IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 11 Issue 02, February 2023
ISSN (Online) 2348 – 7968 | Impact Factor – 6.72
www.ijiset.com

Image Steganography and Compression using DWT and DCT: A Review

Pooja Bisht[1], Er. Priyanka Jarial[2]

[1]M.Tech Scholar, Punjabi University, Punjab

[2]Department of Computer science & Engineering, Punjabi University, Punjab

ABSTRACT: Compression of data is a crucial element in information security because it eliminates all unnecessary information from data and makes compressed data safe and simple to use. Compressed data requires less storage room on devices and transfers over the internet more quickly. Both lossy and lossless data compression are the two kinds of compression methods that can be employed for compression. Steganography is a technique for concealing sensitive information in a cover media package. Images, text, videos, and music files can all be used as cover material. Image files are the most popular cover media for data concealing. Image steganography is the process of concealing information in picture files. Data compression techniques as well as picture steganography techniques have been researched in this work. In this study image steganography and lossy compression techniques such as discrete wavelet transform and discrete cosine transform have been discussed and it is found that wavelets are better than other compression algorithms in preserving image quality. Discrete wavelet transform is less exposed to invasion and distortion, while discrete cosine transform is better in most parameters and image steganography is the simplest approach to hide any message in the cover file. Combining compression and steganography techniques can offer two layers of protection for transmitting data over the internet.

KEYWORDS: Steganography, image steganography, LSB, Compression, lossy compression, DWT, DCT.

I. INTRODUCTION

In the contemporary digital era, there are many more options to transmit information. The increasing popularity of media has presented significant problems to security issues [9]. With the rising usage of the internet, data exchange has become an important tool, and data integrity has become a major issue in the area of communication. Data authentication and reliable techniques of controlling data integrity are in high demand. This is owing to the ease to which digital data may be tampered with [10]. There has been a complete shift in the methods and forms of communication, with digital media being the major medium of communication. Even in the workplace, individuals have migrated from paper memos to electronic messages for communication. Transfer of photographs and films has become possible thanks to infinite processing power and storage. Pictures and videos are the primary modes of communication. On the other hand, with all of these technical advancements comes the necessity to preserve the security, privacy, and the confidentiality of the information being exchanged. Information concealment strategies

may be effective in facilitating the secure transport of data [3]. The transfer of huge amounts of information from the monitoring area to central unit for processing is a difficult operation for the system, especially when connection bandwidth is restricted. The loss of vital data will result from a data overflowing in the single-board computer. Because our application's sampling frequency is fixed and the communication channel's capacity cannot be raised, the only method to minimize data overflow and loss is to use data compression techniques [13]. Perceptual transparency, hiding capability, and robustness are the primary criteria used to assess the performance of steganography strategies. Steganography hides hidden communications and their presence in an innocent bearer in a secure manner [1]. Images, videos, text, and music are just a few examples of digital material that steganography techniques can work with [3].

STEGANOGRAPHY

The majority of people now prefer to work with security data that is transmitted across networks from originator to recipient as a result of this evolution. The main goal of steganography is to safeguard important data during transmission between sender and recipient, including text, picture, video, and audio. It provides a security to protect letters by embedding them into digital means and making them opaque and unreadable to prying eyes [5]. Steganography, defined as secret writing, comes from the Greek word steganos, where stego means cover and grafia means writing [9]. Secret communications can be transmitted by concealing them in a picture or text so that only the sender and the recipient can read or see them [4]. Steganography is a technique for hiding the presence of the communication. It involves concealing sensitive data within a data source. It can be used in a wide range of fields, including medicine, internet shopping, defence, and many others [17]. The cover image is known as the stego-image, and steganography is a subset of information concealment, evolving at the rate of the Internet and other global networks [5]. It relies on a steganographic technique's capacity to preserve the message as secret as is realistically possible and, in addition, how much information can be concealed while still remaining large enough to be permitted [17].

