THE SCIENCE OF DIGITAL STEGANOGRAPHY

Doç. Dr. Esra ŞATIR

SERÜVEN YAYINEVİ

Genel Yayın Yönetmeni / Editor in Chief • C. Cansın Selin Temana

Kapak & İç Tasarım / Cover & Interior Design • Serüven Yayınevi

Birinci Basım / First Edition • © Aralık 2025

ISBN • 978-625-8671-06-3

Serüven Yayınevi / Serüven Publishing

Türkiye Adres / Turkey Address: Kızılay Mah. Fevzi Çakmak 1. Sokak Ümit Apt No: 22/A Çankaya/ANKARA

Telefon / Phone: 05437675765

web: www.seruvenyayinevi.com

e-mail: seruvenyayinevi@gmail.com

Baskı & Cilt / Printing & Volume

Sertifika / Certificate No: 47083

THE SCIENCE OF DIGITAL STEGANOGRAPHY

Doç. Dr. Esra ŞATIR[1]

1 Esra ŞATIR, Doç.Dr., Düzce Üniversitesi, Bilgisayar Mühendisliği, Konuralp, Düzce; 0000-0003-1793-2472

SERÜVEN YAYINEVİ

CONTENTS

1. Introduction

The wide usage of Internet by the public masses and the availability of public and private digital data in a large scale has caused industry professionals and researchers to focus on data protection. For this purpose, three main methods are being used; cryptography, watermarking, and steganography. Cryptography techniques are based on elaborating the content of a message for the unauthorized people. In watermarking, data are embedded to hide the information about the cover medium like ownership and copyright. Even though cryptography and watermarking techniques are in demand for securing the data, an increasing research in discovering better or complementary new techniques has been the focus of ongoing studies. In Figure 1 the differences and the similarities between steganography, watermarking and cryptography has been mentioned (Djebbar et al., 2012).

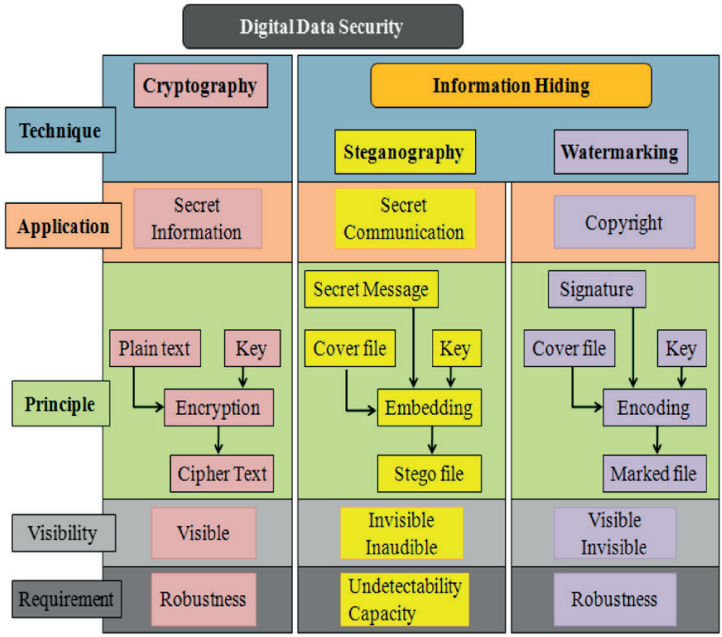

Fig. 1. *Comparison among cryptography, watermarking, and steganography (Djebbar et al., 2012).*

Encryption namely, cryptography is used to elaborate the secret message by rendering it extremely complicated to be solved or to be decoded by the observers. However, this situation always draws attention. Therefore, it is necessary to establish an invisible communication channel which is undetectable and not noticeable to anyone whether communication is happening. That's why we need information hiding techniques. Information hiding field contains two sub disciplines. They are steganography and watermarking. Steganography and also watermarking are used to hide the secret information. Besides, they are closely related to each other. However, their purposes are too different in case of usage. The main purpose in all of steganographic systems is to hide the existence of communication and protection of secret data. However different from steganography, the aim of watermarking is to protect the integrity of secret data with or without considering the covertness of the communication from the observers (Hussain et al., 2018).

Steganography is the science of communicating in a way where the existence of the communication is hidden. The goal of Steganography is to hide the messages inside other harmless messages in a way such that an observer will not be able to detect the presence of a second message. More clearly, steganography embeds the secret message into a cover media which can be an image, a text, an audio or a video in such a way that observers don't have any idea about the existence of the original message and also the existence of the used algorithm for embedding or retrieving the secret message. In a steganography system, the hidden message is called the embedded message. At transmitter side these two are combined using the designed algorithm, thus presence of secret message cannot be recognized. Thus, this combination is called as stego-message. Data type of cover message and stego message must be of the same; however the data type of embedded message may be different. At receiver side reverse steganography algorithm is used to extract the embedded message or secret message (Dhall et. Al., 2015).

