ABSTRACT

Information hiding is a subject of study from past to present. Information hiding processes, called steganography, have been the focus of interest since the beginning of history because they are strategically interested in valuable information. In our study, the applications of Steganography with different fields from basic and primitive applications to today's technological applications have been studied. Image Steganography, Video Steganography, Audible Steganography, Text Steganography, Protocol Steganography were examined. Steganography techniques were examined under two headings. Protocol Steganography and Discrete Fourier Transform Technique, Discrete Cosine Transform Technique and Discrete Wavelet Transform Technique are examined. Spatial Domain Methods and Least Important Bits, Optimal Pixel Adjustment Procedure, Pixel Value Difference, Edge Based Data Embedding Method were examined.

General Terms

Discrete Fourier Transformation Technique, Discrete Cosine Transformation Technique, Discrete Wavelet Transformation Technique, Least Significant Bit, Optimum Pixel Adjustment Procedure, Pixel Value Differencing, Edge-Based Data Embedding Method.

Keywords

Steganography, Cryptography, Data hiding, Techniques of Steganography

1. INTRODUCTION

People have tried to hide elements and information they deemed valuable from past to present. To do that they used many different methods. Steganography is one of them. Also, Steganography is not a new working area [1]. The first use of steganography originated in 440BC. Demeratus the King of Sparta warned people with a message that is written on a wooden block and covered with a wax [2].

Another well-known steganography example belongs to the Greek nobleman, Histaes was the name; what he did was, something to remember. With the help of his trusted man, he successfully delivered the note he wants to send to his son. By cut the hair of the man he trusts, and tattooing the message to slaves head. Of course they did not do it directly, they wait for the slave’s hair to grow [3]. Steganography word is coming from Greece, named stegos grafia, meaning cover writing.

The methods of hiding information from the ancient Greek era to the present have undergone many improvements. In Nazi Germany, scientists developed a Microdot technique in the World War Two. Thanks to the Microdot method, information, especially photographs, has been lowered to the capacity of a post. A usual covered message was sent within an unsecured channel through one of the points on the paper, which was extremely difficult to detect [4]. Another invention well known in steganography was the code of Ave Maria.

Book containing a set of tables with a list of words per letter in each table. To encode the message, letters are being replaced by related words. The Encrypted message, if an order is used like having a table for every letter, each, it would look like a normal innocent prayer [5]. Steganography today, is mostly used on computer-related areas with digital datasets (Like video, image, text and audio can be represented as a digital data [6]).

Steganography makes secret message safely hidden, but cannot prevent the knowledge that two sides have been communicating [7]. Human senses like perception have not been trained to search for files containing confidential information [8] [9]. Therefore, steganography is one of the information hiding systems and there are some requirements for hiding different formats such as images, video, audio and text. These include high visual quality, high hiding capacity, robustness and safety [10]. There are three techniques of interconnected steganography, watermarking and cryptography. A watermark diagram changes the cover of the object (for example, the identity of the owner). In other words, adding a watermark improves the cover source using only additional data [11]. The robustness of the digital watermark diagram (i.e., protecting against malicious attacks like signal process operations) is crucial. Rather, steganography is used for confidential communication. An insensitive steganographic method replaces a cover object to hide a hidden message. Therefore, steganographic methods may conceal the existence of confidential communication [12]. Steganography video, audio, image and so on. As can be divided into different sections. Scientific methods are being used to hide a message within technical steganography, while linguistic steganography makes the message hide in carrier, explicitly. And all this is also classified as semagram or open codes. Semagram stores the data they use with symbols or signs. Visual semagram handles ordinary log physical materials to transmit a message; if the text is a semagram, small changes in font details to hide the message by changing the display of the carrier text with character plug-ins. Accessible codes hide the message in a reasonable carrier message that is not open to an innocent observer [13]. Steganography and Cryptography are the main areas of security and information hiding [14]. When the existence or suspicion of confidential information is disclosed, goal of steganography is partially lost. In this case, the power of steganography should be combined with cryptography [15]. Both sciences can come together to ensure good protection of the message [16].

Steganography helps us send information without changing or censoring the content of the information and retrieving it by the other party. Information about a place is also can be kept hidden with steganography. For example, some information sources, such as people's banking information, data from intelligence services, the secrets of the army, can be safely
Steganography can also be used to apply watermarks. Although the concept of watermarking is inevitably not steganography, various steganographic techniques are used to store watermarks in data. While steganography conceals information, watermarking only extends the cover source with additional information. Steganographic methods are being used to hide the desired information, as a visible change in images, video files, or audio files cannot be accepted due to the use of watermarks. In this context, e-commerce provides effective use of steganography. In existing internet shopping transactions, many users are protected by a user name and password without a real method to verify that the user is the actual cardholder. Biometric fingerprint scanning with uniquely crafted session IDs embedded in steganography and fingerprint images provides a very secure option to translate internet shopping benefit transaction verification. Steganography can also be used to make hidden changes associated with the currently used communication methods. Today's governments prefer those that supports and not, national security. Digital steganography is remarkable in both methods. Small or large businesses, it can be special trade secrets or information about a new product, may have similar concerns. The execution of important and delicate data is an additional application of steganography. In a possible encryption question, it is important that confidential listeners recognize it when they see the encrypted message [17]. Steganography allows the transmission of sensitive data in the history of confidential listeners without realizing the use of sensitive data. Steganography can be used in any way, from email to images on websites. Steganography can also be applied on Confidential Communication and Confidential Data Storage, Protection of Data Changes, Access Control System for Digital Content Distribution, Media, Digital Watermark, Database Systems and Internet Shopping [18]. Comparisons between shared cryptography, steganography, and watermarking is in Table 1.

