access is minimized. A high-security reversible information hiding technique should have good concealment, and even if an attacker is aware that the image may contain hidden information, it is difficult to extract the information through conventional methods.

2.3.4. Robustness. Robustness refers to the ability of embedded information to be correctly extracted after image processing operations. These operations may include compression, cropping, rotating, scaling, and other common editing operations of the image. In practice, images tend to be processed multiple times, and if the embedded information is lost or damaged during processing, it will greatly reduce the usefulness of the technology. Robustness holds particular significance in the context of JPEG images, given that the JPEG format inherently employs lossy compression, which can compromise the integrity of the embedded information.

3. Key Algorithms and Technologies

3.1. Modification based on JPEG quantization table

Fridrich et al. suggested that when the quantization step size is currently even, it should be reduced by half, while the associated DCT coefficient value should be increased twofold [10]. Additionally, the least significant bit (LSB) of the coefficient is used to embed the hidden information. Wang et al. Improved this method by dividing certain specific elements in the quantization table and integers greater than 2 to achieve greater embedding capacity [11]. Chin-Chen Chang et al. proposed a method where the mid-frequency coefficients in the standard quantization table were adjusted to 1, creating a new 8x8 quantization table. Subsequently, Almohammad et al. introduced a approach that was further refined by enlarging the basic quantization table to a 16x16 pixel matrix and embedding concealed information within the two least significant bits of mid-frequency DCT coefficients across each quantized block. Senthooran and Ranathunga, building on previous research, proposed a new 8x8 and 16x16 quantization table in which both the low-frequency and mid-frequency AC coefficients were set to 1 [12, 13]. This approach increased the number of redundant bits to enhance the steganographic capacity. Although this method was effective in maintaining image quality, it significantly increased the file size and failed to adequately ensure information security.

3.2. Methods based on modifying huffman tables

The method based on modifying the Huffman table, also known as a lossless data hiding method, achieves data embedding by adjusting the coding table during the image compression process. This method is well-suited for applications demanding a specific standard of image quality while simultaneously facilitating covert data embedding throughout the compression process. Mobasseri et al. proposed a JPEG reversible data hiding technique in 2010 that involves modifying the Huffman table [14].The approach that relies on variable-length coding creates a mapping relationship by altering certain used bits within the employed codes. Qian et al. proposed an innovative method that, after analyzing the JPEG bitstream, divides all variable length codes (VLC) with the same Huffman coding length into used and unused categories [15]. They defined 162 different VLC values for the AC coefficients based on the JPEG standard. By updating some unused VLC values to used ones, they constructed a VLC mapping and subsequently embedded secret data into the entropy-coded bitstream. However, during the compression process, many codes remained unused. By statistically analyzing the VLC of the AC coefficients in JPEG images, they were able to replace unused codes with used codes based on the secret information, thus achieving data hiding. This method has minimal impact on the pixel values and file size of the JPEG images used in the experiments and is compatible with common JPEG decoders.

While these information hiding methods have good performance, their embedding capacity is still limited. In view of this shortcoming, Qiu et al. proposed a novel framework for information hiding based on JPEG images [16]. This framework incorporates variable length coding (VLC) mapping, combination and permutation techniques, and an extended lossless data hiding algorithm (LDH). It innovatively combines relay shifting algorithms for VLCs of varying lengths, resulting in a higher hiding capacity while effectively constraining file size and pixel values.

Building upon this foundation, Du et al. updated the method by proposing a universal variable length coding (VLC) mapping strategy [17]. This strategy allows for the use of VLCs of varying lengths within the same mapping set. Additionally, they transformed the VLC mapping model into a histogram shifting model, generating a feasible solution space and establishing a simulation embedding model to find the optimal solution through an exhaustive search method. Nonetheless, this method is limited in that it can only be applied to JPEG images that have been compressed with Huffman tables.