Multiple cover file formats can be used to execute the steganography method. The cover file used during the embedding process is the primary factor used to determine the steganography kinds, and any media file type can be used as the cover file. Audio steganography is the practice of embedding hidden messages into digital audio files. The Human Auditory System is used to integrate data into a cover media file [16]. Image steganography is the art and technology of concealing sensitive information within a picture file [3]. It is used to insert hidden information and stop it from being used for hiding information [10]. Picture steganalysis is a way to decrypt and extract the image's hidden information, and is used to hide the presence of such data by enclosing the relevant information inside a cover image, creating a new picture that is essentially identical to the original [14]. Video steganography is a method of information concealment that uses high-definition digital video as distributed signals [17]. Video frames serve as the carrier source and the cover frame enables the originator to insert a

hidden message. Cover files in text format are used in text steganography techniques, and the hidden messages inserted in cover files are also primarily of text type. Text steganography embedding techniques are based on the amount of lines, empty spaces, and capital letters [16].

IMAGE STEGANOGRAPHY

The research community has shown a great deal of interest in image steganography, which has led to substantial improvements that are in line with the most current developments in digital media technologies. A secret picture can be concealed in clear sight inside of a cover image using image steganography. Image steganography is the art and science of hiding confidential data within a picture file. Picture Steganalysis, on the other hand, is a method of decrypting and extracting the image's secret information. Bob and Alice are inmates, and the prisoners' dilemma is linked to image steganography. They want to run away, but Eve is listening in on all of their conversations. Eve is wary of Alice and Bob, so she carefully examines all of their correspondence. In this situation, Bob and Alice should speak in a language that is only understood by them. It ought to appear like a typical communication to Eve [3]. Digital image steganography conceals the existence of all such information by enclosing the crucial data within a cover image, resulting in a new image that is nearly identical to the original [14].

For encoding information in a cover file, LSB insertion is a well-liked and frequently used method in steganography. With the LSB embedding method, data can be embedded in the LSB of the cover file so that it is invisible to the naked eye. The embedded content may vanish with even the smallest alterations to the media cover. It is quick and easy, but has some disadvantages such as the size of the secure communication, the cover media's encoding messes up the private message bits, and the embedded content may vanish with even the smallest alterations to the media cover [4]. To be more precise, LSB-based algorithms replace LSBs of pixels in cover picture with bits from the hidden message, maintaining the visual clarity of the image. This conceals the secret information that is encoded within the cover image [14]. The cover image utilizes its least significant bits to hold the most significant bits of the secret information image, as suggested by the method's name [6]. For example, the intensity of grayscale image is stored in the 8 bits per pixel, whereas a color image is stored in 24 bits per pixel.

Data encryption involves encrypting data in the LSB replacement, extracting the top four-bit layers of the secret image, and converting it to a steganographic image. Data decryption involves performing RGB to monochrome conversion using the original steganographed picture, and recovering the message picture through a bit shift procedure [15].

COMPRESSION

Data compression is a crucial component of information security. Data that has been compressed effectively is reliable, private, and simple to link. Lossy and lossless

compression coding methods are the two types [4]. Compacting involves eliminating all the unnecessary information from the picture, increasing the memory space needed without particularly distorting the image. Different methods can be used to calculate compression ratio, some are lossless, retaining the original data, while others are lossy, frequently losing the distinctive data during compression [4]. Image compression is required because of the quick expansion of digital content and the ensuing need for less storage and efficient picture transmission. It decreases both the total processing time and the storage needs. Because fewer bits are transmitted, the likelihood of transmission mistakes is decreased [6]. Despite advancements in storing and transfer technology, there is a greater demand for storage space and communication bandwidth than there is room for. Therefore, picture reduction has shown to be a useful method [7]. Image Compression (IC) is the process of reducing the size of a picture while maintaining the image's clarity [8]. By decreasing the size of data file using either lossy or lossless compression methods, data compression reduces the amount of data that needs to be saved and transmitted[13].

There are two types of picture compression: lossy and lossless. For natural pictures like photographs, there is a lack of accuracy when using lossy compression. Many lossy compression techniques exist including discrete cosine transform, wavelet transform, chroma subsampling, transform coding and fractals. Medical imagery, illustrations, and cartoons frequently use lossless compression.

Lossless encoding can be achieved using a variety of techniques, including run-length encoding, predictive coding, entropy encoding, Huffman coding, and LZW [2]. In lossless compression methods, the rebuilt picture is essentially the same as the original image. Lossless encoding benefits file delivery over the Internet because smaller files transfer more rapidly. Lossless image compression methods typically consider pictures as a group of pixels arranged in row-major order. A lossy encoding system may examine the color information for a variety of pixels and identify minute variations in the color values of the pixels that human eye or brain would not be able to discern. The highly graded bits are then removed from the system [7].