| Criteria       | Cryptography | Steganography | Watermarking |
|---------------|--------------|---------------|--------------|
| Capacity      | High         | High          | Low          |
| Carrier Object| Text Files   | Any Media File| Digital Image|
|               | or Image     | Secret        | Audio        |
| Objective     | Protection   | Secret        | Copyright    |
|               |              | Communication | Protection   |
| Secret        | Text         | Any Type of   | Watermark    |
| Information   |              | File          |             |
| Secret Key    | Necessary    | Optional      | Optional     |
| Security      | High         | Very High     | High         |
| Visibility    | Yes          | Never         | May or May   |

2. STEGANOGRAPHY

Steganography is the combination of science and art for writing secret messages, so no one will know the existence of the message except the intended recipient [20] [21]. It aims to send a hidden message by placing it in a detectable way on multimedia such as digital image. When designing a steganographic algorithm, two key features, undetectability and embedding capacity, should be considered. There is a balance between the two features. Generally, the more bits you place in the cover image, the more detectable tracks appear in the stegonal image, which allows some steganalysis algorithms to attack. The process of hiding information with steganography can be explained like this; the data is first hidden in a cover file (video, image, text or audio) using a key transmitted to the recipient. Thus, once the message has been received, the recipient uses the same key to read the encrypted message and thus provides unopened transmission [22]. The steganography process can be described as follows:

![Steganography model](image)

**Fig 1: Steganography model [23]**

To understand above figure 1, the terminology of steganography is following:

A confidential message that is intended to be sent / transmitted securely is called a Message [24].

- Cover object: The Cover Object is the object to hide the data. It can be an image, video and Audio [24].
- Stego object: The object created after hiding the hidden message in the cover image. The Stego Object is then passed. At the recipient, the Stego object is side-processed to receive the message [25].
- Stego-key: The key used to encrypt and decrypt the confidential message [24].
- Embedding algorithm: The algorithm used to hide the message on the cover [24].
- Extraction algorithm: An algorithm used to display / open the message from the stego object [24].

Rules of steganography are the following:

- The information within the container should not be distorted significantly with the embedded data [26].
- Embedded data should avoid detection as much as possible [26].
- Embedded data must be directly encoded into the media to maintain data consistency [26].
- Embedded data should be resistant to modifications, manipulations and attacks as possible [26].
- Embedded data should use error correction codes [26].
- Embedded data should be self-clocked [26].

All embedded data must be recoverable, even if only part of the cover data is available [26]. The Steganography method used should have:

- Insensitivity: means that the steganographic system is not performed by the human eye. After embedding the steganographic message on the carrier element, the changes in the picture should not be noticed by the human eye. Because the human eye is sensitive to visual values such as brightness and blur, these values should be considered.
- Embedded Capacity: The capacity of the important message is not greater than the capacity of the carrier message. It is recommended that you do not exceed 51% of this maximum.
Otherwise, the element of invisibility, one of the elements of steganography, is pierced.

Robustness: Refers to the difficulty level that is required to destroy the embedded information while not damaging the cover object [27]. The attacker is in a situation where it is impossible to reveal the message even if the carrier detects a hidden message in the object. PSNR was generated from the initials of the Peak Signal to Noise Ratio. The higher this unit of measure, the safer our system.

Confidentiality: The removal of confidential information from the video should not occur without the prior consent of the intended user’s password [24].

Accuracy: The removal of confidential data must be accurate and reliable [24].

PSNR: is a metric that indicates the ratio of the maximum possible power of a signal to the power of noise on the signal. The signal represents the original data and the noise represents the compression-related error. When comparing compression codes, PSNR can actually be considered as an approach to human quality perception. The following formula calculates the PSNR:

\[
\text{PSNR} = 10 \log_{10} \left( \frac{\text{MAX}^2}{\text{MSE}} \right)
\]

The PSNR formula is calculated based on another measurement parameter, MSE, as shown. MAX1 is the highest pixel value available.

MSE (Average Frame Error): Defined as the mean square difference between the distorted image and the reference image. Low MSE increases the efficiency of the image steganography technique. MSE is calculated by pixel-by-pixel sum by summing the square differences of all pixels and dividing them by the total number of pixels [28]. According to the following formula, MSE tries to find a similarity:

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

In formula:
- The value I (i, j) represents the original carrier image.
- K (i, j) represents the steganographic image.
- m, n indicate the dimensions of the image.

