Digital Image Steganography: An Overview

Article *in* Insurance Mathematics and Economics · April 2024

DOI: 10.15680/IJIRCCE.2024.1204003

CITATIONS
0

READS
78

2 authors:

Onyedinma Ebele Gr
Nnamdi Azikiwe University, Awka
15 PUBLICATIONS **23** CITATIONS
SEE PROFILE

Ikechukwu Onyenwe
Nnamdi Azikiwe University, Awka
49 PUBLICATIONS **164** CITATIONS
SEE PROFILE

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204003 |

Digital Image Steganography: An Overview

[1]Onyedinma, E.G., [2]Onyenwe, I.E.

[1, 2] Department of Computer Science, Nnamdi Azikiwe University, Awka Anambra State, Nigeria

ABSTRACT: With the advent of the internet, there have been ease of data transmission as well increase in security challlenges. One approach to maintaing data integrity and confidentiality is by the use of steganography. Steganography is the art of concealing the existence of seceret information without arousing suspicion. There are different types of steganography :text, audio, image and video. However, image steganography is the most commonly used for data transmission due to its high rate of imperceptibility and robust security . This work provides general overview of image steganography techniques. Background of steganography, its applications and performance evaluation parameters are equally presented.

I. INTRODUCTION

Steganography was derived from Greek word "Stego" which means "Covered" and "Graphia" which means "writing". Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia when Greece ruler named Histiaeus used to tonsure the head of his most trusted servants and tattooed the scalps with secret message and waited for the hair to grow. The servant used to travel between the borders without carrying anything contentious freely. At the reception end his head would be tonsured again and the message will be conveyed. Similarly, during the World War II, the Germans invented the use of microdots. Image containing great details were scaled down to the size of microdots.[21]. The German usage of secret sharing is regarded as the recent evolution of Steganography. Today, with the advent of computers and internet, steganography has assumed digital dimension : evolving and adapting with these technological trends. Steganography is the art and science of communicating in such a way that it hides the existence of the communication[23]. It is a method of hiding a secret message within an innocuous host medium so that the resulting medium appears to be unaffected by the inserted secret message. The aim is to make it difficult or impossible to distinguish between an original medium and a medium modified by the insertion of a secret message.

With the advancement in technology, data can be transmitted over the internet from one party to another. Sensitive information like banking transactions, credit card information and confidential data can also be shared through the same channel. Unfortunately, privacy and data security cannot be guaranteed without proper security measures in place. Malicious threats, eavesdropping and other subversive activities have become common with transimitted data resulting in breach of the privacy, data integrity and security of the data being transmitted [24] . Consequently, different techniques have been adopted among which is steganography to secure data along the communication channel. Steganography has emerged as a powerful tool to protect and secure the transmitted data by hiding sensitive information within an ordinary, non-secret file or message so that it will not be detected. It thus hides the existence of information by embedding information in undistinguished media contents that are unattractive to the attacker. The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection. Steganography does not change the structure of the secret message, rather it hides inside the media so that the change is not visible [24, 25]. The folowing are components of steganography:

- *cover(carrier):* which is the object or item (image, audio, text, video) where secret information will be hidden,
- *Embedding algorithm* : an algrithm that decides how to hide the information
- Extraction Algorithm: an algrithm that will be used to extract the hidden information
- Message: text, a secret image, an audio, ciphertext or video that is going to be transmitted securely.
- Stego *key* : In the time of encoding and decoding , key is used to randomize the placement of the data
- Stego object: cover object that has embedded information

A sender embeds informaton in a cover object using an embedding algorithm to obtain a stego object which is transmitted over a communication channel. At the receiving end, the process is reversed to retrieve the message.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204003 |

Types of steganography

There are different forms of steganography depending on the type of cover media adopted in embedding the secret data. These forms include: Text Steganography, Video Steganography, Audio Steganography, Network Steganography, E-mail Steganography and Image Steganography. Generally, all digital mediums, signals, or files can be used in steganography process as cover media, but some formats are more suitable than others depending on the level of redundancy. Text steganography is believed to be the hardest type of steganography because of the low degree of redundancy in text as compared to image, audio or video. These steganography techniques utilize natural limitations in human auditory and visual perceptions to minimize the difference between the cover medium and the stego medium. steganography techniques that use image or video as a cover depend on the limited human visual system while those that use audio file as a cover exploit human auditory system.

