

A Comparative Study of Data Hiding Techniques for Different Image Categories

Fazila Rafiq¹ and Er. Hem Priya²

¹M.Tech Scholar, Department of Electronics and Communication Engineering,
Rayat Bahra University, Punjab, India.

²Assistant Professor, Department of Electronics and Communication Engineering,
Rayat Bahra University, Punjab.

Abstract

The study focuses on enhancing the perceptual appearance of shortened pictures that contain concealed content within them. It proposes a two-phase data concealment approach that integrates natural visual abilities to achieve this enhancement. The context in which this study is conducted is in intelligent capitals, where the Internet of Things (IoT) plays a significant role in gathering various sources of visual data for enhanced administration. When transmitting data over a public network, safety concerns are crucial. To address this, the study introduces a unique information concealing procedure for picture decompression using Absolute Moment Block Truncation Codes (AMBTC). AMBTC is utilized as a means to improve bandwidth utilization while satisfying safety requirements. By employing AMBTC, the study aims to maintain the original moments of the image while reducing mean squared errors (MSE) more effectively than with Block Truncation Code (BTC). The study also highlights the importance of being able to restore the original picture after data concealment. However, the amount of recoverable knowledge may be reduced, or additional knowledge might be required for recovery from the stego picture (the image with concealed data) to maintain the ability to revert to the associated stego image. The approach known as Least Significant Bit (LSB) is mentioned, which involves altering the LSB of images to incorporate digital hidden information into the host picture. This technique does not require additional information for restoration and recovery, but it may not fully restore the stego picture to its original state. In summary, this study presents a two phase data concealment approach using AMBTC to enhance the perceptual appearance of shortened pictures containing concealed content. The ability to restore the original picture is emphasized, and the LSB approach is mentioned as a means of digital information concealment.

Keywords— *Absolute Moment Block Truncation Coding (AMBTC), Least Significant Bit, Two-Phase Data Concealment, Image Compression, Tampering chunks.*

1. Introduction

The following section discusses the difficulties created by the growing volume of digital multimedia data as well as the necessity for safe data transfer. It mentions that data can be encrypted using cryptography or concealed within other media, such as images, videos, and audio, to enhance confidentiality. Data hiding schemes are categorized into spatial, frequency, and compressed domains [1]. The study emphasizes the importance of content concealing strategies in the Internet of Things (IoT) and visual Internet of Things [2] to prevent theft or unauthorized distribution of private data. It mentions that reversible data hiding techniques allow for the restoration of the original image after concealment, which is useful in fields requiring high levels of detail [3]. However, reversible techniques may reduce the amount of content that can be concealed or require additional information for recovery [4, 5]. For irreversible data hiding, three popular methods are mentioned: exploiting modification directions, pixel value differencing, and concealing the least significant bit. The LSB technique replaces the least significant bit of pixels in the source image with encrypted information to create the stego image [6]. EMD and PVD techniques modify pixel values or variances to embed information while maintaining the presence of the stego picture. It also discusses picture information concealing, which aims to protect proprietary information and prevent misuse [7, 8]. Picture information concealing is often based on specific

image compression standards. Lossy and lossless compression methods are mentioned, with lossy compression (such as AMBTC) being more effective in reducing image size but losing some information. The use of AMBTC compression is highlighted due to its low computational resource requirements and satisfactory image quality. Several studies have focused on AMBTC-based data hiding techniques, including approaches that separate AMBTC chunks, hybrid secret hiding methods, and concealing approaches to minimize distortion [9-12]. Reversible data hiding and combination theory-based schemes for AMBTC compressed images are also mentioned. In short it discusses the challenges of handling large-scale data and the need for secure data transmission. It explores different data hiding techniques, including reversible and irreversible approaches, as well as the use of AMBTC compression for picture information concealing [13-16].

It also highlights various studies and their contributions to the field of data hiding in AMBTC compressed images.