As a result of the formula, if the MSE value is low, it indicates that the similarity is high and the algorithm is successful. In other cases, our algorithm is considered unsuccessful.

SNR (Signal to Noise Ratio): This is the ratio between signal strength and noise strength. Compares the level of the desired signal with the background noise level [28].

Steganography measures [24]:

Invisibility: A steganographic process cannot be caught with human eye because it cannot distinguish between the lid image and the stego image.

Load: Shows the amount of confidential information that can be encapsulated in the cover object. The embedding rate is given in unabbreviated measurement, like the quantity of the hidden message.

Statistical Attacks: The operation of extracting confidential information from a Stego object. The chosen method for steganography should be robust to statistical attacks.

Security: The security of a steganographic system is defined as non-guaranteed if statistical tests cannot distinguish between cover and stego-image.

Computational Cost: Required time lapse to run that selected algorithm, like counting the minimum iterations together supposing that each of it have fixed time to work.

Perceptual Quality: Increasing the load decreases the quality of the video, so the approach should be used in such a way that quality should remain intact to prevent insight.

3. TYPES OF STEGANOGRAPHY

Depending on the type of the cover object there are many proper steganographic techniques which are to obtain security.

3.1 Image Steganography

Image steganography, which is embedded in digital images, poses a threat to protecting sensitive information and gathering intelligence. A steganographic image scheme is a kind of steganographic system in which the confidential message is hidden in a digital image by some concealment methods [29]. Almost all file types can be used in digital image steganography, but due to their high degree of redundancy, images have proven to be best suited for embedding [30]. Many steganographic methods have been proposed to hide hidden data in an image [31]. In general, image steganography uses pixel densities to hide information [32]. An image for a computer is a collection of numbers that produces different light intensities in different areas of the image. This numeric representation creates a grid, and individual dots are called pixels. Most of the images on the Internet consist of a rectangular map of the image pixels (shown in bits) where each pixel is located and colored. These pixels are displayed horizontally, line by line [15].

Some images are monochrome and grayscale and use 8-bits per pixel. Normal digital color images are usually 24 bits, which means they use 24-bits per pixel to improve the quality of the image and improve color accuracy. All of these pixel bits are derived from three primary colors, red, blue, and green. Each primary color is represented by 8-bit data. This means that there can be 256 different amounts of red, blue, and green from a single 8-bit pixel. With these bit combinations we can create 16 million colors, which can define the human eye. The large size of the image can contain these many colors [33]. There are several ways to hide information in a digital environment. Traditional approaches include masking, least significant bit placement and filtering, unnecessary pattern coding, encryption and scattering, and transformations and algorithms [34].

The basic steps in image processing are as follows [35]:

Image retrieval: For digital image processing and compression.

Image preprocessing: An improved image acquisition process with a variety of techniques.

Image segmentation: Helps to divide the input image into sub-picture.

Image display: Convert input data to a computer-compatible form.
3.2 Video Steganography

Because video files consist of sounds and images, most of the methods used to hide data are applied in video formats. In the case of video, the steganography sender sends the confidential message to the recipient via the video sequence. The optional “K” can also be used when embedding the confidential message in the cover media to produce “stego-video”. The stego video is then transmitted to the receiver via the common channel. At the receiving end, the receiver uses the secret key in conjunction with the extraction algorithm to extract the confidential information from the stego object. The original cover video consists of frames represented by the total number of frames, Ck (m, n), and m, n are the row and column indexes of the pixels, respectively. The binary secret message indicated by mk (m, n) is modulated into a signal and the cover is embedded in the video medium. Mk (m, n) is defined in the same domain as host Ck (m, n). The stego-video signal is represented by the equation:

\[ S_k(m, n) = C_k(m, n) + a_k(m, n)M_k(m, n), \]

\[ k = 1, 2, 3, ..., N \]

\( a_k(m, n) \) is a scaling factor. To make it simple, it can be considered constant at all the pixels.

Video steganography measures imperceptibility, burden, security, statistical attacks, cost of computation and perceptual quality [36].

Insensitivity: indicates the visibility of the change in the cover environment. High Insensitivity means increasing the invisibility of small changes in the cover object. Today, steganalysis approaches are very clever to detect small changes. High Insensitivity has motivated research to design steganalysis resistant video steganography methods.

Load: or capacity refers to the amount of hidden messages that can be hidden within the cover media. Video is gaining popularity as a widely used cover media object due to its high insertion capacity and insertion efficiency.

Statistical Attacks: Attacks or methods applied to a stego object to obtain confidential or confidential information are known as statistical attacks. Steganography algorithm should be robust against statistical attacks.

Security: The most important part of steganography. The operation should have high security with minimum sensitivity to attacks. Various approaches have been proposed to secure the message in steganography.

