2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS)

A Resilient Approach to Robust JPEG Steganography: Ensuring Hidden Data Integrity

1st Rakesh Kumar
Department of ECE
MRSPTU
Bathinda, Punjab, India
kumarrakesh0791@gmail.com

2nd Savina Bansal
Department of ECE
MRSPTU
Bathinda, Punjab, India
savina.bansal@gmail.com

3rd RK Bansal
Department of ECE
MRSPTU
Bathinda, Punjab, India
drrakeshkbansal@gmail.com

2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS) | 979-8-3503-1545-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICIICS59993.2023.10421695

***Abstract*—Modern-day steganography algorithms leveraging the Joint Photographic Experts Group (JPEG) images have made impressive progress in achieving imperceptibility and undetectability by employing cost-effective embedding techniques. However, these algorithms often fall short in effectively addressing the challenges posed by JPEG re-compression, limiting their practical viability. To transcend this limitation, the paper introduces a novel method that judiciously embeds confidential data in discrete cosine transform (DCT) coefficients to enhance robustness. Experimental results demonstrate superiority of the proposed approach compared to state-of-the-art techniques. Under JPEG recompression with same quality factor, the technique achieves less than 1% message extraction error rate in most test cases, significantly lower than 10-50% error rates of existing methods. Besides, imperceptibility is maintained with PSNR of 51-62 dB. Moreover, by selectively modifying DCT coefficients, computational time is reduced to tens of milliseconds. These advancements hold great potential for various real-world applications, including secure communication over social networking platforms, where JPEG re-compressions are prevalent.**

Keywords—JPEG, Robust steganography, Data hiding, SNP

I. Introduction

Steganography, the discipline of disguising secrets within seemingly innocuous cover objects, has emerged as a crucial technique in the context of data security. By embedding confidential information within existing digital content provides a mean to covert communication and protect sensitive information from unauthorized access. Among the various digital media formats, the JPEG image format stands out due to its efficient compression capabilities and widespread usage. JPEG is a lossy compression method widely employed for storing and transmitting photographic images across mobile devices and social networking platforms (SNPs). Its popularity can be attributed to the balance that it strikes between image quality and file size. However, the characteristics of JPEG compression itself poses challenge to steganographic. JPEG performs quantization and frequency domain transformation, resulting in irreversible modifications of image data. This lossy nature of JPEG compression raises concerns about the concealment and integrity of embedded data [1] [2] [3].The motivation behind this research paper is to explore and develop robust steganographic techniques specifically tailored for JPEG images. The goal is to improve the invisibility and resilience of encapsulated data, thus addressing the limitations of traditional JPEG steganography methods. By improving the robustness of the embedding process, the aim is to withstand the most common image processing operation, JPEG recompression. This research paper will provide insights into the existing methods for steganography in JPEG images and highlight their limitations. It will delve into the trade-offs between compression and steganographic capacity, as well as the impact of JPEG compression on the imperceptibility and robustness of the embedded data. Furthermore, this paper will present a new approach for robust embedding in JPEG images, focusing on quantized DCT Coefficients. By developing and evaluating these robust embedding algorithms, we seek to enhance the robustness of the hidden information while maintaining a significant imperceptibility in trade-off with payload capacity. The evaluation will involve analyzing the statistical properties of the stego images and assessing message extraction accuracy. Key contribution includes a new efficient and robust embedding algorithm for robust JPEG steganography. The following sections of this research paper will provide a comprehensive analysis of the background and related work, proposed robust embedding algorithm, imperceptibility and robustness analysis, performance evaluation, and future directions. Through this investigation, the aim is to contribute in the field of robust JPEG steganography and advance the understanding of its potential applications and implications for information security and privacy.

