PENINSULA PUBLISHING LLC

SHIFRA

Vol. **(2024)**, 2024, **pp**. 74–87
ISSN: 3078-3186

Research Article

An Overview of Image Steganography Techniques: Historical Development, Methodologies, and Evaluation Criteria

Omar Mejbel Hammad [1,2,*], Ikram Smaoui [3], , Ahmed Fakhfakh [4], , Mohammed Mahdi Hashim [5],

[1] *University of Sfax, Sfax, Tunisia*

[2] *Department of Anesthesiology, College of Medical Technology, Al-kitab University, Iraq*

[3] *LETI Laboratory, University of Sfax, Sfax, Tunisia.*

[4] *SM@RTS Laboratory, CRNS, University of Sfax, Sfax, Tunisia.*

[5] *Ministry of Higher Education and Scientific Research Baghdad, Iraq.*

ARTICLE INFO

Article History

Received 18 Feb 2024

Revised: 13 Apr 2024
Accepted 12 May 2024
Published 3 Jun 2024

Keywords

Image Steganography,

Least Significant Bit (LSB),

Discrete Cosine Transform (DCT),

Payload Capacity,

Imperceptibility.

ABSTRACT

This paper provides a detailed overview of image steganography, tracing its historical roots and examining the development of modern techniques. Steganography, derived from the Greek words "stegos" (cover) and "graphia" (writing), refers to the practice of concealing information within a host medium. Historically, steganographic techniques included tattooing hidden messages and using invisible ink, but the digital age has introduced new possibilities for secure data embedding, particularly within images. With the advent of the internet, the need for robust steganographic techniques has increased, leading to advancements in both spatial and frequency domain methods, including Least Significant Bit (LSB) replacement, Discrete Cosine Transform (DCT), and wavelet-based techniques. This paper also reviews evaluation criteria such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Structural Similarity Index Measure (SSIM) to assess the effectiveness of various steganographic methods in achieving high security, capacity, and imperceptibility. Challenges such as balancing these criteria, developing multi-criteria evaluation tools, and optimizing embedding processes are highlighted. This review aims to provide insights into current advancements, limitations, and future directions for research in image steganography.

1. INTRODUCTION

This This provides a comprehensive analysis of the existing literature in the domain of data-concealing methods as a whole, with a specific focus on image steganographic methodologies. This comprehensive synopsis presents an extensive overview that seeks to summarize all the research goals and problems derived from the existing research gaps. The concept of data concealment predates the advent of communication itself. The concept of steganography originates from the combination of two Greek terms, namely "Stegos" and "graphic", which respectively denote "cover" and "writing". Consequently, steganography may be precisely described as the practice of concealing information under a hosting medium [1]. Indeed, in the realm of steganography, the concealment of secret data inside media (namely images) has historically been accomplished via the use of either invisible ink or tattoos. These covert techniques serve as vehicles for transmitting concealed messages within older steganographic methods. The development of contemporary communication technology has facilitated the ease of data conveyance across a variety of hosting mediums. The advent of the World Wide Web necessitated the concealment of private data, rendering it concealed or unidentifiable to unauthorized individuals [2]. The primary concern when examining steganography as the practice of covert communication is the proliferation of the World Wide Web and the consequent need for security measures [3].

The practice of concealing information has a lengthy historical background, originating from a time when a nobleman sought to communicate with his son. To do this, he developed a technique involving the tattooing of messages into selected slaves, namely on their scalps after the removal of hair. Subsequently, with the regrowth of his hair, the individual transmitted the enslaved individual to his offspring, concealing the tattooed communication under the epidermis of his

*Corresponding author email: omar.hammad@uoalkitab.edu.iq
DOI: https://doi.org/10.70470/SHIFRA/2024/009

cranium, marking the inception of steganography. Later, the Germans devised novel methodologies throughout the "Second World War" by using microdots to reduce typing durations, so making the message elusive and challenging to discover when delivered across a secure channel [4] (Fig1) illustrates the overall progression of this chapter, with the numerical labels denoting the respective sections and subsections.

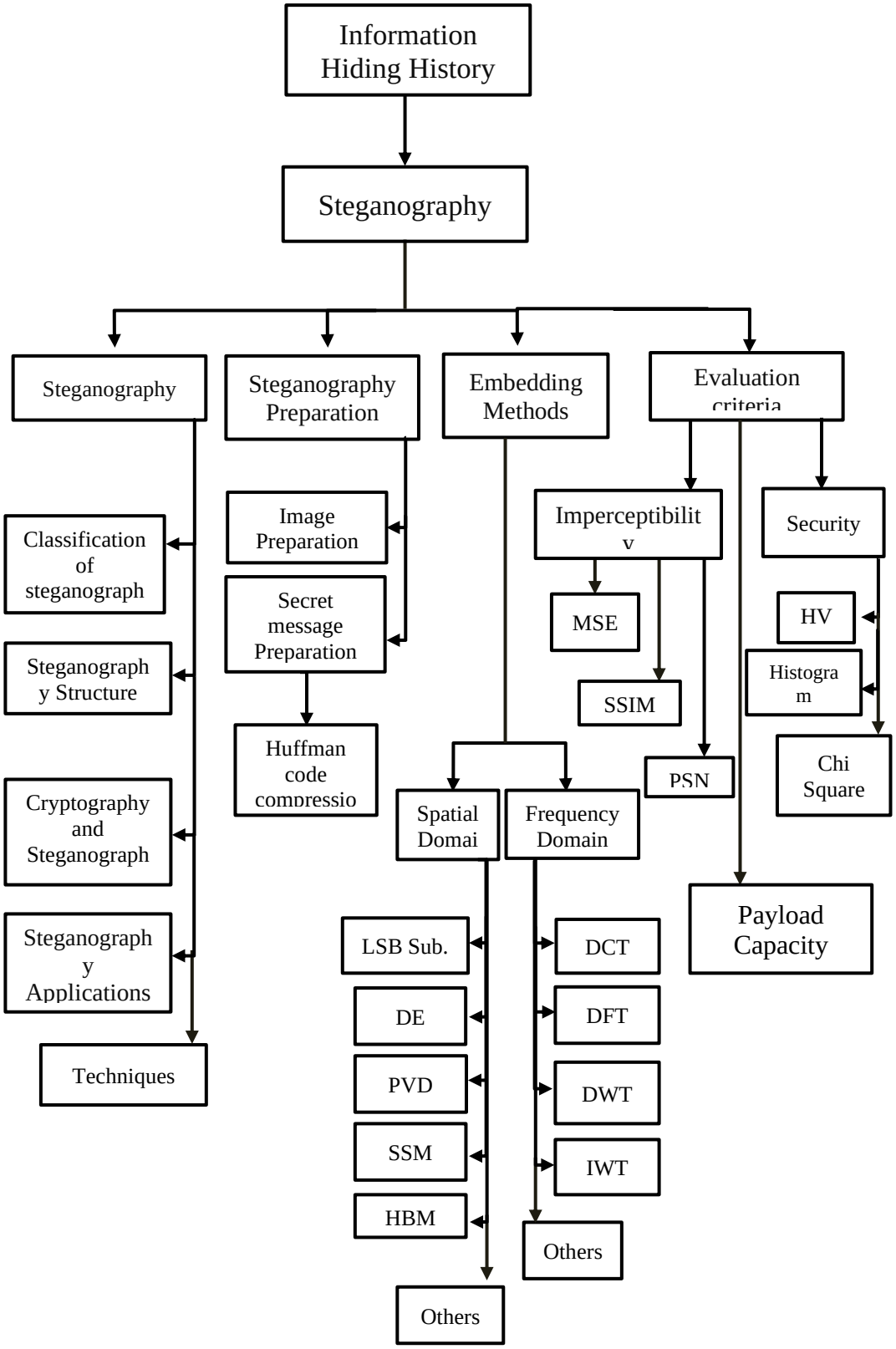

Fig. 1. Comprehensive structure of information hiding

The information hiding system has two major aspects. First one is the steganography that is considered here. Second concept is the watermarking which is not considered here. The early iteration of steganography had challenges due to the message transmission of messages, which gradually evolved via the utilization of email, postal systems, and telephones [5]. Throughout history, from ancient Greece to the present day, the concealment of data within the physical bodies of messengers has persisted, despite the advent of advanced information technology. The ancient Romans utilized a technique known as steganography, whereby they utilized invisible ink to write concealed messages inside the original lines. This included the use of a specific substance that, when subjected to heat, would become black, revealing the hidden message [6][7]. Through the historical period of World War II, a renowned technology was utilized for the transmission of covert communication. This approach included the utilization of invisible ink, which was accompanied by a changeable extraction code methodology. Currently, invisible ink is employed in several ways, including the use of Ultraviolet radiation in conjunction with anti-counterfeit devices.