Text steganography

Text steganography imainly deals with concealing Text in Text Files and in Binary Files. This is done by changing the format of the existing text, altering the words in a text, producing random character sequences, or using context-free grammars (CFG) in order to create readable texts [26]. In text steganography, there is no redundant information as obtainable in other forms of steganography; hence it is assumed the trickiest. Its structre is identical with the secrete message while in other structures such as audio, the structure differs from the secrete message. Thus, information can be hidden by altering the structure such that the changes made will not be noticeable in the the resultant output[3][4].

Video steganography

Video can be considered as combination of audio and collection of still images which moves in constant time sequence.Video steganography is therfore a technique which hides message in a video and conceals the fact of its transmission. This technique is getting popular as a cover object due to its high embedding payload as well as providing perpetual redundancy[7]. In addition, due to availability of large number of frames, secret data can be easily disguised inside a video. The secrete message can be in any media form such as text, image, audio, video and binary file while the cover video can be in a raw or compressed format. Compressed videos have less storage space compared to raw videos. Embedding of the secret information is done during or after the compression of the video.

Audio steganography

Audio steganography is a technique that hides information within an audio signal. The information is transmitted by modifying the audio signal in an imperceptible manner[8]. Audio based steganography has more potential to conceal information because audio files are larger than other cover media and small change in amplitude can store huge amount of information[9]. More so, digital audio signals possess higher redundancy and high data transmission rate that make them suitable for use as covers.

Image steganography

Image Steganography refers to the process of hiding data within an image file. The hidden data can include text, images, audio, or any other form of binary information. The aim is to conceal information within digital images without altering their visual appearance. Pixel intensities are the key to data concealment in image steganography. Thus, it serves as a clandestine communication method, providing a means to transmit sensitive information without arousing the suspicion of adversaries or unauthorized individuals and as well offers an additional layer of security and confidentiality in digital communication. There are two broad classifications of steganography techniques based on the operational domains. These include: frequency domain and spatial domain. In the spatial domain, the secret message is inserted into the pixels of the carrier image, whereas in the frequency domain the pixels are transformed into coefficients, and the secret message is inserted in these coefficients [9].

Frequency domain techniques

Techniques, such as Discrete Cosine Transform (DCT) or Discrete Fourier Transform (DFT), manipulate the frequency domain representation of an image to embed secret data. This allows for the concealment of information within the frequency components of an image The message is inserted into the transformed coefficients of the image, which has the effect of bringing more robustness against attacks. Frequency steganography is an essential technique for concealing secret information: nowadays most steganography systems operate in the frequency domain. The frequency steganography will thus make it possible to hide the information in areas of the image less sensitive to compression, cropping and various image processing. Some of frequency domain techniques include:

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204003 |

- **Spread Spectrum Technique**

Spreads data over a wide range of frequencies, used in audio and video steganography to avoid detection by blending in with background noise. Direct Sequence Spread Spectrum (DSSS) as well as Frequency Hopping Spread Spectrum (FHSS) are the two primary subcategories, with FHSS being even more difficult to identify.

- **Randomized Embedding Technique**

Uses randomization to hide secret data in images, making detection difficult with algorithms like the F5 algorithm that uses frequency domain analysis and randomness. It shuffles the position of each bit within an image, creating a modified version of the original image that contains hidden information. It is useful in various applications, including forensic investigations.

Spatial domain techniques

Spatial domain techniques involves direct modifications on the pixel values. Spatial domain techniques involve modifying the pixel values directly to embed secret data. These techniques include modifying pixel intensities, color values, or rearranging pixels based on a predefined pattern[10]. Spatial domain techniques include:

- **Pixel Value Differencing (PVD) Technique**

This technique Identifies and modifies pixels with small value differences to encode information in both grayscale and color images. It requires precise changes to pixel values. However, using it on highly compressed or low-quality images may result in artifacts or distortions resulting in revealing the presence of hidden data.

- **Palette Based Steganography**

The Palette based steganography is proposed in [**11**] to utilize the palette-based images as cover images. Image formats such as TIFF, PNG and GIF are appropriate for such a technique. In palette-based steganography, the colour that has a similar parity of a secret bit within a palette is used for the embedding procedure. The major advantage of the palette-based steganography is that the entire distortion within the stego-image is seen to be smaller in comparison with other related spatial techniques. On the other hand, the major drawback of this technique refers to the demand of particular images, which have lossless compression formats.