DISCRETE WAVELET TRANSFORM

Wavelet Transform (DWT) is a frequency domain technique that employs the Wavelet transform. The use of wavelets in the shape of a summary model is based on the fact that wavelet transform clearly separates high- and low reluctance information based on pixels. The mostly used basic wavelet transform technique is Haar wavelet [5]. The Discrete Wavelet Transform achieves great compression ratios with no discernible loss of image clarity. It preserves picture clarity by decreasing errors, which is the benefit of using the wavelet transform method (DWT) for compression techniques. The benefit of using DWT is that it includes Fourier Transforms, which provide time precision. It is used to record frequency and position information (in time). Wavelet has an uneven structure and is nothing more than a waveform with a mean value of zero. DWT is best adapted for picture compression and produces a limited representation of signal than all the other

compression techniques [2]. The cover media in this variety is split into four main sub-bands (LL, LH, HL, and HH). The primary characteristics of cover file are mostly in LL, and if a hidden message is included, it will not be obliterated by various compression [4]. The concealed message image is embedded in this technique by modifying the coefficients of wavelet of the picture used as cover for safely sending the secret image. The Discrete Wavelet Transformation ease is one of its main advantages [7]. The procedure used is a two dimensional, three level discrete wavelet transformation. It is a two-dimensional Wavelet Transformation as frequency sub-bands are divided into horizontal or vertical planes twice. Three level DWT provides superior picture analysis than one level and two level. The DWT technique divides the primary component frequency band into four distinct smaller bands defined as sub-bands. Sub-band LL includes both horizontal and vertical low pass filters. Sub-band LH includes Low pass as well as high pass filters that operates in horizontal and vertical sub-bands, respectively. Sub-band HL includes High pass as well as low pass filters that operates in vertical and horizontal sub-bands, respectively. Sub-band HH includes both horizontal and vertical high pass filter sub-band. When high pass filtration is combined with low pass filtering, HL and LH sub-bands are achieved, and the bulk of host image information is collected into LL image sub-band. This approach is less vulnerable to assaults and results in minimal image distortion [15].

DISCRETE COSINE TRANSFORM

A DCT sums cosine functions with different frequencies and magnitudes to describe the incoming data points. One and two-dimensional DCTs are the most common types. It is a typical compression technique. This is how JPEG works: 8x8 is the original block dimension. Second, the DCT technique is applied to each component in a top-to-bottom and left-to-right direction. Then, quantization is used to reduce data that is stored in the memory and data is kept precisely [7]. The DCT transformation is used to convert each picture fragment into a frequency domain [20]. Lossy compression algorithm, DCT is used to analysis picture feature traits. When using this method, the picture should be resized to 8x8 or 16x16 proportions first. Quantized discrete cosine transformation coefficients arrange for lightweight picture shaping for each sub-square DCT transition, last encodes, transmits and transmits after the change [21].

The Discrete cosine transform is used after RGB to YCbCr conversion phase. By thresholding the encoded DCT coefficients using the bisection technique, so the desired quality is guaranteed. The DCT coefficients are retrieved from the stored DCT block coefficients using two scan orders (vertical and zigzag). An index vector is created by the duration of zero-run sequence that came before a non-zero DCT coefficient after a scan order. The optimal scan is determined by the minimum number of the two maximum index vectors. The compact picture is created by encoding the non-zero Discrete cosine transform coefficients and also encoding the index vector for each block [23].

II. LITERATURE SURVEY

In [1], AlSabhany, A. A. and et al. provides a paper that is based on audio steganography and LSB substitution. This paper suggests a new category for audio steganography based on the key concept in embedding techniques. It focuses on how each approach is embedded and suggests a framework for describing and comprehending the most popular methods. The three basic criteria for steganography methods used to gauge how well they work are perceptual transparency, concealing power, and robustness. Audio steganography is a method of hiding messages within an audio cover file. To prevent attackers from deciphering a secret communication, cryptography transforms it into an unintelligible and unreadable format.