Steganography is the process of transmitting secret information, which is embedded in another data. Accordingly in this process, there are secret data and the covered data. Here, an observer will only have the opportunity to read the cover data, while the existence of confidential data will be kept secret. In steganography, the cover and the secret data can be in the form of text, audio, image, or video. The process of steganography is shown in Figure 2.

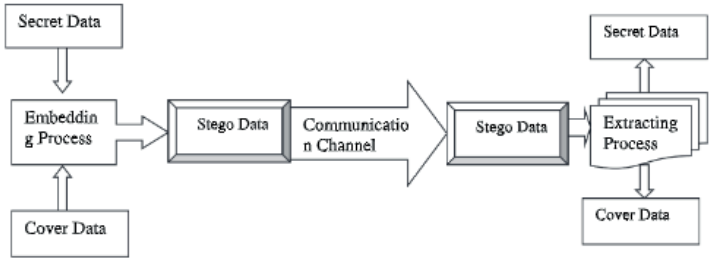

Figure 2. *Block diagram of steganography (Dhawan and Gupta, 2021).*

2. Types of Steganography

In steganography, the employed carrier medium determines the type of steganography. The communication object which is used to hide the secret message can be any medium or any carrier, device like smartphone, switch or a service like browser, Facebook.

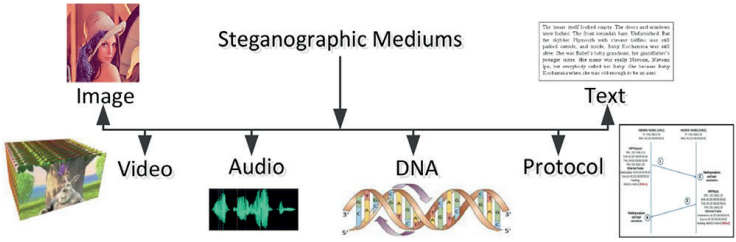

Figure 3. *The carrier mediums for stegaography*

Generally, the used communication mediums or information carriers can be in the form of digital files or in the form of data like image, video, text, audio, network protocol as depicted in Figure 3. Recently, DNA has been used as another carrier medium as mentioned in Figure 3. Different properties of different digital mediums are used to hide the secret information. For example, in text steganography, line/word shifting encoding and emoticons in textual chat can be used to achieve secret communication.

In audio steganography, phase coding, spread spectrum and low-bit encoding are generally employed. Network protocol can be used another medium where the secret information can also be embedded into packet payload and packet headers. Besides, they employ the characteristics of acknowledgment and retransmission of packets known as retransmission steganography. In DNA-based steganography, the characteristic randomness of DNA sequences are used to embed the secret data. Video steganography can be considered as the combination of image and audio steganography. It also has more capacity to embed more secret data due to a different combination of images considering the video stream.

The chosen of best cover medium to hide the secret data must obviate two features. Firstly, the cover medium should be widely used and secondly, the arrangements in the cover medium should not be visible or understandable for a third party or the observer (Hussain et. Al., 2018).

2.1. Image steganography

In image steganography, the carrier medium where the secret information was concealed, is an image. A basic image steganography flow is shown in Figure 4. Here, the term "cover image" denotes the image that is used to embed the secret information as a payload or "secret message". The "embedding technique" is the algorithm that is used to hide the "secret

message" inside the "cover image" namely "stego-image" with an optional "stego-key". The optional "stego-key" must be shared with both the sender and the recipient. The "stego-image" corresponds to the final output image where the secret information is hidden.

Similarly, in embedding part where the secret information is extracted, "extraction technique" is the process to recover the "secret message" from "stegoimage" with an optional "stego-key". Moreover, "steganalysis" is known as an attack on steganography to extract the hidden information. Namely, steganalysis is the art and the science of detecting the existence of the secret information and recovering the secret information from stego images.

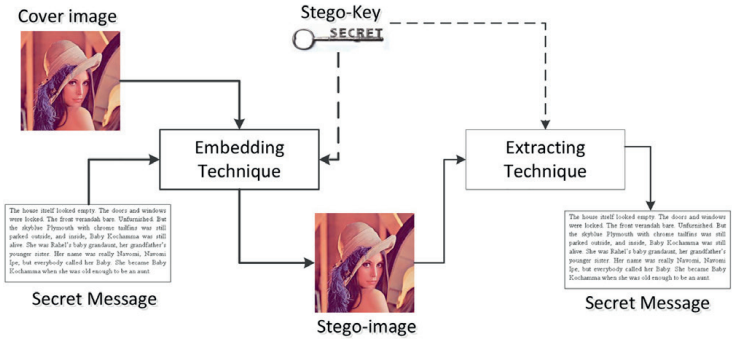

Figure 4. *A basic images steganography diagram.*

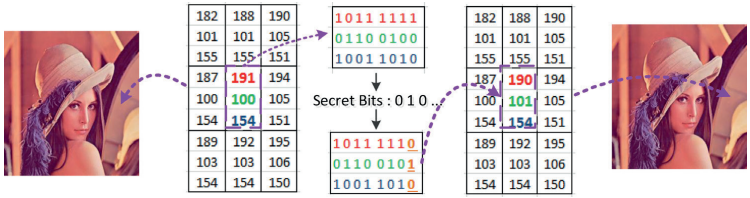

Figure 5. *Basic 1-bit LSB embedding mechanism.*

Least significant bit (LSB), steganography is one of the traditional methods where, a large number of information

can be embedded in a cover image without making noticeable distortions. It works by replacing the selected or random LSB pixels in the cover image with the bits of secret message. Pixels selection or the order of embedding can be determined by the help of a stego-key. A traditional and basic LSB substitution mechanism is demonstrated in Figure 5. Within the time, different variation of LSB's pixel or bit-planes has been employed in steganographic methods. These methods have been developed with the aim of payload optimization, improving visual quality and undetectability.

