Kafrelsheikh Journal of Information Sciences ISSN (Online): 2535-1478, ISSN (Print): 2537-0677 Volume 3, Issue 2, 2022, PP. 1-23

A Survey Paper of Information Hiding by Using Steganography Techniques

Abdelmgeid Amin Ali[1], Waled Makram Mohamed[1], Mentllah Essam Hassan Sayed[1]

Faculty of Computers and Information, Minia University

Abstract:

The practice of hiding communication by enclosing data in other data is known as steganography. There are many different carrier file kinds available, but due to their popularity on the Internet, digital photographs are the most popular. From ancient times to the present, the protection of secret information has always been a major concern. The basic goal of steganography is to hide the existence of the message so that an attacker cannot detect it. To incorporate hidden information, any type of cover item, such as text, image, or video, can be used. In this paper, a brief overview of steganography which is one of the main branches of information hiding is explained and covers its primary forms, categorization, and uses.

Keywords: Steganography, Information Hiding, Cover image, Data hiding, Coverless image steganography.

1. Introduction:

Data transfer is becoming faster and easier as communication technology advances. As a result, it is simpler for unauthorized users to intercept data transmissions and get access without authorization. Therefore, maintaining the privacy of data while it is in use or being transmitted is a crucial concern. Two important information security methods for preserving data confidentiality are data encryption and data hiding.

1.1 Information Security

Information security, sometimes abbreviated to (infosec), is the protection of data and information systems against unauthorized access, use, disclosure, interruption, alteration, deletion/destruction, or corruption. Maintain its secrecy while ensuring its integrity and availability of information assets. Information can be in any form, such as digital or analog, tangible (like paperwork) or intangible (like knowledge) [1, 2, 3].

Confidentiality, Integrity, and Availability, often known as the (CIA) triad and depicted in Figure 1 [2, 3, 4], serve as the cornerstones of data protection laws and industry standards for information security.

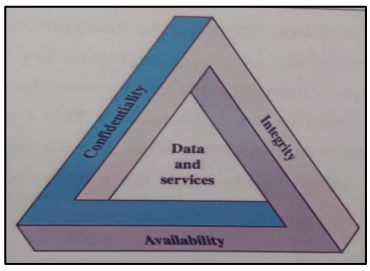

Figure (1) CIA Triad of Security Services

Confidentiality: The hiding of information or resources, as well as protection from disclosure or exposure to unauthorized users or systems, is known as confidentiality. When information or resources are confidential, they are hidden from everyone save the systems or individuals who have been given permission and privileges to access them [3, 6]. When unauthorized users or systems get access to or can view information, confidentiality has been violated.

Integrity: When data stays in the same condition as when it was last accessed by a valid user, it is said to have integrity. Information integrity assures that data won't be accessed, modified, altered, destroyed, or otherwise interfered with by unauthorized people. Information can become corrupted while being sent or stored [2, 3, 6].

Availability: When something is available, it may be accessed when needed, including data and other crucial resources. The ability to obtain and receive information in the desired format and within a fair amount of time without hindrance or interference, in other words, is referred to as availability [6]. Secret communication can be secured in two main ways as shown in figure (2) [11]. Cryptography and Information hiding. They play a significant role in maintaining secrecy. Information is encrypted by cryptography to render it unintelligible, and a cryptographic key regulates access to the encrypted data. Data hiding covers both the existence and the substance of data. No one can argue that information protection is increased by information hiding.

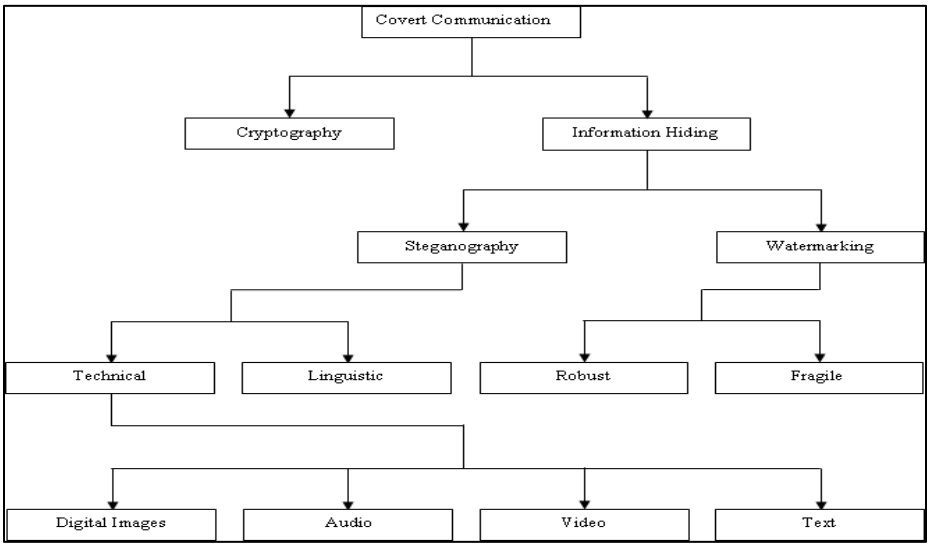

Figure (2) Covert communication classification [11]

1.1.1 Cryptography

The study and application of methods for secure data protection and communication are known as cryptography. When exchanging information with external parties known as adversaries, data in cryptography might shift into unintelligible forms [7, 8].

Ordinary data (known as plaintext) is transformed through the process of encryption into an incomprehensible form (called ciphertext). In contrast, decryption recovers the original plaintext from the incomprehensible ciphertext [2]. A cypher is a set of algorithms that produce both encryption and reversal decryption. The ciphertext must be encrypted and decrypted using a secret key, which is preferably only known by the communicants. As seen in Figure 3, these algorithms and keys govern how a cypher functions.

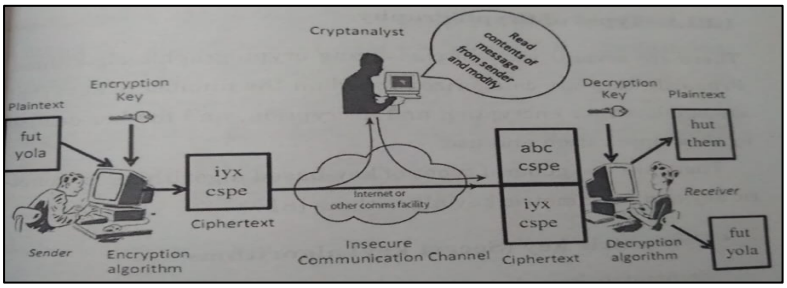

Figure (3) Covert communication classification [9]

The sender uses a key to encrypt plaintext into ciphertext. The sender gives the intended recipient the key (using a secure channel). The original data is eventually decrypted by the recipient using the key and the ciphertext.