- **LSB (Least Significant Bit) substitution:**

The LSB technique is one of the simplest and most common techniques. It consists of hiding a secret message in the least significant bits of the pixels of the image so that the distortions brought by the insertion process remain non-perceptible. The reason is that for the human eye, variations in the value of the LSB are almost imperceptible. The insertion of secret message bits may be done sequentially or pseudo randomly[**10**].

II. RELATED LITERATURE

Many researchers have proposed different steganographic techniques as a way of enhancing data security over open channel. In the work of [1] Pixel pixel-value differencing for image steganography was proposed. This method embeds secret message into a gray-value cover image by first partitioning the cover image into non-overlapping blocks of two consecutive pixels. A difference value is then calculated from the values of the two pixels in each block. All possible difference values are classified into a number of ranges. The selection of the range intervals is based on the characteristics of human visions sensitivity to gray value variations from smoothness to contrast. The difference value then is replaced by a new value to embed the value of a sub-stream of the secret message. Again, the number of bits which can be embedded in a pixel pair is decided by the width of the range that the difference value belongs to. The embedded secret message can be extracted from the resulting stego-image without referencing the original cover image. This method provides an easy way to produce a more imperceptible result than those yielded by simple least-significant-bit replacement methods.

[2] proposed the use of a secret data modification based high capacity image steganography technique. In their work, the least significant bit (LSB) replacement steganography was used to embed the secret data after rearranging and modifying the message by genetic algorithm(GA). The GA used flexible chromosone to interprete the chromosone value in different ways. This method produced a high visual quality image of the stego images was produced thereafter.

An improved image steganography technique in which data is embedded in the edge pixels of the carrier image was proposed by [3]. The technique used different types of edge detection filters like Prewitt, Sobel, Laplacian and Canny in an existing image steganography using edge based data hiding in DCT domain algorithm. An intruder has less suspicion about the existence of data bits in edges, because edge pixels appear to be different than their neighbours and thus ensures better security. Results of the system was improved visual quality as well reduction of image size.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204003 |

A new hybrid method called compressed encrypted data embedding (CEDE) was proposed in [4]. In CEDE, the secret information is first compressed with Lempel Ziv Welch (LZW) compression algorithm. Then, the compressed secret information is encrypted using the Advanced Encryption Standard (AES) symmetric block cipher. In the steganographic technique, the compressed and encrypted secret data bits are divided into pairs of two bits and pixels of the cover image are also arranged in four pairs. The four pairs of secret data are compared with the respective four pairs of each cover pixel which leads to sixteen possibilities of matching in between secret data pairs and pairs of cover pixels. The least significant bits (LSBs) of current and imminent pixels are then modified according to the matching case number. Accordingly, the proposed technique provides double-folded security and the results show that stego image carries a high capacity of secret data with adequate peak signal to noise ratio (PSNR) and lower mean square error (MSE).

in [5] , deep learning modules using the Adam algorithm and LSB were used to train the model that hides and reveals the network. Here, the encoder neural network determines where and how to place the message, dispersing it throughout the bits of the cover image. The decoder network on the receiving side, which is simultaneously trained with the encoder, reveals the secret image. This method produces minimal distortion to the secret message. Thus, preserving its integrity. Also, the network is only trained once, irrespective of different container images and secret messages given as inputs. Thus, this work has wide and secure applications in many fields.

A hybrid data compression algorithm was used to increase the amount of input data to be encrypted by RSA cryptography for both lossy and lossless data in [6]. The plain text is compressed by the Huffman coding algorithm while the cover image is compressed by Discrete wavelet transform DWT before embedding the encrypted data using the least significant bit LSB . The method reduced the physical space on the various storage media as well as the time of sending data over the Internet while maintaining data integrity.

The work of [7]proposed a roust steganographic technique based on Multi-Level Encryption (MLE), an achromatic component of an image, and Huffman LSB. Huffman coding scheme was used to encrypt the secret message. The secret message is then embeded by utilizing the I-plane of the HSI (Hue Saturation Intensity) variety model for the cover image rather than the RGB model.

[8] proposed an image steganographic technique based on Integer Wavelet Transform (IWT). The tehnique works by transforming the cover image using IWT to suppress the secret message into the high frequency bands HH, LH, and HL of the cover image. The coefficients of these bands are labelled into six categories according to their most significant bits (MSBs). All coefficients from different bands which belong to the same category are collected. The embedding process starts from the highest category and continues to the next category by controlling the number of coefficients to match the size of the secret message.