2. Related work

This paper introduces a novel self-embedding technique based on a unique signature exchange mechanism. Its primary objective is to efficiently recover content by generating reference bits. To accomplish this, the authors propose an innovative approach called optimal iterative block truncation coding, which improves the optical standard of decrypted pictures compared to conventional BTC. The OIBTC description is used to encode reduction bits of the original image, employing a process that involves restoration stages and digital structures. Compression bits, encoded using OIBTC, are then interleaved through an inconsistent trading system to produce citation values, exploiting redundancy to aid in the recovery of damaged compression bits. Reference bits, along with newly generated reduction elements from intact sections, are employed to recover lost compressed bits. Leveraging OIBTC decoding and intra-block and inter-block correlations, the scheme effectively restores tampered image regions, outperforming existing methods in terms of alteration restoration efficiency. Comprehensive experiments validate the scheme's effectiveness, highlighting its superior performance, and demonstrate its potential applications in tampering recovery and image content restoration across various domains.

In this paper [9], the focus is on developing two specific Reversible Data Hiding (RDH) approaches tailored for images subjected to vector quantization compression. These proposed techniques are designed to work seamlessly with switching-tree coding and dynamic tree-coding scheme. Unlike existing VQ-ground RDH methods that may produce unauthorized codes as a result; this research emphasizes safeguarding the authenticity of the integrated VQ codes. To achieve this, the proposed approach employs a mechanism known as "database coding" and adopts a selective embedding technique, choosing a specific encoding method from several possibilities. This ensures that the resulting code remains valid and can be decoded back into the actual VQ index table using traditional STC/DTCS decoders. The study's findings demonstrate the viability of these proposed schemes, highlighting their advantages over previous RDH approaches. The first approach excels in embedding efficiency, enabling the concealment of larger volumes of data. Meanwhile, the second scheme achieves significant data embedding capacity while maintaining lower bit rates compared to most prior designs, striking a balance between efficiency and compression. Overall, these RDH schemes based on STC and DTCS generate legitimate codes, ensuring compatibility with standard decoders. They offer practical and efficient solutions for concealing data within VQ-compressed images while preserving code integrity, advancing the field of VQ-reduced image concealment.

This paper [21] introduces an innovative content concealment approach tailored specifically for AMBTC-reduced pictures. The suggested approach hinges on optimizing compression rates to strike a balance between payload capacity and minimal disruption to visual quality. The core concept involves categorizing elements within AMBTC-compressed images into two groups: "seamless" and "complex." For "seamless" elements, the method replaces the bitmap with hidden information for embedding while adjusting relative quantization levels to minimize distortion. This ensures that embedded data has minimal impact on the appearance of smooth blocks. For increased data capacity, quantization volume can be further manipulated to incorporate two extra bits without compromising quality. For "complex" blocks, the approach allows one data bit to be fixed without introducing deformation by switching quantization levels' contents and inverting data representation, capitalizing on the inherent complexity of these blocks. To maintain image quality, a dynamic suppress threshold

mechanism is employed, preventing disturbance at low capacity levels. This ensures image quality is preserved while achieving high payload capacity. Overall, this method aims to minimize block deformation while enabling high capacity, enhancing embedding efficiency, and providing an improved solution for information concealing in AMBTC-reduced pictures. Experimental results validate its superiority over related works, emphasizing enhanced embedded capability, reliability, and distortion control. By maximizing payload capacity while minimizing distortion, this method offers an efficient solution for content concealment in AMBTC-compressed images.

3. Experimental performance and debate

The suggested approach aims to validate photos that have undergone reduction using the Absolute Moment Block Truncation Code (AMBTC) and detect tampering chunks in the images. The approach involves dividing the images into units based on shared features, storing combined data for restoration, duplicating and jumbling the data, and inserting it in a pattern of uniform chunks. The LSBs of the quantization stages are utilized to identify codes with the lowest deformation. By aggregating untampered blocks with the same measure, manipulated chunks can be located. The study claims that this approach produces labeled images with clarity, detectability, and a good recovery outcome. In order to evaluate the efficacy of this approach, several evaluation metrics are mentioned, including:

3.1 Peak Signal to Noise Ratio:

PSNR is a measurement which is used to assess the quality of a data, such as an image or audio, by comparing it to the amount of interference or noise present in the signal. Greater PSNR values indicate best image quality.

