Steganography on JPEG Images: Issues and Challenges

Rakesh Kumar (*IEEE Member*)
Department of ECE
GZSCCET-MRSPTU, Bathinda
Punjab, India
kumarrakesh0791@gmail.com

Savina Bansal
Professor ECE
GZSCCET-MRSPTU, Bathinda
Punjab, India
savina.bansal@gmail.com

RK Bansal
Professor ECE
GZSCCET-MRSPTU, Bathinda
Punjab, India
drrakeshkbansal@gmail.com

2024 International Conference on Communication, Control, and Intelligent Systems (CCIS) | 979-8-3315-2820-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/CCIS63231.2024.10932073

***Abstract*—This paper examines the progression and challenges of JPEG steganography, a technique that hides secret messages within seemingly innocuous JPEG images. The paper traces the development of JPEG steganography through three phases: early DCT domain adaptations, the introduction of syndrome trellis codes and distortion framework, and the shift towards robust steganography techniques. While STC-based methods initially enhanced security against steganalysis, they remain vulnerable to modifications during transmission, such as social media recompression, which has driven the need for more resilient approaches. This paper reviews notable advancements in robust steganography, including dither modulation and sign-based techniques, and concludes with an exploration of open research challenges, emphasizing the need for effective recompression models and solutions that balance capacity, security, and robustness.**

Keywords—JPEG, Robust steganography, Data hiding, Issues and challenges

I. Introduction

In an era where digital information flows freely across networks, protecting sensitive data has become more critical than ever. Modern security strategies are evolving beyond conventional cryptography, which simply encrypts data, towards more sophisticated approaches. Steganography has emerged as a potential complementary technique, offering a distinct advantage by concealing the very presence of secret communications within everyday digital media [1] [2] [3] [4] [5]. This hidden transmission of information, seamlessly blend within common files like images, audio, or video. JPEG images, in particular, are ubiquitous and offers promising opportunities for steganography applications. However, the lossy nature of JPEG compression poses a host of challenges, as it can distort the embedded data and compromise its integrity.

Building on these challenges, the prevailing state of JPEG steganography is largely dominated by heuristic-based techniques. These methods rely upon empirical observations on image's statistical and perceptual behavior post-embedding. The secret message is typically embedded by subtly modifying the discrete cosine transform (DCT) coefficients. While this approach offers some protection against steganalysis, it remain vulnerable to lossiness of JPEG compression. Furthermore, the growing prevalence of social media platforms, which often recompress and resize images, has amplified the difficulty of maintaining the robustness of hidden messages.

This paper comprehensively explores these critical issues by tracing developmental trajectory of JPEG steganography across three distinct evolutionary phases: (1) Early DCT domain adaptations, where initial algorithms attempted to adapt spatial domain techniques to the DCT domain; (2) the introduction of Syndrome Trellis Codes (STC) and the distortion framework, which brought greater control over embedding distortions and improved security; and (3) the contemporary shift towards robust steganography techniques, focusing on resilience against steganalysis, and recompression on today's social networking platforms (SNPs). The paper concludes with a discussion on open research issues and challenges.

II. Early DCT Domain Adaptations

The initial phase of JPEG steganography was characterized by straightforward attempts to translate successful spatial domain techniques into the DCT domain. Researchers primarily focused on adapting well-established spatial domain methods, such as least significant bit (LSB) replacement, to work with DCT coefficients. One of the earliest algorithms, JSteg [6], implemented a simple sequential LSB replacement in quantized DCT coefficients, avoiding DCT coefficients equal to 0 or 1. While groundbreaking at the time, this approach soon revealed significant vulnerabilities to statistical analysis due to its deterministic nature and the distinct statistical artifacts it created in the coefficient histograms. OutGuess attempted to address these initial shortcomings through a two-pass system: first embedding the data, then attempting to restore the statistical properties of the cover image [7]. However, these solutions often came at the cost of significantly reduced embedding capacity and still couldn't fully address the fundamental challenges of preserving higher-order statistics and ensuring security against increasingly sophisticated steganalysis techniques.