Computational Cost: The timeout required to run the selected algorithm, such as counting the minimum iterations together, assuming each has a fixed time to run.

Perceptual Quality: Increased insertion capacity may cause deterioration of video quality or deterioration of the original content of the video. The video steganography approach should address the deterioration of video quality control.

3.3 Audio Steganography

When confidential data to be sent is embedded in digital audio, it is technical audio steganography. The method embeds the confidential message in WAV, AU and MP3 audio files [37].

Audio steganography consists of a carrier or message, password and audio file. A carrier known as a cover file that hides confidential information. Steganography requests that the encrypted message sent by the sender remain confidential. Text, image, sound or any confidential message to be sent to any file can be chimney. For the recipient, it is important that the corresponding decoding key is in the stego key, which he knows can extract the message from a cover file. A cover file that contains confidential information is known as a stego file. The storage process consists of two stages. The first step is to define the backup bits in a cover file. Unnecessary bits are detected at this stage. Unnecessary bits are bits that can be changed without destroying the quality or integrity of the cover file. In the second step of embedding hidden data in the cover file, the backup bits in the cover file are replaced by the bits of the hidden data. We may modify audio files so that the signal cannot be destroyed, including confidential information such as document images. With the Human Hearing System (HAS), information can be added to the music file in voice steganography.

HAS recognizes additional random noise and can also detect complexity in an audio file. But of course not perfect. Digital sound is created by converting from analog sound to digital field. One of the most common formats for sounds is Audio Interchange File Format (AIFF) and Windows Audio Visual (WAV). International Standards Organization There are also compression algorithms such as Moving Pictures Expert Group-Audio (ISO MPEG-AUDIO). When hiding data in an audio file, it must be checked whether the audio signal is between encoding and decoding. The change will take place in two areas we think. The first is in the storage medium or the digital signal, the other is the transmission path of the signal. After the confidential message is hidden, some methods are used to place the data in the digital voice. These methods range from the more powerful ways of concealing data that make a secure or powerful signal processing technique in placing information in the form of signal noise [38].

3.4 Text Steganography

Text steganography is one of the most common types of steganography. The main reason for the most common use is a practical method. However, this method has lost its importance because of its ease of decoding and less carrying capacity [39]. However, text steganography is protecting its place about being most challenging steganography technique. That is because text files have little unnecessary data to hide a message relative to an image or audio file [40]. The structure of the text documents is the same as that of the other files. That is, although our observations in different materials may seem different, the structure of the text documents is the same as that we observe. Therefore, instead of making changes to the document, we can change the structure of the document and hide the information. Confidentiality of information using text documents is based on very old times compared to other media. Today, many websites store information in electronic form [41].

Text steganography is generally divided into two categories: Linguistic Steganography. which is also divided into syntactic and semantic methods. Another category is Format steganography, and that is divided into categories of: word shift coding, open field coding, feature coding and line shift coding [42].

Format-based techniques are used in physical text formatting as a place where text can be hidden. This technique replaces existing data to hide steganographic text. Text placement, deliberate typographic errors distributed throughout the text, resizing fonts, are some of the form-based methods used in text steganography [29].
3.5 Protocol Steganography

Protocol Steganography is an array of rules used to manage communication (transmit) that is being known as protocol. UDP, TCP/IP are some of the protocols used for communication [43]. Protocol steganography is used to hide information, as with other steganography methods. However, the most important point here is that it uses any network protocol to transmit confidential information. In doing so, it also hides the protocol header information. In addition, protocol steganography retains the characteristics of both cover traffic and cover load. Protocol steganography uses two different approaches to embedding and extracting data, such as the traditional embedding process used and the evolutionary removal of information [44]. Some application methods of protocol steganography are [45]:

- Hidden channel communication using the “Flags” field: If the sender and receiver already know about the Maximum Transmission Unit (MTU) of their network, they communicate with each other using the DF flag bit of the IP header and interact with each other.
- Hidden channel communication using the ‘ID’ field: ‘16-bit identification field in the IPv4 header Ip is used to identify the packaged part of an IP datagram. If the datagram is not fragmented, this ID field can be used to embed the information specified by the sender.
- Hidden channel communication using the ISN (initial sequence number) field: The large 32-bit address space of the Sequence Number field can be used for a hidden channel. The sender creates a TCP / IP packet in which the hidden binary message can be placed over the Sequence Number field and can passively listen to the receiving party data. The Source Port and Checksum in the UMP header The Code field in the ICMP header is also the right candidate for Network Steganography Scope.

4. STEGANOGRAPHY TECHNIQUES

So far, different techniques have been proposed and research has been conducted in the field of recycled data hiding. Similarly, many strategies have been developed for hiding and visual encryption of recycled data [46]. Steganographic technique consists of embedding and extraction mechanism. Frequency (transformation) domain based techniques and spatial domain methods are two basic categories of image-based steganographic techniques [47].