Modern cryptography places a strong emphasis on several information security principles, including data secrecy, data integrity, authentication, and non-repudiation [10]:

- Data Confidentiality: Making sure that no one else can interpret the information than the intended recipient.
- Data Integrity: Ensuring that the information received hasn't been altered from the state in which it was sent by an authorized organization.
- Authentication: The sender and receiver can verify each other's identities and the information's origin and destination.
- Non-repudiation: The sender is unable to later retract the information he or she created or transmitted.

1.1.1.1Types of Cryptography

Symmetric, asymmetrical, and hash encryption are the three main categories of encryption techniques.

- Symmetric Encryption

Conventional cryptography, symmetric encryption, and secret-key encryption are all terms for symmetric key encryption. It is a single-key encryption where you encrypt the plaintext with one key and decrypt the cypher text using the same key. The Figure illustrates how simple and quick symmetric encryption is (4):

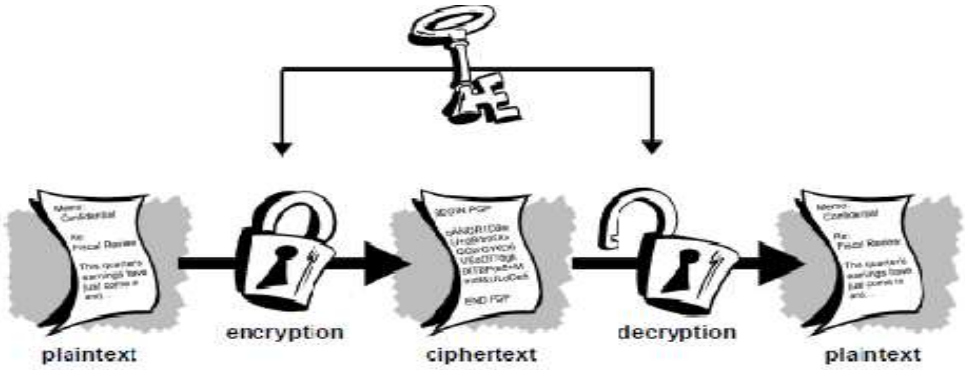

Figure (4) Conventional Encryption

- Asymmetric Encryption

The encryption method known as asymmetric encryption is another form. A public key and a private key are the two keys it employs. Only using the other key can anything encrypted with one key be unlocked.

- Hash Encryption

Finally, the hash algorithm. The plaintext message has undergone an irreversible, one-way modification. Any size of plaintext can be input into a hash, which yields a smaller, irreversible output of a defined length. It is impossible to generate the original plaintext message from the encrypted text. Because there is no key, hashes help store passwords and digital signatures [12].

1.1.2 Information Hiding

With the advent of the Internet and the quick development of information technologies, digital material has become a necessary component of daily life. The internet is used for the majority of information sharing and communication. Information security is essential due to the rising unlawful access to private data. So reducing the chances of information discovery during transmission is currently a major concern [13]. The term "steganography" is derived from two Greek words "steganos", which means "cover," and "graphia", which means "writing," and generally means to hide data and information from view [13]. Techniques for hiding information have recently grown in significance in some application fields. When used in this context, the word "hide" can mean both making the information undetectable (as with watermarking) and keeping its presence a secret (as in steganography) [14]. So, information hiding could be classified into two classes as shown in figure 5 [39]

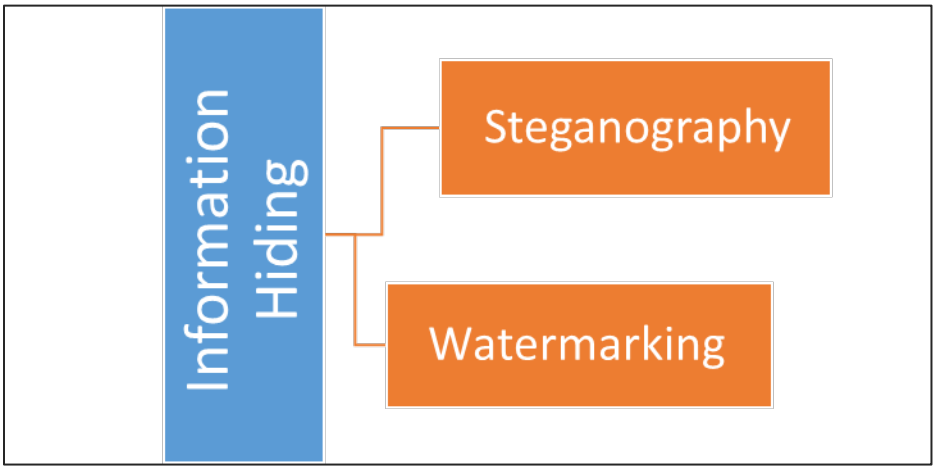

Figure 5: Information Hiding Classification

The idea of information hiding is nothing new in history. As early as ancient Greece there were attempts to hide a message in trusted media to deliver it across the enemy territory. In the modern world of digital communication, there are several techniques used for hiding information in any medium. One such technique is steganography [15] in which digital media mainly digital images are used as a medium for hiding information and the information in the form of text, digital image, video, or audio file may be used as secret messages. The basic goal of steganography is to improve communication security by replacing any extraneous or unnecessary pixels and adding a secret message to a digital image. Recently, it has become more significant in a wide range of application