LSB based methods are handled as a basic way for information hiding. Besides, they are extremely suitable to integrate with other methods. But the main disadvantage of LSB based methods is that the embedding capacity can directly affect the visual quality of the resulting stego-image. The more the payload is increased, the more the overall visual quality of stego-image corrupts.

To handle the visual quality problem, pixel difference value methods can be employed. Here, the difference value between two neighbouring pixels is used to decide the amount of embedded secret bits. In this method, a cover image is separated into two blocks which have non-overlapped consecutive in a zig-zag direction. In each block, the difference value between two pixels is estimated to determine the embedded bit size. Here, the difference values corresponds to a number of ranges. Finally, the difference value is arrabged with the new difference value along the secret data. The number of embedded secret data relies on the texture area of an image which is controlled by range levels. The larger the difference, the more secret bits can be embedded into pixel pair. Overall, PVD method embeds a larger amount of secret data into images with higher visual imperceptibility when compared with LSB substitution method. A sample diagram of the PVD based embedding method is illustrated in Figure 6.

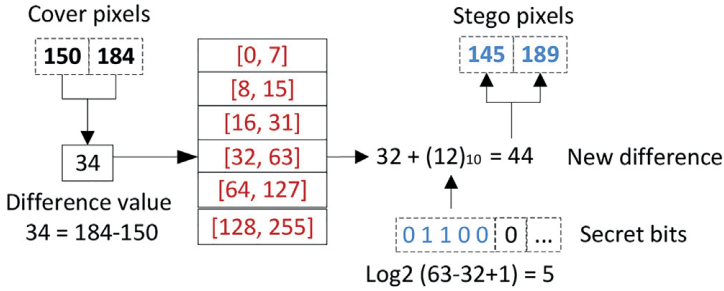

Figure 6. *A sample pixel value differencing embedding scheme.*

Exploiting modification direction (EMD) is another well-known steganographic method which provides the high fidelity of stego-images. Generally in embedding process, the digit aimed to be hidden is transformed by the $(2n + 1)$-ary system, where n are the number of cover pixels. The maximum pixel value of distortion range here is just about (± 1). Namely, EMD method employs a specific base to detect the local variation of pixel intensity in the image. For this reason, more secret data can be embedded in the pixels in high texture areas. As the result, EMD method can achieve good visual quality when compared to LSB and PVD methods (Hussain et. Al., 2018).

2.2. Video steganography

Videos are more popular to hide the secret data, since they are frequently used in the Internet. Videos have many advantages when compared to the other steganographic mediums especially like an image and like an audio. These advantages make them more suitable for steganography mentioned as follows:

1. By considering the survey of Facebook in 2015, the organic access of videos was 8.71%. This is very high when compared texts (5.71%) and images (3.73%) in the time interval from 2014 to 2015.

2. In every minute, 400h of videos are uploaded to YouTube by considering November, 17 YouTube statistics.

3. By considering a Cisco study performed in 2020, it is estimated that 80% of the world's internet traffic will include videos.

4. Videos are widely transmitted on the Internet, due to the advancement in digital media and the compression techniques.

5. Portable small cameras and softwares for video editing are widely used. They allow people to record, to edit, and to send videos via Yahoo, Facebook, and YouTube.

6. Due to the very complicated statistics and various content, videos are the most suitable medium for steganography.

7. The most important requirement of steganography is to embed and transmit a sufficient amount of information. Accordingly, videos have a very high potential to carry significant amount of secret data more than an image or audio.

Image and audio steganography methods can also be used in video steganography since the video can be considered a combination of both of them. However, there are certain differences between them explained as follows:

- *Size:* Images size is very insufficient when compared to videos in terms of the number of pixels.

- *Perceptual Redundancy:* Videos have temporal features which provide perceptual redundancy to embed hide secret information without making any corruption.

- *Complex Structure:* Videos have a more complex structure when compared to images. This makes it difficult for observers to detect the existence of hidden data.

Videos have more statistical features like motion vectors, macroblocks, and so forth which can be very useful for embedding. Data can be embedded in three ways when videos are considered as carriers:

1. Handling the video as one complete file.

2. Considering only the frames in the video.

3. Both audio and frame parts in the video.

Generally, the audio part in video is frequently omitted while embedding because of its limited capacity. The fundamental flow of video steganography is indicated in Figure 7. Here, the frames are obtained by benefitting the original video in sender side. By using video steganography embedding algorithm, secret data is hidden in the selected frames. After embedding process, the frames are reformed and then the stego video is produced for transmission to the recipient. At the recipient side, the stego video frames are mined and the extraction algorithm is employed to extract secret data from the stego video frames. Thus, the original video is rebuilt (Dalal and Juneja, 2021).