4.1 Protocol Steganography

Frequency-based steganography methods are safer, but more complex and difficult to understand. In these methods, as in other pixel-based change methods, it aims to find and replace bits in the picture, but it does not make a difference in the whole picture. In short, logic is the same as other methods, but paths are more complex and less effective in the picture. In the DCT method, the picture is divided into 8x8 size matrices and 64 DCT coefficients are obtained from each matrix block. As with LSB logic, bits that do not include the brightness values of images and cause minimal distortion are bits and can be changed. For general information, image extensions symbolize the compression methods of images and are performed under the leadership of a group or organization, as in the JPEG extension. Although GIF images are one of the platforms used to store data in GIF format, it is possible to quickly find GIF images in a color histogram and allow data to be hidden, so it is an image extension commonly used in the JPEG data store. Because it has the most efficient compression method. In this method, playback at the values of the compressed images will distort the image. However, when changing the values with the least effect, it will be difficult to notice because the shade of the images may change rather than the brightness values. When histograms and entropy analyzes of the images are performed locally, it is possible to understand the confidentiality of the data by monitoring the distortions of the images. In the DWT method, the image values are converted to frequency values using the DCT logic and the data can be embedded according to the different characteristics of the different frequency bands. For example, in the high frequency band, hide too much data in the low frequency band [48].

4.1.1 Discrete Fourier Transformation Technique

DFT, Discrete Fourier Transform (Discrete Fourier Transform), created by Joseph Baptiste Fourier, is one of the most widely used and well-known methods in the analysis of time-based sequences. Fourier transform is used primarily in steganography to draw a space-based visual image to the frequency base. In other uses of Fourier, the disadvantage is that all time information is lost when switching from the time sequence to the frequency sequence. However, in steganographic practice, the time criterion is tolerable for us. There is no need to hide data because temporal surveys allow the examination of the moment of change in signals.

Like other transformations, the Fourier transform begins by drawing the field and the carrier, the image and the message on the frequency base. The image converted to frequency base is converted to 2x2 pixel blocks and the LSB logic changes the frequencies of the pixels and the message frequencies. After the entire message has been hidden, all frequency bands are converted back to the space-based pixels to obtain a steganographic image.

4.1.2 Discrete Cosine Transformation Technique

In all frequency-based transformation steganography, images are drawn from the spatial base to the frequency base. For this, a system called NxN is passed through a systematic process arrangement, which is usually transferred to the 8x8 matrix block. This processing device is called a converter. The differences between the transducer types are the signal types they use to process and study the picture and the mathematical formulation differences in the transducer mechanism. The mathematical formulation of DCT is as follows:

\[
F(u, v) = \frac{c(u)c(v)}{4} \sum_{i=0}^{2} \sum_{j=0}^{2} \cos \left( \frac{(2i + 1)u \pi}{16} \right) \cos \left( \frac{(2j + 1)v \pi}{16} \right) f(i, j)
\]

In the formula:

- The function \( F(u, v) \) is in the coordinate of a DCT \((u, v)\).
- The \( f(i, j) \) function uses the pixel values of a DCT \((i, j)\) shows.

In Discrete Cosine Transform, cosine signals are used, and their pictures are transformed from the spatial base to the frequency based matrix structure by the cosine converter.
4.1.3 Discrete Wavelet Transformation Technique

Discrete Wavelet Transform is a method used for image and data compression. This method divides the main signal, which we call wavelet, into mathematical small waves in time and frequency bands and processes in these bands. The advantage of these wavelets over other methods is that they allow us to investigate small but small fluctuations that may affect the result. As with the Discrete Fourier Transform, it does not examine the signal in a single frequency band, but it can be examined at smaller and more detailed wavelets and allows us to make better observations. As with the Discrete Cosine Transform, DWT is applied and the carrier image and message are converted to frequency. The DWT carrier divides the image into two frequency waves, high and low frequency. High frequency quality is a characteristic frequency. If less data is to be stored, it is ideal for storing data. The human eye may detect distortion of the carrier image due to excessive changes in this region. Another possibility is to select a low-band carrier for intensive information storage. This section contains a lot of data, so we can store a lot of data. Of course, capacity values should not be exceeded and deteriorations should be observed. However, selecting the low frequency of the conveyor belt has some disadvantages. They are not as robust as high frequencies. Because storing data at high frequencies is a very discernible process, changes in this region cause changes in energy values. Pictures are set to the lowest energy level according to JPEG standards. In this set of pixels, any change in the matrix creates a change that will exponentially affect the average energy of the image, and these changes can be easily discovered in histogram and entropy analyzes.

The wavelet function used in the DWT algorithm is as follows:

\[ W_{jk}(t) = 2^{\frac{j}{2}} W(2^{-j}t - k) \]

Where, a continuous function, 
\( j, \) scale parameter, 
\( k \) is the shift parameter.