domains, especially for military and intelligence organizations that require secret communications. Computer systems can store digital images as an array of a finite number of components, each of which has a specific location and value and is most commonly referred to as a pixel. Each pixel in a 24-bit color picture consists of the colors red, green, and blue (RGB). Three bytes are used to represent each pixel to convey the strength of these three colors (RGB). In contrast to cryptography, which is more concerned with protecting message content, steganography is more concerned with hiding the existence of communication. [16].The term "cryptography" comes from the Greek words "kryptós," which means "hidden," and "gráphein," which means "to write." It is the study of ways to transform information from its usual, understandable structure into an impenetrable format. The primary goal of encryption is to present messages in an unintelligible format to those who lack special understanding. Both steganography and cryptography can be used to shield information from unauthorized individuals, however, neither method is infallible and can be broken. The goal of steganography is partially undermined if hidden information is suspected to exist or even discovered [16]. The same objective is accomplished by steganography and cryptography in various ways. Encryption converts the data into an unintelligible form known as a cypher so that a recipient who is not intended cannot decipher its intended meaning. Steganography, on the other hand, aims to make it so that the data cannot be detected by an unintentional recipient [17]. Information security has been increased in the modern period by combining steganography with other techniques like cryptography. Steganography is utilized in many different domains, such as copyright, to prevent e-document forgery in addition to being used for covert information exchange. There have been numerous steganographic methods for still photos presented over the last ten years. A method for a 24-bit color image is then created based on the LSB technique to enhance the stego-image quality of the color image. When an organization wants to prevent data from leaking into the public domain, digital watermarking is a widely used technique. When a business has a direct fiduciary relationship with its consumers and must safeguard their personal information, it is very important [18]. Digital watermarking is a technique for offering defense against any manipulation or alteration [19, 20]. It authenticates and secures digital content. Signals and data are inserted into the original media content as part of the digital watermarking process. The embedded data is then uncovered and retrieved to reveal who the true owner of the digital media is.

2. Literature Review

Data and information are hidden in [21] in digital image format since the internet is the primary market for it. Many different ways have been created for data hiding, some of which are simple while others are a little more laborious. Each technique has its advantages, applications, and restrictions. The primary objective of this essay is to provide an overview of steganography, along with information about its demand, benefits, and methodologies. This study also makes an effort to determine which steganography approaches are more beneficial and what are required of them. It also illustrates which applications will be more compatible with each steganography methodology.

In [22] Combining cryptography and steganography techniques, a methodology for securing hidden handwritten signatures have been devised in this article. By combining the Blowfish encryption method with modified Least Significant Bit (LSB) steganography to hide the output encryption in a

cover picture, this methodology provides multi-level security. The ciphered data is randomly placed in the last 3-bits of the red and blue planes of the colored cover image, as well as the last 3-bits of the grey cover image after the handwritten signature is encrypted. Cover images in gray-scale and colorful picture formats are used to hide differing amounts of sensitive data.

The improved LSB method for 24-bit color images is shown in [23] to be superior to the LSB technique for 8-bit color images. Before comparing their results, the peak signal-to-noise ratio (PSNR), mean squared error (MSE), and histogram analysis are calculated for the LSB approach for both 8-bit and 24-bit color images. The improved LSB method for 24-bit color images is then discussed. The hidden image's MSB was integrated into the cover image's LSB using the LSB algorithm. Two approaches are provided for the 24-bit color image. Firstly, 2 MSB of the secret image are used in place of the final 2 LSB of each plane (red, green, and blue) of the cover image. In the second technique, the first MSB of the secret picture is substituted for the last LSB of each red plane, followed by the following two MSBs of the secret image for each green plane, and the next three MSBs of the secret image for each blue plane. This indicates that a total of 6 bits of a secret image can be hidden in a 24-bit color image. According to experimental findings, in the case of a 24-bit stego-image, the original cover-image cannot be visually distinguished. The LSB substitution approach is described in [24] as the most straightforward method for hiding data within a picture. The LSB replacement method overwrites the low-order bit (LSB) of each byte in a cover picture using the binary representation of hidden data. In the existing method, there used the cover image of 256*256 and split the image into four parts then they are using LSB substitution and pixel indicator in a zigzag manner. They achieved a stego image with PSNR of greater than 50 DB and also the MSE value of the existing method is low. In the proposed method, we are going to flip the image into 8 parts. By using pixel indicator and LSB substitution method we are trying to achieve the stego-image having greater than 60 DB PSNR value and lower MSE value. A simple LSB substitution-based data hiding method is proposed in [25]. The picture quality of the stego - image can be considerably enhanced with minimal additional computing cost by using an optimum pixel adjustment technique to the stego image created by the straightforward LSB substitution method. It is determined what the worst-case mean-square error is between the cover and stego images. According to experimental findings, there is no visual difference between the stego image and the original cover-image. In comparison to earlier work, the obtained results demonstrate an improvement.

In [37], additional security is provided by using a two-layer defense system that combines encryption and information hiding. The PSNR and MSE parameters are used to gauge the security level of the hidden image. Low MSE and high PSNR values are preferable in stenography. In terms of PSNR and MSE, the proposed study enhances the outcome of earlier work. Add the cryptographic steganography procedure as well to strengthen and safeguard image security.

In [38], at the receiver's end, compression and steganography are switched. This work has several issues, which makes it an interesting topic to pursue. The most crucial step in this process is by far choosing the appropriate steganography and image reduction technique. The suggested approach, which combines compaction with image steganography, performs more effectively in terms of peak signal-to-noise.

3. Basics and background

3.1 History of steganography

The history of steganography dates back to ancient times. Around 440 B.C., Herodotus is the first author to discuss steganography and provides examples in several of his writings. A man by the name of Harpagus killed a hare and hid a note inside it. He disguised himself as a hunter and sent it that way. [26]. Herodotus mentions Histaeus, who shaved the head of a trusted slave, tattooed a message on his scalp (see figure 6[27]), waited for his hair to regrow, and then sent the slave on his way. The slave could safely travel to the message's recipient with the message hidden [27].

Figure 6: A Message on a Scalp

Herodotus also records the account of Demeratus, who informed Sparta of the Persian Great King Xerxes's intention to invade Greece. To write his warning on a wooden writing tablet, Demeratus scraped the wax off of its surface. The tablet was then covered with a fresh layer of wax to make it appear like a blank writing tablet that could be safely transported to Sparta without raising any red flags [27].

Another suggestion he made was to place tiny pinpricks over the letters of a neutral message. This method was employed throughout the Renaissance, and the Germans even poked letters in magazines during World War 1. It then needed to be cooked to reveal the plaintext letters [26].

The Chinese also employed a somewhat distinct type of steganography. They employed a device known as a La wan, which is a small piece of silk with writing on it. A ball of wax made out of the silk was afterward sent from the sender to the recipient. Several successful steganography techniques were employed during World War I. A Turning Grille was the name of one technique. It resembled a typical grille in appearance, consisting of a square cardboard sheet separated into cells, some of which had holes punched into them. The encoder wrote the first series of letters first, then rotated the grille 90 degrees and wrote the second sequence, and so on, rotating the grille between each sequence [28].

François Bacon described modern steganographic techniques. He encoded binary representations of characters in his compositions using italic or regular fonts. The cover work's five letters may each carry five bits. This strategy was somewhat ambiguous due to the diversity of the sixteenth-century type [28].