The PSNR (in decibels) is calculated as follows:

$$\text{PSNR} = 10 \cdot \log_{10}(\text{MAX}_I^2 / \text{MSE})$$

$$= 20 \cdot \log_{10}(\text{MAX}_I / \sqrt{\text{MSE}})$$

$$= 20 \cdot \log_{10}(\text{MAX}_I) - 10 \log_{10}(\text{MSE})$$

MAX_I denotes the highest achievable pixel count.

3.2 Mean Squared Error:

The MSE is a commonly used metric for quantifying the difference within two images, such as an original image I and its imperfect estimate K . It measures the average squared distinction within the pixel values of corresponding pixels in the two images. A lower MSE indicates better reconstruction accuracy.

$$\text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} x_i \sum_{j=0}^{n-1} x_j [I(i, j) - K(i, j)]^2$$

3.3 Signal-to-Noise Ratio:

SNR is a commonly used parameter in technological and scientific fields to assess the quality and reliability of a signal in the presence of noise or interference. It measures the proportion of the power of the signal of interest to the power of the background or undesired noise.

$$\text{SNR} = \frac{P_{\text{signal}}}{P_{\text{noise}}}$$

Where P is average power.

3.4 SSIM (Structural Similarity Index):

SSIM is a widely used statistic for assessing the resemblance within two pictures. Greater SSIM values indicate superior resemblance.

The calculation of the Structural Similarity Index (SSIM) involves comparing two provided pictures and producing a value between -1 and +1. A value of +1 indicates that the pictures are very similar, while -1 suggests a high degree of dissimilarity. However, it is common to modify these values to fall within the range of [0, 1], where the extremes still carry the same significance. To obtain an SSIM value within the range [0, 1], a simple transformation can be applied.

The SSIM formula can be expressed as:

$$\text{SSIM}(x, y) = (2 * \mu_x * \mu_y + C1) * (2 * \sigma_{xy} + C2) / (\mu_x^2 + \mu_y^2 + C1) * (\sigma_x^2 + \sigma_y^2 + C2)$$

Where: x and y are the aperture of the reference and distorted pictures respectively.

μ_x and μ_y are the average values of x and y .

σ_x and σ_y are the standard deviations of x and y .

σ_{xy} is the cross-covariance of x and y .

$C1$ and $C2$ are constants to stabilize the division.

To calculate the overall SSIM value, you average the SSIM values of multiple windows or blocks across the entire image.

3.5 Capacity:

It indicates the quantity of hidden data which can be inserted in the images without significantly degrading the image quality. Higher capacity values indicate a larger amount of hidden data that can be stored. These metrics are often used in pictures processing and compression to assess the quality, precision, similarity, and capacity of reconstructed images. By calculating and comparing these metrics for the suggested approach and previously published approaches, the effectiveness and performance of the suggested approach can be evaluated.

4. Comparative Analysis

4.1 Horng et al's Data Hiding Method:

The suggested information concealment scheme for AMBTC pictures employs a multi-phase approach to maximize the capacity for embedding secret data while simultaneously preserving image quality. This method ensures secure data transmission within the framework of AMBTC compression. The three key phases in this scheme are as follows:

Phase 1 - QVD and LSB Substitution: This initial phase leverages the quantization levels inherent in AMBTC, known as L and H levels, to conceal secret data. The process combines Quotient Value Differencing with Least Significant Bit substitution techniques. QVD calculates the quotient difference between L and H levels, allowing for the determination of embedding capacity based on predefined ranges. Within these ranges, data is embedded by strategically adjusting the quotient values and substituting LSBs, achieving the delicate balance between data hiding and image quality preservation.