4.2 Spatial Domain Methods

In the Spatial Domain, image-based steganography, the main purpose is to change the bits of the hidden message generated according to the ASCII table of the pixels of the carrier image. If the image to be used is a black and white image, it is recommended that we store data at each byte. If the carrier image is a color image, Red-Green-Blue will have a 3-byte, 24-bit change block according to the three primary color rules, thus expanding our storage space. The advantage of this method is that it is easy to understand and easy to apply, and its disadvantage is that it can be easily found by a histogram or entropy analysis if not used skillfully. Skillful use means that the byte structure is dominant and noise can be adorned. As is known, the first and last bits in a byte block are the Most Significant Bits, the MSB and the Least Important Bits, LSB. As the name implies, the LSB must be replaced with message bits. The exception here is that some bytes may be related to the brightness values of the image. The human eye is compassionate and successful in distinguishing brightness, no matter how unsuccessful the details are. When making some changes, care should be taken not to change the brightness values. In recent years, there have been efforts to strengthen many systems related to the choice of picture channels and the displacement of lice. As a result of these studies, it was found that randomness and variation of adjacent values were more beneficial with functions such as zero decay and chaotic sorting, and the margin of error and reliability increased.

4.2.1 Least Significant Bit

A well-known steganographic method is the least significant bit (LSB) substitution [49]. Steganography application hides info by reinstating only the least significant bits (LSB) of an image with the bits in the file to be concealed. Figure 2 shows an example of the bit substitution.

![Example of Least Bit Substitution](image1)

**Fig 2:** Example of Least Bit Substitution [50]

The idea is to store the information in the first bit of the color (RGB) component of each pixel. In the worst case, the decimal value is different from a value not seen by the human eye. In practice, it should start using the second bit, even if it will store all data in the first bit of each pixel. The higher the repository data in an image, the more it will be detected. Figure 3 represents 2-bit LSB [51].

![Explanation of LSB Technique](image2)

**Fig 3:** Explanation of LSB Technique [51]

Mathematical representation of LSB following equation is like [52];

\[ x_1 = x_i - x_i \ mod \ 2k + mi \]

In this equation;
\( x_i \) stegetographic image i num
\( xi \) represents the pixel of the carrier image to be modified,
\( mi \) is reliable data in the first block,
The number k in the mode value in the formula indicates the number of operations to be changed in the LSB.

All of these extracted bits or inference operations are to provide the most right value changes in k value. Mathematically, the message is as follows [52];

\[ mi = x_i \ mod \ 2k \]
4.2.2 Optimum Pixel Adjustment Procedure
Distortion caused by the LSB substitution method is minimized by OPAP (Optimal Pixel Adjustment Procedure). After the data is safely hidden, the pixel value is set in the OPAP method. Therefore, without disturbing confidential data, the quality of the stego image is improved [53].

4.2.3 Pixel Value Differencing
The PVD, Pixel Value Difference, is capable of embedding more data on the carrier image than the algorithm LSB method. In doing so, it performs pictures without leaving traces on the image and making high-resolution quality images. This is an improved method for storing data in 8-bit White & Black images. In this method, the carrier moves from the upper left corner of the image to the zigzag point on the entire image. Images divide into arrays of pixels that do not match. Since the first two of these blocks are smooth, the data is not embedded in the smoothness blocks in each row. However, the differences between these pixels and other pixels are measured. The higher the difference, the more data can be embedded in the blocks in this row.

4.2.4 Edge-Based Data Embedding Method
The edges of a digital image can bury or hide more confidential data without compromising image quality, because the distortion of the edges is not easily perceived by the human eye. Therefore, the edge detection method is created. Various edge detectors have been proposed to detect edges in the digital image. After detection of the edges, hidden data was embedded in the edges using an LSB-based spatial field steganographic technique. Edge detection is a method of identifying points in an image where the brightness of the image has sharp or formal discontinuities. Figure 4 shows several approaches to edge detectors [54].

Fig 4: Various Edge Detector Methods, (a) Cover Image, (b) Sobel Method, (c) Prewitt Method, (d) Roberts Method, (e) Canny Method [54]

5. CONCLUSION
In this paper, we provide an overview of different steganography techniques including spatial and frequency based steganography applications. We briefly describe the type of steganography method that extends to spatial application methods such as LSB, PVD, OPA and edge-based embedding methods, as well as frequency application methods such as DFT, DCT and DWT. Then, we explained the variability of steganography in multimedia content such as images, audio, video and text, depending on the field of application. Finally, we have described the important types and classifications of information starting from steganography to the present day in the literature.