A significant breakthrough came with the development of the F5 algorithm [8], which introduced several innovative concepts to address the limitations of earlier approaches. F5 employed matrix embedding, a coding technique that minimized the number of necessary changes to embed a given message. This marked a crucial shift from simple replacement-based strategies to more sophisticated coding-based methods. Additionally, F5 introduced permutative straddling to scatter the embedding changes uniformly throughout the image. The algorithm's ability to preserve the shape of the DCT histogram while achieving higher embedding efficiency represented a significant improvement over its predecessors. The introduction of matrix embedding in F5 was particularly significant, as it laid the groundwork for future coding-based approaches. The technique demonstrated that it was possible to embed multiple message bits while minimizing the number of modifications, achieving better embedding efficiency than simple LSB replacement. However, despite these advancements, F5 still faced challenges with wet paper codes [9] and the shrinkage problem [10], where zeros created during embedding led to capacity loss. These early experiences, particularly the success of matrix embedding (or syndrome coding) in improving embedding efficiency while maintaining security, would later

influence the development of STCs [11], marking a transition to a new era in JPEG steganography.

An another approach explored during this phase was perturbed quantization [12], which aimed to introduce small, controlled changes to the quantization tables used in JPEG compression. The core idea was to minimize the overall visual impact from both quantization and embedding, making the modifications less detectable. However, the effectiveness of this technique was limited. The number of DCT coefficients available for modification was constrained by the quantizers used and coefficients available for embedding was restricted by the limited contributing coefficients.

III. STC AND DISTORTION FRAMEWORK

The introduction of Syndrome-Trellis Codes (STC) [11] marked a pivotal advancement in JPEG steganography, fundamentally changing how researchers approached the problem of secure data hiding. STCs, binary linear convolutional codes represented by a structured parity-check matrix, provided a pragmatic and efficient framework for implementing minimal-distortion steganography. This framework effectively separated the tasks of embedding and designing distortion functions. By achieving embedding efficiency close to theoretical limits, researchers could now focus on optimizing distortion functions, which calculate the cost of modification for each element. Typically, higher costs were assigned to smooth regions and lower costs to textured areas.

At first, distortion functions were designed to be additive, meaning the total distortion was computed as the sum of individual distortions caused by modifications to each coefficient. This additivity was important for the implementation with STCs, as it enabled efficient computation of minimal embedding changes using the Viterbi algorithm. However, additive distortion functions proved inadequate in capturing the interdependencies between neighboring DCT coefficients, leading to development of non-additive distortion functions. These functions better modeled the intricate dependencies between coefficients and improved statistical undetectability. Additionally, these functions could be approximated as additive, thus, easing implementation with STCs. However, the computation complexity of these functions got increased.

The universal wavelet relative distortion (UNIWARD) [13] function emerged as a significant advancement in distortion function design. UNIWARD introduced a universal approach to measuring the costs of pixel/coefficient modifications, providing a content-adaptive model that could be applied across different domains, including the JPEG domain. Its JPEG-specific variant, J-UNIWARD, while technically additive, incorporated sophisticated wavelet-based residuals to capture local image complexity, allowing it to better preserve complex textures and edge structures while maintaining high security against statistical detection. However, with a total computational complexity of O(1664MN) (MN is size of the cover image) UNIWARD presents a significant challenge in real-world applications [14]. The uniform embedding revisited distortion (UERD) emerges as an alternative [14], offering computational complexity of O(13MN) while achieving comparable undetectability to UNIWARD. UERD leverages inter-block correlation between adjacent DCT blocks in JPEG images to determine embedding costs, capitalizing on the natural dependencies between neighboring blocks. The distortion function computes costs by measuring inter-block energy for each DCT coefficient across eight horizontal, vertical and diagonal block neighbors. This function implements an inverse relationship for cost assignment where higher inter-block energy regions (typically textures) receive lower costs, while smooth regions with low inter-block energy receive higher costs. The field has further evolved with various cost functions like IUERD [15], GUED [16], BBC [17], BBM [18], U2ED [19], each exploiting unique aspects of DCT block relationships to determine individual element costs. Typically, these approaches favored embedding in textured regions, such as edges, since these areas are less susceptible to detection through steganalysis.

An important aspect of these STC and distortion-based algorithms is that they operate on the critical assumption that the stego image will remain unaltered during transmission. When this assumption is violated, faithful message extraction can no longer be guaranteed. A common way to exploit this vulnerability is through the recompression of stego images, a prevalent operation on images shared over SNPs such as Facebook, WhatsApp, and LinkedIn and likewise. These platforms often apply lossy recompression on uploaded images to minimize the storage and network bandwidth requirements.