The first endeavor to conceal a covert message inside seemingly harmless writing was initiated by the monk Johannes, who explored the realm of contemporary encryption [8][9]. The book titled "Steganographia" authored by Gaspari Schott in 1665 is widely recognized as the first known reference of steganography. The principles presented in this book were derived from the teachings of the monk Trithemius. In contrast, the science of cryptography was first established in the publication named "Cryptographie Militaire" authored by Auguste and published in 1883 [10]. This book also suggested the principles of steganography system for their design. The null cipher were used by the Germans during the World War II to hide information, wherein it always appeared honest (innocent) to the enemy for instance: "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils".

This secret message was taken from the second letter in each word to extract the given message (Pershing sails from NY June 1). Thereafter, the field steganography was rapidly progressed with the emergence of the communication and the internet. The dependence of modern life on the WWW and internet made it necessary to maintain the development of various efficient steganography techniques for hiding the sensitive and private information in the good hosting media to achieve absolute security[11].

Steganography developed rapidly because of too fast progress in communication and internet. Maintaining of such development is necessary this will be helpful when proposed method and choose efficient method to embedd information in good cover object.

2. STEGANOGRAPHY

The steganography can be defined as an steganography to hide secret data in reliable hosting media, in a manner that makes the media which carry the secret is not detectible and unseen by the intruder or attacker . In the realm of digital technology, both cryptography and steganography have the same objective of safeguarding confidential messages from unauthorized access or interception. Both of these strategies proved to be beneficial whether they were used in a collaborative or individual [12]. The mix between two techniques also give excellent output but should be in multiple layers all this to keep high security[13].

Various data types are currently utilized in the field of steganography, including .jpeg, .bmp,. gif, .docx, .mp4, PPT, etc. When contemplating the extent of steganography, one may appreciate the significance of contemporary steganography, particularly in the context of the internet, for the sake of enhancing security and maximizing capacity. Due to strict rules imposed by governments and their limitation with the cryptosystems strength that will make the weakness in the internet community. This is the reason for using steganography [14].

In the steganography world, the message send is secure and no one can catch it even impossible extract it from hosted media just by using the key.

2.1 Classification of Steganography

Four major kinds of steganography according to hosting media (that hold the secret message) used by steganography. The famous and important one is the image which is used by proposed method as illustrated in (fig 2) Different algorithms used based on file formats that hold the message [15].

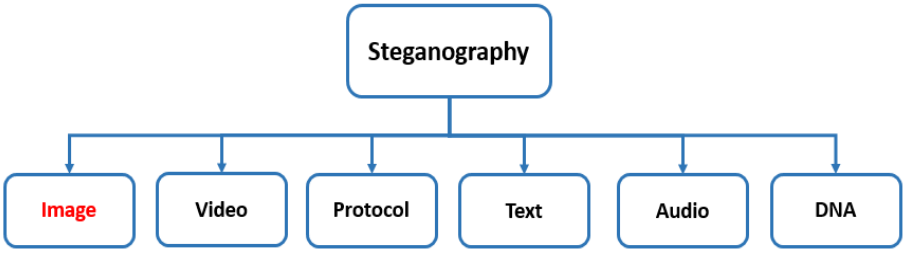

Fig. 2. Steganography classification

The pixels always used to hold the information last bit position in the image steganography. Insertion in pixel some time become sensitive because of changing pixels' value and its behaviour like filters effect with resizing and squeezing. For audio class embedding or hiding data is similar to process in image, but here we have to exploit the feature that recognized by the human ear for embedding the data. The used sound is ranging from inaudible to louder. In addition, the steganography designer exploits the weak position that human ear dose not detected. In protocol domain we use TCP/IP (Transmission Control Protocol/ Internet Protocol) position to host the secret message in one place, this domain considers untrusted till now. In video class embedding process look like image but with sequence of images which make frame of video, embedding will be in the image of frame in additional to the space interval between frames. (Fig 3)shows the classification of data security in detail which is derived from [16]. Different colours used in this classification.

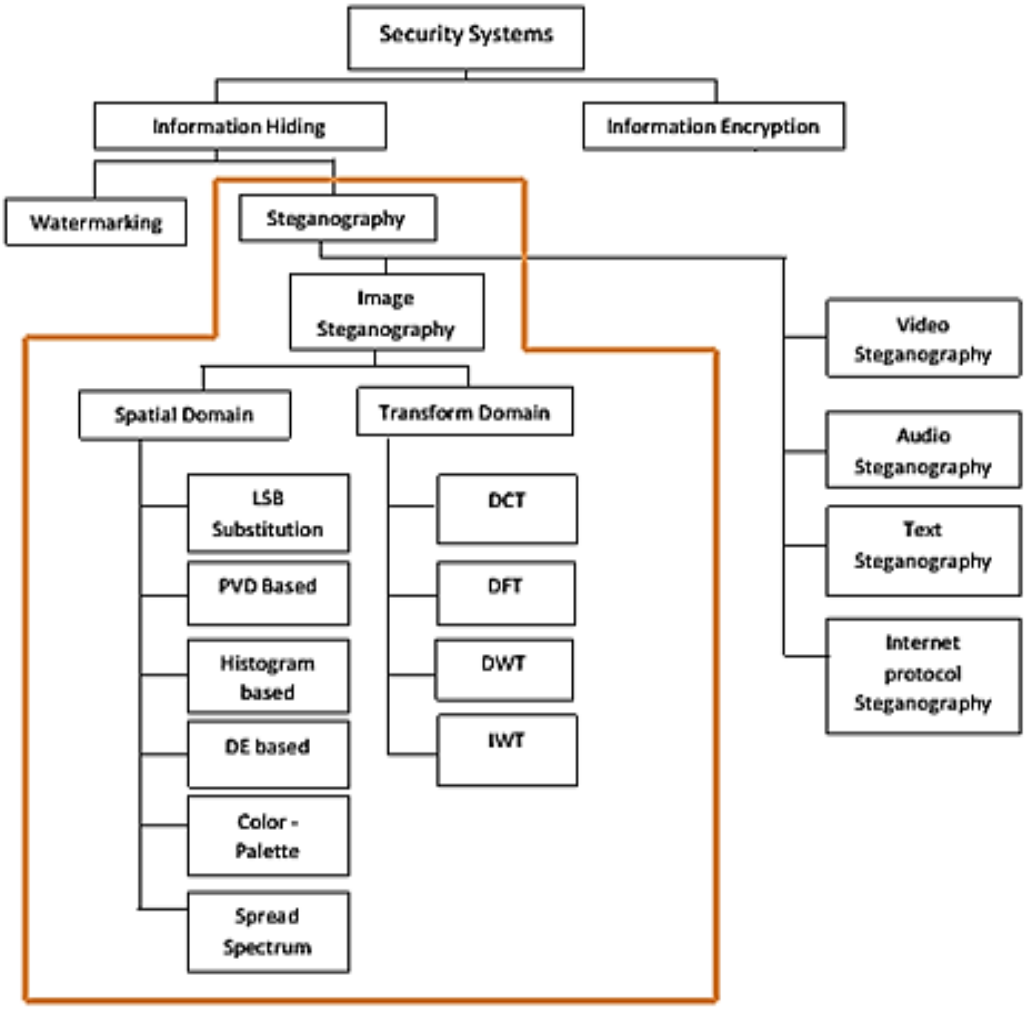

Fig. 3. Classification of steganography in spatial and frequency domains.