Recently, hundreds of stenographic goods have become available for download on the internet. Some of these tools employ robust encryption techniques that encrypt the covert messages to add an extra level of protection if the steganographic approach is compromised [28].

3.2 The Basic Steganography Model

The basic model for steganography is shown in figure 3 [27]. The model illustrates the fundamental steganography procedure, which includes a carrier, secret message, stegokey, stegofile, embedding, and extraction steps [29]:

• Cover file (Carrier): It is the original or benign file on which the secret message is hidden. The hidden information will be held in the cover carriers, which can be images, audio, video, or text.
• Payload (Secret Message): This is the information that must be hidden in the suitable cover file. Plaintext, an image, or anything else that can be represented as a bit stream can be used as the payload [27].
• Stegokey: This is an optional password that may be used to encrypt secret information and add an extra layer of security [27].
• Stegofile (Stego-object): This is the final file that is created once the payload has been embedded in the cover file. It should have attributes comparable to the cover file [27].

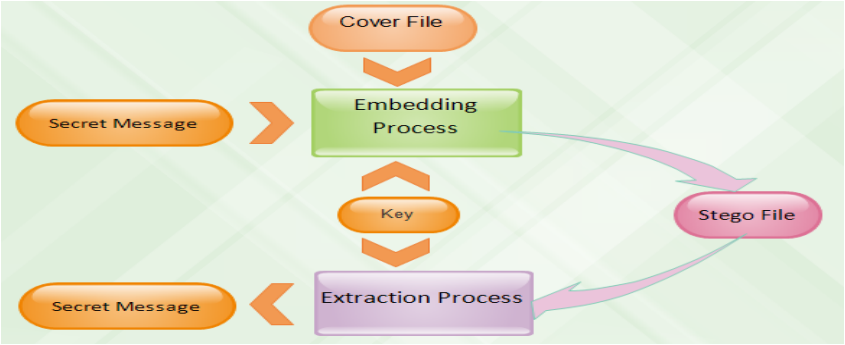

Figure 7: Basic Steganography Model

As shown in figure 7 the two algorithms that makeup steganography are one for embedding and one for extracting. The embedding method focuses on hiding a secret message behind a cover; the extracting technique, on the other hand, is typically a much simpler procedure because it is just the opposite of the embedding process and retrieves the hidden message at the end [30].

The embedding procedure calls for two inputs. The first is the cover file used to embed the hidden message, which is typically a text file. The image after embedding the secret message should have similar properties to that of the cover [30].

3.3 Steganography Requirements

When creating a steganography system, a few elements/factors should be taken into account [27]:

- Invisibility / imperceptibility (Undetectability): Steganography's power is in its ability to go undetected [27]. This property would be satisfied if the difference between stego file and the original cover file is unnoticeable for the observer (i.e., the hidden data should cause minimum distortion on the cover file).
- Capacity (Payload): It is the most private data that may be contained in a file. The embedding function and cover qualities both affect the capacity value. It's crucial to

be aware that hiding a lot of data results in significant image quality distortion. Therefore, imperceptibility should also be considered when the capacity of the system is tested [31].

- Robustness: A stego file may undergo some signal processing (filtering, compression, etc.) or geometric distortions while being sent (rotation, translation, scaling, etc.). The system is considered reliable if the hidden data can still be found despite these manipulations and distortions. [29].
- Security: is related to the eavesdropper's inability to detect hidden information. Due to this restriction, targeted assaults cannot find or display the hidden message unless they fully understand the embedding process [27].

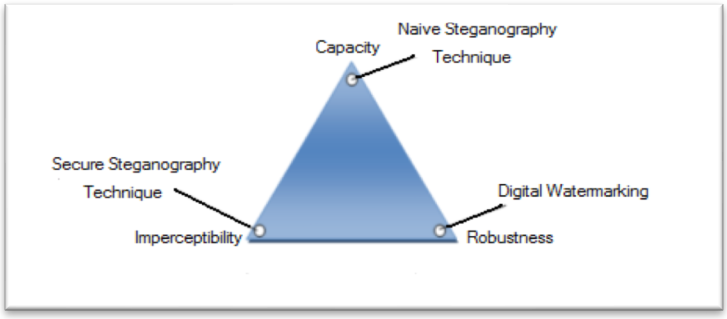

Figure 8: Competing Factors in Steganography Systems.

As shown in figure 8 [29], we can conclude some important points:

- A compromise between these needs must be struck by steganography systems [27].
- Robustness is not a problem or a major concern for steganography systems, thus they don't necessarily need to be.
- High steganography capacity and imperceptible secret data should be met by steganography systems.
- However, watermarking systems demand a high level of robustness against malicious attacks rather than great embedding capacity or imperceptibility of the watermark [27].

3.4. Types of Steganography

Based on the type of cover file utilized, such as text files, image files, audio files, and videos, as illustrated in figure 9 [27], there are numerous steganography strategies. Text steganography can be accomplished by changing the formatting of the text or specific textual parts. Text steganography is rarely employed since there is very little redundant data in it.

- Text Steganography: Text steganography can be accomplished by changing the formatting of the text or specific textual parts. Text steganography is rarely employed since there is very little redundant data in it.

- Image Steganography: When an image is taken as a carrier for hiding secret information use of pixel intensities then it is called image Steganography.
- Audio Steganography: Steganography that uses audio as a carrier for hidden information is known as audio steganography. It is a very important media that utilizes several codecs, including WAVE, MPEG, AVI, etc.
- Video Steganography: Video steganography utilizes digital video format to hide any kind of information. The discrete cosine transform (DCT), which is not obvious to the human eye, modifies the value in this method of hiding data in video images. Video steganography utilizes Mp4, AVI, etc. video formats.

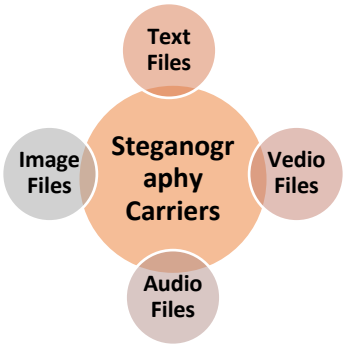

Figure 9: Different types of Steganography

3.5 Steganography cover Files (Carriers)

There are several steganography techniques, however, they are employed in various ways depending on the type of cover file being used to hide the message [27]. There are four digital covers, as shown in figure 9 [27].