Though the modifications introduced during recompression are minimal, they result in significant errors in the extracted message due to the fragile nature of STCs. Even small alterations in the stego image content can corrupt the decoding of message bits. This highlights a critical vulnerability in these sophisticated steganographic methods. To illustrate this, we conducted experiments using 100 grayscale images from the benchmark BOSSbase dataset [20]. Each image was JPEG-compressed at quality factors (QFs) of 90, 80, and 70, creating three separate datasets of 100 images each. Five payload levels - 1%, 5%, 10%, 30%, and 50% of the total non-zero AC coefficients (nzAC) in each image - were selected for embedding and labeled as P1, P5, P10, P30, and P50, respectively. Random binary bits of length equal to payload length were then embedded using STCs, with QDCT coefficients serving as cover elements. The cost of modifying cover elements was calculated using the UERD [14] cost function. Following embedding, the stego images were recompressed at the same quality factor, and attempts were made to retrieve the embedded messages. Recompression with same QF is chosen to introduce minimum alterations due to recompression. As observed in TABLE I, for QF 90-90 recompression scenario, on average, even a minor percentage change of 0.13% in stego elements can result in a significant number of error bits (41%) in the extracted message. Particularly for lower payloads, the error rates are notably high. Although the error rate decreases gradually with larger payloads, it remains considerable. Moreover, higher QFs generally lead to more bit alterations after recompression, primarily due to the use of finer quantization steps, which increases the likelihood of DCT coefficients shifting into different quantization bins. As discussed before, these results validate the fragility of STCs under JPEG recompression. Moreover, if the recompression QF is smaller than the initial QF then the message extraction error rate increases further.

IV. TOWARDS ROBUST STEGANOGRAPHY

The third and current phase of JPEG steganography research has been largely driven by the challenges posed by

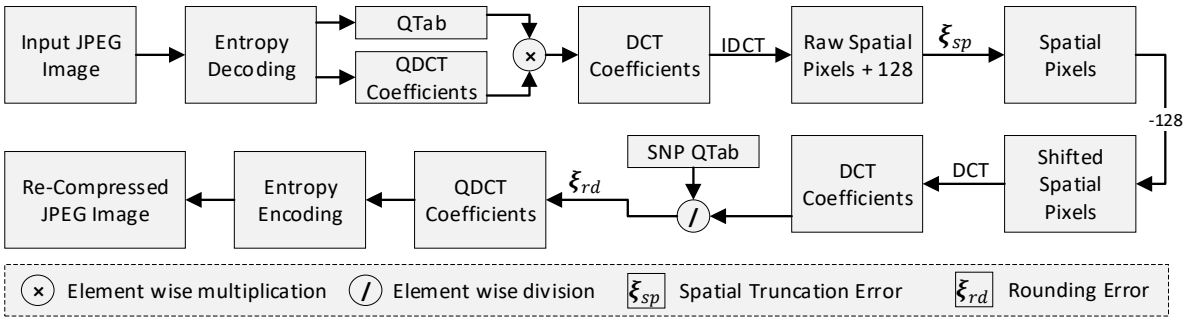

Fig. 1. Typical JPEG recompression process on social networking platforms.

TABLE I. STCs PERFORMANCE UNDER JPEG RECOMPRESSION WITH SAME QUALITY FACTOR

Scenarios	Payload	# Changed elements/Total elements	# Corrupted message bits/ Total message length	Percentage Error
QF 90-90	P1	340/262144	332/796	41%
	P5	342/262144	1051/3979	26%
	P10	347/262144	1518/7957	19%
	P30	373/262144	2362/23869	9%
	P50	419/262144	2970/39781	7%
QF 80-80	P1	183/262144	181/551	32%
	P5	187/262144	532/2752	19%
	P10	192/262144	761/5505	13%
	P30	213/262144	1227/16513	7%
	P50	248/262144	1617/27520	5%
QF 70-70	P1	340/262144	126/438	28%
	P5	342/262144	358/2189	16%
	P10	347/262144	511/4377	11%
	P30	373/262144	863/13132	6%
	P50	419/262144	1177/21885	5%

real-world deployment scenarios, particularly in SNPs. While STC-based methods demonstrated excellent security against steganalysis, they showed significant vulnerability to any modifications in the stego image content during transmission. This weakness became particularly apparent in social media applications, where images routinely undergo multiple rounds of processing and recompression, often resulting in corruption of the hidden message. To understand the primary sources of stego-element modifications, it is essential to analyze the recompression process typical of SNPs, as shown in Fig. 1. For simplicity, we are assuming the input images are grayscale JPEG images. When a JPEG image is uploaded to an SNP, it undergoes a series of operations, including decompression, recompression, and possibly resizing. Some of these operations are lossy and can irreversibly alter the image content.