Indicator-based Pixel-Value Differencing Steganography methods (IPVDS) utilized in two ways was proposed in [9]. The technique derived from the PVDS method depends on an Indicator pixel (IP) to extract the secret data correctly. The study applied Genetic Algorithm (GA) approach to rearrange and modify the order of the image pixels corresponding to the secret message before embedding it. In the first proposed technique GA-IPVD, GA concentrates on the imperceptibility of embedded data and maximizes the quality of the stego-image according to the given secret data while in the second proposal GA-IPVDM. , the GA maximizes the capacity of embedded data while maintaining an acceptable amount of stego-image quality. These techniques address steganography as an optimization problem and seek to determine the optimal order of the pixels that enhance the matching between the cover image and stego-image to reduce distortion despite high embedded capacity. Comparing the proposed methods to standard techniques demonstrated that the proposed methods yielded superior results. In addition, they satisfy high PSNR values with lower modification rates due to the use of GA. Furthermore, the proposed GA-IPVD and GA-IPVDM techniques successfully resist the PDH and RS analyses and avoid BI problems, the results show that the proposed systems offer excellent anti-steganalysis ability against different stego-attacks.

In [10], a data hiding approach based on the flipping approach that reduces variability and provides less time complexity was proposed. In this method, firstly, data hiding is performed using the k-bit LSB method in the cover image to obtain stego image. The absolute difference between the cover and stego image is thereafter determined and compared with the threshold value. If the absolute difference is higher than the threshold value, then the adjacent bit of the k-bit LSB method is flipped. Results show that this process reduces the variability because flipping the adjacent bit will make the pixel value of the stego image closer to the cover image. More so, good visual quality, less time complexity than Genetic and Bayesian Optimization algorithms as well as the existing flip method were obtained.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204003 |

[11] proposed a secure method for hiding secret messages in an image based on an enhanced standard Least Significant Bit (LSB). However, before embedding using the LSB, the secret message's size is reduced by compression using the Huffman algorithm, followed by two operations: Boolean operation Exclusive-NOR (XNOR) operation and the Fibonacci algorithm when selecting pixels to embed the secret message. As a result of these processes, a stego-image is created with two secret keys. This technique resulted in higher PSNR against standard images with higher Peak Signal-to-Noise Ratio (PSNR) values as well as increased level of security and imperceptibility.

A steganographic technique based on Golden Ratio and Non-Subsampled Contourlet Transform (GRNSCT) model was proposed in [12]. This technique provides both high embedding capacity as well as the confidentiality of the embedded images. The high embedding capacity was achieved using a combination of mosaic process and two level NSCT (Non-Subsampled Contourlet Transform), while confidentiality was attained as a result of double layer encryption based on shuffling method of a deck of cards. The experimental results showed that the proposed multi-image steganography technique achieved better embedding capacity with PSNR up to 42.38 dB.

In the study[13], image steganography using least significant bit and secret map techniques was proposed. This works by applying 3D chaotic maps, namely, 3D Chebyshev and 3D logistic maps on the cover image before embedding the secret message therin in order to obtain high security. This technique is based on the concept of performing random insertion and selecting a pixel from a host image. Results show that the proposed algorithm is efficient in hiding secret data and preserving the good visual quality of stego image. In addition, it is resistant to different attacks, such as differential and statistical attacks, and yields good results in terms of key sensitivity, hiding capacity, quality index, MSE, PSNR and image fidelity

Proposal made in [14] utilizes a Generative Adversarial Network (GAN) to improve the ability of a spatial domain steganalysis method and to insert secret information with minimal image alteration. Through a training process, the GAN learns how to adapt an image to later introduce a message using the Least Significant Bit steganography algorithm. The results evidence that the approach is successful at avoiding detection by a state-of-the-art Deep Learning steganalysis architecture.

[15] Proposed pixel-based adaptive directional pixel value differencing (P-ADPVD) method. The original pixel value differencing (PVD) uses only one embedding direction for all pixels of the cover image, whereas the content of the digital images has different edge direction for each pixel. Thus, they proposed P-ADPVD method based on a pixel-of-interest (POI) to hide secret data bits in the dominant edge direction for each pixel. Histogram of oriented gradient (HOG) algorithm was then employed to find the dominant edge direction for each block of the POIs using gradient magnitude and angle information calculated from the cover image and determined by a threshold value. Results show significant improvement on the quality and security of the stego-images without sacrificing the embedding capacity. More so, the P-ADPVD method provides better visual quality of the stegoimage compared with other adaptive and nonadaptive PVD-based methods.