II. Related Works

Steganography techniques for digital images have a rich history, dating back to ancient times, and they continue to evolve with the advent of digital technology [1]. The emergence of digital media has presented new opportunities and challenges for concealing information within such media. Throughout the years, numerous steganographic techniques have been proposed and explored, however the primary focus of this research paper is on steganography specifically in the context of JPEG images. JPEG steganography has garnered significant research interest due to its potential to effectively and covertly conceal data, leveraging the features offered by JPEG compression, thus making it applicable for real-world applications. Traditional JPEG steganography techniques [4] [5] primarily rely on least significant bit (LSB) modification, where the secret message is concealed by substituting LSBs of carrier image elements. Conversely, transform domain techniques based on DCT, encode confidential data within LSBs of DCT coefficients, taking advantage of the perceptual capabilities of human visual system. These approaches offers simplicity but are vulnerable to statistical attacks [6]. The limitations of traditional JPEG steganography methods have led to the development of more advanced techniques. One notable direction is the exploration of adaptive steganography, where embedding is dynamically adjusted based on image characteristics. Adaptive LSB-based methods [7] [8] [9] [10] [11] adapt embedding strategy according to pixel and its neighboring pixel values, thus reducing the visual impact of hidden data. In parallel, adaptive DCT-based techniques employ selective modification of quantized DCT coefficients in specific DCT blocks and frequencies, aiming to minimize alterations in cover image [12] [13]. Furthermore, the introduction of syndrome trellis codes (STC) [14]

revolutionized JPEG steganography by emphasizing heuristic-based or distortion-based techniques. STCs are binary linear convolutional codes represented by a parity-check matrix. They provide near-optimal embedding efficiency while minimizing distortion in stego images. This breakthrough has had a profound impact on steganography research, with a significant portion of the literature adopting this approach. STCs have proven to be effective in handling the embedding of secret messages. However, an essential aspect of the process lies in designing the distortion function. Distortion function determines the modifications to be made during embedding, directly affecting the imperceptibility of resulting stego image. Researchers have focused on careful designing of distortion function to strike a balance between imperceptibility and embedding capacity, ensuring that the hidden data remains covert while minimizing any noticeable visual artifacts. Notable contributions include [15] which introduced a distortion-based uniform encoding scheme (UED) for JPEG steganography. UED minimizes statistical artifacts by modifying non-zero quantized DCT coefficients. Building upon this, Holub et al. proposed UNIWARD [16], a content-adaptive approach utilizing wavelet domain for deriving distortion functions in spatial and JPEG domain. Despite achieving good security performance against steganalysis, UNIWARD incurs substantial computational time. In an effort to improve upon the UED scheme, Guo et al. developed Uniform Embedding Revisited Distortion (UERD) [17], which evenly distributes embedding changes across all DCT coefficients. Pan et al. introduced IUERD [18], leveraging inter-block correlation for enhanced statistical undetectability. Additionally, Bansal et al. proposed U2ED [19], a novel distortion measure that preserves the statistical invisibility of embedded information in both spatial and DCT domains, by confining the confidential data into textured areas of carrier image. Notably, non-additive distortion-based approaches have also been explored, offering new strategies for achieving covert steganography. Denemark and Fridrich achieved synchronization of modification directions for adjacent pixels [20], while Li et al. employed a technique called Cluster Modification Direction (CMD) [21] to subdivide carrier image into sub-images. They reduced additive-distortion for each sub-image separately, ensuring precise control over the modification process. Zhang et al. introduced DeJoin, [22] an approach that comprehends the influence of adjacent modifications on pixel blocks. They decomposed the collective cost of modifying adjacent-pixel blocks into additive distortion on each individual pixels, thereby reducing the average distortion. Li et al. proposed [23] to maintain seamless transitions in spatial domain while embedding in JPEG domain by preserving block boundaries. Further advancements include CMD inspired work by Wang et al. [24] for color image. They proposed a strategy to adaptively embed in RGB channels while maintaining low modification rates. Wang et al. enhanced BBC with BBC++ [25], synchronizing modification directions of inter-block boundaries. They also presented Block Boundary Maintenance (BBM) [26], which leveraged intra-block DCT coefficient correlation to minimize modifications on spatial block boundaries, ensuring high security against modern JPEG steganalysis techniques.

While the existing techniques in JPEG steganography excel in imperceptibility, security against steganalysis, and offer sufficient payload capacity, they often overlook the challenges posed by real-world scenarios. These techniques typically assume that the stego image will reach the receiver without any loss or alteration during transmission. However, in practical situations, transmission channels with storage and bandwidth constraints may subject the stego image to post-processing operations, leading to potential data alterations and impairments. SNPs like WhatsApp, Facebook, X and likewise are examples of such channels, where stego images are susceptible to post-processing operations like JPEG recompression. Due to the lossy nature of JPEG (as discussed in section I), these operations can significantly impact the accuracy of message extraction, making the exact recovery of secret message uncertain. In this work, a technique is proposed that can effectively handle JPEG re-compression with same quality factor.