3.5.1 Text File

The most difficult kind of steganography is using a text file as a cover file for embedding secret messages. This is because text files have a very small amount of redundant data that can be replaced with a secret message as compared with an image or audio file. Another disadvantage of using text files for embedding is that they can be changed by unauthorized parties by simply modifying the content itself or reformatting the text in another way (from .txt to .pdf, etc.). There are various techniques of hiding information in text steganography, for example, open space methods, syntactic methods, semantic methods, and feature coding [34].

1. Open space method

This technique involves increasing the amount of white space in the text to hide information. Adding white space at the end of each line, the end of each paragraph, or in between the words [32] will achieve this. A single space is understood as "0" with this method, while two straight spaces are interpreted as "1". The size of the information hidden is quite little, which is a disadvantage of this technology. Additionally, some text editor systems automatically remove superfluous white space, erasing the secret data [27].

2. Syntactic method

In this strategy, information is hidden by strategically putting punctuation marks like full stops (.) and commas (,). Finding the appropriate locations to apply punctuation signals is necessary for this technique. This method hides a small amount of information [32].

3. Semantic method

In this method, hiding information is done by using synonyms words for certain words. Semantic steganography assigns two synonyms primary and secondary values for certain words. The decoded values for the primary and secondary values are 1 and 0, respectively [27]. The protection of information in the event of retyping or the use of OCR systems is one of this method's key features [32].

4. Feature coding

Hiding information is done by altering some of the text features. For instance, when information is hidden in the text, the ends of particular characters, including h, d, and b, are slightly lengthened or shortened. The benefit of using this technique is that a lot of information may be inserted into the text without the reader realizing it. The drawback of this method is the hidden information is lost if the characters are placed in a fixed shape. The secret information is also destroyed by retyping the text or by using an OCR tool [32].

3.5.2 Audio Files

The secret message is hidden in a digitized audio signal using audio steganography, which results in a straightforward modification of the binary sequence of the related audio file. The audio signals are also appropriate for use as a cover for hiding hidden communications because of their redundancy and unpredictable nature [35]. Audio steganography algorithms such as:

1) Low-bit Encoding

In low-bit encoding, the LSB of information at each sampling point of the audio cover file is replaced with the binary string of the secret message. The advantage of this method is simple and can be hidden in large size of information. However, this technique is unable to shield the hidden information from slight alterations brought on by format conversion or loss compression [35].

2) Echo Hiding

By adding an echo to the discrete audio stream, this technique allows for the information to be hidden. Data transmission rates can be increased thanks to echo hiding, which also offers great robustness. Three echo parameters—amplitude, decay rate, and offset (delay time) from the original signal—need to be changed for the data to be successfully hidden. As all three parameters have been adjusted below the upper limit of human audibility, the echo is difficult to resolve. The hidden binary message is also represented by changing the offset. A binary one is represented by the first offset value, and a binary zero by the second offset value (binary) [35].

3.5.3 Video Files

Video files contain a large number of images and sound data. So, all the methods which are applied in image or audio can also be used in video steganography to hide a message. This technique is based on the video data stream and the bit plane complexity. The message is hidden in the bit stream of video and this stream is then used on the receiver side to recover the message [27].

Due to the constant flow of information and the substantial amount of room for hidden information, video steganography offers an advantage over static images. The vast size of a video clip makes it difficult to consistently transmit it using standard transmission routes, which is a downside of video steganography. [27].

3.5.4 Image Files

In a computer, the image is defined as an array of numbers that represent light intensities at various points (pixels) in the image. A pixel is a single point in an image or it is the smallest possible discrete picture element. Pixels are displayed horizontally row by row. Each pixel has an address that corresponds to its coordinates [17].

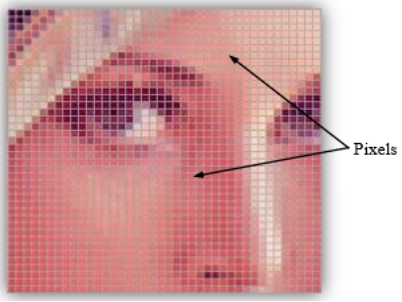

Figure 10: Example of Image Pixels [27].

In a color scheme, the bit depth refers to the number of bits assigned to each pixel in an image or video frame. This concept is also known as bits per pixel (bpp) [27]. Moreover, the smallest bit depth in the color scheme is 8 bits which represents the color of each pixel [29].

3.5.4.1 Image Types

According to colors, images can be categorized depending on their bit depth into three types, which are:

1) 1-Bit Images

It is the simplest type of image, also called 1-bit monochrome image, since it contains no color. Each pixel stores a single bit (0 or 1), therefore it has only two colors white and black where value 0 represents black and value 1 represents white as shown in figure 11 [27].

Figure 11: Monochrome I-bit Lena

2) Greyscale Image

Grayscale is a range of gray shades without clear color. The black color is the darkest possible and the white color is the lightest possible shade. So, in a greyscale image, everything is black, white, and shades of grey as shown in figure 12 [36]. Since each pixel is represented by a single byte (8-bit depth), there are 256 different color shades and a range of grayscale values for each pixel (0 and 255). For instance, "00110101" denotes a shade of grey, while "00000000" denotes the value of 0, which means it is black, and "11111111" denotes the number 255, which means it is white [36].

Figure 12: Grayscale Image of Lena

3) RGB Color Image

In an RGB color image, each pixel contains 24 bits (i.e., three bytes), usually representing R, G, and B (i.e., 8 bits for red, 8 bits for green, and 8 bits for blue) as shown in figure 13 [24]. Red, green, and blue all have 256 different color shades, while red has 256 different color shades. The total number of combined colors supported by this format is 16,777,216, or 256 × 256 x 256. RGB is an additive color model which can be used in plasma TV and a computer display [27, 36].

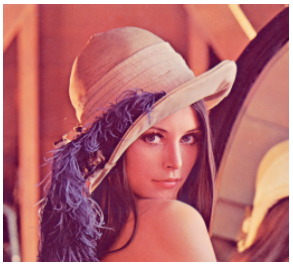

Figure 13: Color Image of Lena

3.5.4.2 Popular Image File Formats (Extensions)

According to extensions, images are divided into many types but the most popular formats are GIF, JPEG, PNG, and BMP:

1) Graphics Interchange Format (GIF)

Because it was the first sort of picture that was recognized by web browsers and has a long history with the WWW and HTML markup language, GIF is one of the most significant image formats. Only 8-bit (256) color images are allowed by the GIF standard. While the color it generates is adequate, it works best for photographs with few contrasting hues (e.g., diagrams, cartoons, and logos). For animation effects, GIF is still the preferred format [35].