During decompression (Fig. 1, upper half), the JPEG file is first entropy decoded to obtain the quantization table and the QDCT coefficients. These coefficients are then multiplied element-wise with the quantization table to generate the DCT coefficients. The DCT coefficients are subsequently transformed back into spatial pixels using the 2D inverse-DCT (IDCT) operation. This process is performed in a block-wise manner, the image is divided into 8 × 8 blocks, and each block is processed independently. To recover the original pixel values, the initial level shift applied during compression is reversed by adding 128 to each pixel value. Finally, rounding and truncation are applied to ensure the spatial pixels fall within the unsigned integer range of 0 to 255. This step introduces spatial errors, which are represented as $\boldsymbol{\xi}_{sp}$. The entire decompression process can be represented mathematically as:

$$\boldsymbol{\mathcal{P}} = [\text{IDCT}(\mathbf{D} .* \mathbf{Q})] + 128 \quad (1)$$

Here, $\mathbf{D}$ is the quantized DCT coefficients $\mathbf{Q}$ is the quantization table and $[x]$ is the spatial rounding and truncation operation, where $[x] = round(x)$ for $0 \leq x \leq 255$, $[x] = 0$ for $[x] < 0$, and $[x] = 255$ for $[x] > 255$.

During recompression (Fig. 1, bottom half), the spatial pixels are shifted by subtracting 128 to center their values around zero. These shifted spatial pixels are then transformed into DCT coefficients using the 2D DCT in a block-wise manner. The DCT coefficients are divided by the SNP quantization table and rounded to the nearest integer, resulting in the QDCT coefficients. This quantization process introduces rounding errors, represented as $\boldsymbol{\xi}_{rd}$. Finally, the QDCT coefficients are entropy encoded to generate the recompressed JPEG file. Mathematically, this process can be represented as:

$$\mathbf{D} = \text{nint}(\text{DCT}(\boldsymbol{\mathcal{P}} - 128) ./ \mathbf{Q}) + \boldsymbol{\xi}_{rd} \quad (1)$$

Here, $\text{nint}(x)$ is the nearest integer rounding operation, where $\text{nint}(x) = \lfloor x \rfloor$ if $x - \lfloor x \rfloor < 0.5$ and $\lceil x \rceil$ if $x - \lfloor x \rfloor \geq 0.5$. The cumulative errors $\boldsymbol{\xi}_{sp}$ and $\boldsymbol{\xi}_{rd}$ from decompression and recompression stages are the primary contributors to distortion in the stego content. Therefore, techniques for

robust steganography must be designed to minimize these errors, ensuring reliable message extraction.

To address these robustness issues, researchers have explored various robust steganography techniques. One such approach is based on dither modulation, initially developed for watermarking [21]. Specifically, dither modulation often targets the mid-frequency DCT regions rather than high-frequency regions, as these frequencies tend to withstand recompression better. Studies have shown [22], [23], [24], [25], [26] that mid-frequency embedding helps balance robustness and perceptual quality, making dither modulation a valuable approach for robust steganographic embedding in JPEG images.

Another prominent technique is sign-based steganography that takes advantage of the inherent resilience of sign bits in DCT coefficients, which remain relatively stable even after recompression. In sign-based steganography [27], [28], [29], message bits are embedded by selectively flipping the signs of chosen non-zero quantized DCT coefficients. However, due to the sensitivity of high-magnitude DCT coefficients, only low-magnitude coefficients are generally considered suitable for sign flipping. Flipping the signs of high-magnitude coefficients can introduce detectable distortions, thus, reducing the undetectability of the hidden message.