3.3. Modifying quantized dct coefficients

A commonly employed technique consists of incorporating alterations into the quantized coefficients of the Discrete Cosine Transform (DCT). This approach was first developed by Upham in 1993, who invented a well-known JPEG image data hiding tool called Jpeg-Jsteg. In this method, secret information is embedded into the Least Significant Bits (LSB) of the quantized DCT coefficients [18]. Later, in 2007, Chang et al. introduced a lossless steganography approach that involved embedding information within the quantized coefficients of the DCT in JPEG images [19]. In 2016, Huang et al. introduced a novel method based on the principles of encoding and the distribution of quantized DCT coefficients [20]. In their approach, zero coefficients remained unchanged, while only quantized alternating current (AC) coefficients with values of 1 and -1 were extended to carry message bits. Di et al. embedded data into zero AC coefficients to improve performance and enhance the coefficient distortion cost function [21]. Subsequently, Xiao et al. proposed a new technique that extended JPEG image reversible data hiding based on Histogram Shifting (HS) into a Multiple Histogram Modification (MHM) embedding framework [22]. This allowed for different modifications to be applied to different histograms, resulting in better embedding performance. Additionally, they established a rate-distortion model capable of accurately estimating JPEG image degradation, which could adaptively manage the expansion bins of different histograms. The aforementioned methods involve selecting coefficients, blocks, and embedding points, which are typically designed by constructing optimization models tailored to the specific image content. However, these methods often face challenges such as high computational complexity and significant optimization costs. To address these issues, Zhang Cheng et al. introduced a modular reversible data hiding technique for JPEG images [23]. This technique uses a generalized embedding parameter set based on adaptive multi-histogram modification, which reduces the adaptive solution space to a fixed, small-scale sample space. This enables precise matching of the most appropriate quantized DCT coefficient modification method for each embedding module, achieving nearly optimal performance with minimal computational cost. Building on this, Mao et al. introduced further innovations, allowing for the adaptive selection of the optimal frequency band length of DCT coefficients [24]. Their approach utilizes algorithmic ranking to prioritize frequency bands, quickly identifying the best solution.

Furthermore, Pan Xinlu enhanced the methods for DCT block selection and embedding frequency selection by developing a quantized AC coefficient distribution estimation model [25]. Pan also proposed an algorithm for reversible data hiding specifically tailored for color JPEG images, thereby addressing the limitations of earlier studies that mainly concentrated on grayscale JPEG images.

4. Applications

This paper categorizes and analyzes the algorithms that are used in reversible information hiding techniques specifically for JPEG images. This provides a foundation that can be used to explore their practical applications. With digital information being widely spread and the internet developing quickly, there is a growing concern about the security and the integrity of information. Because of this concern, reversible information hiding techniques are being used more and more in different fields. These fields include digital content creation, the medical field, the military, and digital forensics.

4.1. Digital content creation

For the works that are created by individuals, whether these works are digital content or physical content, it is very important to protect the copyright of the work. RDH technology is able to embed copyright information, the author's identification, or digital signatures into JPEG images. This embedding does not affect the visual quality of the images. Because of this, even when the works are shared or widely distributed, the embedded copyright information will stay intact and can be verified. This verification can provide strong evidence if a copyright dispute happens. By using RDH technology and the methods that come from it, creators and copyright holders can effectively stop infringement and protect their legal rights. An example of this is the use of RDH technology in digital libraries.

4.2. Medical field

With the growth of digital information technology, the healthcare system is also gradually becoming more digital. In recent years, remote consultations and remote diagnoses by experts have become more and more common. To help patients get better treatment, RDH technology is used. This technology can embed patient identification information, examination records, or other related data into medical images like X-rays and CT scan images. It does this without affecting the quality of the images used for diagnosis. This way, doctors can have the most accurate and full understanding of the patient's condition [26]. At the same time, RDH technology can improve data security, which prevents malicious attacks or tampering. In the medical field, many efficient watermarking algorithms have also been developed.

4.3. Military and national security domains

In the military and national security fields, RDH technology can be used to secretly embed military intelligence or operational instructions into satellite images or other important image data. With this technology, key information can be transmitted securely while still keeping the quality and usability of the images intact. Because the embedded data does not make any big changes to how the images look, it can stop hostile forces from finding hidden information through image analysis or the content of the images. This technology not only makes data transmission more secure but also gives an important way to communicate confidentially during military operations.