2) Joint Photographic Experts Group (JPEG)

JPEG is an important current standard for image compression and is the most popular among the image formats used on the web. JPEG is short for Joint Photographic Experts Group. Also, JPEG images are primarily used in photographs. Despite having a smaller file size, they are nevertheless very popular because of the superb image quality. By using loss compression, this is accomplished. Users of some imaging apps can regulate the compression level. This is useful because users can trade off image quality for a smaller file size and vice versa [27, 35].

3) Portable Network Graphics (PNG)

Given that PNG is a relatively new format, not everyone is familiar with it. The PNG format is far superior to the GIF. The PNG format saves a maximum of 256 colors, just like the GIF format, but it does so more effectively. Additionally, 8-bit transparency is supported [36].

4) Bitmap (BMP)

Images stored in the Microsoft Windows operating system are called Windows Bitmap, or BMP, files. All Windows operating systems and apps are compatible with the BMP format, which is regarded as a basic picture file format. BMP files are also big and uncompressed, but the images they contain have excellent resolution and are full of color. Also known as raster or paint images, BMP files are. The number of bits per image pixel can be 1, 8, 24, or 32. The fourth channel that converts 24-bit images to 32 bits per [15, 23] can also store an alpha channel for transparency.

The important issue here is that most of the steganography techniques exploit the structure of these formats. However, several literary works use the bitmap format (BMP) due to its simple and simple data structure [36].

3.6 Image Steganography techniques

3.6.1 Image or spatial domain:

In this technique, the information is immediately included in the brightness of the original image pixels. The image format to be used as a cover affects this procedure. Under this strategy, we have two methods: Least significant bit LSB and Pallet Based. In the LSBs of pixel value, a secret message is buried. BMP files are frequently taken into account since they use lossless data compression. Pallet-based LSB images have a color lookup table, with an index to color recorded in the pallet for each pixel.

The cover artwork is mostly made up of GIF files. 256 different colors can be used to represent a Palette-based image.

3.6.2 Transform or frequency Domain:

This technique involves first transforming the cover image and then embedding the hidden message in significant areas. Discrete wavelet transforms, discrete cosine transforms, and discrete Fourier transforms are examples of transform levels.

Data embedding in the frequency domain of a signal is far more powerful than data embedding principles in the time domain. The transform domain is preferable to image transform because it hides information in the cover file that is less susceptible to cropping and compression.

3.6.3 Spread Spectrum:

Hidden data is dispersed over the cover image in the spread spectrum technique, making it harder to detect. The general criterion for spread spectrum is to spread the bandwidth from narrowband to wideband frequencies. To make the stego image, embed the hidden message in noise and then mix it with the cover image. Because the power of the embedded signal is lower than the power of the cover image, it is impossible to detect the secret.

3.6.4Patchwork:

It's a statistical technique that uses redundant pattern encoding to encrypt the secret message. The secret data is redundancy-enhanced before being dispersed over the image. If two patches are considered, the intensity of pixels in the first patch is increased by a constant value, while the intensity of pixels in the second patch is decreased by the same constant amount. It is impossible to predict the changes because they are so slight. This method's drawback is that it can only incorporate one bit. If you want to embed more bits, divide the image into sub-images. Because the hidden message is dispersed across the image, even if one patch is damaged, the others will survive. Patchwork is best for storing little amounts of data.

3.6.5 Distortion Technique:

Signal distortion is used to store hidden messages in this technique. During the decoding process, it is necessary to know the original message to restore the hidden message. A "stego" file is created when the cover image has been modified. In this technique, we must first determine whether the cover image and "stego" image are different or similar and then set message bit '1' or '0' accordingly. Every technique has one limitation: the cover image should never be used more than once, as this allows an attacker to simply alter the stego file. In rare circumstances, such as when a message is encoded with error correcting information and the original message can be recovered, the modification can be reversed.

3.6.6 Basic image steganography process:

The image steganography process consists of two procedures: an embedding procedure and an extraction procedure. The embedding procedure, which is the more meticulously designed of the two, is focused on hiding a secret message behind a cover medium (cover image). Much care is taken to make sure that if someone were to intercept the cover medium, the secret message would remain undetected (cover image). As the hidden message is only exposed after the embedding procedure, the extraction process is typically significantly simpler [45].

The embedding procedure needs the following inputs:

1. Secret message: It is the message that we want to hide.
2. Cover image: It is employed to create a stego image with a hidden message.

The stego- process encoder is the next phase, which is carefully designed to embed the message within a replica of the cover media with the least amount of distortion possible since the less distortion there is, the greater the likelihood that the message won't be detected [39]. The stego picture is the output from the stego- process encoder, as seen in figure (14). This was most likely the most widely used method of image steganography at the time, with significant consideration given to stego- process encoder development. If steganography is to be successful, the stego picture must exhibit no trace of embedding a hidden message [45].

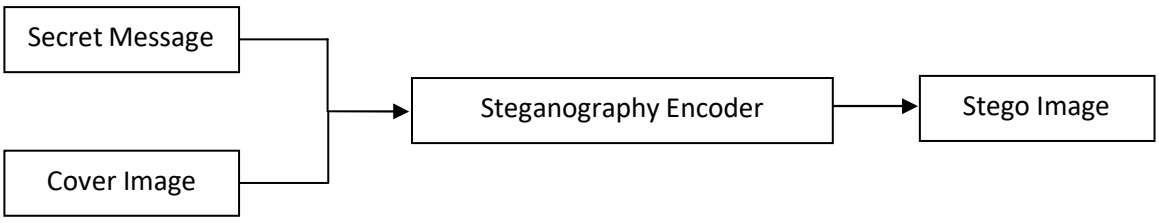

Figure (14) Basic image steganography process

3.7 Steganography vs. Cryptography

Although both cryptography and steganography are used to provide data security, each of them has its characteristics, so the following table illustrates some of the characteristic differences between them as shown in Table 1.

Table 1. Steganography vs. Cryptography

Steganography	Cryptography
Hides a message within digital material, such as a photograph, video, or sound file, making the message invisible [27].	The message is encrypted, so it is still accessible to the attacker, but it cannot be interpreted because it appears to have no purpose [27].
The result of steganography is stego-file [22].	The result of cryptography is cipher text [22].
Its objective is to hide the message's existence to prevent the detection of hidden communications [20].	Its goal is to obfuscate the communication such that its original meaning cannot be understood [20].
Certain formats continue to develop steganography algorithms [16].	Most algorithms of cryptography are well-known [16].
Its issue is that once the hidden message is found, it is made public [22].	The ciphertext appears useless, which is a problem since it makes it easier for an attacker to sabotage the transmission or run more comprehensive checks on the data being sent from the sender to the receiver [24].
Focuses on secrecy [27].	Focuses on privacy [27].
The majority of security goals cannot be met by it alone. However, it already offers confidentiality because, for the most part, nobody knows what sort of media the communication is hidden in [20].	It can achieve all security goals by combining the public and private key(s) with hash functions, authentication codes, or digital signatures [20].