III. Proposed Work

Functional block diagram of proposed scheme is illustrated in Fig. 1. The process begins with an input JPEG cover image, which undergoes entropy decoding and quantization as a pre-processing step to acquire quantized DCT coefficients. Among these coefficients, specific ones are chosen as cover elements for embedding purposes. These selected cover elements, along with secret message and prior knowledge of public channel characteristics, serve as inputs to the message embedding algorithm. Here, the term public channel characteristics refers to the specific quantization table employed by the public channel to quantize input images. Consequently, the algorithm produces a stego image with the hidden message concealed within it. This image is then sent to the receiver via same public channel. At receiver's end, the channel-compressed stego image is pre-processed to facilitate the extraction of stego elements from the quantized DCT coefficients. Subsequently, these stego elements are used for the extraction of secret message. To simplify, the cover image with dimensions m × n, undergoes a pre-processing step, leading to a quantized DCT coefficients matrix of size m × n. This matrix is then sub-divided into 8×8 disjoint boxes containing 64 DCT coefficients. Within each block, the algorithm scans for all possible embedding locations that are suitable for embedding.

A. Embedding Process

In the proposed scheme, non-zero DCT coefficients at lower frequency region are selected from each 8×8 grid as embedding domain. These positions are chosen for their higher likelihood of having non-zero coefficients. A key is generated from these locations and must be shared with the receiver for faithful extraction of concealed message. Next step is to embed the secret message into the selected embedding domain. This step is a significant contribution of this research paper. The proposed algorithm calculates the minimum embedding offset ξ needed to conceal a secret message $\mathbb{T}_m \in \{0,1\}$ within a DCT coefficient $\mathbb{X}$, ensuring successful retrieval of the concealed message. This change is added to the magnitude of $\mathbb{X}$, generating a modified coefficient $\mathbb{X}$. Notably, ξ depends on the prior knowledge of the public channel's quantization table δ and the quantization step Δ associated with the current coefficient $\mathbb{X}$. To embed secret message $\mathbb{T}_m = 1$ in DCT coefficient $\mathbb{X}$, the modified DCT coefficient is calculated using equation (1)

$$\mathbb{X}' = \begin{cases} |\mathbb{X}| + \xi\,; & if\ \mathrm{mod}(\mathbb{X}, 2) = 1 \\ |\mathbb{X}| - \beta + \xi\,; & if\ \mathrm{mod}(\mathbb{X}, 2) = 0 \end{cases} \quad (1)$$

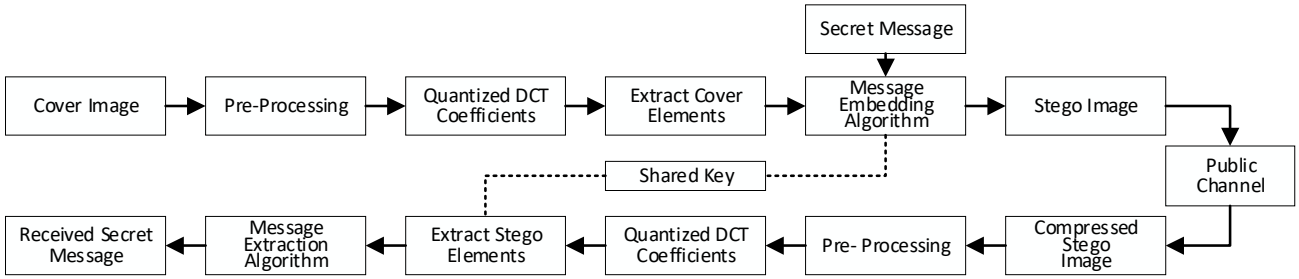

Fig. 1. Framework of proposed work.