Pre-processing approaches [30], [31], [32], [33], aim to minimize the impact of quantization errors $\boldsymbol{\xi}_{rd}$ by iteratively modifying the cover image to match stego i characteristics after recompression. However, these methods require detailed knowledge of the JPEG encoder and involve computationally expensive repeated recompressions, limiting their practical application. Additionally, they do not fully address the lossy rounding and spatial truncation errors $\boldsymbol{\xi}_{sp}$ introduced during decompression. Autoencoder-based models [34] are another approach, trained to minimize JPEG compression artifacts, potentially safeguarding concealed data and resisting compression-induced distortions. However, their training process can be computationally demanding, and their effectiveness might be dependent on the specific JPEG encoder used. Zeng et al. [35], addressed the issues of $\boldsymbol{\xi}_{sp}$ and $\boldsymbol{\xi}_{rd}$ by minimizing spatial overflows and devising pre-processing techniques on scaling and truncation to enhance robustness. They also introduced post-processing of embedding costs using scaling functions for message hiding in high quality images. In recent developments, Kumar et al. [36] focused on finding robust coefficients and refining the embedding process to prioritize these locations, aiming to improve message recoverability. However, their approach required additional information of the robust locations to be shared with the receiver.

Most of the discussed robust techniques requires error correction codes (ECC) like Reed-Solomon codes, and BCH codes to sustain the robustness against transmission channel impairments. The integration of error correction introduces its own set of challenges. The additional redundancy required for error correction reduces the effective payload capacity, and increases the necessary modifications required, potentially raising detectability. Additionally, selecting an optimal error correction parameter proves challenging given the varying and often unpredictable nature of image modifications across different platforms.

V. Open Research Issues and Challenges

Despite significant advancements in JPEG steganography, several open research issues and challenges remain, particularly in the context of ensuring robustness against real-world image processing and recompression. The ability to anticipate and adapt to the diverse compression parameters and algorithms used by different platforms is crucial for developing truly robust steganography techniques. Current approaches often rely on simplified models of recompression processes, highlighting the need for more accurate and dynamic models that can learn from real-world data, potentially leveraging machine learning. Moreover, accurately predicting the impact of recompression on embedded data remains challenging. Researchers need to develop techniques that can estimate the errors introduced during recompression, allowing for more effective countermeasures. Achieving a balance between embedding capacity, security against steganalysis, and robustness to recompression is a complex optimization problem. As the STCs are proved to be fragile, exploring novel coding techniques and embedding strategies that minimize the trade-off between these factors is essential.

Steganalysis techniques are becoming increasingly sophisticated, emphasizing the need to develop secure and robust steganography algorithms that are resilient to these evolving attacks. The use of deep learning in steganalysis poses new challenges. Researchers need to develop steganographic techniques that can effectively counter deep learning-based attacks.

References

[1] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," Neurocomputing, vol. 335, pp. 299–326, Mar. 2019, doi: 10.1016/j.neucom.2018.06.075.

[2] K. D. Michaylov and D. K. Sarmah, "Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations," Journal of Cyber Security Technology, pp. 1–27, Jan. 2024, doi: 10.1080/23742917.2024.2304441.

[3] S. Kaur, S. Bansal, and R. K. Bansal, "Steganography and classification of image steganography techniques," in 2014 International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India: IEEE, Mar. 2014, pp. 870–875. doi: 10.1109/IndiaCom.2014.6828087.

[4] S. Kaur, S. Bansal, and R. K. Bansal, "Image steganography for securing secret data using hybrid hiding model," Multimed Tools Appl, vol. 80, no. 5, pp. 7749–7769, Feb. 2021, doi: 10.1007/s11042-020-09939-7.

[5] Sumeet Kaur, Savina Bansal, and R. K. Bansal, "An Efficient Adaptive Data Hiding Scheme for Image Steganography," in Proceedings of the International Congress on Information and Communication Technology, vol. 438, S. C. Satapathy, Y. C. Bhatt, A. Joshi, and D. K. Mishra, Eds., in Advances in Intelligent Systems and Computing, vol. 438. , Singapore: Springer Singapore, 2016, pp. 371–379. doi: 10.1007/978-981-10-0767-5_40.

[6] D. Upham, "JSteg." [Online]. Available: http://www.nic.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz

[7] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography," IEEE Secur. Privacy, vol. 1, no. 3, pp. 32–44, May 2003, doi: 10.1109/MSECP.2003.1203220.

[8] A. Westfeld, "F5—A Steganographic Algorithm: High Capacity Despite Better Steganalysis," in Information Hiding, vol. 2137, I. S. Moskowitz, Ed., in Lecture Notes in Computer Science, vol. 2137. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 289–302. doi: 10.1007/3-540-45496-9_21.