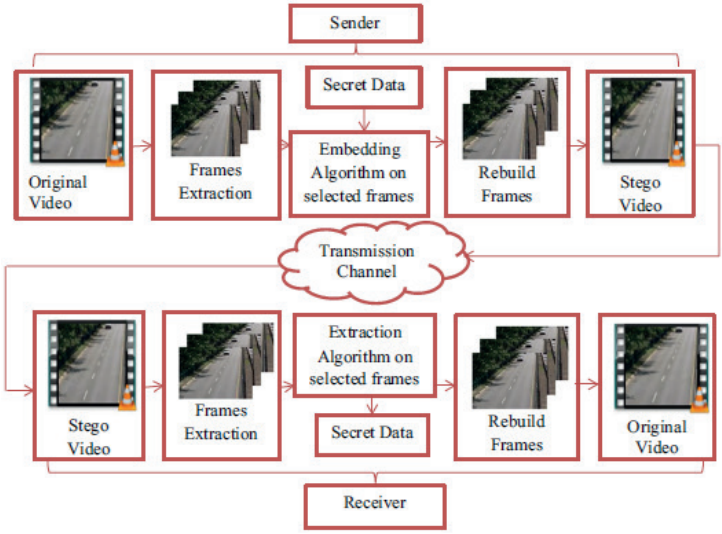

Figure 7. *General structure of video steganography (Dalal and Juneja, 2021).*

2.3. Text steganography

The capacity of text steganography methods is limited when compared to the other steganographic methods. Namely, a small volume of information can be embedded in stego-medium. This is due to the structure of text files since they are vulnerable in terms of imperceptibility. For example, an additional letter or a sign of the punctuation in the text can be easily recognized by a casual reader (Urbanovich and Plaskovitsky, 2012). Text steganography methods are classified into two groups:

A) Changing text format: In the methods belonging to this group, the format of the text or text file is modified.

B) Changing the meaning: In the methods belonging to this group, text meaning is modified. However, the examples of this group is limited.

Some examples of text steganography methods are described below.

Semantic Method: This method is based on employing the synonym of a certain word. Here, data is hidden by using synonym substitution. Synonym substitution may hide single bit or multiple bist of secret information. This method is generally classified under changing the format but sometimes meaning of the text can be altered by using this method. M. Hassan Shirali-Shahreza (Shahreza and Shahreza, 2008(a)) have used semantic method for embedding secret message in a text file as depicted in table 1.

Table 1. *Semantic method*

WORD	SYNONYM
Lazy	Idle
Hard	Difficult
Unhappy	Sad

Text Abbreviation or Acronym: In this method, abbreviations and acronym of the words are used for data hiding by changing text format. The concerning word is substituted by its acronym like replacing as soon as possible by ASAP etc. This method is generally employed in SMS, social networking applications and sites, since the nature of these platdorm are suitable for this type of communication. Mohammad Sirali-Shahreza and M.Hassan Shirali Shahreza have used this method (Shahreza and Shahreza, 2008(b)) as indicated in Table 2.

Table 2. *Abbreviation or acronym method*

ACRONYM	WORD
ID	Identification
DOB	Date Of Birth
ASAP	As Soon As Possible

Change of Spelling: In the method proposed by Khan (Khan, 2009), this method has been used to embed secret data in a text file as demonstrated in Table 3. Here, they benefitted the same words which are spelled differently in American and British English. This method is also classified under changing the format (Sharma et. Al., 2016).

Table 3. *Word Spelling method*

American English	British English
Airplane	Aeroplane
Fiscal	Financial
Unalike	Unlike

White spaces: This method works by inserting spaces in a cover text file (Sharma et. Al., 2016). The sign "space" is replaced with a sign "underlining". So, for example, the first line of the message in Figure 8 contains the two bits of information: 01, while the second line contains another two bits - 11; the third line contains one bit -1 etc. Thus, the container contains the following message: 011111110. The important feature is that the text is formatted from both sides.

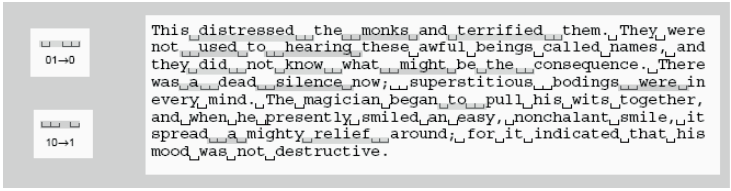

Figure 8. *An example of using white spaces in text steganography (Urbanovich and Plaskovitsky, 2012).*

Line-Shift Coding: This method is based on modifying a document by vertically shifting the locations of text lines in encoding phase. The format file or to the bitmap of a page image can be used for application of this method in embedding phase. The embedded information may be extracted from the format file or bitmap. In some cases the decoding can be performed without needing the original image, since the

original is known to have uniform line spacing (i.e., "leading") between adjacent lines within a paragraph.