Similarly, to embed secret message $\mathbb{T}_m = 0$, the modified DCT coefficient is obtained using equation (2)

$$\mathbb{X}' = \begin{cases} |\mathbb{X}| - \beta + \xi\,; & if\ \mathrm{mod}(\mathbb{X}, 2) = 0 \\ |\mathbb{X}| + \xi\,; & if\ \mathrm{mod}(\mathbb{X}, 2) = 1 \end{cases} \quad (2)$$

The embedding offset ξ is calculated as

$$\xi = \delta * \left(\alpha - \left(\frac{|\mathbb{X}|}{\Delta} - \left\lfloor\frac{|\mathbb{X}|}{\Delta}\right\rfloor\right)\right) \quad (3)$$

After applying the necessary magnitude changes, the new DCT coefficient $\mathbb{X}_{new}$ is obtained using equation (4)

$$\mathbb{X}_{new} = sign(\mathbb{X}) * \mathbb{X}' \quad (4)$$

Here, α and β are constants used to control the impact of embedding offset. Through experimentation we have found $= 0.5$ and $\beta = 1$ to provide stable response. In final step, the original DCT coefficients $\mathbb{X}$ are replaced with modified DCT coefficients $\mathbb{X}_{new}$. Followed by inverse DCT and de-quantization to generate the stego image. Subsequently, the stego image with encapsulated secret information is sent to the intended receiver through public channel.

B. Extraction Process

The first step of extraction process is to pre-process the re-compressed stego image. Entropy decoding is applied to obtain the quantized DCT coefficients. Next step is to select the stego elements using shared key. To extract the concealed secret message parity check operation is performed on the selected DCT coefficients $\mathbb{Y}$. The algorithm determines the parity of selected coefficients by applying the modulo 2 operation. If the result is 1, it indicates that the concealed message bit is 1. Conversely, if the result is 0, it signifies that the concealed message bit is 0. The extraction process can be succinctly expressed as:

$$\mathbb{R}_m = \begin{cases} 1 & if\ \mathrm{mod}(\mathbb{Y}, 2) = 1 \\ 0 & if\ \mathrm{mod}(\mathbb{Y}, 2) = 0 \end{cases} \quad (5)$$

This simple yet effective approach ensures efficient message retrieval without the need for complex computations or additional processing steps.

IV. Experimental Setup and Performance Metrices

In this paper, a testbed comprising 50 randomly chosen images from the BOSSbase1.01 database [27] is employed for all experiments. The experiments are conducted on MATLAB platform, running on an i3 Intel Core processor with 8GB RAM. The BOSSbase 1.01 database contains images in portable gray map (pgm) format, therefore, selected images are first subjected to JPEG compression of 95 to 70 with a step size of 5 to generate a test bed for six different scenarios. All images are grayscale images with dimension 512×512. The primary goal of this research is to investigate the effect of JPEG recompression with same quality factor on average message extraction error. Additionally, imperceptibility and computational complexity are evaluated. To accomplish this, the original JPEG cover images, after embedding, are channel compressed. Subsequently, the message is extracted from these channel recompressed images. To provide a comparative analysis, two existing JPEG steganography algorithms, namely UERD [17] and U2ED [19], are used as benchmarks alongside the proposed algorithm. This comparison enables the assessment of the effectiveness and superiority of proposed approach compared to these techniques. It is important to note that the channel transmission is simulated using MATLAB's 'imwrite' command, and the recompression quality factors are chosen accordingly. All the reported results are averaged over the 50 selected images.

A. Embedding Rate

The embedding rate refers to the capacity of a cover image to carry a secret message. In this research, the secret message is represented as a string of randomly generated binary numbers, and its length is determined by the chosen embedding rate. Maximum embedding rate is set to one bit per DCT block. Considering a fixed image dimensions of 512×512 pixels, the maximum payload capacity amounts to 4096 bits. To investigate different payload capacities, five distinct scenarios are established. The first scenario represents the minimum payload capacity of 20%, and then the payload capacity is increased progressively in 20% increments for the remaining four scenarios. This range of payload capacities allows to assess the trade-off between message size and the potential impact on the cover image.

B. Performance Metrices

Message Extraction Error (MER) is used to evaluate robustness of the proposed scheme. It is assessed using equation (6)

$$MER = \frac{\sum xor(\mathbb{T}_m, \mathbb{R}_m)}{length\ (\mathbb{T}_m)} \times 100 \quad (6)$$

The message extraction error rate is calculated as bitwise XOR between the transmitted message $\mathbb{T}_m$ and the received message $\mathbb{R}_m$, divided by the total length of transmitted message. This error rate indicates the integrity of embedded message after channel recompression. A lower error rate is desirable and signifies higher robustness against potential distortions and impairments during the transmission process.