2.2 Steganography Structure

Wendy aims to establish a connection between the sender and receiver nodes, both positioned in the middle of the diagram (2.2). She consistently makes efforts to comprehend the message or discern the data exchanged among these individuals. Due to the inherent secrecy embedded within the communication process, characterized by the distribution of confidential information between the sender and the recipient, the extraction of the data from this particular framework is only feasible for the intended receiver [17]. The concept of a distributed secret can be seen as a potential method for obtaining the unique variables of a program, which can be represented as a "key". (Fig 4) shows the steganography structure in details.

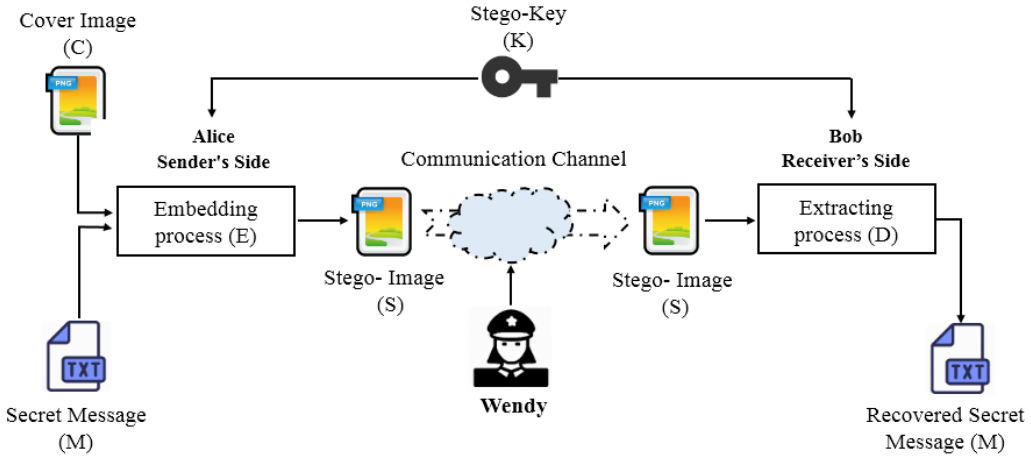

Fig. 4. The image steganography structure in details.

2.3 Cryptography vs. Steganography

The main purpose of both steganography and cryptography is preparing secret message transfer. Steganography does not like cryptography; it's concealing the data of secret information of intruders, while steganography also hides secret data. In cryptography the detector can use the same procedure to confuse the receiver in other parts, but in steganography the intruder cannot use the finding message again and the carrier is destroyed along with the message. In cryptography the message structure is designed to be meaningless to the attackers and the message can only be understood with the key by decryption [18][19].

In the field of cryptography, it is a common practice for private data to be made publicly accessible, so inviting anyone to engage in the pursuit of deciphering it, as seen in (Fig 5) In the field of steganography, the primary objective is to ensure the imperceptibility of the concealed data. Within the field of cryptography, confidential communication is susceptible to interception by unauthorized parties, but steganography aims to remain imperceptible to human perception.

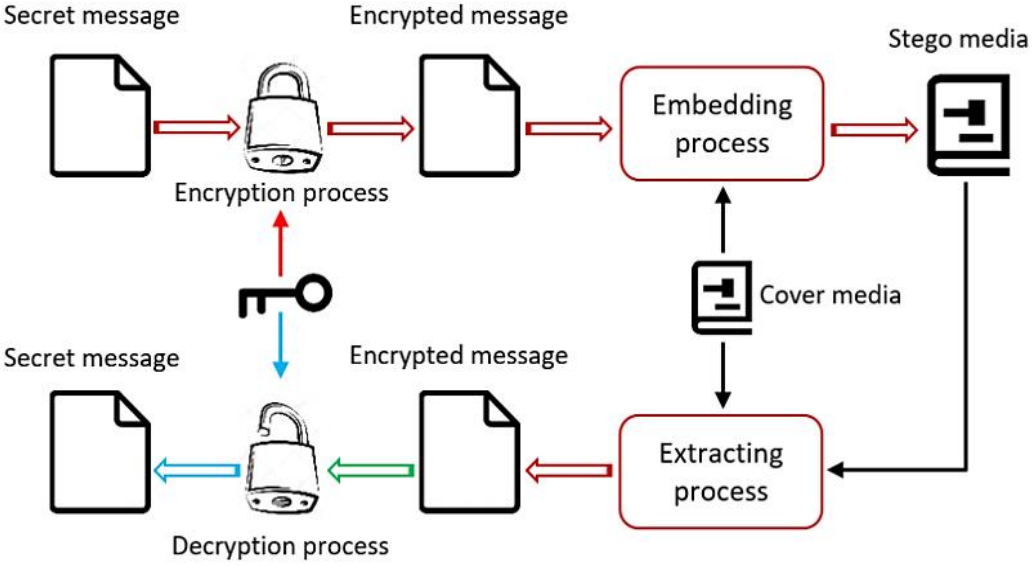

Fig. 5. The cryptography structure based on [20].

In cryptography system there is no need to hide the secret and the system is designed to encrypt the known secret. In steganography, the important goal is to hide the secret so as to be undetectable. (Fig 6) shows the build of a steganography system.

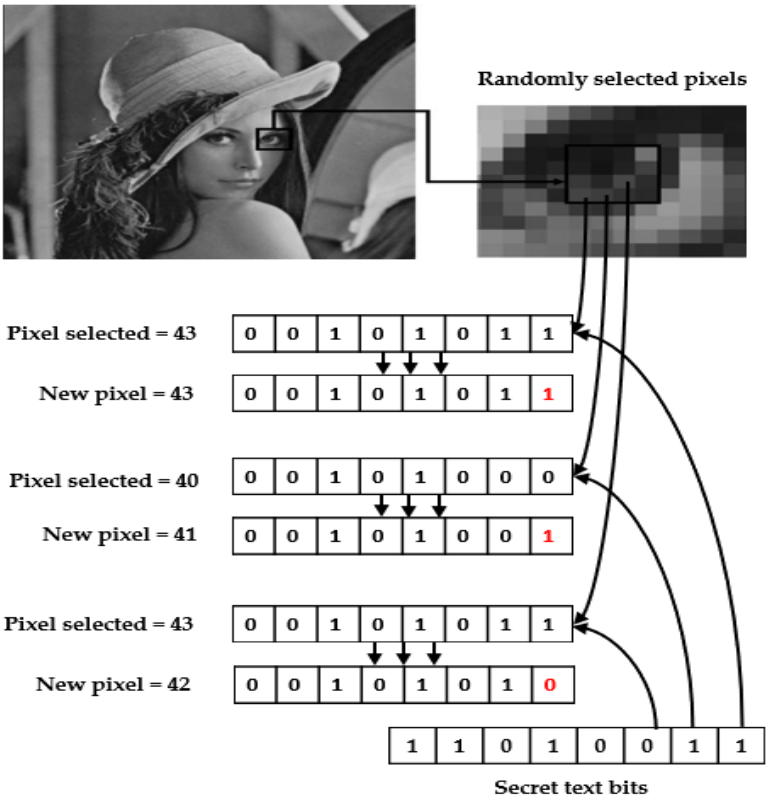

Fig. 6. The structure of steganography within grayscale image

Developing a steganography scheme as shown in (fig 6) is primarily concerned with the embedding method, and insert secret data within an image without changing the image properties and the image itself.