6. ACKNOWLEDGMENTS
We would like to thank the reviewers for all useful and instructive comments on our manuscript.

7. REFERENCES
[1] L. M. Marvel, C. G. Bonculet, and C. T. Retter, “Spread spectrum image steganography,” in IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075-1083, Aug. 1999.
[2] M. Kumar, and A. Rani, "A Short Survey on Steganography", International Journal of Computer Science and Technology, 4(1), 181-185, 2013.
[3] Internet: J. Silman, Steganography and Steganalysis: An Overview, SANS Institute, https://www.sans.org/reading-room/whitepapers/steganography/steganography-steganalysis-overview-553, 16.12.2001.
[4] T. Jamil, “Steganography: The art of hiding information is plain sight”, in IEEE Potentials, 18(01), 192-194, 1999.
[5] R. Doshi, P. Jain, and L. Gupta, “Steganography and Its Applications in Security.” International Journal of Modern Engineering Research (IJMER) 2(6), 4634-4638, 2012.
[6] D. C. Wu, and W. H. Tsai, "A steganographic method for images by pixel-value differencing,” Pattern Recognition Letters, 24(2003), 1613–1626, 2003.
[7] V. O. Waziri, A. Isah, A. Ochoche, and S. M. Abubakar, "Steganography and Its Applications in Information Dissemination on the Web Using Images as Security Embedment: A Wavelet Approach,” International Journal of Computer and Information Technology, 1(2), 194-202, 2012.
[8] S. Naskar, A. S. Gaya, and S. K. Bandyopadhyay, "Text Steganography an Approach.” Journal for Research, J4R, 4(6), 1-4, 2018.
[9] S. A. Laskar, and K. Hernachandran, “Steganography Based on Random Pixel Selection for Efficient Data Hiding,” International Journal of Computer Engineering and Technology (IJCET), 4(2), 31-44, 2013.
[10] S. Y. Shen, and L. H. Huang, "A data hiding scheme using pixel value differencing and improving exploiting modification directions." ELSEVIER, ScienceDirect, Computers & Security, 48, 131-141, 2015.
[11] N. Singh, "Survey Paper on Steganography.” International Refereed Journal of Engineering and Science (IRJES), 6(1), 68-71, 2017.
[12] D. Kieu, and C. C. Chang, "A steganographic scheme by fully exploiting modification directions." ELSEVIER, ScienceDirect, Expert Systems with Applications, 38(2011), 10648-10657, 2011.
[13] F. Kabadvand, "New Methods for Text Steganography." International Journal of Scientific Research in Science, Engineering and Technology, IJSRSET, 1(5), 383-385, 2015.
[14] P. Chandarana, and P. Ahirao, "Advanced Image Steganography.” International Journal of Innovative Research in Information Security (IJRIS), 7(5), 471-474, 2018.
[15] Internet: T. Morkel, J. H. P. Eloff, and M. S. Olivier, "An overview of image steganography.” Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, South Africa, http://repository.rootme.org/St%C3%A9ganographie/EN/%20Image%20Steganography%20Overview.pdf, 01.06.2005.
[16] D. H. Jagadeesha, Y. Manjula, and M. Z. Kurian, “FPGA Implementation of X-Box Mapping for an Image Steganography Technique.” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, IJAREEIE, 2(6), 2548-2554, 2013.

[17] A. Kumar, and K. Pooja, "Steganography- A Data Hiding Technique." International Journal of Computer Applications, 9(7), 19-23, 2010.

[18] T. Vyas, and A. Sharma, “Survey Paper on Steganography.” International Journal of Engineering Sciences & Research Technology, IJESRT, 5(12), 706-708, 2016.

[19] B. Chandel, and S. Jain, “Video Steganography: A Survey,” IOSR Journal of Computer Engineering (IOSR-JCE), 18(1), 11-17, 2016.

[20] A. A. Chincholkar, and D. A. Urkude “Design and Implementation of Image Steganography,” Journal of Signal and Image Processing, 3(3), 111-113, 2012.

[21] S. Natanj, and S. R. Taghizadeh, "Current Steganography Approaches: A survey.” International Journal of Advanced Research in Computer Science and Software Engineering, IJARCSS, 1(1), 1-8, 2011.

[22] N. Singh, and V. K. Yadav, “Trends in Digital Video Steganography: A Survey.” International Journal of Computer Applications, 169(7), 6-18, 2017.

[23] S. Singh, P. Singh, R. Garg, and P. K. Mishra, "Some Observations of Image Steganography on Implementation of Least Significant Bit Technique with Mapping Method.” International Journal of Advanced Research in IT and Engineering, IJARIE, 2(2), 97-105, 2013.

[24] N. Singh, "Survey Paper on Steganography.” International Refereed Journal of Engineering and Science (IRJES), 6(1), 68-71, 2017.

[25] R. M. Kirandeep, “A Comparative Analysis of Steganography Techniques.” The International Journal of Engineering and Science (IJES), 5(4), 67-70, 2016.

[26] M. I. S. Reddy, M. P. Reddy, and K. S. Reddy, “Different Medias of Steganography- An Emerging Field of Network Security.” International Journal of Computer Science and Information Technologies, (IJCST), 3(2), 3517-3522, 2012.

[27] C. P. Sumathi, T. Santanan, and G. Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding.” International Journal of Computer Science & Engineering Survey (IJCES), 4(6), 9-25, 2013.