Phase 2 - Single Bit Embedding: In this stage, a solitary hidden bit is inserted per block. If the bit is '1', a clever manipulation is employed - the image's bit is reversed, and the quantification values are switched accordingly. In the case of a '0', the compression code remains unaltered. This single-bit embedding approach adds another layer of security and data capacity to the scheme.

Phase 3 - Bitmap Replacement: The final phase assesses the difference (dp) between the modified quantization levels and compares it to a predetermined threshold (dth). If dp is found to be less than dth , this signals an opportunity to replace the bitmap with secret data. Blocks characterized by very close quantization levels are considered suitable candidates for bitmap replacement, while those with more significant differences are considered non-embeddable.

This hybrid data hiding approach combines elements such as Quotient Value Differencing, Least Significant Bit substitution, quantification value switching, and bitmap substitution to maximize the capacity for embedding secret information within the compressed AMBTC images. Importantly, this is achieved while minimizing any potential degradation in image quality.

The extraction procedure mirrors the embedding process in reverse, utilizing the same threshold and knowledge of the data structure to accurately retrieve the hidden information. This scheme presents an effective and secure means of concealing data within AMBTC-compressed images, ideal for applications where data privacy and image quality are both paramount concerns.

4.2 Lee et al's Data Hiding Method:

This method introduces a novel information concealment scheme tailored for AMBTC and modified AMBTC reduced pictures. The approach involves segmenting grayscale images into non-overlapping blocks and utilizing the quantization levels within these blocks, along with a 2-bit bitmap, as the canvas for concealing confidential data. A standout feature of this technique is the introduction of a "turtle-shell matrix," a structured 2D hyper-cube framework that plays a pivotal role in the embedding process. Remarkably, each pixel within a block

becomes a carrier of 2 bits of secret information, and these pixel ethics are meticulously potray to specific positions within the turtle-shell matrix.

The embedding process unfolds through a sequence of three distinct stages:

Building the Turtle-Shell Matrix:The foundation of this method involves the creation of a sizeable 256x256 turtle-shell matrix, serving as a comprehensive representation of pairs of gray values. These turtle-shells intricately contain 8 numbers, each conforming to a predefined pattern of differences.

Embedding Hidden Information into Quantification Size: Here, the quantification size associated with every chunk is systematically mapped to corresponding positions within the turtle-shell matrix. Secret data, denoted as S1, are subtly incorporated into the quantization levels by skillfully adjusting them to align with specific positions in the matrix.

Threshold-Based Classification: This phase introduces an element of classification found on the complete distinctness in the middle of the newly adjusted quantification sets. A user-defined threshold parameter, TH, determines whether a block falls into the "smooth" or "complex" category. Smooth blocks, characterized by small differences, serve as candidates for concealing further secret data (S2) within their bitmaps, while complex blocks remain unaltered to preserve image fidelity.

The extraction procedure, which serves as the reverse operation of embedding, meticulously recovers secret data elements S1, S2, and S3 if present. This involves a comprehensive analysis of the sequence of quantification sets and the bitmap to meticulously extract the concealed information.

This innovative scheme impressively combines robust data storage capacity with commendable image quality preservation. Users are afforded the flexibility to fine-tune the threshold parameter to strike an optimal balance between data storage capacity and image quality, aligning with their specific requirements. Overall, this approach offers a robust and versatile solution for securely embedding data within AMBTC-compressed images.

4.3 Pei Chun Lai's Data Hiding Method:

The suggested hybrid AMBTC-based information concealment method combines AMBTC image compression with LSB (Least Significant Bit) substitution to enhance data embedding capacity while maintaining image quality. This method aims to leverage the characteristics of image content, particularly distinguishing between smooth and complex image blocks. It modifies the AMBTC compression process to embed an additional secret bit in each block. The process begins with dividing the image into $w \times w$ distinct chunks.

For every chunk, the mean pixel assess is computed, and pixels are categorized as either high or low relative to this mean. Smooth blocks exhibit a small and disparity within the arithmetic means of the two groups, while complex blocks have a larger difference. This difference (denoted as d) influences the number of hidden bits (n) which can be inserted. n -LSB substitutes are made to conceal n hidden bits in mean values while minimizing image distortion. A special encoding process ensures that a modified smooth block maintains good visual quality. If a block's difference is within a threshold (T_{hr}), it is considered smooth.