In [2], Mody, D. and et al. provides a paper that is based on the image compression and optimization. Image compression is a method used in multi-media services to improve image quality and size. Discrete Wavelet Transform coding methods are used in this research to optimize the compressed picture. Evolutionary algorithms are used to optimize the compressed picture, offering high ratios of compression with no discernible loss of image quality. Wavelets are superior than other compression algorithms, preserving picture quality by decreasing mistakes. The evolutionary algorithm produces superior optimization outcomes, and metrics such as PSNR, MSE, CR, and Entropy aid in determining which delivers the best outcomes.

In [3], Bouridane, A. and et al. provides a paper that is based on the Image steganography, deep learning, autoencoder, information hiding. Picture steganography can be used to conceal a hidden image within a cover image, but traditional techniques' concealment capacity is restricted. This research developed a light weight and deep convolutional autoencoder framework to embed a secret picture and extract the hidden data from the embedded image. Three datasets were used to assess the proposed method: COCO, CelebA, and ImageNet. The performance was measured using the test set's peak signal-to-noise ratio, concealing capacity, and imperceptibility scores. The experimental findings showed that the proposed technique outperforms previous deep learning picture steganography algorithms in terms of concealing capacity. It also has an advantage in terms of invisibility, since it may generate stego pictures that are quite identical to the input cover image.

In [4], Wahab, O. F. and et al. provides a paper that is based on the Cryptography, data compression, DWT, Huffman coding and steganography. Compression is an essential component of information security, as it generates data that is efficient, safe, and simple to link. There are two kinds of compression algorithms: lossy and lossless. This research proposed a hybrid data compression methodology that increases the input information to be encrypted using the RSA (Rivest-Shamir-Adleman) cryptographic method to improve security. The plain text is compressed using the Huffman coding technique, while the cover picture is reduced using Discrete wavelet transform DWT-based lossy compression to minimize the cover image's size. A mix of RSA, Huffman Coding, and DWT was used to encrypt a message and conceal it inside the cover picture, resulting in a condensed size

with high image quality. This system outperforms existing strategies in terms of visual quality and storage, as well as excellent security and reasonable durability against assaults.

In [5], Khodher, M. A. and et al. provides a paper that is based on the image and text steganography methods. Steganography is a branch of information concealment that is growing in popularity as the Internet and networks spread around the globe. It is used to secure significant data, such as text, picture, video, and audio, during transmission between sender and recipient. This article compares steganography methods between images and texts when concealing a hidden message in both words and images. The results reveal that the compression of image and text steganography is good and efficient while being unnoticed by attackers. The text is difficult to conceal secret messages, but the image is simple to hide secret messages since image small features cannot be seen with the naked eye.

In [6], Ahirwar, P. and et al. provides a paper that is based on the review of the image compression. Image compression is a hot issue for both commercial and military academics due to the rise of digital data and the demand for decreased storage and effective image transmission. Picture compression aims to reduce the amount of bits needed to represent an image digitally while preserving its perceived visual quality.

In [7], Kumar, R. and et al. provides a paper that is based on the analysis of different image compression techniques. With the growth of modern technology, more data is being transferred, requiring greater bandwidth. To limit the amount of bandwidth used, the picture should be compacted before transmission. Picture availability has grown due to technical advancements, but demands for storage space and communication bandwidth far outstrips available capacity. This review of several compression strategies assists in identifying positive aspects and selecting the appropriate compression method. Lossy compression outperforms lossless compression in terms of compression ratio.

In [8], Chaturvedi, S. and et al. provides a paper that is based on the image compression techniques. This document provides an overview of picture types and compression algorithms. An image, in its original form, carries a great amount of data, which necessitates not only a considerable amount of memory capacity for storage, but also problematic transmission across a restricted bandwidth channel. Image compression allows for larger file sizes that are practical, storable, and communicative. After analyzing all tactics, it was discovered that lossless compression approaches are far superior to lossy compression procedures. Compression ratio of lossy compression is high than lossless compression.

In [9], Tevaramani, S. S. and et al. provides a paper that is based on the image steganography. Steganography is a technique that allows for the safe transmission of data, using an audio, video, or picture designed to elicit no suspicion. This study uses cover and payload photos of various sizes and shapes, live webcam images, and prepared images of many other formats. The payload and cover pictures are subjected to the Haar

Discrete Wavelet Transform (DWT). Entropy, PSNR, and MSE are among the outcome metrics that are measured. Alpha is a scaled factor in the proposed study.