In Figure9, an example has been illustrated for the of of *Line-Shift Coding* method. Here, the last line has been shifted up by 1 pt.

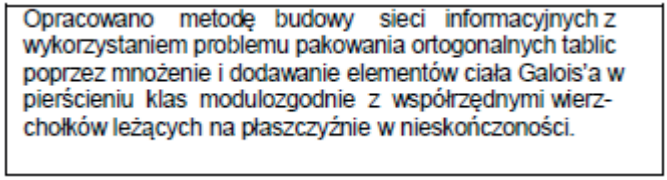

Figure 9. *An example of the use of Line-Shift Coding method*

Here, using three various three various inter lower case distances in the text. The maximal and minimal distances between the lines corresponds to symbol 1 and symbol 0. Other distances increase or reduce till the sizes allocated.

Word-Shift Coding: This method is performed by altering a document via horizontally shifting the locations of words. The format file or to the bitmap of a page imagecan be employed for embedding. Accordingly, decoding may also be performed by employing the format file or bitmap. This method is least visible when applied to documents with variable spacing between adjacent words. Because of this variable spacing, decoding requires the original image. An illustrative example of this method is seen in Figure 10.

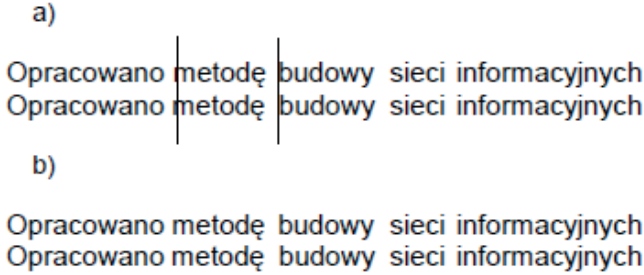

Figure 10. *An example of Word-Shift Coding*

In Figure 10(a), the top text line has added spacing (0.1 mm) before the "metodę" (in the first line) and the same spacing before the "budowy" (in the second line); the bottom text line has the same spacing after the "budowy". In Figure 10(b) the same text lines without the vertical lines are shown to demonstrate that either spacing looks natural (Urbanovich and Plaskovitsky, 2012).

2.4. Network Steganography

Three main functionalities can be concerned, if we focus on any communication network: services/applications, information transport and flow control of information. The services/applications are provided by the network, the transport is carried out via clear channels. Moreover, the control and functions of transportation are virtually distinguished. Information like voice or data is transported via the network without any interference when the end-to-end connection and transportation channel are constituted. The user has a little effect on the service delivered by the network but he/she doesn't have any effect on the information flow.

The discovery of Internet has changed the classical circuit-switched network method. Here, services/ applications are formed by the network users, not by the network itself. Besides, the transport and control functions are not separated and they can be influenced by the user. This situation is one of the main sources of the huge success of the Internet. But these advances brought some common problems about the quality of service and about protecting the network. Therefore, Internet revealed many new options for secret communication. This concept may be generalised to all types of contemporary fixed and mobile networks, easily. And besides, it can be easily generalised especially to the communication protocols that are becoming diverse and complex day by day. Network steganography techniques are taking the advantage of this susceptibility.

Some basic communication protocol functions can be employed to form a steganography scheme. Generally, these following features can be formulated in order to establish a network steganography method:

C1: Arrange some functions of communication protocols

C2: The arrangement is about:

C2a: the communication protocol functions that are introduced to handle the intrinsic lacks of communication channels like errors, delays, etc. and/or to

C2b: the functions of the protocols which are used for defining the information type exchange (e.g. query-response, file transfer, etc.) and/or to adapt the form of the messages (e.g. fragmentation, segmentation, etc.) to the information transmission carrier;

C3: The arrangements are employed by the parties in communication to render the apparent effects of revisions difficult to be noticed (e.g., to seem to result from the imperfectness of the communication network and/or protocols).

C1, C2 and C3 conditions can be used for a suggested definition of network steganography. If condition C1 is not met, for example, if there is no drawback in the communication protocol, then hidden communication in some form still may be performed. This means that if the secret data shared by the sender and receiver is of the form: messages a, b, c, …, then they are interpreted as x, y, z …. Such hidden communication cannot be discovered via observations about the exchange of messages. Because these messages are interpreted on the semantic/pragmatic level both by the sender and recipient. In fact, such hidden communication can be discovered only if the shared secret data is disclosed. It is obvious that this was not a very interesting case for research.

C2 corresponds to the fact that communication protocols used in real world, must realise functions (C2a) where the required quality-related performance of communication is provided and functions (C2b) where the "logic" of communication is guided and where the messages are adapted to the format of information carriers. If the communication functions are decomposed into functional layers, like in the OSI RM (Open Systems Interconnection Reference Model), then C2a functions are related with lower layers whereas C2b functions are associated with upper layers. In Figure 11, these functions, which are related with OSI RM protocol layers, are presented in a general manner.