Peak Signal to Noise Ratio (PSNR) is used to evaluate imperceptibility of the proposed scheme. Imperceptibility ensures that the cover and stego images appear visually

indistinguishable to the human visual system. This measure allows for a quantitative comparison between the cover images $\mathbb{C}$ and generated stego images $\mathbb{S}$.

$$PSNR(\mathbb{C},\mathbb{S}) = 10\log_{10}(peakVal^2/MSE) \quad (7)$$

Here, $peakVal$ is equal to 255 for 8bit grayscale images and MSE is the mean square error between the cover image and stego image.

Structural Similarity Index Measure (SSIM) calculates the structural similarity index for stego image using cover image as reference. A value closer to 1 indicates greater similarity between the two images. It is calculated as

$$SSIM(\mathbb{C},\mathbb{S}) == \frac{(2\overline{\mathbb{C}}\overline{\mathbb{S}}+\lambda)(2\sigma_{\mathbb{C}\mathbb{S}}+\kappa)}{(\overline{\mathbb{C}}^2+\overline{\mathbb{S}}^2+\lambda)(\sigma_{\mathbb{C}}^2+\sigma_{\mathbb{S}}^2+\kappa)} \quad (8)$$

Here, $\overline{\mathbb{C}}$, $\overline{\mathbb{S}}$ are mean of cover and stego image, $\sigma_{\mathbb{C}\mathbb{S}}$ is covariance, $\sigma_{\mathbb{C}}^2$, $\sigma_{\mathbb{S}}^2$ are variance and λ, κ are stabilizing constants.

Computational Time measures the algorithm's efficiency in terms of execution time. This is an important metric as real-world applications demand minimal processing delays. The time taken to embed secret message and generate stego image is calculated using MATLAB's inbuilt tic-toc functions. The tic command starts the timer before embedding, and toc command stops it after completion. The final elapsed time in seconds provides the computational time metric. A lower value indicates greater computational efficiency and faster processing speed of the algorithm.

V. Results and Discussion

A. Robustness Evaluation

The robustness of the proposed method is evaluated by measuring the message extraction error rate (MER) after JPEG recompression. As seen in Fig. 2 to Fig. 7, the proposed technique maintains error rates below 1% for most test cases across various quality factors and payload sizes. In comparison, existing methods like UERD and U2ED result in substantially higher error rates between 10-50% under the same test conditions. The significant performance gap highlights the superior resiliency offered by the proposed approach. This robustness originates from judicious modifications of selected DCT coefficients and concentrating changes in lower frequencies. The proposed method maintains near perfect extraction accuracy even when the JPEG quality vary between 95 and 70 (Fig. 2-7). While these results validate reliability of proposed technique, it is acknowledged that the approach has its limitations in terms of low payload carrying capacity. However, the robustness demonstrated against recompression remains a noteworthy success for practical JPEG steganography.