Additionally, an extra secret bit (s_j) is embedded in the compression code, expanding the data hiding capacity. Depending on s_j , the compression code is either left unchanged or modified. Finally, the compression code is received from transmitter.

On the receiver side, the secret information and the decompressed picture are extracted using an inverse process. The compression code is segmented, and secret bits are sequentially extracted until all data is recovered. The process accounts for the differences between smooth and complex blocks and reconstructs the decompressed image.

The proposed method enhances data hiding capacity within AMBTC compression, ensuring secure data transmission while preserving image quality. Decryption at the receiver end is performed with the appropriate key to obtain the original human-readable data. This method improves upon existing AMBTC-based data embedding techniques by combining the benefits of AMBTC compression and LSB substitution.

4.4 K. Anggriani Data Hiding Method:

This research endeavor delves into the formidable challenges stemming from the exponential growth of multimedia data in online environments. It seeks to provide a solution in the realm of compressed images, specifically focusing on the AMBTC framework. Given the paramount importance of information compression

for curbing data volume and transport costs, concealing data within this context becomes an intricate endeavor. The core objective of this proposed method is to strike a harmonious balance between embedding confidential information and preserving the natural visual integrity of the compressed images.

Unlike conventional data-hiding techniques that may necessitate alterations to multiple pixels, this innovative scheme adopts a more surgical approach. It strategically modifies just one pixel within each image block to effectively embed confidential data. The key aspiration here is to ensure that the modifications remain imperceptible to the human eye while accommodating a significant capacity for concealment.

The experimental outcomes of this study underscore the remarkable success of the proposed approach. It achieves an exceptional level of visibility, rendering the concealed information readily accessible to authorized recipients. Simultaneously, it boasts an extensive capacity for concealment, implying that the embedded data remains exceptionally well hidden within the image. This robust concealment makes it exceedingly challenging for unintended or malicious entities to detect or manipulate the covert information.

In summary, this research marks a significant advancement in the domain of content concealment within compressed images, particularly within the AMBTC framework. By adeptly balancing imperceptibility and concealment capacity, it contributes to the evolution of secure and efficient multimedia transmission and storage practices. This innovative approach holds promise for addressing the ever-growing demands of multimedia data management in the digital age.

4.5 Modified Data Hiding Method:

The proposed approach can be adapted to embed information into color images while maintaining data security within Absolute Moment Block Truncation Code (AMBTC) blocks. In this extended version, we'll elaborate on how to apply this method to color images.

In the first phase, which is applicable to color images, we break down the image into 4x4 pixel blocks as before. However, for colour pictures, every pixel mainly contains three colour medium: Red (R), Green (G), and Blue (B). Instead of calculating a single mean value as in grayscale images, we compute separate mean values for each color channel within each block (\bar{R} , \bar{G} , \bar{B}). For each channel, we compare the pixel's value to its respective mean. If the pixel's value in a particular channel is greater than the channel's mean, we replace it with '1'; otherwise, we replace it with '0'. This binary representation is stored separately for each color channel, creating the basis for our color AMBTC image.

The second phase for color images remains the same as for grayscale images. We calculate the high and low means for each color channel's binary data separately. This entails generating histograms for '1' and '0' values for each channel and computing the means of the high histogram values and low histogram values individually.

The critical step, which is consistent for color images as well, is to hide information in the least significant bit of each pixel to maintain image integrity while concealing information. Initially, the LSBs of each pixel in each color channel are cleared, ensuring there is no visible distortion in the image's appearance.

When recipients wish to bring out the hidden data from the color picture, they can securely retrieve the data by examining the LSB of each pixel in each color channel and reversing the process separately for each channel. This adapted two-phase approach ensures data security within the color AMBTC image while preserving the visual integrity of the original color image. It provides a method for securely embedding and extracting information in the context of color images, enhancing data transmission security.