A novel hybrid algorithm was proposed in [16]. The technique works by carefully manipulating higher frequency coefficient of Discrete Cosine Transform (DCT) to maintain the perceptual quality of the image followed by embedding secret bits in the controlled DCT coefficients using random locations identified by deterministic Coupled Chaotic Map (CCM). Result of the study demonstrate that the proposed technique has excellent stego-image quality while keeping zero Bit Error Rate at maximum embedding capacity (EC). The proposed method has capability to withstand against malicious users as well as outperforms existing steganography techniques in terms of EC, and Peak Signal to Noise Ratio.

In [17], a grouping of wavelet domain & Salp Swarm based Optimization Algorithm (SSOA) was proposed. Initially, the integer discrete wavelet transform is utilized to process the cover image and DWT to extract the hidden image accurately. Furthermore, an edge localization process was adopted to localize the edge region of detail bands efficiently, by the use of SSO Algorithm. To enhance the quality of the stego pictures, a deep enhanced stacked auto encoder (DESAE) was also utilized. The technique achieved good image quality, high security and increase in the payload capacity of the existing methods, which confirms the superiority of the proposed method compared to previous related techniques.

An advanced DT-CWT based image steganographic approach was presented in [18] to embed secret data over appropriate coefficient planes of the cover image. Payload capacity is boosted while reducing the embedding error

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204003 |

using super-pixeling and intensity mapping in the preprocessing stage of the secret image. A template matching based embedding location detection is used to reduce the embedding error by making use of the similarity between secret data and DT-CWT planes. Further, a machine learning classifier is employed for selecting the best cover-coefficient planes. Cover and stego-image difference is minimized to the barest. Again, an automatic geometric correction stage is also proposed to defend against geometric attacks. Results show that the secret data is secured high payload capacities achieved.

In [19], a new steganography technique based on remainder replacement (RR), adaptive quotient value differencing (AQVD), and quotient value correlation (QVC) was proposed. This works by performing embedding and extraction operation on 3-by-3 disjoint pixel blocks to produce new blocks : (i) the remainder block and (ii) the quotient block. Each remainder in 3-by-3 remainder block is decimal equivalent of two binary bits, so it is substituted by decimal equivalent of two secret bits. Each quotient in 3-by-3 quotient block is decimal equivalent of six binary bits. The AQVD procedure is used to conceal data in four corner quotients of the quotient block. In three quotients of the middle row of the 3-by-3 quotient block, QVC embedding procedure is applied to hide the secret bits. The average hiding capacity is 3.21 bits per byte and the average peak signal-to-noise ratio is 35.27dB. Furthermore, regular-singular and pixel difference histogram attacks could not detect this technique.

Combination of Diffie-Hellman Key Exchange with a modified Collatz Conjecture to generate unique random numbers was proposed in [20]. The generated random numbers are used to identify the unique pixel locations where the secret message will be embedded using LSB. Results show that the employed method generates highly imperceptible and resistant to statistical attack stego-images.

III. APPLICATIONS OF IMAGE STEGANOGRAPHY

There are numerous application areas where steganography can be employed. Some of these are:

- **Protecting Confidential Information** − Image Steganography is used to hide sensitive data, such as passwords and PINs, from unauthorized access.
- **Preventing Cyber Attacks** − By hiding data within images, Image Steganography makes it difficult for cybercriminals to detect sensitive information.
- **Enhanced Security in Online Communications** − Image Steganography provides an extra layer of security by providing a shield over an encrypted message.
- **Law Enforcement** − Digital forensics units employ Image Steganography techniques to extract hidden information from images during investigations.
- **Covert communication:** Image steganography finds applications in covert communication where parties need to exchange sensitive information discreetly. This includes intelligence agencies, law enforcement, and whistleblowers who require secure channels for sharing classified or confidential data.
- **Digital watermarking:** Steganography techniques can be employed for digital watermarking to embed copyright information, ownership details, or authentication codes within images. This allows for tracking and protecting intellectual property rights.
- **Information hiding in multimedia:** Image steganography can be extended to other forms of multimedia, including audio and video, allowing for the concealment of information within these media formats. This can be used for copyright protection, digital rights management, or covert messaging.
- **Steganalysis and forensics:** Image steganalysis focuses on detecting the presence of hidden information within images. Forensic investigators can employ steganalysis techniques to identify potential steganographic content, aiding in digital investigations.