4.4. Digital forensics

In the field of digital forensics, RDH technology is used to embed important evidentiary information or audit data into images. This helps in supporting investigations and efforts to recover data later on. For instance, RDH technology can embed information related to the GPS location into images [26]. When disputes arise and lead to legal proceedings, judicial authorities have the ability to extract this GPS data from the digital images. This allows them to obtain information about the time and location where the image was created. The technology’s lossless nature ensures that the image data is not altered in any way during processing and storage. As a result, the accuracy and effectiveness of forensic work are greatly improved.

5. Future Development Directions

The widespread use of short videos in the digital age highlights the important need for privacy protection in video content. In dynamic and real-time scenarios, such as video streaming or live image transmission, RDH technology needs to achieve efficient real-time data hiding as well as processing capabilities. Future research will aim to develop RDH algorithms that are suitable for real-time image data streams. These algorithms will support efficient real-time data embedding, data extraction, and data recovery. This will help meet the demands of real-time applications like video surveillance and live broadcasting. In addition, the introduction of Artificial Intelligence (AI) and machine learning technologies will create new opportunities for the development of RDH technology. At present, the accuracy of the DCT coefficient prediction strategy in JPEG-based reversible data hiding algorithms, which are based on prediction errors and location selection, still has a lot of room for improvement. By using deep learning algorithms, future research can explore more intelligent methods for data embedding and extraction. It can also automate the optimization of parameters and adjustments to the algorithms. This will help to improve the intelligence and adaptability of the technology. Furthermore, as cross-domain data exchange and sharing increase, future RDH technology will need to achieve effective cross-domain data hiding and protection. Research will focus on how to hide data seamlessly across different types of images and data formats. It will also aim to ensure that data remains secure and recoverable in various environments.

6. Conclusion

This paper has extensively explored the domain of reversible data hiding (RDH) techniques specifically designed for JPEG images, classifying the current methodologies into three distinct categories: modifications to the JPEG quantization table, alterations of the Huffman table, and adjustments to the Discrete Cosine Transform (DCT) coefficients. These methods primarily aim to enhance the data embedding capacity while minimizing the increase in file size, demonstrating their effectiveness in maintaining the integrity and quality of the original images. However, the application of these technologies often encounters challenges such as increased complexity, computational overhead, and compatibility issues, which are critical considerations for practical deployment.

Future Research Directions: Looking forward, the paper identifies several key areas for further research in RDH technology. With the rising prevalence of video content and the need for privacy protection in dynamic scenarios such as live broadcasting and video surveillance, there is a pressing need to develop RDH algorithms capable of efficient real-time data hiding and recovery. The integration of Artificial Intelligence (AI) and machine learning technologies presents a promising avenue to enhance the intelligence and adaptability of RDH methods. Future research will focus on leveraging deep learning algorithms to refine prediction error strategies and optimize algorithmic parameters for JPEG images. Additionally, as cross-domain data exchange becomes more commonplace, further studies will be essential to ensure seamless data hiding across different image and data formats, maintaining data security and recoverability in diverse environments. This will address the urgent need for RDH technologies that can operate effectively across various platforms and under different operational conditions.

References

[1] Qian Z, Zhang X, and Wang S 2014 Reversible Data Hiding in Encrypted JPEG Bitstream IEEE Transactions on Multimedia vol 16 no 5 pp 1486–1491

[2] Barton J M 1997 Method and apparatus for embedding authentication information within digital data U.S. Patent

[3] Standard J 1992 Information technology-digital compression and coding of continuous-tone still images-requirements and guidelines International Telecommunication Union CCITT recommendation vol 81 no 09

[4] Wang Yilin 2023 Reversible Information Hiding for JPEG Images (Master's Thesis Shanghai Electric Power University)

[5] Wang Y, Ni R, and Zhao Y 2018 A Novel Block Sorting Scheme for Reversible Data Hiding in JPEG Images 14th IEEE International Conference on Signal Processing (ICSP) Beijing China pp 389–394

[6] Zhang C, Ou B, and Liao X 2024 Modular reversible information hiding method based on JPEG image Computer Application Research pp 1177–1183

[7] Zhang C, Ou B, and Tang D 2020 An improved VLC mapping method with parameter optimization for reversible data hiding in JPEG bitstream Multimed Tools Appl vol 79 pp 19045–19062