5. Comparison table

Image	Metrics	Horng et al [19]	Lee et al [17]	Pei Chun Lai [20]	K.Anggriani [18]	Proposed
Airplane	PSNR	29.839	33.86	30.835	38.25	43.01
	Capacity	192827	81920	198999	195928	2881550.79
Baboon	PSNR	27.314	30.85	27.867	37.97	40.18

	Capacity	154156	81920	150139	104284	1212199.80
Boat	PSNR	24.675	31.74	30.072	36.27	39.58
	Capacity	296142	81920	159897	158440	2846309.60
Lena	PSNR	30.905	33.42	31.78	37.42	38.83
	Capacity	190667	81920	183257	201364	2874847.65
Peppers	PSNR	30.995	32.69	31.974	35.89	36.32
	Capacity	188080	81920	155958	197632	2783733.15
Average	PSNR	28.745	32.512	30.505	37.16	39.584
	Capacity	204374.4	81920	449650	171529.6	2519728.1

6. Conclusion

In the course of the analysis, the study discerns that the proposed modified technique distinctly outperforms other methodologies in the comparison. Notably, it exhibits a notably superior Peak Signal-to-Noise Ratio when juxtaposed with its counterparts. In the realm of picture refining, a higher PSNR value invariably signifies reduced distortion in the resultant image, which, in turn, translates to heightened image quality.

The pronouncedly elevated PSNR achieved by the proposed modified technique implicitly underscores its prowess in preserving intricate image details and upholding an elevated standard of privacy and security. The technique, by delivering an augmented PSNR, effectively conveys its capacity to maintain the integrity of visual information, thereby enhancing the confidentiality and safeguarding of sensitive data.

The research report unfolds a meticulous comparative analysis, pitting the proposed modified technique against other methodologies in the context of fortifying privacy and security. The empirical findings unambiguously accentuate the efficiency and effectiveness of the proposed modified technique in fulfilling its intended objectives. Crucially, the performance evaluation centers around the metric of PSNR, a widely acknowledged yardstick for appraising the fidelity of the output image concerning the original.

In essence, the proposed modified technique's conspicuous superiority, as illuminated by its exceptional PSNR outcomes, substantiates its prominence in the realm of image security and privacy enhancement. This substantiates its potential to serve as a robust and dependable tool for fortifying confidentiality and security in the handling of visual data. As a result, it emerges as a noteworthy contribution to the landscape of image processing and data protection, promising heightened efficacy and resilience in safeguarding sensitive information.

References

- [1] S. Q. Saleh, "Digital Image Steganalysis : Current Methodologies and Future Challenges," IEEE Access, vol. 10, no. August, pp. 92321–92336, 2022, doi: 10.1109/ACCESS.2022.3202905.
- [2] Liao, X.; Yu, Y.; Li, Z.; Qin, Z. A new payload partition strategy in color image steganography IEEE Trans. Circuits Syst. Video Technol. 2019.[Google Scholar] [Cross Ref]
- [3] Li, C.; Lin, D.; Lu, J.; Hao, F. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography IEEE Multimedia 2018, 25, 46–56. [Google Scholar] [Cross Ref]
- [4] Sharma, D.; Saxena, R.; Singh, N. Dual domain robust watermarking scheme using random DFRFT and least significant bit technique. Multimedia Tools Appl. 2017, 76, 3921– 3942. [Google Scholar] [Cross Ref]
- [5] Liu, Y.; Yang, C.; Sun, Q. Enhance embedding capacity of generalized exploiting modification directions in data hiding. IEEE Access 2017, 6, 5374–5378. [Google Scholar] [Cross Ref]
- [6] Shukla, A.; Singh, A.; Singh, B.; Kumar, A. A secure and high-capacity data-hiding method using compression, encryption and optimized pixel value differencing. IEEE Access 2018, 6, 51130–51139. [Google Scholar] [Cross Ref]