2.4 Steganography Applications

Within the field of image steganography, several applications have been developed using their respective contributions. These applications include areas such as feature labeling, copyright protection, and communication security [21][22]. The process of embedding, whether in copyright or watermarking, occurs inside a designated region of the image, often associated with intellectual property. Consequently, the utilization of an image without obtaining explicit authorization from the creator is facilitated by the provision of evidence. Contemporary stamping techniques include intelligent integration into images and other security measures, including labeling, captions, and descriptive components. Through the process of duplicating or transferring a stego picture, the inherent qualities of the image remain intact across many transformations. The steganographic key, whether implicit or explicit, retains the embedded information throughout the process of copying [23]. This is because all the confidential data is included inside the steganography-based communication, hence ensuring its preservation.

2.5 Steganography Approaches

In the literature, many methods have been introduced for embedding secret data in steganographic method [24]. For all these proposed methods aims to find easy and better method for conceal hidden data within a specific image. The normal techniques contents [25]:

1. Embedding in LSB location.
2. Covering and filter key.
3. Transferring media or channel.

In steganography system the simplest method for embedding secret data inside the image is LSB. The method of embedding going through replacing secret data (bit) directly with LSB of the pixels of cover image to produce stego image. human perception cannot differentiate when LSB modulation due to less changing in impact pixel values of minimize the amplitude. Discuss in detail will be provided in LSB embedding technique due to proposed method relay on this technique. The cover image or can be called hosting image uses 8-bits for Gray image or 24-bits for colour image for hiding secret message. Significant place used to hold the message considered in this approach in cover image. Like watermark used paper aims to hide the information in noise layer this procedure follows in steganography approach [26].

In frequency domain, embedding the secret message done by modulating of coefficients and named transform embedding. JPEG compression always used Discreet Cosine Transform (DCT) with Wavelet Transform (WT) significant place used

to hold the secret message in this method for cover image [27]. Because of using frequency technique of the image this method considered more robust than other. In this regard the whole image transformation data used to achieve better embedding.

2.6 Data Preparation

In terms of preparation, both cover images and secret messages need to prepare prior embedded process. The suitability of the image for concealing covert signals lies in its ability to manipulate pixel prioritization via rearrangement. The process of concealing secret data inside certain images requires particular manipulations.

2.6.1 Image Preparation

The original image in steganography called cover image used to host the secret information or can say an image before embedding process. Preparing stage is the stage that fall in context of preparation and the cover image always handle in this stage as followed in the literature [28][29]. According to the embedding method, the cover image should be manipulated to be suitable for host the data, this process includes the normalizing, segmenting, or denoising. In the digital world, the cover image normally consists of 8-bit planes.

In case of Image = $\{X_i , i \in n\}$ where n is considered as a set of bits located in cover image, and in image definition n divided into 8 subsets like $\{a_1, a_2, \ldots, a_8\}$ and in this case $n= U_{i=1}^{8} a_i$ and $a_i \cap a_{i+1} = \emptyset$.

Stego image is the cover image after embedding which means image contains the message. Embedding method normally used LSB of the cover image. This bitplane is hosted the secret message and at LSB part. The LSB part is not visible for human eyes.

2.6.2 Secret Bit Preparation

In the secret bit preparation, the Huffman coding algorithm is used as a compression algorithm before the embedding process. The outcomes of the Huffman procedure consist of a variable and a table that includes symbol and corresponding letters. The determination of character weights is achieved by the use of the probability associated with that particular symbol [30]. The method in question can be characterized as follows:

- Input: The letters $A=\{A_1,A_2,\ldots,A_n\}$ that are symbols of m size.
  $W=\{W1,W2,..,Wn\}$ that represent the weight of each symbol like depth in the tree wi=weight of ai such as $1 \leq i \leq n$
- Output: codeword $C(A,W)=(c_1,c_2,..,c_n)$ that are the rout code which refers to code word of each i.
  The main reason is:

$L(C)=Sum (W_i \times length (c))$ represent the code word length C when L(c) less than L(T)

Numerous research in previous research studies have utilized the Huffman coding technique within the domain of steganography, specifically in relation to least significant bit (LSB) images. The primary objectives of using this approach are to achieve a substantial secret capacity and to categorize the secret code into three distinct groups for the encoding process [31]. The act of compressing the secret data prior to its embedding in a carrier medium serves to enhance both the capacity and security of the steganographic process. Various techniques are utilized in this context throughout the creation of steganography. The process of embedding lossy data in images while maintaining lossless quality. In [32], authors utilized Huffman coding as a means to enhance the system's resilience against histogram and statistical assaults. The utilization of a unique coefficient approach was employed to enhance the resilience, as seen in the schematic diagram presented in (Fig 7).

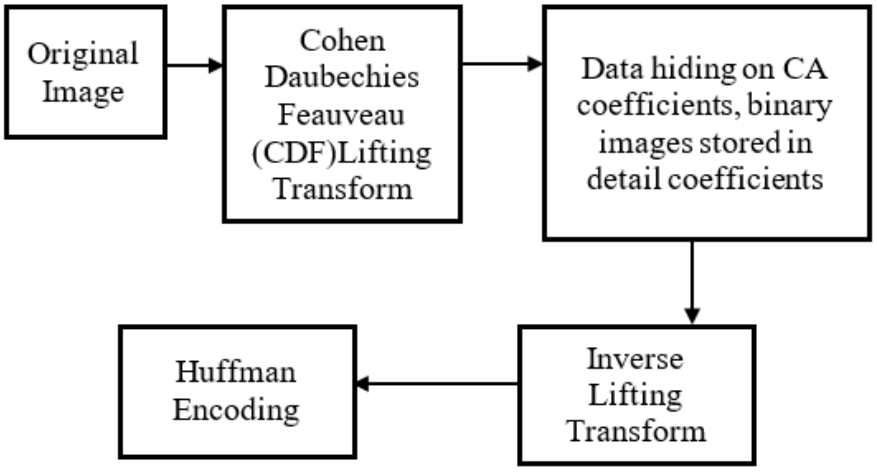

Fig. 7. Image steganography with Huffman algorithm [33].

Huffman coding was utilized to enhance capacity and PSNR results. The proposed methodology utilizes a Canny filter to detect edges and smooth regions inside the image. Subsequently, the pixels within these identified areas are chosen for the

embedding procedure [34]. The technique of second block correction was implemented in order to enhance the imperceptibility of the steganographic image.

In [36], authors demonstrated superior outcomes in the context of compressing. In the context of mobile healthcare, the lost data is compressed utilizing the TCP/IP standard=]

Following this compression, the noisy data is eliminated and the compressed information is recovered for decoding, ultimately resulting in the retrieval of the final information. The use of Huffman encoding is prevalent across several disciplines, and the integration of steganography with encryption is a widely observed practice [35]. When constructing a steganography method aimed at enhancing compression, the consideration of the probability or frequency of the symbol code becomes crucial. This is performed in conjunction with the compression form JPEG to achieve greater effectiveness [36]. The name "Huffman" is often used as a synonym for the concept of payload capacity in steganography techniques. Numerous approaches have been proposed in scholarly works to address this topic, as documented by [37][38]. The Huffman method was utilized to compressed the data such a text by coding the characters' code according to the ASCII character code and sort the numbers. Then encoding by distributed as a tree and find the frequency for each character and its path in this tree as shown in (fig 8).