In [10], Shyla, M. K. and et al. provides a paper that is based on the image steganography using genetic algorithm. Steganography can replace encryption and watermarking for secure data exchange and data privacy. In this study, the carrier image is chosen in such a way that the payload/secret picture and the carrier image's least significant bits are matched with a higher degree of compatibility, and the concealing procedure causes insignificant changes in the resulting stego image based on evolutionary algorithm. The performance of the suggested method has improved by 30 to 40%. The process of choosing a good cover picture and concealing the secret information to increase imperceptibility is difficult, but genetic algorithms have enabled the exploration of an impossible job of selection from trillions and millions of alternatives. The findings reveal considerable improvements, which is evidenced by better performance.

In [11], Subramanian, N. and et al. provides a paper that is based on the review of image steganography. This paper examines and explains the various deep learning techniques used in the field of picture steganography. It includes a detailed overview of the technique, datasets used, experimental setups taken into consideration, and evaluation criteria. It also provides a table summarizing all the information. This work seeks to assist other researchers in understanding the present trends, difficulties, and potential directions for the future in this topic.

In [12], Ahsan, I. and et al. provides a paper that is based on the data encryption and image steganography. This project focuses on being familiar with the different kinds of steganography that are accessible. For pictures, image steganography is used, and the relevant information is also decrypted to get the message image. Using other video or image file to cover up information, such as text, photos, or audio files, is known as image steganography. The goal of the current study is to employ spatial domain approach to steganograph a picture with another image. Using MATLAB programmes, the photos are encrypted and decrypted. This project focuses on being familiar with the many kinds of steganography that are accessible.

In [13], Gopinath, A. and et al. provides a paper that is based on the data compression methods. Data compression is a very hard process for hardware to transmit large amounts of data from the observing area to the central system for further processing. To prevent data overflow and loss, data compression techniques are used to reduce the size of the information file using either lossless or lossy compression techniques. This study focuses on a thorough analysis of several lossless compression techniques using data files for each technique, comparing their performance to determine the optimum approach of compression for transmission and storage.

In [14], Gutub, A. and et al. provides a paper that is based on the cryptography and steganography. Digital picture steganography is used to hide the presence of private data by enclosing the relevant information behind a cover image, creating a new image that is

essentially identical to the original. This study examines the effectiveness and capability of discrete wavelet transform and least significant bit steganography methods for hiding numerous pictures under a single cover image. To provide informed comments, the effectiveness of these algorithms has been assessed in terms of the cover image's capacity, the data's imperceptibility, and security data concealing.

In [15], Yadahalli, S. S. and et al. provides a paper that is based on the image steganography using least significant bit and discrete wavelet transform techniques. Steganography is an important technique used in data protection to hide and protect sensitive information in sent data. This study explains steganography and demonstrates its application on various pictures using two distinct methods: the least significant bit approach and the discrete wavelet transform method. The effectiveness of the methods suggested in the study is shown by empirically acquired and compared efficiency values. The Discrete Wavelet Transform approach (DWT) is less vulnerable to assaults and results in less image distortion. Transform domain methods (like DWT) perform better in the majority of the parameters.

In [16], Jayapandiyan, J. R. and et al. provides a paper that is based on the image steganography, information hiding and secret text sharing. Text steganography has emerged as a dominating study subject in the sphere of information exchange, with several studies being undertaken to enhance this area. The quantity of secret message that may be kept in a particular cover picture is always crucial for any steganography approach used to convey the secret text. This research paper's enhanced Least Significant Bit embedding approach improves the quality of the cover picture by optimizing the secret message during the embedding phase. This approach offers high capacity embedding rate, greater security as a result of secret message pretreatment, and improved cover picture quality. Quantitative comparisons of the LSB method and the proposed eLSB algorithm show that the proposed technique preserves better picture quality while dealing with hidden words and images of different sizes.

In [17], Bansal, K. and et al. provides a paper that focuses on the survey of steganography using least significant bit embedding approach. Steganography is a technique for concealing sensitive data within a data source. It is used in a wide range of fields, including medicine, internet shopping, defense, and many more. It depends on a steganographic procedure's capacity to keep the message as secret as possible and the amount of data that can be concealed. This study provides an overview of the LSB methodology applied in this field and determined that various steganography methods work well for communicating secret data. New strategies are suggested to improve information security.