3.8 Steganographic Systems Evaluation

A steganographic system evaluation scheme is required to compare several steganography systems and determine which is superior [27].

Actually, no accepted test or measurement can be used to assess the performance or efficiency of steganographic systems. However, there are a few standards and basic practices that can be taken into account when analyzing steganographic systems [27].

The two most crucial components of any steganographic system are how much information is concealed and how difficult it is to detect stego files. Which steganography system or technique is therefore better than another will be determined by comparing these two factors. The effectiveness of steganographic systems must therefore be evaluated using the measures of hidden capacity and un-detectability [27].

3.8.1 Evaluation of Imperceptibility

The degree of difference (distortion) brought about by data hiding in the original cover is measured by imperceptibility (stego-image quality), and the more invisible the hidden message, the higher the stego-image quality [42]. Peak Signal Noise Ratio (PSNR), one of the metrics to identify the distortion in the stego picture for the cover image, can be used to measure the stego-image quality. It is used to measure the stego quality of the image in dB [27]. If the greyscale image's PSNR is more than 36 dB, the human visual system (HVS) is unable to discern between the cover image and the stego image [31]. According to the following equation, PSNR is calculated:

$$\mathbf{PSNR}=10 \log_{10} (C^2_{max}/MSE)\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where, C_{max} represents the image's maximum value of 255 and MSE represents the mean square error, which may be calculated as follows:

$$\boldsymbol{MSE} = \frac{\mathbf{1}}{\boldsymbol{MN}} \sum_{\boldsymbol{x=1}}^{\mathbf{M}} \sum_{\boldsymbol{y=1}}^{\boldsymbol{N}} (\mathbf{S_{x\,y} - C_{x\,y}}) \ldots\ldots\ldots\ldots \mathbf{(2)}$$

In this equation, S_{xy} is the generated stego-image, X and Y are the image coordinates, M and N are the numbers of rows and columns in the input images, respectively, and C_{xy} is the cover image [40].

While the MSE calculates the difference between these two photos, the PSNR calculates how similar the two images are (i.e., how near they are to one another). These two metrics are easy to calculate and quick to employ, making them highly common [27].

3.8.2 Evaluation of Capacity (Payload)

The term "payload" describes how much information can be hidden within a cover image without clearly degrading its quality. Knowing that an algorithm generates significant distortion in the quality of the images and hides a lot of data has no significance. Therefore, it is possible to claim that a steganographic technique is an addition if it demonstrates an increase in payload while keeping an acceptable degree of stego-image quality, improves stego-image quality while also improving hiding capacity, or if can do both [41].

3.9 Steganography Applications

Applications for steganography in the sphere of covert communication are interesting. Steganography has generally been utilized for a range of purposes, both legal and illegal, including [27]:

1. Storing sensitive information using steganography is its most basic application. For instance, a cover source that is kept on your computer may contain multiple information sources, such as our private banking information [42].
2. Steganography is employed in patient medical records since this information is extremely sensitive and requires high security during storage and transmission to prevent patient records from becoming mixed up. Exam results and other medical information are maintained in each patient's EPR (an electronic patient record). Additionally, X-ray and scan images of the patient can be altered using steganography to conceal sensitive patient data. This offers a safe way to connect a patient's information to their X-rays and scans [43] [27].
3. Regrettably, terrorist organizations may be adopting steganography to communicate by using websites that incorporate text and images to covertly interact with terrorist cells operating all over the world [27].

4. Computer warfare is a further application of steganography. The use of steganography by new worms and spyware to transmit user data while evading detection by antivirus software, firewalls, or data stream analysis [27] has resulted in the theft of a large amount of user information.

5. Key presses in ATM (Automated Teller Machine) camera feeds could be hidden using image steganography by embedding secure information such as customer name, account information, and key presses.

6. Inconspicuous communication is often used by military and intelligence personnel. The identification of a signal on a contemporary battlefield can prompt an attack on the transmitter right away, even if the content is encrypted. To keep these signals hidden, steganography can be used [44].

4. Conclusion

Image steganography is an important and challenging problem in information security and has received considerable attention. An in-depth analysis of a steganography survey was done in this paper. First, its background and fundamental model are described, followed by discussions of the needs, categorization, carriers, evaluation, and applications. The distinction between encryption and steganography is then discussed.

5. Bibliography

[1] J. Anddress, "The basics of information security: understanding the fundamentals of InfoSec in theory and practice", Syngress, 2014.

[2] L. M. Mohamed, "Steganography for secure and imperceptible data communication ", Master's thesis, Faculty of Science, Assiut University, Egypt, 2015.

[3] F.S.A. Al-Afari, "Steganography for secure data communication ", Master's thesis, Faculty of Science, Assiut University, Egypt, 2009.

[4] B.Matt et al., "Introduction to computer security Pearson Education India, Egypt, 2006.

[5] A.Singh, A. Vaish, and P.K.Keserwani, "Information security: Components and techniques, "International Journal, Vol.4, no.1, 2014.

[6] M. E. Whitman and H. J. Mattord, "Principles of information security." Cengage Learning, 2011.

[7] N. M. Ali, "High Secure and Imperceptible Techniques for steganography." Ph.D. thesis, Faculty of Science, Assiut University, Egypt, 2014.

[8] R. L. Rivest, "Cryptography." In Algorithms and Complexity pp. 717-755, Elsevier, 1990.

[9] Z. P. Buba and G.M.Wajiga, "Cryptographic algorithms for secure data communication." International Journal of Computer Science and Security (IJCSS), Vol.5, no. 2, pp.227-243, 2011.

[10] J. Menezes Alfred, "Handbook of applied cryptography/Alfred J. Menezes, paul c. van Oorschot, Scott a. Vanstone," 1997.

[11] J. A. Mathew, "Steganographic Techniques for Subliminal Communication in Open Systems Environment", Sam Higginbottom Institute of Agriculture, Technology and Sciences, Ph.D. Thesis, 2010.