The success of a network steganography technique is based on how efficiently C3 is met. For this situation, three important measures can be considered: the potential throughput of hidden messages that refers to steganographic bandwidth — and the resistance to discovering the hidden communication, namely, resistance to steganalysis, and robustness. Robustness is defined as the amount of alteration a steganogram that can withstand without corrupting the secret data. A good network steganography method should be robust and hard to detect as much as possible, while enabling the network to have the highest bandwidth.

These three measures have a trade-off. If the steganographic bandwidth is higher, this will render the robustness and resistance to steganalysis lower. The last one is usually difficult to estimate quantitatively. Because it does not depends only on the complexity of a steganography method. However it also depends on the knowledge and efficacy of potential observers in the communication (Lubacz et. al., 2014).

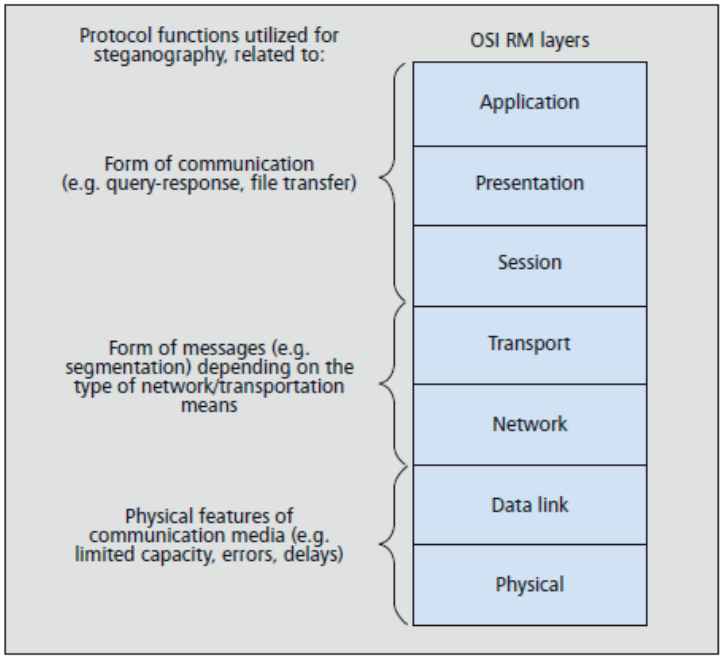

Figure 11. *The protocol functions of OSI RM layers used for network steganography (Lubacz et. al., 2014).*

2.5. DNA steganography

In order to have a satisfying capacity rate, DNA has been tackled as a potential carrier medium. DNA steganography can be considered as an extension of DNA cryptography. In this type of steganography, DNA sequences are used as carriers to provide secure transfer of secret data. The main idea in DNA steganography is to encrypt the secret data, basically and then conceal it in a large number of DNA strands thus preventing the observers from reading and deciphering the secret data. This can be achieved, if the original DNA sequences are protecte and isolated from the observers. Using DNA sequences for data hiding is a new and evolving research field od steganography.

2.5.1. Elements of DNA

Deoxyribonucleic acid (DNA) is a molecule which exists in the cells of all living organisms. It contains the genetic information of the living organisms. This genetic information enables the living organisms functioning, reproduction, and evolution. DNA has small subunits called nucleotides. There are four type of nucleotides in a DNA molecule. They are called Adenine (A), Thymine (T), Guanine (G), and Cytosine (C). The two strands are held together by bonds between these bases. Accordingly, Adenine binds with Thymine and Cytosine binds with Guanine. Every three neighbouring nucleotides make up a codon. Since there are four types of nucleotides, we get $4^3 = 64$ different possible codon combinations. In living organisms, the combinations of these nucleotides determines the structure and function of the resultant protein. DNA encoding techniques can be considered as binary coding schemes for the purpose of DNA computation. The widely used binary mapping is given in Table 4.

Table 4. *DNA digital coding*

DNA nucleo-tide	Decimal	Binary
A	0	00
C	1	01
G	3	10
T	3	11

An example of a DNA data hiding method that is proposed by Malathi (Malathi et. al., 2017) has been explained. Two different keys are used in this method. The first key (K1) is a numeric content between 0 – 255. This key is used in XOR operation with the last character in the message (*M*). Then the result will be XORed with the character preceding the last one in the M. This operation goosed on like this till the end of *M*.

Briefly here, the first key is necessary for encrypting the message whereas the second key (K2) is randomly generated and it is necessary to seperate the DNA sequence into the segments which have the same-length. The resulting cipher characters are substituted with binary bits one by one at the beginning of each segment. Then, this binary sequence is transformed to DNA bases via Table 4. The second key should be a small number. Thus, the DNA sequence will have a minimum length while hiding the secret message. The encoding process has been demonstrated in Figure 12.