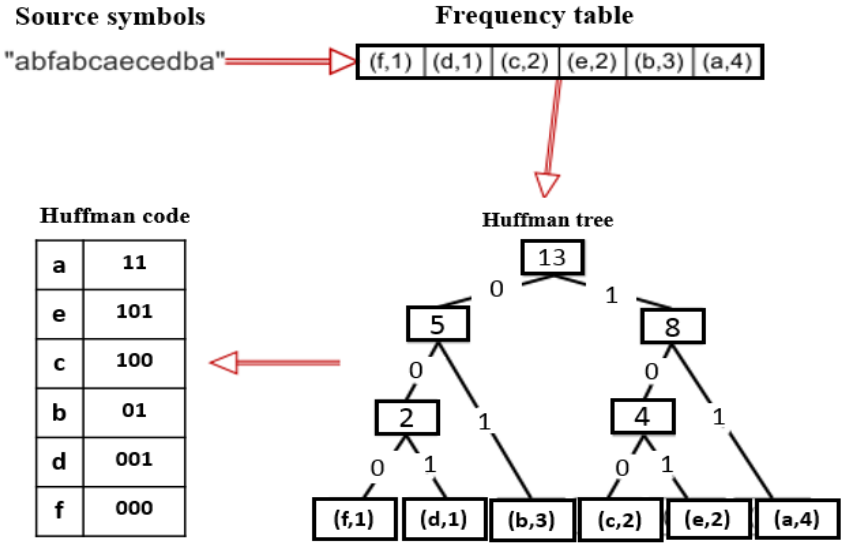

Fig. 8. The Huffman method steps [39]

- The study's conclusion suggests that the use of the Huffman codes technique in steganography methods may effectively enhance the secret capacity by encoding the secret data prior to embedding. Simultaneously, the system is enhanced in terms of resilience against histogram and statistic assaults.

2.7 Image Steganography Domains

The steganography method has been classified into two categories based on the hosting sites and image characteristics [40][41].

1. Spatial domain
   The hidden message is inserted or embedded using pixel intensity in this context. This particular category or classification offers several benefits for concealment, such as enhancing capacity without any limitations and minimizing complexity. Hence, the concealment of messages is imperceptible [42][43]. One drawback of this course is its deficiency in providing instruction on statistical analysis methodologies.
2. Frequency Domain
   In this regard given image will change or be transformed into a frequency class (domain) then embedding the secret message will be in the coefficient's factors. In this scenario, the image offered will undergo a conversion or alteration into a frequency domain. Subsequently, the secret data will be embedded inside the factors of the coefficients. The use of the frequency domain has the advantage of enhanced resilience against statistical assaults. However, it is accompanied by a notable drawback of limited capacity [44][45].

The use of spatial cases is prevalent among researchers due to its simplicity and enhanced efficiency. Different technique related to spatial and frequency domains. Next subsection we discussed the most important techniques used in literature review. [46][47].

2.7.1 LSB Method for Substitution

The use of LSB replacement in the watermark methods has been seen around 1994. The steganography method often employs the use of replacement techniques, namely the least significant bit (LSB) approach, for the purpose of embedding

hidden messages. In [43], authors introduced the use of LSB as a method for embedding messages inside the Optimal Pixels Adjustment Process (OPAP). This methodology is used to enhance the visual fidelity of steganographic pictures that include concealed information while minimizing the difficulty of computing. In [48], authors colleagues proposed a methodology that utilizes the adaptive least significant bit (LSB) replacement steganography technology. The strategy involves the division of images into two segments: non-sensitive and sensitive areas, which is achieved using texture analyses. In the context of non-sensitive regions, a significant proportion of bits are allocated for the storage of confidential communications, while the remaining bits are situated inside areas of concern.

2.7.2 Pixel Value Differencing (PVD)

This strategy yields an enhanced steganographic image, resulting in an increased payload capacity due to the utilization of all pixels within the image [49]. The process of embedding in this manner occurred at the periphery of regions characterized by smoothness, where pixels in close proximity exhibited a heightened intensity. The human retina is capable of seeing any alterations in the smooth region of an image [50]. Consequently, this technique disregards the smooth zone and focuses on embedding information mostly in the edge area. The edge zone is characterized by variations in pixel intensity and is considered less receptive to changes.

The method of using edge detection has a resemblance to the Perceptual Video Quality Metric (PVD) introduced by [46]. The use of the Canny filter for edge detection is seen as a means to determine the location of embedding. The use of this technique resulted in an enhancement in the image's quality, namely in terms of imperceptibility. In [48], authors have presented a steganography system based on the modifying of four pixels and their LSB. In this method, classifying of smooth and edge area inside the image before the embedding process. The image is partitioning into 2 by 2 blocks and the difference of intensity pixels includes of these blocks determine if this area belongs to smooth or edge one. Promising results will not provide by this method and by discarding smoothing area. This method increased by 2 dB of PSNR this actually not encouraging comparing with other existing methods. A method based on PVD system proposed by [50] that used two continuous pixels' intensity to make decision where the embedding occurs in certain block. High security and capacity should achieve in this method theoretically, due to used non-overlapping pixels of different neighbour pixel intensity. This meaning the system will check the pixel location in the image if located in edge position then embedding will take action or else neglect this location and calculate other pixels. This decision will make actually by system designer. Different embedding method suggested by [46] for hide secret message into gray cover image. Cover image is divided in this method into blocks according to sensitive and non-sensitive pixels, and then intensity calculated for each block. High imperceptibility achieved by this method.

2.7.3 Based Method of Histogram

This approach utilizes the pixel coordinates to encode concealed data, which is symbolized by a histogram formed via the technique of histogram shifts. The histogram exhibits a correlation with the frequency distribution of pixels in the cover picture. By constructing a histogram, it is possible to identify the pixels with the lowest frequency. This approach uses raster scanning to distinguish between high and low frequencies. According to , the procedure for embedding in a histogram occurs either at the high or low peak point. In this approach, a satisfactory peak signal-to-noise ratio (PSNR) of around 57 dB was attained while embedding a secret message consisting of 191,000 bits. Once the steganographic picture has been embedded, it may be sent to the recipient. The process of extracting the hidden information from the image can then be performed with relative ease since the image can be reconstructed without any discernible errors. In authors produced an improved Peak Signal-to-Noise Ratio (PSNR) by using two-dimensional histograms for concealing and modifying the secret data. One drawback associated with this particular approach is its inherent restriction in terms of capacity.

2.7.4 Color Palette Based (CPB) Method

The investigators in [49] utilized the correlation of color space for the goal of embedded. This approach involves the insertion of a bit into each color pixel to create a color picture. The randomized function is responsible for generating numerical values, which subsequently correspond to the pixels that store the concealed bits. The steganographic key is responsible for storing the pixel numbers that will be used throughout the extraction procedure in a separate component, namely the receiver. The process involves the selection of pixels by looking for the closest colors that remain unaffected by the embedding procedure. The technique described in this study generates a robust degree of security due to its reliance on a random method dependence [48]. The RGB pixel is represented by 24 bits, while an additional 3 bits are used to encode the secret data using the cycle color technique. The use of a random method makes this approach more resilient against statistical assaults in comparison to the sequential hiding process.

2.7.5 Steganography based on DFT

The Discrete Fourier Transform (DFT) is utilized to analyse the frequency elements that comprise the pixel intensity results in the hosting picture.