[8] Yu C Q, Peng Q, and Chen Y 2015 Review on reversible information hiding Modern Computer (Pro) vol 11 pp 68–72

[9] Jia J, Xiang Z, Wang L, and Xu Y 2019 An Adaptive JPEG Double Compression Steganographic Scheme Based on Irregular DCT Coefficients Distribution IEEE Access vol 7 pp 119506–119518

[10] Fridrich J, Goljan M, and Du R 2002 Lossless data embedding for all image formats Proc SPIE Security and Watermarking of Multimedia Contents IV vol 4675 pp 572–583

[11] Wang K, Lu Z M, and Hu Y J 2013 A high capacity lossless data hiding scheme for JPEG images Journal of Systems and Software vol 86 no 7 pp 1965–1975

[12] Chang T-S C A, Chung L-Z 2002 A steganographic method based on JPEG and quantization table modification Information Sciences vol 141 pp 123–138

[13] Zhu, X., Huang, Y., Wang, X., & Wang, R. 2023. Emotion recognition based on brain-like multimodal hierarchical perception.Multimedia Tools and Applications, 1-19.

[14] Senthooran V, and Ranathunga L 2013 An investigation of quantization table modification on JPEG steganography 8th IEEE International Conference on Industrial and Information Systems Peradeniya Sri Lanka pp 622–626 doi: 10.1109/ICIInfS.2013.6732056

[15] Mobasseri B G, Berger R J, Marcinak M P, and NaikRaikar Y J 2010 Data embedding in JPEG bitstream by code mapping IEEE Transactions on Image Processing vol 19 no 4 pp 958–966

[16] Qian Z, and Zhang X 2012 Lossless data hiding in JPEG bitstream Journal of Systems and Software vol 85 no 2 pp 309–313

[17] Zhu, X., Guo, C., Feng, H., Huang, Y., Feng, Y., Wang, X., & Wang, R. 2024. A Review of Key Technologies for Emotion Analysis Using Multimodal Information. Cognitive Computation, 1-27.

[18] Du Y, Yin Z, and Zhang X 2022 High Capacity Lossless Data Hiding in JPEG Bitstream Based on General VLC Mapping IEEE Transactions on Dependable and Secure Computing vol 19 no 2 pp 1420–1433 doi: 10.1109/TDSC.2020.3013326

[19] Upham D 1993 Steganographic algorithm Jsteg Available: http://zooid.org/paul/crypto/jsteg

[20] Wang, R., Zhu, J., Wang, S., Wang, T., Huang, J., and Zhu, X. 2024 Multi-modal emotion recognition using tensor decomposition fusion and self-supervised multi-tasking International Journal of Multimedia Information Retrieval vol. 13, no. 4, pp. 39.

[21] Huang F, Qu X, Kim H J, and Huang J 2016 Reversible Data Hiding in JPEG Images IEEE Transactions on Circuits and Systems for Video Technology vol 26 no 9 pp 1610–1621 doi: 10.1109/TCSVT.2015.2473235

[22] Di F, Zhang M, Huang F, Liu J, and Kong Y 2019 Reversible data hiding in JPEG images based on zero coefficients and distortion cost function Multimed Tools Appl vol 78 no 24 pp 34541–34561

[23] Xiao M, Li X, Ma B, Zhang X, and Zhao Y 2021 Efficient Reversible Data Hiding for JPEG Images With Multiple Histograms Modification IEEE Transactions on Circuits and Systems for Video Technology vol 31 no 7 pp 2535–2546 doi: 10.1109/TCSVT.2020.3027391

[24] Mao N, He H, Chen F, Yuan Y, and Qu L 2023 Reversible Data Hiding of JPEG Image Based on Adaptive Frequency Band Length IEEE Transactions on Circuits and Systems for Video Technology vol 33 no 12 pp 7212–7223 doi: 10.1109/TCSVT.2023.3278284

[25] Pan X 2020 Research on reversible information hiding Algorithm of JPEG image (Master's Thesis South China University of Technology) doi: 10.27151/d.cnki.ghnlu.2020.004374

[26] Meng X, Wu D, and Yang G 2007 Data hiding and Digital Forensics Microcomputer Information vol 23 no 29 pp 57–58 235 doi: 10.3969/j.issn.1008-0570.2007.29.023