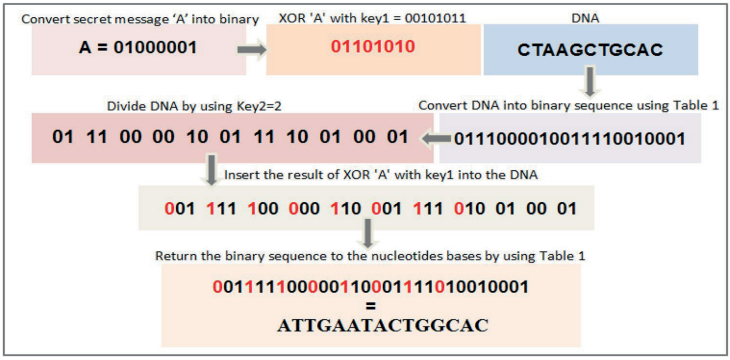

Figure 12. *Encoding process*

The encoding process in Figure 12 has the following steps:

1. Split M into characters, $M = m_1, m_2, m_3,\ldots, m_n$, and then convert each character into its 8-bit binary equivalent according to the ASCII standard.

2. Generate a number in the range of 0 - 255, randomly to form K1. Then convert K1 transformed into an 8-bit binary sequence.

3. XOR the last character of M with K1.

4. XOR the result with the character preceding the last one in M. This operation goes on till all the characters are transformed and hold in A.

5. Convert *A* into a protein sequence.

6. Chose a sample DNA sequence; *S* randomly and transform S to a binary bit sequence via Table 4.

7. Generate a small random number to form K2. And then split the DNA sequence into the segments each of which length is equal to K2.

8. Add the first binary value of *A* in the beginning of the first DNA binary segment. And then insert the second binary value of K1 into the second binary segment, and so on.

9. Concatenate all the binary sequences. Then transform it to form a fake DNA sequence via Table 4.

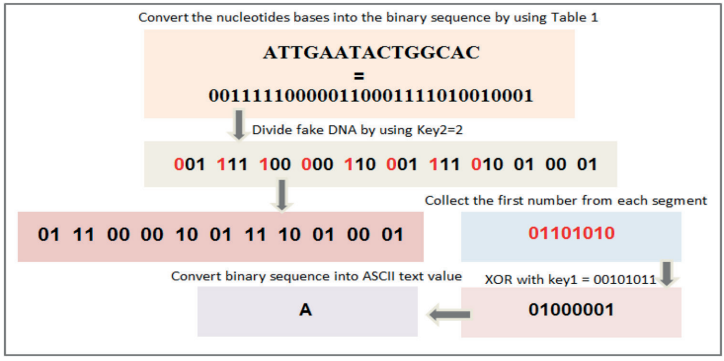

Figure 13. *Decoding process*

As explained in Figure 13, the recipient must have the knowledge about K1 and K2 for decrypting the message. Besides, the recipient must receive the original DNA sequence from the sender. The steps are performed to obtain the original message:

1. Transform the received fake DNA sequence to its binary equivalent sequence by employing Table 4.

2. Split the binary sequence into the segments each of which size are equal to K2 + 1.

3. Obtain the first bit of each segment and concatenate them to form significant bits *B*.

4. XOR the first 8 binary bits of *B* with K1 and then XOR the second 8 bits in *B* with the previous 8 bits of *B*, and so on.

5. Transform the binary bits to ASCII text value (Al-Harbi et., al., 2020).

3. Main Requirements of Steganography

There are three important properties of any steganographic systems. They are imperceptibility, security and capacity. Moreover, robustness has been mentioned as the fourth one of these requirements. They are the most effective parameters for evaluating the effectiveness of a steganographic scheme.

There is a trade-off among these mentioned properties. This situation is demonstrated in Figure 14. When the amount of secret data in the stego-cover is increased, the corruption of the stego -cover increases. However, immunity towards modification of stego-cover decreases. Therefore, it is an essential requirement to keep all the properties at an optimum level. High level of robustness is not always a requirement or a critical requirement but high security, capacity and imperceptibility of secret information are more critical (Kadhim el. al., 2019).

Figure 14. *Main requirements of steganographic systems (Altaay et., al., 2012).*

3.1. Imperceptibility

The most essential requirement for a data embedding method is imperceptibility. It means that the secret information in the stego-cover could not be comprehended by the human visual system; naked eye or with the use of statistics. Hence, steganographic techniques must not distinguish the cover media in terms of perception. More briefly, if the statistical data for the stego-file and the original data file are similar, then it can be claimed that the security was better. Since embedding secret data in the cover image causes corruptions by adding some amount of noise, the quality of cover image should not be decreased during sharing via unsecured channels.

3.2. Security

Security" indirectly refers to "unnoticeability"or "undetectability" in a steganographic system. Accordingly, a steganographic technique can be considered as secure if the secret data is not detectable by statistical means or removal after it is detected by the observer. Secure transmission of

secret data is the key requirement of a steganographic method. So security is the primary issue to avoid the data access by unauthorized observers or computer while transmitting through an open channel.

3.3. Capacity

The purpose of an efficient steganographic system is to embed maximum volume of information by using the minimum volume of cover media. This will a significant effect to reduce the possibility of interception while sending through an unsecure network. Therefore this usually demands high embedding capacity. In the study proposed by Venkatraman (Venkatraman et., al., 2004) ,embedding rate is defined as the amount of secret information (in bits) relative to the size of the cover medium. The major challenge in steganography is, keeping higher payload in capacity without sacrificing imperceptibility and security.