[28] J. Surana, A. Sonsale, B. Joshi, D. Sharma, and N. Choudhary, "Steganography Techniques," International Journal of Engineering Development and Research, IJEDR, 5(2), 989-992, 2017.

[29] V. Rabara, and A. Goswami, “A Survey of Image Based Steganography.” International Journal of Computer Engineering and Sciences (IJCES), 1(2), 1-4, 2015.

[30] Z. Al-Omari, and A. T. Al-Tani, “A Survey on Digital Image Steganography.” 7th International Conference on Information Technology (ICTI), pp.109-115, 2015.

[31] H. C. Wu, N. I. Wu, C. S. Tsai, M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods.” IEE Proc.-Vis. Image Signal Process, 152(5), 611-615, 2005.

[32] M. Hussain, and M. Hussain, "A Survey of Image Steganography Techniques.” International Journal of Advanced Science and Technology, 54(1), 113-124, 2013.

[33] Internet: B. Sharonyah, “Image steganography.” Faculty of Information Technology University of Moratuwa Sri Lanka, https://www.coursehero.com/file/38840672/Computer-Science-114128Ppdf/, 2019.

[34] S. Kaur, A. Kaur, and K. Singh, "A Survey of Image Steganography." International Journal of Computer Applications Technology and Research, 3(7), 479-483, 2014.

[35] R. Bhuvanya, K. Vijayalakshmi, S. Uma, and A. Suresh, “Secret data sharing using steganography and image processing.” International Journal of Engineering & Science, 7(1.7), 100-104, 2018.

[36] B. Chandel, and S. Jain, "Video Steganography: A Survey." IOSR Journal of Computer Engineering (IOSR-JCE), 18(1), 11-17, 2016.

[37] Rakhi and S. Gawande, "A Review on Steganography Methods." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, IJAREEIE, 2(10), 4635-4638, 2013.

[38] N. Kaur, and S. Behal, "Audio Steganography Techniques-A Survey." International Journal of Engineering Research and Applications, IJERA, 4(6), 94-100, 2014.

[39] A. Koyun, and H. B. Maci, "Generating a stego-audio data using LSB technique and robustness test." Journal of Engineering Sciences and Design, 6(1), 87-92, 2018.

[40] S. Agarwal, and J. S. Bhist, "Data hiding in digital image processing using cryptography and steganography." International Research Journal of Engineering and Technology, (IRJET), 3(5), 1600-1603, 2016.

[41] M. Shirali-Shahreza, and M. H. Shirali-Shahreza, "Text Steganography in SMS.” International Conference on Convergence Information Technology (ICCIT), IEEE, Gyeongju, 2007, pp. 2260-2265.

[42] H. Singh, P. K. Singh, and K. Saroha, “A Survey on Text Based Steganography,” Proceedings of the 3rd National Conference; INDIACom, 2009.

[43] C. Gayathri, and K. Kalpana, "Study on Image Steganography Techniques.” International Journal of Engineering and Technology (IJET), 5(2), 572-577, 2013.

[44] M. Kumar, and A. Rani, "A Short Survey on Steganography.” International Journal of Computer Science and Technology, IJCST, 4(1), 181-185, 2013.

[45] D. Rana, "A Review paper on Steganography Techniques.” International Journal of Modern Trends in Engineering and Research, (IJMTER), 1(6), 74-82, 2014.

[46] A. Singh, and C. Verma, "Image Steganography Techniques: A Review.” International Journal of Engineering Sciences & Research Technology, IJESRT, 7(7), 18-23, 2018.

[47] K. M. Jeevan, and S. Krishnakumar, “Image hiding technique using a pseudo hexagonal structure approach.”
International Journal of Computers and Applications, 41(5), 359-366, 2018.

[48] F. Sönmez, F. Takaoğlu, and O. Kaynar, "Ideal Steganography Scenario: Calculation of Capacities of Carrier Images, OPA Method in Frequency Based Steganography." ACTA INFOLOGICA, 2(1), 12-21, 2018.

[49] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems." IEEE Transactions on Information Forensics and Security, 3(3), 488-497, 2008.

[50] Internet: F. Zioner, LSB-Steganography, https://www.kitploit.com/2018/02/lsb-steganography-python-program-to.html, 2018.

[51] R. Kaur, and Pooja, "Steganography based image compression." International Journal of Advanced Engineering, Management and Science (IJAEMS), 2(6), 685-690, 2016.

[52] F. Takaoğlu, Performance Analysis in DWT and DCT Steganography, Master's Thesis, İstanbul Aydın University, Graduate School of Natural and Applied Sciences, 2016.

[53] D. V. Patil, and S. Dubey, "Review Paper on Image Steganography." International Journal of Research in Computer Applications and Robotics, IJRCAR, 2(6), 35-40, 2014.

[54] S. U. Maheswari, and D. J. Hemanth, "Different methodology for image steganography-based data hiding: Review paper." International Journal of Information and Communication Technology, 7(4/5), 521, 2015.