$F(x, y)$ interduce the hosting image with m x n image size and the the formula of DFT can be given by:

$$f(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{m-1} \sum_{y-0}^{n-1} f(x,y) e^{-j2\pi \left(\frac{ux}{M} + \frac{vx}{N}\right)} \quad (1)$$

The reconstruction of the original picture is necessary after the embedded procedure, and this is achieved via the use of the Inverse Discrete Fourier Transform (IDFT) technique, which is responsible for retrieving the pixel values from the converted image. The DFT algorithm may be described as a series of straightforward procedures. To begin, the hosing image (C) should be examined in order to access the secret data (S). Next, the Discrete Fourier Transform (DFT) should be applied to the hosting image (C). Following this, the Real portion of the DFT coefficients should be separated. Subsequently, the data-embedded bits should be included in the Realspace of the DFT. Finally, the Inverse DFT should be performed to get the stego result image (C'), as seen in (Fig 9).

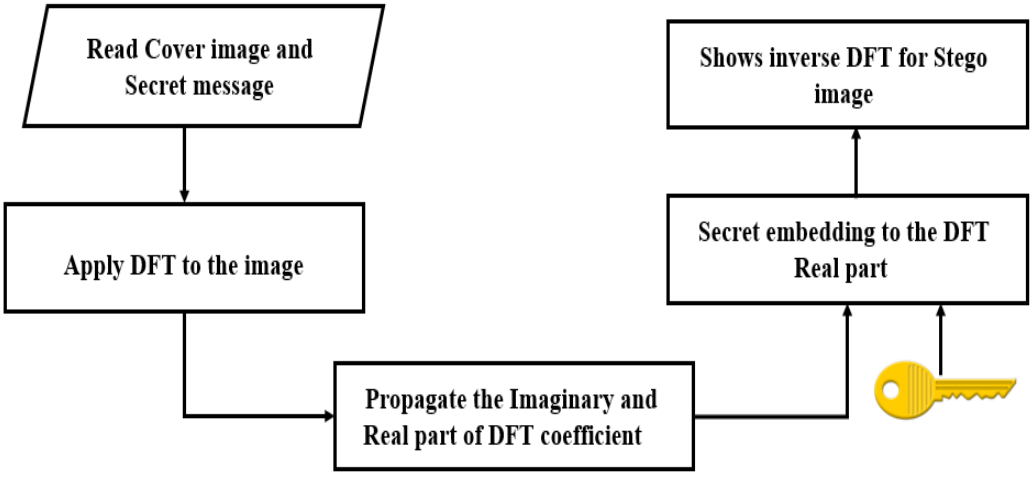

Fig. 9. The embedding strategy based on DEF.

To do extraction, one must reverse the process of embedded, starting from the lower levels and progressing upwards In, authors introduced a novel embedding technique utilizing Discrete Fourier Transform (DFT). In their approach, a sliding windows approach was used, where a 2 \times 2 block division was utilized. The Discrete Fourier Transform (DFT) was used on individual blocks of the cover picture, taking into account the coefficient. The embedded process was then carried out only inside the rear section of the DFT. The reported findings indicate an important enhancement in both security and resilience. In authors proposed an alternative approach to the Discrete Fourier Transform (DFT) utilizing the Weight Fractional Fourier Transform (WFRFT) as a substitute for the conventional DFT technique. The secret data was embedded using two least significant bits (LSBs), specifically in the actual component. Fractional Fourier Transform (FRFT) method was suggested by [33] and this method transferred cover image by FRFT via the order of α=0.78 and β=0.25. By this method the PSNR and security increased.

2.7.6 Steganography based on DCT

The use of the Two Dimensional (2D) - Discrete Cosine Transform (DCT) in steganography systems is a prevalent practice. The DCT, which is employed in this context, can be precisely characterized as follows:

$$B_{p,q} = \alpha_p \alpha_q \sum_{m=0}^{m-1} \sum_{n=0}^{n-1} A_{m,n} \cos\frac{\pi(2m+1)p}{2m} \cos\frac{\pi(2n+1)q}{2n} \quad (2)$$

Such as $A_{m,n}$ represent the size of image m x n and $B_{p,q}$ introduce a Coefficient Transform(CT).

To do the reverse of 2D-DCT, which is a necessary step in the extraction procedure as described by:

$$A_{m,n} = \sum_{m=0}^{m-1} \sum_{n=0}^{n-1} \alpha_p \alpha_q B_{p,q} \cos\frac{\pi(2m+1)p}{2m} \cos\frac{\pi(2n+1)q}{2n} \quad (3)$$

The first phase in the process is implementing the 2D-DCT processes or steps. This entails dividing a cover image into sub-image blocks of size 8 × 8, which are denoted as (Bi), where i represents the ith block. In the second step, the 2D Discrete Cosine Transform (2D_DCT) is applied to each block or sub-image in order to determine the coefficients of the DCT. This process results in the generation of one DC coefficient and 63 AC coefficients for every block. In the third step, the stego result key is generated using the coordinates (u1,v1) and (u2,v2). In the fourth step, the user is instructed to interpret the variable "mi" as a concealed binary digit inside the set of "ith" bits. In order to get the original sub-image or block, the inverse discrete cosine transform (DCT) will be used in Step 5. In order to identify the stego picture, it is necessary to iterate over all blocks and follow the aforementioned processes.

In the process of extracting the private data on the receiver side, it is necessary to follow the same stages as in the embedding procedure, but in reverse order. Numerous academics have used and adapted the Discrete Cosine Transform (DCT) method in order to ascertain the objectives of the steganography method.

In, authors proposed a novel approach that integrates DCT steganography with affine transformation. They observed promising results, attributing the effectiveness to the inherent property of DCT steganography, which exhibits a lower loss

invertibility. The diffusion of the Laplacian shape is utilized in the process of changing the integer discrete cosine transform (DCT). This strategy is often regarded as being more resilient to statistical assaults compared to other approaches. The approach proposed by [39] involves the use of Integer Wavelet Transform (IWT) in conjunction with Discrete Cosine Transform (DCT) for steganography purposes. The embedding process involves two distinct steps: the Discrete Cosine Transform (DCT) is used for the development of the private message, while the Inverse Wavelet Transform (IWT) is utilized for the preparation of the picture. The whole embedding was performed using Munker's assignment technique in this approach. In [24], authors introduced a novel steganography system that operates in the Discrete Cosine Transform (DCT) domain specifically designed for color pictures. The suggested approach utilizes the DCT coefficients to conceal images via modification. The first step involves encrypting the confidential message during the preparatory phase, followed by embedding the encrypted private message within the DCT coefficients section. Utilization of the frequency coefficient in this approach leads to an improvement in the peak signal-to-noise ratio (PSNR). In authors introduced a novel steganography technique known as zero-steganography. This strategy utilizes a low pass filter combined with noise reduction in JPEG compression pictures. Through evaluation against three different types of assaults, this method demonstrates commendable imperceptibility and resilience.

2.8 Steganography Criteria

In [22], argue that the comprehensive examination of steganography techniques necessitates the implementation of a robust and dependable evaluation and benchmarking tool. This tool enables the assessment of established methods across many scenarios.

In authors identified a dearth of comparison instruments available for the assessment of reversible steganography approaches. The authors of this article have formulated a number of suggestions based on their perspective on the advancement of steganography. Firstly, to secure steganography approaches, several additional forms of steganography techniques need the use of dependable evaluation instruments to facilitate the comparison between various methods. Secondly, an analysis is conducted on the effectiveness of different digital steganography methods in terms of their capacity, imperceptibility, and computational cost. Furthermore, the authors have emphasized the existence of a deficiency in the measurement of the trade-off between payload, imperceptibility, and security.

Imperceptibility, payload capacity, and security in statistical un-detectability are the key criteria in designing for steganography scheme [10]. The steganography criteria are discussed in detail in the next subsections.