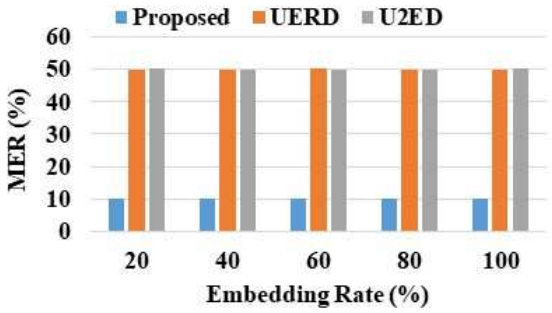

Fig. 2. Message extraction error rate for Q95

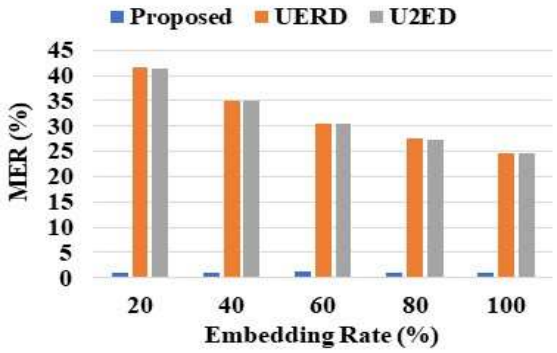

Fig. 3. Message extraction error rate for Q90

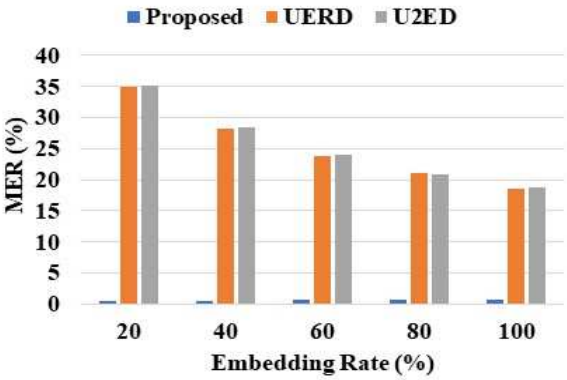

Fig. 4. Message extraction error rate for Q85

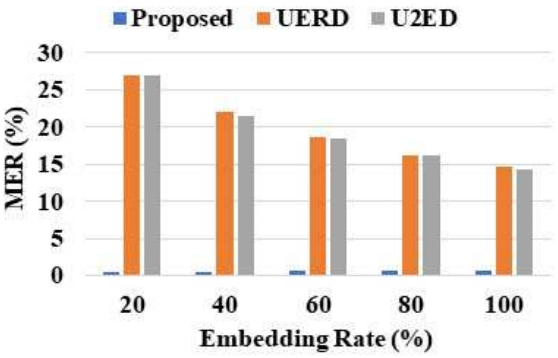

Fig. 5. Message extraction error rate for Q80

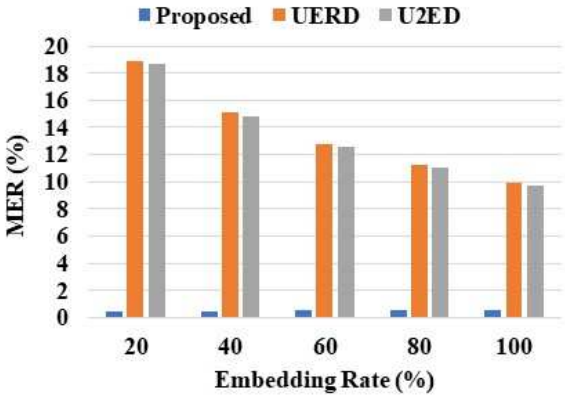

Fig. 6. Message extraction error rate for Q75

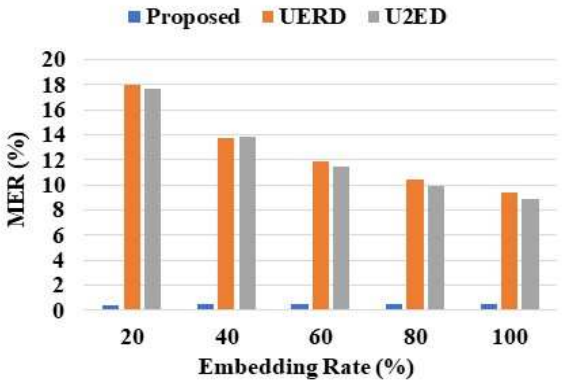

Fig. 7. Message extraction error rate for Q70

TABLE I. COMPARATIVE ANALYSIS OF PSNR FOR DIFFERENT QUALITY FACTORS

Emb Rate (%)	Q95			Q85			Q75			Q70		
	Proposed	*UERD*	*U2ED*	*Proposed*	*UERD*	*U2ED*	*Proposed*	*UERD*	*U2ED*	*Proposed*	*UERD*	*U2ED*
20	61.44	61.92	61.88	62.81	65.88	65.70	59.87	62.95	62.99	58.68	61.78	61.69
40	60.81	61.64	61.55	59.79	63.17	62.96	56.89	60.01	60.04	55.66	58.74	58.70
60	60.26	61.34	61.24	58.04	61.43	61.27	55.12	58.08	58.16	53.88	56.84	56.84
80	59.76	61.06	60.95	56.81	60.14	60.00	53.88	56.67	56.78	52.66	55.39	55.47
100	59.32	60.79	60.68	55.82	59.08	59.01	52.93	55.57	55.70	51.71	54.23	54.37