IV. EVALUATION CRITERIA FOR IMAGE STEGANOGRAPHIC TECHNIQUES

The performance of a steganography technique can be rated by three parameters; hiding capacity, distortion measure and security.

- **Hiding capacity**: the hiding capacity means the maximum amount of information that can be hidden in an image. It can also be represented as the number of bits per pixel. The higher the hiding capacity the better the steganography technique.
- **Distortion**: stego-images should be imperceptible. This means the distortion should not be noticeable. The distortion is measured by using various metrics like mean square error, root mean square error, PSNR, quality

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204003 |

index, correlation, structural similarity index and compression speed. Each of these metrics can be represented mathematically[28, 29].

- **Security**: A steganographic technique is said to be secured if it is resistant to various steganalytic attacks. This can be determined by testing the steganography technique with the steganalysis schemes like pixel difference histogram analysis, RS analysis among others. Security Analysis. A LSB substitution based technique can be tested by RS analysis and a PVD based technique can be tested by pixel difference histogram analysis[28].

V. SUMMARY AND CONCLUSION

An overview of image steganography techniques were presented. These techniques are basically classified into spatial and frequency domains. Spatial domain techniques involve modifying the pixel values directly to embed secret data while the frequency domain techniques, such as Discrete Cosine Transform (DCT) or Discrete Fourier Transform (DFT), manipulate the frequency domain representation of an image to embed secret data. The origin of steganography, detailed review , applications were also discussed.

REFERENCES

1. Da-Chun W. , Wen-Hsiang T. A steganographic method for images by pixel-value differencing. Pattern Recognition Letters 24 (2003) 1613–1626
2. Pratik D. , Rajankumar S. (2021). Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure. Engineering Science and Technology, an International Journal (JESTECH)
3. Nadish A. , Arvind S.(2020). An improved image steganography technique using edge based data hiding in DCT domain. https://doi.org/10.1080/09720502.2020.1731949
4. Hamza A., Shehzad D., Sarfraz M. ,Habib U. Shafi N.(2021).Novel Secure Hybrid Image Steganography Technique Based on Pattern Matching KSII Transactions on Internet and Information Systems (TIIS) Volume 15 Issue 3 Pages.1051-1077. 1976-7277(pISSN) 1976-7277(eISSN) https://doi.org/10.3837/tiis.2021.03.013.
5. ijay K., Saloni L., Aniket N. (2020). Steganography Techniques Using Convolutional Neural Networks. International Information and Engineering Technology Association: Review of Computer Engineering Studies Vol. 7, No. 3, September, 2020, pp. 66-73.https://doi.org/10.18280/rces.070304
6. O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques," in IEEE Access, vol. 9, pp. 31805-31815, 2021, doi: 10.1109/ACCESS.2021.3060317.
7. Rahman, S., Uddin, J., Hussain, H. et al(2023). A Huffman code LSB based image steganography technique using multi-level encryption and achromatic component of an image. Sci Rep 13, 14183 (2023). https://doi.org/10.1038/s41598-023-41303-1
8. Nisreen I. and Enas M.(2022). Image Steganography Technique Based on Integer Wavelet Transform Using Most Significant Bit Categories. International Journal of Intelligent Engineering and Systems, Vol.15, No.1, 2022 DOI: 10.22266/ijies2022.0228.4
9. Alaa F. and Yara R.(2023). Optimized steganography techniques based on PVDS and genetic algorithm. Alexandria Engineering Journal, Volume 85,2023,Pages 245-260,ISSN 1110-0168, https://doi.org/10.1016/j.aej.2023.11.013.
10. Kamil S.,Abdullah S., Hasan M. and Bohani F. "Enhanced Flipping Technique to Reduce Variability in Image Steganography," in IEEE Access, vol. 9, pp. 168981-168998, 2021, doi: 10.1109/ACCESS.2021.3133672.
11. Almayyahi, A., Sulaiman, R., Qamar, F., & Hamzah, A.E. (2020). High-Security Image Steganography Technique using XNOR Operation and Fibonacci Algorithm. International Journal of Advanced Computer Science and Applications.
12. Adel A., Khalid A. and Sayed A.(2023) Image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption,.Alexandria Engineering Journal, Volume 75, Pages 41-54,ISSN 1110-0168, https://doi.org/10.1016/j.aej.2023.05.051.
13. Ashwak A., Maisa'a A. and Adnan S.(2020). Image steganography using least significant bit and secret map techniques. International Journal of Electrical and Computer Engineering (IJECE), Vol. 10, No. 1, February 2020, pp. 935~946ISSN: 2088-8708, DOI: 10.11591/ijece.v10i1.pp935-946
14. Alejandro M., Alfonso H., Moutaz A., Jason J., David C., Evolving Generative Adversarial Networks to improve image steganography, Expert Systems with Applications, Volume 222, 2023, 119841,ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2023.119841.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204003 |