2.8.1 Security

Numerous methodologies and methods have been created to assess the benchmarking of steganography. Nevertheless, the primary focus of their development has been centered on evaluating the effectiveness of the steganography technique by subjecting the steganography medium to various forms of assault. In [44], argues that there is a need for improved steganography algorithms in order to effectively retrieve concealed messages after exposure to various possible assaults, as shown in several benchmarking methodologies.

According to [9], the inclusion of security measures is a prominent and crucial aspect in the development of steganography systems. The authors reached the conclusion that there exist many benchmark programs for assessing the security of steganography, including Chi-square.

In the context of the protected embedded method, it is not possible to delete the embedded private message after it has been reliably detected by targeted assaults, unless the attacker has complete knowledge of the embedded method, with the exception of the secret key. Due to the similarity of techniques used in cryptography and steganography then attacks will be almost the same. If hosting images or media known in public then detecting procedure will be easy by the unauthorized person, using the sequence of image bits to check the relation among them. In this case, hackers will suspect the message and can modify or destroy it if it is secured. In the steganography system, there are three important attacks Chi-square (X 2), Human Visual System (HVS) attack and Histogram analysis attack. These important attacks have discussed in detail in chapter three.

2.8.2 Payload Capacity

The highest payload refers to the upper limit of the secret data size that may be concealed inside a hosting file, taking into account a certain condition. The concept of imperceptibility entails that the highest payload denotes the upper threshold of covert information that may be concealed inside voice, picture, or video files. If the limit is surpassed, noticeable alterations would occur in the hosting file, leading to a breakdown of the steganography method. However, the observation of such a transformation is contingent upon the possession of the initial media file by the perpetrator. The quantification of the digital steganography payload is accomplished via the use of the data hiding rate (DHR), which denotes the proportion between the highest possible payload and the size of the original hosting media [21].

In [35], authors assert that the threshold for high-capacity picture steganography should exceed 1.5%. Nevertheless, categorizing any technique that exceeds 5% of the original hosting as a high rate may lead to the inclusion of several unqualified methods being classified as high data rate methods. Moreover, augmenting the data concealed size would lead to a decrease in the quality of the hosting file and the resilience of the method, perhaps resulting in a failure of the

watermarking technique. Hence, it is essential for the comparison of the methodologies to include an assessment of the data concealing size, the quality of the hosting file, and several other relevant parameters. The aforementioned characteristics can be standardized into a consistent scoring system in order to facilitate comparability.

2.8.3 Imperceptibility

In recent times, there has been a growing interest in using steganography methods as a potential option for copyright protection and content authentication. The primary objective of steganography is to enhance data security by concealing data inside a different medium. Both methodologies used identical procedures, although with distinct objectives. Therefore, it is feasible to retrieve the encoded message at any given moment, irrespective of any modifications made to the text as a result of the assaults.

Researchers have shown significant interest in information-concealing strategies, which serve the purpose of covertly transmitting data and establishing concealed connections between the message and its recipient. In authors assert that the use of data concealment techniques is mostly seen in the context of photos, audio, protocols, etc. Currently, a universally accepted instrument or methodology for evaluating the efficacy of data masking techniques is lacking. Therefore, the Peak Signal-to-Noise Ratio (PSNR) , Mean Square Error (MSE) [43], and Structural Similarity Index Metric (SSIM) were used by researchers.

The common major issue in the steganography method is imperceptibility which is measured via Peak Signal to Noise Ratio (PSNR) based on changing the value of Mean Square Error (MSE) in which of inverse proportion with PSNR. The payload capacity is a trade-off with imperceptibility. Therefore, when authors need to control PSNR have to manipulate MSE and make it less as possible to get high PSNR. The MSE is related to payload capacity, so increase the secret message will reflect on MSE (MSE will increase) and this makes PSNR less when comparing the original image with stego image. High PSNR means better quality of image then better steganography. So, the new steganography scheme is required to solve this problem with suitable impact value instead of the previous impact value that have used with all researchers, for the distribution of embedding in order to increase security and improving imperceptibility [19].

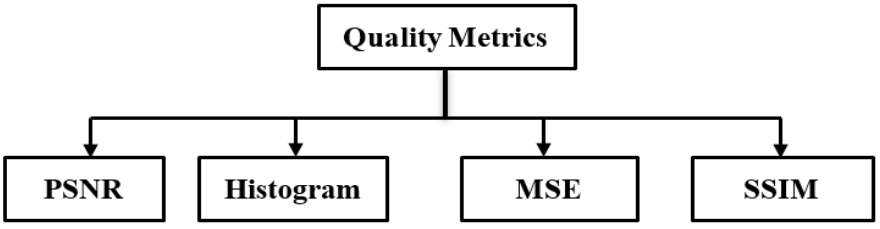

Fig. 10. Imperceptibility evaluation in steganography

However, it is important to note that there are other goals that must be met by any steganography or digital watermarking methods. These goals include payload capacity, security, and imperceptibility. (fig 10) shows three quality evaluation metrics (imperceptibility evaluation). More explanation about these measurements will be provide in the next chapter three. In [35], authors have proposed two new image steganography methods that are based on fuzzy logic. In this work, similarity is proposed to select the non- sequential least significant bits (LSB) of image pixels. In this study, the EEG and MR images of 22 epilepsy patients were tested by the proposed steganography methods. The Structural Similarity Measure is used and the value 0.999712 is obtained from SSIM. In [27], authors have used Structural Similarity Index Measure (SSIM) to evaluate the stego images produced in this method. different evaluation parameters have been used in this method.

Funding:

This study did not receive any form of external financial assistance or grants. The authors confirm that all research costs were covered independently.

Conflicts of Interest:

The authors have no conflicts of interest to disclose.

Acknowledgment:

The authors are sincerely grateful to their institutions for their continued support and trust, which greatly contributed to the completion of this research.

References

[1] G. Budiman and L. Novamizanti, "White Space Steganography on Text by Using LZW-Huffman Double Compression," *Int. J. Comput. Netw. Commun.*, vol. 7, no. 2, pp. 136A, 2015.

[2] K. L. Chiew and J. Pieprzyk, “Blind steganalysis: A countermeasure for binary image steganography,” in 2010 Int. Conf. Availability, Reliability and Security, pp. 653–658, 2010.

[3] P. Moulin and J. A. O'Sullivan, "Information-Theoretic Analysis of Information Hiding," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 563–593, Mar. 2003.

[4] P. Chen and H. J. Lin, "CNN-based Image Steganalysis Using Additional Data Embedding," *Multimedia Tools Appl.*, vol. 79, no. 1–2, pp. 1355–1372, 2023.

[5] Westfeld, "F5—A Steganographic Algorithm: High Capacity Despite Better Steganalysis," in *Information Hiding*. Springer, 2001, pp. 289–302.

[6] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Anti-Forensics of JPEG Compression," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1050–1065, 2011.

[7] K. U. Raju and N. A. Prabha, "A review of reversible data hiding technique based on steganography," ARPN J. Eng. Appl. Sci., vol. 13, no. 3, pp. 1105–1114, 2018.

[8] Gutub, A. Al-Qahtani, and A. Tabakh, "Triple-A: Secure RGB Image Steganography Based on Randomization," in *IEEE/ACS Int. Conf. Comput. Syst. Appl.*, pp. 400–403, 2009.

[9] H. R. Kanan and B. Nazeri, "A Novel Image Steganography Scheme with High Embedding Capacity and Tunable Visual Image Quality Based on a Genetic Algorithm," *Expert Syst. Appl.*, vol. 41, no. 14, pp. 6123–6130, 2014.

[10] M. F. Tolba, M. S. Ghonemy, I. A. H. Taha, and A. S. Khalifa, "High Capacity Image Steganography Using Wavelet-Based Fusion," in *ISCC 2004: Proc. Comput. Commun.*, vol. 1, pp. 430–435, 2004.