[9] J. Fridrich, M. Goljan, and D. Soukal, "Efficient Wet Paper Codes," in Information Hiding, vol. 3727, M. Barni, J. Herrera-Joancomartí, S. Katzenbeisser, and F. Pérez-González, Eds., in Lecture Notes in

Computer Science, vol. 3727. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 204–218. doi: 10.1007/11558859_16.

[10] J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable jpeg steganography: dead ends challenges, and opportunities," in Proceedings of the 9th Workshop on Multimedia & Security, in MM&Sec '07. New York, NY, USA: Association for Computing Machinery, 2007, pp. 3–14. doi: 10.1145/1288869.1288872.

[11] T. Filler, J. Judas, and J. Fridrich, "Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes," IEEE Trans.Inform.Forensic Secur., vol. 6, no. 3, pp. 920–935, Sep. 2011, doi: 10.1109/TIFS.2011.2134094.

[12] J. Fridrich, M. Goljan, and D. Soukal, "Perturbed quantization steganography," Multimedia Systems, vol. 11, no. 2, pp. 98–107, Dec. 2005, doi: 10.1007/s00530-005-0194-3.

[13] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," EURASIP J. on Info. Security, vol. 2014, no. 1, p. 1, Dec. 2014, doi: 10.1186/1687-417X-2014-1.

[14] L. Guo, J. Ni, W. Su, C. Tang, and Y.-Q. Shi, "Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited," IEEE Trans.Inform.Forensic Secur., vol. 10, no. 12, pp. 2669–2680, Dec. 2015, doi: 10.1109/TIFS.2015.2473815.

[15] Y. Pan, J. Ni, and W. Su, "Improved Uniform Embedding for Efficient JPEG Steganography," in Cloud Computing and Security, vol. 10039, X. Sun, A. Liu, H.-C. Chao, and E. Bertino, Eds., in Lecture Notes in Computer Science, vol. 10039. , Cham: Springer International Publishing, 2016, pp. 125–133. doi: 10.1007/978-3-319-48671-0_12.

[16] W. Su, J. Ni, X. Li, and Y.-Q. Shi, "A New Distortion Function Design for JPEG Steganography Using the Generalized Uniform Embedding Strategy," IEEE Trans. Circuits Syst. Video Technol., vol. 28, no. 12, pp. 3545–3549, Dec. 2018, doi: 10.1109/TCSVT.2018.2865537.

[17] Y. Wang, W. Li, W. Zhang, X. Yu, K. Liu, and N. Yu, "BBC++: Enhanced Block Boundary Continuity on Defining Non-Additive Distortion for JPEG Steganography," IEEE Trans. Circuits Syst. Video Technol., vol. 31, no. 5, pp. 2082–2088, May 2021, doi: 10.1109/TCSVT.2020.3010554.

[18] Y. Wang, W. Zhang, W. Li, and N. Yu, "Non-Additive Cost Functions for JPEG Steganography Based on Block Boundary Maintenance," IEEE Trans.Inform.Forensic Secur., vol. 16, pp. 1117–1130, 2021, doi: 10.1109/TIFS.2020.3029908.

[19] S. Bansal, R. K. Bansal, and R. Kumar, "A Novel Upgraded Uniform Embedding Technique for JPEG Steganography," in Intelligent Sustainable Systems, vol. 333, A. K. Nagar, D. S. Jat, G. Marín-Raventós, and D. K. Mishra, Eds., in Lecture Notes in Networks and Systems, vol. 333. , Singapore: Springer Nature Singapore, 2022, pp. 723–730. doi: 10.1007/978-981-16-6309-3_68.

[20] P. Bas, T. Filler, and T. Pevný, "Break Our Steganographic System: The Ins and Outs of Organizing BOSS," in Information Hiding, vol. 6958, T. Filler, T. Pevný, S. Craver, and A. Ker, Eds., in Lecture Notes in Computer Science, vol. 6958. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 59–70. doi: 10.1007/978-3-642-24178-9_5.

[21] B. Chen and G. W. Wornell, "Dither modulation: a new approach to digital watermarking and information embedding," presented at the Electronic Imaging '99, P. W. Wong and E. J. Delp Iii, Eds., San Jose, CA, Apr. 1999, pp. 342–353. doi: 10.1117/12.344684.

[22] Y. Zhang, X. Zhu, C. Qin, C. Yang, and X. Luo, "Dither modulation based adaptive steganography resisting jpeg compression and statistic detection," Multimed Tools Appl, vol. 77, no. 14, pp. 17913–17935, Jul. 2018, doi: 10.1007/s11042-017-4506-3.