- [7] Qian, Z.; Zhou, H.; Zhang, X.; Zhang, W. Separable reversible data hiding in encrypted JPEG bit streams. *IEEE Trans. Dependable Secure Compute* 2018, 15, 1055–1067. [Google Scholar] [Cross Ref]
- [8] Qin, C.; Ji, P.; Chang, C.; Dong, J.; Sun, X. Non-uniform watermark sharing based on optimal iterative BTC for image tampering recovery. *IEEE Multimedia* 2018, 25, 36–48. [Google Scholar] [Cross Ref]
- [9] Rahmani, P.; Dastghaibiyfard, G. Two reversible data hiding schemes for VQ-compressed images based on index coding IET Image Process. 2018, 12, 1195–1203. [Google Scholar] [Cross Ref]
- [10] He, J.; Huang, S.; Tang, S.; Huang, J. JPEG image encryption with improved format compatibility and file size preservation. *IEEE Trans. Multimedia*. 2018, 20, 2645–2658. [Google Scholar] [Cross Ref]
- [11] Li, X.; Meng, X.; Yang, X.; Yin, Y.; Wang, Y.; Peng, X.; He, W.; Dong, G.; Chen, H. Multiple- image encryption based on compressive ghost imaging and coordinate sampling. *IEEE Photonics J.* 2016, 8, 3900511. [Google Scholar] [Cross Ref]
- [12] Ou, D.; Sun, W. High payload image steganography with minimum distortion based on absolute moment block truncation coding. *Multimedia Tools Appl.* 2015, 74, 9117–9139. [Google Scholar] [Cross Ref]
- [13] Qin, C.; Zhang, X. Effective reversible data hiding in encrypted image with privacy protection for image content. *J. Vis. Commun. Image Represent.* 2015, 31, 154–164. [Google Scholar] [Cross Ref]
- [14] Xiong, L.; Xu, Z.; Shi, Y. An integer wavelet transform based scheme for reversible data Hiding in encrypted images *Multidimensions Syst. Signal Process* 2018, 29, 1191–1202. [Google Scholar] [Cross Ref]
- [15] Huang, F.; Qu, X.; Kim, H.; Huang, J. Reversible data hiding in JPEG images. *IEEE Trans. Circuits Syst. Video Technol.* 2016, 26, 1610–1621. [Google Scholar] [Cross Ref]
- [16] Qian, Z.; Zhang, X. Reversible data hiding in encrypted images with distributed source Encoding. *IEEE Trans. Circuits Syst. Video Technol.* 2016, 26, 636–646. [Google Scholar] [Cross Ref]
- [17] C.-F. Lee, C -C Chang, and G. Li, “A Data Hiding Scheme Based on Turtle-shell for AMBTC Compressed Images,” *KSII Trans. Internet Inf. Syst.*, vol. 14, no. 6, pp. 2554–2575, 2020, doi: 10.3837/tiis.2020.06.013.
- [18] Anggriani, K.; Chiou, S.; Wu, N.; Hwang, M. “High Imperceptible Data Hiding Method for AMBTC Compressed Images Based on Combination Theory”, *Preprints.org* 2023, 2023040341. <https://doi.org/10.20944/preprints202304.0341.v1>.
- [19] J.-H. Horng, C.-C. Chang and G.-L. Li, “Steganography using quotient value differencing And LSB substitution for AMBTC compressed images,” *IEEE Access*, vol. 8, pp. 1
- [20] Pei-Chun Lai, Jau-Ji Shen, and Yung-Chen Chou, “High Embedding Capacity Data Hiding Technique Based on Hybrid AMBTC and LSB Substitutions,” *International Journal of Network Security*, Vol.25, No.2, PP.221-234, Mar. 2023 (DOI: 10.6633/IJNS.202303 25(2).05)
- [21] Hong, W.; Chen, T.; Yin, Z.; Luo, B.; Ma, Y. Data hiding in AMBTC images using quantization levelmodificationandperturbationtechnique. *MultimediaToolsAppl.* 2017, 76,3761–3782.[GoogleScholar][CrossRef]