[11] R. G. Van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A Digital Watermark," in *Proc. 1st Int. Conf. Image Process. (ICIP 1994)*, Austin, TX, USA, pp. 86–90, Nov. 1994.

[12] Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, 2010.

[13] A. Kuznetsov, A. Onikiychuk, O. Peshkova, T. Gancarczyk, K. Warwas, and R. Ziubina, "Direct spread spectrum technology for data hiding in audio," Sensors, vol. 22, no. 9, p. 3115, 2022.

[14] M. Wu and B. Liu, "Data Hiding in Image and Video: Part I—Fundamental Issues and Solutions," *IEEE Trans. Image Process.*, vol. 12, no. 6, pp. 685–695, June 2003.

[15] J. Fridrich, M. Goljan, and R. Du, "Reliable Detection of LSB Steganography in Color and Grayscale Images," in *Proc. 2001 Workshop Multimedia Security: New Challenges*, Ottawa, Canada, pp. 27–30, 2001.

[16] Yahya, Steganography Techniques for Digital Images. Cham: Springer, 2019.

[17] N. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," *Computer*, vol. 31, no. 2, pp. 26–34, Feb. 1998.

[18] Westfeld, "Detecting Low Embedding Rates," in *Information Hiding*. Springer, 2002, pp. 324–339.

[19] Y. Wang, J. Doherty, and R. Van Dyck, "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images," *IEEE Trans. Image Process.*, vol. 11, no. 2, pp. 77–88, Feb. 2002.

[20] J. J. Chae and B. S. Manjunath, "Data hiding in video," in Proc. 1999 Int. Conf. Image Process. (ICIP), vol. 1, pp. 311–315, 1999.

[21] V. Himthani, V. S. Dhaka, M. Kaur, G. Rani, M. Oza, and H. N. Lee, "Comparative performance assessment of deep learning based image steganography techniques," Sci. Rep., vol. 12, no. 1, p. 16895, 2022.

[22] T. Filler and J. Fridrich, "Gibbs Construction in Steganography," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 705–720, Dec. 2010.

[23] S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, 2000.

[24] D. Megías, W. Mazurczyk, and M. Kuribayashi, "Data hiding and its applications: Digital watermarking and steganography," Appl. Sci., vol. 11, no. 22, p. 10928, 2021.

[25] P. Moulin and R. Koetter, "Data-Hiding Codes," *Proc. IEEE*, vol. 93, no. 12, pp. 2083–2126, Dec. 2005.

[26] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2706–2722, 2008.

[27] M. Kharrazi, H. T. Sencar, and N. Memon, "Image Steganography: Concepts and Practice," in *Proc. Int. Conf. Inf. Technol.: Coding Comput. (ITCC 2004)*, Las Vegas, NV, USA, pp. 404–408, Apr. 2004.

[28] C. V. Wright, L. Ballard, F. Monrose, and G. M. Masson, "Language Identification of Encrypted VoIP Traffic: Alejandra y Pablo or Alice and Bob?" in *Proc. 16th USENIX Security Symp.*, Boston, MA, USA, pp. 43–54, 2007.

[29] R. Chandramouli, M. Kharrazi, and N. Memon, "Image Steganography and Steganalysis: Concepts and Practice," in *Proc. Int. Workshop Digit. Watermarking (IWDW 2003)*, Seoul, South Korea, pp. 35–49, Oct. 2003.

[30] T. Pevny and J. Fridrich, "Merging Markov and DCT Features for Multi-Class JPEG Steganalysis," in *Proc. SPIE: Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505, pp. 03–13, Jan. 2007.

[31] Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, "HiDDeN: Hiding Data With Deep Networks," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2018, pp. 6579–6588.

[32] Sharma, A. Aggarwal, T. Singhania, D. Gupta, and A. Khanna, "Hiding Data in Images Using Cryptography and Deep Neural Network," *arXiv preprint arXiv:1912.10413*, 2019.

[33] B. Bai et al., "Information Hiding Cameras: Optical Concealment of Object Information into Ordinary Images," *arXiv preprint arXiv:2401.07856*, 2024.

[34] S. Nokhwal, M. Chandrasekharan, and A. Chaudhary, "Secure Information Embedding in Images with Hybrid Firefly Algorithm," *arXiv preprint arXiv:2312.13519*, 2023.

[35] D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, "A novel image steganography method via deep convolutional generative adversarial networks," IEEE Access, vol. 6, pp. 38303–38314, 2018.

[36] Y. Shi, X. Chen, and W. Chen, "A Markov Process Based Approach to Effective Attacking JPEG Steganography," in *Information Hiding*. Springer, 2006, pp. 249–264.

[37] S. Lyu and H. Farid, "Steganalysis Using Color Wavelet Statistics and Support Vector Machine," *SPIE Electron. Imaging: Security, Steganography, and Watermarking of Multimedia Contents VIII*, vol. 6072, pp. 607–618, 2006.

[38] J. Blackledge and A. Al-Rawi, “Steganography using stochastic diffusion for the covert communication of digital images,” 2011.
[39] T. Pevny, T. Filler, and P. Bas, "Using High-Dimensional Image Models to Perform Highly Undetectable Steganography," in *Proc. 10th Int. Workshop Inf. Hiding (IH 2008)*, Santa Barbara, CA, USA, pp. 161–177, 2008.
[40] C. C. Chang, M. H. Lin, and Y. C. Hu, “A fast and secure image hiding scheme based on LSB substitution,” Int. J. Pattern Recognit. Artif. Intell., vol. 16, no. 4, pp. 399–416, 2002.
[41] Kharrazi, H. T. Sencar, and N. Memon, "Benchmarking Steganographic and Steganalysis Techniques," in *Proc. SPIE: Security, Steganography, and Watermarking of Multimedia Contents VII*, vol. 5681, pp. 252–263, 2005.
[42] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image Hiding by Optimal LSB Substitution and Genetic Algorithm," *Pattern Recognit.*, vol. 34, no. 3, pp. 671–683, 2001.
[43] A. Kuznetsov, O. Smirnov, V. Zhora, A. Onikiychuk, and O. Pieshkova, “Hiding messages in audio files using direct spread spectrum,” in 2021 11th IEEE Int. Conf. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 1, pp. 414–418, 2021
[44] H. Yang, X. Sun, and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution," *Radioengineering*, vol. 18, no. 4, pp. 509–516, 2009.
[45] Cheddad, J. Condell, K. Curran, and P. McKevitt, "A Secure and Improved Self-Embedding Algorithm to Combat Digital Image Alteration," Signal Process., vol. 90, no. 1, pp. 43–52, 2010.
[46] R. Chandramouli and N. Memon, "Analysis of LSB Based Image Steganography Techniques," in Proc. 2001 Int. Conf. Image Process. (ICIP 2001), Thessaloniki, Greece, vol. 3, pp. 1019–1022, Oct. 2001.
[47] Y. J. Chanu, T. Tuithung, and K. M. Singh, “A short survey on image steganography and steganalysis techniques,” in 2012 3rd Nat. Conf. Emerging Trends Appl. Comput. Sci., pp. 52–55, 2012.
[48] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding—a survey,” Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, 1999.
[49] Hussain, M. Hussain, M. A. Gondal, and S. A. Malik, "Image Steganography in Spatial Domain: A Survey," Digit. Signal Process., vol. 18, no. 3, pp. 233–254, 2008.
[50] Y. Peng, D. Hu, Y. Wang, K. Chen, G. Pei, and W. Zhang, “Stegaddpm: Generative image steganography based on denoising diffusion probabilistic model,” in Proc. 31st ACM Int. Conf. Multimedia, pp. 7143–7151, 2023