[23] X. Yu, K. Chen, Y. Wang, W. Li, W. Zhang, and N. Yu, "Robust adaptive steganography based on generalized dither modulation and expanded embedding domain," Signal Processing, vol. 168, p. 107343, Mar. 2020, doi: 10.1016/j.sigpro.2019.107343.

[24] Y. Zhang, X. Luo, X. Zhu, Z. Li, and A. G. Bors, "Enhancing reliability and efficiency for real-time robust adaptive steganography using cyclic redundancy check codes," J Real-Time Image Proc, vol. 17, no. 1, pp. 115–123, Feb. 2020, doi: 10.1007/s11554-019-00905-7.

[25] J. Zhang, X. Zhao, X. He, and H. Zhang, "Improving the Robustness of JPEG Steganography With Robustness Cost," IEEE Signal Process. Lett., vol. 29, pp. 164–168, 2022, doi: 10.1109/LSP.2021.3129419.

[26] X. Duan, B. Li, Z. Yin, X. Zhang, and B. Luo, "Robust image steganography against lossy JPEG compression based on embedding domain selection and adaptive error correction," Expert Systems with Applications, vol. 229, p. 120416, Nov. 2023, doi: 10.1016/j.eswa.2023.120416.

[27] Z. Zhu, N. Zheng, T. Qiao, and M. Xu, "Robust Steganography by Modifying Sign of DCT Coefficients," IEEE Access, vol. 7, pp. 168613–168628, 2019, doi: 10.1109/ACCESS.2019.2953504.

[28] T. Qiao, S. Wang, X. Luo, and Z. Zhu, "Robust steganography resisting JPEG compression by improving selection of cover element," Signal Processing, vol. 183, p. 108048, Jun. 2021, doi: 10.1016/j.sigpro.2021.108048.

[29] X. Wu, T. Qiao, Y. Chen, M. Xu, N. Zheng, and X. Luo, "Sign steganography revisited with robust domain selection," Signal Processing, vol. 196, p. 108522, Jul. 2022, doi: 10.1016/j.sigpro.2022.108522.

[30] Z. Yin and L. Ke, "Robust Adaptive Steganography Based on Dither Modulation and Modification With Re-Compression," IEEE Trans. on Signal and Inf. Process. over Networks, vol. 7, pp. 336–345, 2021, doi: 10.1109/TSIPN.2021.3081373.

[31] J. Tao, S. Li, X. Zhang, and Z. Wang, "Towards Robust Image Steganography," IEEE Trans. Circuits Syst. Video Technol., vol. 29, no. 2, pp. 594–600, Feb. 2019, doi: 10.1109/TCSVT.2018.2881118.

[32] Z. Zhao, Q. Guan, H. Zhang, and X. Zhao, "Improving the Robustness of Adaptive Steganographic Algorithms Based on Transport Channel Matching," IEEE Trans.Inform.Forensic Secur., vol. 14, no. 7, pp. 1843–1856, Jul. 2019, doi: 10.1109/TIFS.2018.2885438.

[33] J. Butora, P. Puteaux, and P. Bas, "Errorless Robust JPEG Steganography Using Outputs of JPEG Coders," IEEE Trans. Dependable and Secure Comput., vol. 21, no. 4, pp. 2394–2406, Jul. 2024, doi: 10.1109/TDSC.2023.3306379.

[34] W. Lu, J. Zhang, X. Zhao, W. Zhang, and J. Huang, "Secure Robust JPEG Steganography Based on AutoEncoder With Adaptive BCH Encoding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 7, pp. 2909–2922, Jul. 2021, doi: 10.1109/TCSVT.2020.3027843.

[35] K. Zeng, K. Chen, W. Zhang, Y. Wang, and N. Yu, "Robust Steganography for High Quality Images," IEEE Trans. Circuits Syst. Video Technol., vol. 33, no. 9, pp. 4893–4906, Sep. 2023, doi: 10.1109/TCSVT.2023.3250750.

[36] R. Kumar, S. Bansal, and R. K. Bansal, "A Resilient Approach to Robust JPEG Steganography: Ensuring Hidden Data Integrity," in 2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS), Kalaburagi, India: IEEE, Nov. 2023, pp. 1–6. doi: 10.1109/ICIICS59993.2023.10421695.