3.4. Robustness

Robustness indicates the quality of the embedding and decoding processes even if the stego-cover is corrupted by an observer. With steganography, active attack scenario is not considered like there is an assumption of sending stego-files via the internet. Hence the stego-file is not affected and the recipient receives the distortionless stego-file. The steganographic systems are less robust when any modification is done to stego-files like file format conversion, compression and transforming digital files to analog format. However, for a fingerprint system, robustness is required in case of modifying or manipulating files, deliberately (Kadhim el. al., 2019).

4. Conclusion

Steganography is the art and science of secret communication. Through history, steganographic applications has been evolved to computer aided mediums parallel with the developments in computer systems, network technologies and Internet. By considering the carrier medium where the secret data is hidden, there are three main steganography types. They are image steganography, video steganography ant text steganography.

Image and video steganography are advantageous in terms of the amount of hidden data and corruptions. However, text steganography is too risky since the change of one bit causes a change in letter especially when we consider that the human visual system was much more sensitive to reading of text files. Network steganography is another type where the Internet medium and Internet layer protocols are used for data hiding. DNA steganography is an evolving field and a new type of steganography. Here, DNA strands are used as information carriers.

A steganographic system should mainly have three requirements like Imperceptibility, security and capacity. Moreover, robustness is another requirement in most of the researches. It is not possible to meet all of these requirements since there is trade-off between them. But it can be said that keeping higher payload capacity without sacrificing imperceptibility and security was a major challenge in steganography.

References

Al-Harbi, O., A., Alahmadi, W., E., Aljahdali, A.,O., (2020). Security analysis of DNA based steganography techniques. *SN Appl. Sci.* 2, 172. https://doi.org/10.1007/s42452-019-1930-1

Altaay, A., A., J., Sahib, S. B., Zamani, M., (2012). "An Introduction to Image Steganography Techniques," *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, Kuala Lumpur, Malaysia, 2012, pp. 122-126, doi: 10.1109/ACSAT.2012.25.

Dalal, M., Juneja, M., (2021). A survey on information hiding using video steganography, *Artif Intell Rev*, 54, 5831–5895, https://doi.org/10.1007/s10462-021-09968-0

Dhall, S., Bhushan, B., Gupta S., (2015). An in-depth analysis of various steganography techniques, *International Journal of Security and Its Applications*, 9 (8), 67-94

Dhawan, S., Gupta, R., (2021). Analysis of Various Data Security Techniques of Steganography: A Survey, *Information Security Journal: A Global Perspective*, 30(2), 63-87,

Djebbar, F., Ayad, B., Meraim, K.A. et al., (2012). "Comparative study of digital audio steganography techniques." *J AUDIO SPEECH MUSIC PROC.* **2012**, 25 (2012). https://doi.org/10.1186/1687-4722-2012-25

Hussain, M., Wahab, A., W., A., Idris, Y., I., B., T.S. Ho, A., Jung, K., H., (2018). Image steganography in spatial domain: A survey, *Signal Processing: Image Communication*, 65, 46-66, https://doi.org/10.1016/j.image.2018.03.012.

Kadhim, I., J., Premaratne, P., Vial, P., J., Halloran, B., (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research, *Neurocomputing*, 335, 299-326, ISSN 0925-2312,

Khan Farhan Rafat , (2009). "Enhanced Text Steganography By Changing Word's Spelling", *FIT'09*, December 16–18, 2009, CIIT, 2009, ACM.

Lubacz, J., Mazurczyk W., Szczypiorski, K., (2014). "Principles and overview of network steganography", in *IEEE Communications Magazine*, vol. 52, no. 5, pp. 225-229, May 2014, doi: 10.1109/MCOM.2014.6815916.

Pa Malathi, Ma Manoaj, Ra Manoj, Vaikunth, R., Vinodhini, R., (2017). Highly improved DNA based steganography, *Procedia Comput Sci*, 115:651–659

Sharma, S., Gupta, A., Trivedi M.C., Yadav, V. K., (2016). "Analysis of Different Text Steganography Techniques: A Survey," *2016 Second International Conference on Computational Intelligence & Communication Technology (CICT)*, Ghaziabad, India, 2016, pp. 130-133, doi: 10.1109/CICT.2016.34.

Shirali-Shahreza, M., H., Shirali-Shahreza, M., 2008 (a). "A New Synonym Text Steganography". *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 978-0-7695-3278-3/08 © 2008 IEEE.

Shirali-Shahreza, M., Sajad Shirali-Shahreza, S., 2008 (b). "Steganography in Text Documents", *Proceedings of 2008, 3rd International Conference on Intelligent System and Knowledge Engineering.*

Urbanovich, N., Plaskovitsky, V., (2012). The use of steganographic techniques for protection of intellectual property rights. 88. 342-343.

Venkatraman, A., Abraham, S., Paprzycki, M., Significance of steganography on data security, *in: Proceedingsof the ITCC 2004 International Conference on Information Technology: Coding and Computing*, IEEE, 2004, pp. 347–351