TABLE II. COMPARATIVE ANALYSIS OF SSIM FOR DIFFERENT QUALITY FACTORS

Emb Rate (%)	Q95			Q85			Q75			Q70		
	Proposed	*UERD*	*U2ED*	*Proposed*	*UERD*	*U2ED*	*Proposed*	*UERD*	*U2ED*	*Proposed*	*UERD*	*U2ED*
20	0.9996	0.9997	0.9997	0.9998	1.0000	1.0000	0.9996	0.9999	0.9999	0.9995	0.9999	0.9999
40	0.9996	0.9997	0.9997	0.9996	0.9999	0.9999	0.9993	0.9999	0.9999	0.9991	0.9999	0.9998
60	0.9995	0.9997	0.9997	0.9993	0.9999	0.9999	0.9989	0.9998	0.9998	0.9986	0.9998	0.9997
80	0.9995	0.9997	0.9997	0.9991	0.9999	0.9998	0.9986	0.9998	0.9997	0.9982	0.9997	0.9996
100	0.9994	0.9997	0.9996	0.9990	0.9998	0.9998	0.9983	0.9997	0.9996	0.9978	0.9996	0.9995

TABLE III. COMPUTATION TIME (IN SECONDS) FOR DIFFERENT QUALITY FACTORS

Emb Rate (%)	Q95			Q85			Q75			Q70		
	Proposed	*UERD*	*U2ED*	*Proposed*	*UERD*	*U2ED*	*Proposed*	*UERD*	*U2ED*	*Proposed*	*UERD*	*U2ED*
20	0.0306	1.1860	1.7547	0.0205	1.2878	1.7729	0.0201	1.1971	1.7717	0.0177	1.1683	1.7991
40	0.0266	1.1813	1.7419	0.0222	1.2903	1.7867	0.0206	1.2593	1.7658	0.0192	1.1571	1.7616
60	0.0268	1.1728	1.7460	0.0221	1.2939	1.7773	0.0205	1.1971	1.7744	0.0198	1.1696	1.7755
80	0.0277	1.1816	1.7422	0.0251	1.2379	1.7884	0.0207	1.1703	1.7799	0.0192	1.1699	1.7670
100	0.0282	1.1753	1.7713	0.0236	1.1600	1.7838	0.0228	1.1910	1.7899	0.0198	1.1509	1.7864

B. Imperceptibility Evaluation

The imperceptibility performance of the proposed scheme is analyzed by comparing the visual quality of the original cover images and the stego images using PSNR and SSIM metrics. TABLE I and TABLE II present the results for different JPEG quality factors from 95 to 70. The PSNR values achieved by the proposed method range from 51-62 dB across the test cases. This is comparable to state-of-the-art techniques like UERD and U2ED which yield slightly higher PSNR in the range of 59-65 dB. However, the difference is marginal and the proposed scheme still ensures adequate imperceptibility with PSNR above 50 dB. Furthermore, the SSIM results in TABLE II demonstrate the structural similarity between the cover and stego images. The proposed method achieves SSIM greater than 0.99 for all cases, indicating minimal perceptual distortion. Overall, the proposed scheme strikes a favorable balance between embedding modifications and imperceptibility.

C. Computational Time Evaluation

The computational complexity of the proposed scheme is evaluated in terms of execution time, as presented in TABLE III. A key advantage of the proposed approach is its low computational cost, with processing time in the order of tens of milliseconds. This is significantly faster than UERD and U2ED which require 1-2 seconds to process an image. The efficiency of the proposed scheme stems from its targeted embedding strategy which selectively modifies predetermined DCT coefficients instead of perturbing the entire coefficient matrix. By avoiding unnecessary computations, the embedding time is reduced drastically. This makes the proposed method well-suited for real-time multimedia applications where processing delays must be minimized.

VI. CONCLUSION

This paper presents a novel JPEG steganography technique resilient against JPEG recompression, addressing limitations in existing methods. The proposed approach

judiciously embeds data within DCT coefficients to enhance robustness. Experiments demonstrated the superiority of the proposed technique, achieving <1% message extraction error after recompression compared to 10-50% in state-of-the-art techniques. Imperceptibility is maintained with PSNR of 51-62 dB. Additionally, computational time is reduced to tens of milliseconds for real-time performance. The consistent robustness against JPEG recompression represents a major advancement in JPEG steganography research, holding great potential for secure multimedia communication. With further enhancement of payload capacity, this method offers a robust and practical solution.