[12] E. Cole, "Hiding in Plain Sight: Steganography and The Art of Covert Communication", ISBN 0-471-44449-9, Wiley publishing, inc, 2003.

[13] M. H. S. Shahreza and M. S. Shahreza, "Arabic/Persian Text Steganography Utilizing Similar Letters With Different Codes", the Arabian Journal for Science and Engineering, Volume 35, Number 1b pp. 213 - 222, April 2010.

[14] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding—A Survey," Proceedings of the IEEE, special issue on protection of multimedia content, vol. 87, no. 7, pp. 1062–1078, July 1999.

[15] K. R. Babu, S. U. Kumar and A. V. Babu, "A Survey on Cryptography and Steganography Methods for Information Security," International Journal of Computer Applications (0975 – 8887), vol. 12, no. 2, pp. 13–17, November 2010.

[16] A. J. Raphael and V. Sundaram, "Cryptography and Steganography – A Survey," Int. J. Comp. Tech. App, vol. 2, no. 3, pp. 626– 630, 2011.

[17] A. A. Shejul and U. L. Kulkarni, "A DWT based Approach for Steganography Using Biometrics," in International Conference on Data Storage and Data Engineering, 2010, pp. 39–43.

[18] Kumar, C., Singh, A. K., & Kumar, P. (2018). A recent survey on image watermarking techniques and its application in e-governance. Multimedia Tools and Applications, 77(3), 3597-3622.

[19] Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). Digital watermarking and steganography. Morgan kaufmann.

[20] Kumar, S., & Dutta, A. (2016, February). Performance analysis of spatial domain digital watermarking techniques. In 2016 International conference on information communication and embedded systems (ICICES) (pp. 1-4). IEEE.

[21] Ritu Sindhu, Pragati Singh, "Information Hiding using Steganography ", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-4, April, 2020.

[22] Yaser Maher Wazery1, Shimaa Gamal Haridy1, AbdElmegeid Amin Ali1 faculty of Computers and Information, Minia University “Secure the handwritten signature images using Blowfish and a modified LSB Technique”.

[23] Deepesh Rawat MTech (DC 2nd Year) BTKIT, DWARAHAT UTTARAKHAND, Vijaya Bhandari Asst. Professor (ECE), BTKIT, DWARAHAT, UTTARAKHAND, INDI " A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image" International Journal of Computer Applications (0975 – 8887) Volume 64– No.20, February 2013.

[24] Vol. I, Special Issue I association with VEL TECH HIGH TECH DR. RANGARAJAN DR." Data Hiding using Efficient Steganography Techniques" International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST) National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG’15] - 28th August 2015 ".

[25] Chi-Kwong Chan, L.M. Cheng Department of Computer Engineering and Information Technology "Hiding data in images by simple LSB substitution ", City University of Hong Kong, Hong Kong Received 17 May 2002; received in revised form 11 July 2003; accepted 11 August 2003.

[26] D. Kahn, "The History of Steganography," Springer Berlin Heidelberg, pp. 1-5, 1996.

[27] A-H. S. S. Ibrahim, A. A. Ali and B. A. Abdellateef, "Digital Image Steganography," Ph.D. Thesis, Faculty of Science In Minia University, 2014.

[27] A-H. S. S. Ibrahim et al., "Enhancement of Some Image Encoding Techniques," Ms.D Thesis, Faculty of Science In Minia University, 2012.

[29] A. M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality," Applied Mathematical Sciences Journal, vol. 6, no. 79, pp. 3907 - 3915, 2012.

[30] S. Deepa and R. Umarani, "A Study on Digital Image Steganography," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 1, pp. 54 - 57, Jan 2013.

[31] R. O. El Safy et al., "An Adaptive Steganographic Technique Based on Integer Wavelet Transform," in International Conference on Networking and Media Convergence, Mar 2009, pp. 111 – 117.

[32] R. R. Koppola, "A High Capacity Data-Hiding Scheme in LSB-Based Image Steganography," Master of Science Thesis, Graduate Faculty of The University of Akron, May 2009.

[33] S. Sharda and S. Budhiraja, "Image Steganography: A Review," International Journal of Emerging Technology and Advanced Engineering (IJETAE), vol. 4, no. 1, pp. 707 - 710, January 2013.

[34] H. S. Shahreza and M. S. Shahreza, "A New Approach to Persian/Arabic Text Steganography," in Proceedings of the 5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse (ICIS-COMSAR'06), 2006.

[35] S. Bhattacharyya, I. Banerjee and G. Sanyal, "A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier," Journal of Global Research in Computer Science, vol. 2, no. 4, pp. 1 - 16, April 2011

[36] Z.-N. Li and M. S. Drew, Fundamentals of Multimedia. School of Computing Science, Simon Fraser University: Pearson Education Internationa, 2004.

[37] Matted, Sushmita, Gori Shankar, and Bharat Bhushan Jain. "Enhanced Image Security Using Stenography and Cryptography." Computer Networks and Inventive Communication Technologies. Springer, Singapore, 2021. 1171-1182.

[38] Pandey, Digvijay, et al. "Secret data transmission using advanced steganography and image compression." International Journal of Nonlinear Analysis and Applications 12.Special Issue (2021): 1243-1257.

[39] K. R. Babu, S. U. Kumar and A. V. Babu, "A Survey on Cryptography and Steganography Methods for Information Security," International Journal of Computer Applications (0975 – 8887), vol. 12, no. 2, pp. 13–17, November 2010.

[40] R. Sridevi, A. Damodaram and S. V. L. Narasimham, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security," Journal of Theoretical and Applied Information Technology, vol. 5, no. 6, pp. 768 – 771, June 2009.

[41] L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread Spectrum Image Steganography," ieee transactions on image processing, vol. 8, no. 8, pp. 1075 - 1083, august 1999.

[42] A. Kumar and Km. Pooja, "Steganography- A Data Hiding Technique," International Journal of Computer Applications , vol. 9, no. 7, pp. 19 - 23, November 2010.

[43] Y. Srinivasan et al., "Secure transmission of medical records using," Proceedings of the 17th IEEE Symposium on Computer-Based Medical, pp. 122-127, 2004.

[44] R. J. Anderson and F. A. P. Petitcolas, "On the Limits of Steganography," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, vol. 16, no. 4, pp. 474 – 481, May 1998.

[45] A. A. Radwan, A. Swilem and A. H. Seddik, "A High Capacity SLDIP (Substitute Last Digit In Pixel) method", Fifth International Conference on Intelligent Computing and Information Systems (ICICIS 2011), 30 June - 3 July 2011.