15. M. Hassaballah, Mohamed Abdel Hameed, Saleh Aly, A.S. AbdelRady, 2 - A color image steganography method based on ADPVD and HOG techniques, Editor(s): Mahmoud Hassaballah, Digital Media Steganography, Academic Press, 2020, Pages 17-40, ISBN 9780128194386,
https://doi.org/10.1016/B978-0-12-819438-6.00010-4.
16. Kaur, R., Singh, B.(2021). A hybrid algorithm for robust image steganography. Multidim Syst Sign Process 32, 1–23 (2021). https://doi.org/10.1007/s11045-020-00725-0
17. Dhawan, S., Gupta, R., Bhuyan, H.K. et al. An efficient steganography technique based on S2OA & DESAE model. Multimed Tools Appl 82, 14527–14555 (2023). https://doi.org/10.1007/s11042-022-13798-9
18. Inas J., Prashan P., Peter J. Improved image steganography based on super-pixel and coefficient-plane-selection, Signal Processing, Volume 171, 2020, 107481, ISSN 0165-1684, https://doi.org/10.1016/j.sigpro.2020.107481
19. Sonar, R., & Swain, G. (2022). A hybrid steganography technique based on RR, AQVD, and QVC. Information Security Journal: A Global Perspective, 31(4), 479–498. https://doi.org/10.1080/19393555.2021.1912219
20. Molato A., Calanda F., and Medina R. "LSB-based Random Embedding Image Steganography Technique Using Modified Collatz Conjecture," 2022 7th International Conference on Signal and Image Processing (ICSIP), Suzhou, China, 2022, pp. 367-371, doi: 10.1109/ICSIP55141.2022.9886754.
21.UKEssays. (November 2018). The History & Background of Steganography. Retrieved from https://www.ukessays.com/essays/english-language/background-of-steganography.php?vref=1
22. Kefa Rabah, 2004. Steganography-The Art of Hiding Data. Information Technology Journal, 3: 245-269.DOI:10.3923/itj.2004.245.269
23. Jayesh S., Aniruddh S., Bhavesh J., Deepesh S. and Nilesh C.: (2017). Steganography Techniques. International Journal of Engineering Development and Research(IJEDR) Volume 5, Issue 2 , ISSN: 2321-9939 IJEDR1702167
24. Onyedinma E. and Onyenwe I(2024). Two-Tier Data Security Technique: LSB Image Steganography and Columnar Transposition Cipher International Journal of Innovative Research in Computer and Communication Engineering.| e-ISSN: 2320-9801, p-ISSN: 2320-9798|. DOI: 10.15680/IJIRCCE.2024.1204001
25. Johnson N. and Jajodia S (1998) Exploring steganography: Seeing the unseen Computer 31.
26. Khaldi A. Steganographic Techniques Classification According to Image Format.International Annal Science ; Vol. 8, Issue 1, pp: 143-149, 2020SSN: 2456-7132
27. Ashwini K., Keerthana M., Maria C. (2014) Concealing Data Using Audio Steganography, International Journal Of Engineering Research & Technology (Ijert) Ifet – 2014 (Volume 2 – Issue 01),
28. Anita P. , Aditya K., Gandharba S. , Raja K. (2016) .Performance Evaluation Parameters of Image Steganography TechniquesI. International Conference on Research Advances in Integrated Navigation Systems (RAINS - 2016),
29. Onyedinma E., Onyenwe I. , Inyiama H.(2019). Performance Evaluation of Histogram Equalization and Fuzzy image Enhancement Techniques on Low Contrast Images. International Journal of Computer Science and Software Engineering (IJCSSE), Volume 8, Issue 7. ISSN. 2409-4285