REFERENCES

[1] K. Sahu and M. Sahu, "Digital image steganography and steganalysis: A journey of the past three decades," Open Computer Science, vol. 10, no. 1, pp. 296–342, Oct. 2020, doi: 10.1515/comp-2020-0136.

[2] S. Rahman et al., "A Comprehensive Study of Digital Image Steganographic Techniques," IEEE Access, vol. 11, pp. 6770–6791, 2023, doi: 10.1109/ACCESS.2023.3237393.

[3] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," IEEE Access, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[4] 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.

[5] S. Kaur, S. Bansal, and R. K. Bansal, "A Data Security Approach Based on Steganography," vol. 3, no. 2394, 2019.

[6] 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.

[7] 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.

[8] S. Kaur, S. Bansal, and R. K. Bansal, "Reversible Image Steganography Based on Interpolation and Adaptive Approach," ijcse, vol. 7, no. 5, pp. 1394–1398, May 2019, doi: 10.26438/ijcse/v7i5.13941398.

[9] 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.

[10] S. Singh, S. Bansal, and S. Singh, "Robust and Secure Image Watermarking using DWT-SVD and Chaotic Map," vol. 4, no. 9, 2015.

[11] B. Mandal, A. Pradhan, and G. Swain, "Adaptive LSB substitution Steganography technique based on PVD," in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India: IEEE, Apr. 2019, pp. 459–464. doi: 10.1109/ICOEI.2019.8862579.

[12] Q. Liu, A. H. Sung, Z. Chen, and X. Huang, "A JPEG-based statistically invisible steganography," in Proceedings of the Third International Conference on Internet Multimedia Computing and Service, Chengdu China: ACM, Aug. 2011, pp. 78–81. doi: 10.1145/2043674.2043697.

[13] D. Hou, H. Wang, W. Zhang, and N. Yu, "Reversible data hiding in JPEG image based on DCT frequency and block selection," Signal Processing, vol. 148, pp. 41–47, Jul. 2018, doi: 10.1016/j.sigpro.2018.02.002.

[14] 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.

[15] L. Guo, J. Ni, and Y. Q. Shi, "Uniform Embedding for Efficient JPEG Steganography," IEEE Transactions on Information Forensics and Security, vol. 9, no. 5, pp. 814–825, May 2014, doi: 10.1109/TIFS.2014.2312817.

[16] 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.

[17] 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.

[18] 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.

[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] T. Denemark and J. Fridrich, "Improving Steganographic Security by Synchronizing the Selection Channel," in Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security, Portland Oregon USA: ACM, Jun. 2015, pp. 5–14. doi: 10.1145/2756601.2756620.

[21] Bin Li, Ming Wang, Xiaolong Li, Shunquan Tan, and Jiwu Huang, "A Strategy of Clustering Modification Directions in Spatial Image Steganography," IEEE Trans.Inform.Forensic Secur., vol. 10, no. 9, pp. 1905–1917, Sep. 2015, doi: 10.1109/TIFS.2015.2434600.

[22] W. Zhang, Z. Zhang, L. Zhang, H. Li, and N. Yu, "Decomposing Joint Distortion for Adaptive Steganography," IEEE Trans. Circuits Syst. Video Technol., vol. 27, no. 10, pp. 2274–2280, Oct. 2017, doi: 10.1109/TCSVT.2016.2587388.

[23] W. Li, W. Zhang, K. Chen, W. Zhou, and N. Yu, "Defining Joint Distortion for JPEG Steganography," in Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security, Innsbruck Austria: ACM, Jun. 2018, pp. 5–16. doi: 10.1145/3206004.3206008.

[24] Y. Wang, W. Zhang, W. Li, X. Yu, and N. Yu, "Non-Additive Cost Functions for Color Image Steganography Based on Inter-Channel Correlations and Differences," IEEE Trans.Inform.Forensic Secur., vol. 15, pp. 2081–2095, 2020, doi: 10.1109/TIFS.2019.2956590.

[25] 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.

[26] 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

[27] 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.