In [18], Mohammed, H. A. and et al. provides a paper that focuses on the LSB based steganography. Steganography is the study of enclosing confidential information within data to protect it from malicious actions. The McEliece cryptosystem, a public-key cryptosystem dependent on error-correcting codes, will be used to encrypt text using the goppa code. The ciphertext will be embedded as a steganography image using the LSB

approach, which helped to protect the information from attackers. PSNR values for all of the chosen photographs were above the threshold needed to determine the algorithm's effectiveness.

In [19], Majeed, M. A. and et al. provides a paper that is based on the review of text steganography techniques. This text discusses the use of steganography, a technique that allows the user to conceal a message within another message. It is typically not prioritized due to the challenges involved in locating unnecessary content in a text file. To solve this problem, the document must be altered in a way that makes the alteration invisible to the human eye but still computer-decipherable. Three categories of text steganography are described: linguistics, format-based techniques, and statistical and random creation. The existing approaches, difficulties, and future prospects in this subject are compiled in this study with the intention of assisting other researchers. This study demonstrates that expanding the format-based method's capacity factor and enhancing linguistic steganography's security are still hot subjects, yet scholars haven't given robustness much thought in this area.

In [20], Rahardi, M. and et al. provides a paper that focuses on watermarking technique using discrete cosine transform. This research proposes a blind and reliable image watermarking method known as BRIW-DCT for copyright prevention on color photographs. The DCT transformation converts each picture block into a frequency domain, and the watermark picture is integrated into the host picture. The experiment's findings showed that the watermarked picture attained a high PSNR value of 50.4489 decibel and higher SSIM value of 0.9991. The Arnold Transform can be used to strengthen BRIWDCT's resilience against image-tampering assaults in the future.

In [21], Dimililer, K. provide a paper that focuses on DCT based image compression and machine learning. This study uses machine learning algorithms to correlate the contents of medical images with their ratio of compression. The neural network's radial basis function technique may be used to categorize the ideal compression ratio for X-ray pictures while preserving good image quality. Two compression situations are used in the studies, with the proportion of training to testing taken into account. When proposed scenario 1 is taken into consideration, gradient boosting algorithm and support vector machines both achieve a higher recognition accuracy of 79.16%, while proposed scenario 2 achieves an accuracy rate of 89% as the best compression.

In [22], Mahfoudi, G. and et al. provides a paper that focuses on the Double Compression detection method based on DCT coefficient. In order to confirm the integrity of the video, we suggest a way to identify double video compression in this post. The H.264 compression, one of the required video codecs in WebRTC Demands for Comments, will be the subject of our attention. H.264 approximates the discrete cosine transformation using integers (DCT). To detect a double compression, we employ the DCT coefficients, which follow a laplacian distribution. We present a statistical hypothesis test for determining if video has been compacted twice, showing that detection was only achievable if the second quantization parameter was less than the first.

In [23], Messaoudi, A. provide a paper that focuses on DCT based compression. The suggested algorithm for lossy color still picture compression is based on DCT and uses a straightforward way to effectively encode the DCT coefficients. The Discrete cosine transform is used after RGB to YCbCr conversion phase to ensure the desired quality. The DCT coefficients are retrieved from the stored DCT block coefficients using two scan orders (vertical and zigzag). An index vector is created by the duration of zero-run sequence that came before a non-zero DCT coefficient after a scan order. The optimal scan is determined by the minimum number of the two maximum index vectors. The results demonstrate that the suggested algorithm gets excellent performance when compared to current methods.

III. CONCLUSION

In this paper we have studied the image steganography and lossy compression techniques. The techniques that have been studied in this paper are least significant bit and discrete wavelet transform and discrete cosine transform. Wavelets are better than the other compression algorithms that preserve image quality by decreasing errors. It is found that image steganography is the simple way to hide secret message in the cover media because small details cannot be seen with naked eye. Lossy compression techniques surpass lossless compression techniques in terms of compression ratio because compression ratio of these lossy compression techniques is higher than lossless compression techniques. Discrete wavelet transform approach is less exposed to the invasion and that leads to less distortion of the image and discrete cosine transform also performed well in the image compression. In the majority of parameters it is found that transform methods are better. With the use of combination of steganography and compression methods, we can achieve a double layer security in data transfer.

REFERENCES

[1] AlSabhany, A. A., Ali, A. H., Ridzuan, F., Azni, A. H., & Mokhtar, M. R. (2020). Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. computer science review, 38, 100316.

[2] Mody, D., Prajapati, P. H., Thaker, P., & Shah, N. (2020). Image Compression Using DWT and Optimization using Evolutionary Algorithm. Social Science Research Network.

[3] Subramanian, N., Cheheb, I., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). End-to-End Image Steganography Using Deep Convolutional Autoencoders. IEEE Access, 9, 135585-135593.

[4] Wahab, O. F., Khalaf, A. A., Hussein, A. I., & Hamed, H. F. (2021, 02). Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques. IEEE Access, PP.

[5] Khodher, M. A., & Khairi, T. W. (2020, July). Review: A comparison Steganography Between Texts and Images. Journal of Physics: Conference Series, 1591, 012024.

[6] Ahirwar, P., & Nagar, D. (2021, July). Image Compression: A Review. International Journal of Advanced Research in Science, Communication and Technology, 7(2).

[7] Kumar, R., & Garg, G. (2022, 02). Analysis of Different Image Compression Techniques: A Review.

[8] Chaturvedi, S., & Khatri, P. (2022, 02). Different Type of Image Compression using Various techniques, Highlighting Segmentation based image Compression. International Journal for Research in Applied Science & Engineering Technology, 10, 171-177.

[9] J, R., & Tevaramani, S. S. (2022). Image steganography performance analysis using discrete wavelet transform and alpha blending for secure communication. Global Transitions Proceedings, 3, 208-214.

[10] Shyla, M. K., Kumar, K. B., & Das, R. K. (2021). Image steganography using genetic algorithm for cover image selection and embedding. Soft Computing Letters.

[11] Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image Steganography: A Review of the Recent Advances. IEEE Access, 9, 23409-23423.

[12] Ahsan, I., & Bilal, M. (2022, 01). Image Steganography with GUI in Malab.

[13] Gopinath, A., & M, R. (2020). Comparison of Lossless Data Compression Techniques. Proceedings of the Fifth International Conference on Inventive Computation Technologies , (pp. 628-633).

[14] Gutub, A., & Al-Shaarani, F. (2020, 02). Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons. Arabian Journal for Science and Engineering, 2631-2644.

[15] Yadahalli, S. S., Rege, S., & Sonkusare, R. (2020). Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques. Proceedings of the Fifth International Conference on Communication and Electronics Systems, (pp. 1325-1330).

[16] Jayapandiyan, J. R., C, K., & K, S. (2020). Enhanced Least Significant Bit Replacement Algorithm in spatial domain of Steganography using character sequence optimization. IEEE Access, 8, 136537-136545.

[17] Bansal, K., Agrawal, A., & Bansal, N. (2020). A Survey on Steganography using Least Significant bit (LSB) Embedding Approach . Proceedings of the Fourth International Conference on Trends in Electronics and Informatics, (pp. 64-69).

[18] Mohammed, H. A., & Al Saffar, N. F. (2021). LSB based image steganography using McEliece cryptosystem. Materials Today: Proceedings.

[19] Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A Review on Text Steganography Techniques. Mathematics, 9.

[20] Rahardi, M., Abdulloh, F. F., & Putra, W. S. (2022). A Blind Robust Image Watermarking on Selected DCT Coefficients for Copyright Protection. International Journal of Advanced Computer Science and Applications, 13.

[21] Dimililer, K. (2021). DCT-based medical image compression using machine learning. Signal, Image and Video Processing, 16, 55-62.

[22] Mahfoudi, G., Retraint, F., Morain- Nicolier, F., & Pic, M. M. (2022). Statistical H.264 Double Compression Detection Method Based on DCT Coefficients. IEEE Access, 10, 4271-4283.

[23] Messaoudi, A. (2022). DCT-based compression algorithm using reduced adaptive block scanning for color image**.** 19th International Multi- Conference on Systems, Signals and Devices, (pp. 1951-1955).