

A Survey of Spatial Domain Techniques in Image Steganography

Asst. Teacher Ammar Awad
Education College / University of Wasit

Abstract

This paper presents the most techniques of spatial domain that used in image steganography where it is used to hide confidential message under a cover image. Steganography is a much better way to convey a secret message compared to cryptography. This is because cryptography is outlawed while steganography can avoid such policies to pass message covertly. Steganography is one of the most common techniques of securing information, which insists on concealing the clandestine data within the cover image in a way that nobody suspects to its existence. The challenge of steganography techniques is to make a reasonable balance between the file and the size of data that can be exchanged. Furthermore, the strength of the strategy and the security of the mysterious data are the fact that can't be hidden.

Keywords:

Digital image steganography, Adaptive steganography, robustness, Spatial domain.

1. Introduction

The current global explosion on the utilisation of internet and multimedia has raised the need for hiding data. This encouraged data hiding professionals to put more efforts in ensuring data safety for information that uses electronic media to move from one place to another. Steganography refers to the science and art of concealing data by installing them inside other, apparently, innocuous messages. It comes from a Greek term that means "covered writing". The aim of Steganography is to conceal the existence of a message and produce a secret channel in the process. It could be considered as complementing cryptography, whose aim is to conceal a message's content as mentioned in [1, 2, 3, 4].

Steganography is as ancient as the communication of messages from its source to the destination. This began in the Greek period. It was during the time of Greek tyrant Histiaeus, a 5th Century BC prisoner under King Darius. Histiaeus used to send messages to his son-in-law by tattooing and barbing his head and then allowing the hair to grow back again before making the slave go to Miletus. It was during the twentieth century when the steganography system was established by the British during the Boer War. They created maps that used butterflies to indicate the Boer artillery base. Utilisation of internet, computer networks, and multimedia experienced an exponential increase and created a fully metamorphosed steganography system that could be used by entities such as terrorist attackers so that they could plan their criminal activities as stated in [5, 6].

2. Types of Steganography

The ascent of the web and the further improvement of PC innovation have given steganography another life and allowed for the utilisation of several creative methods. Changes to digital carriers were introduced by computer-based Stenographic technologies so that foreign information can be embedded to the native carriers. Such message carriers may bear a resemblance to innocent's texts, sounds, disks, protocols and network traffic in the manner that software or circuits arrange images, audio, video, or any other digital transmission or code as mentioned in [7, 8]. The figure 1 shows the types of steganography.

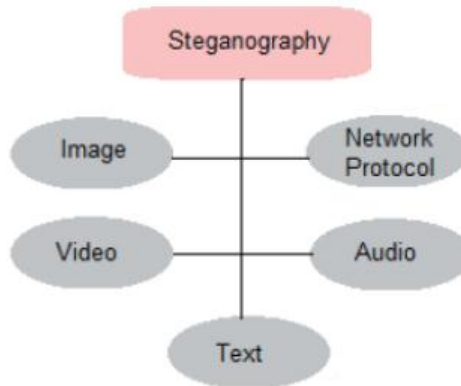


Figure 1 Types of steganography (Adopted from [7])

2.1 Audio Steganography

Modification of sound files is utilised to embed secret information. This task is difficult because the Human Auditory System (HAS) ranges a span of more than a billion and has thousands of frequencies in decibels (dB). Moreover, HAS has sensitivity towards random noise and is able to detect disturbances below 80dB of ambient level in a sound file as stated in [9, 10]. However, HAS is not able to perceive the sound when masking happens, since masking takes advantage of the human ears' ability to hide the secret message. Techniques for audio steganography include several methods, such as least significant bit; phase coding, echo hiding, amplitude modification, and spread spectrum coding. The figure 2 shows the Audio Steganography System.

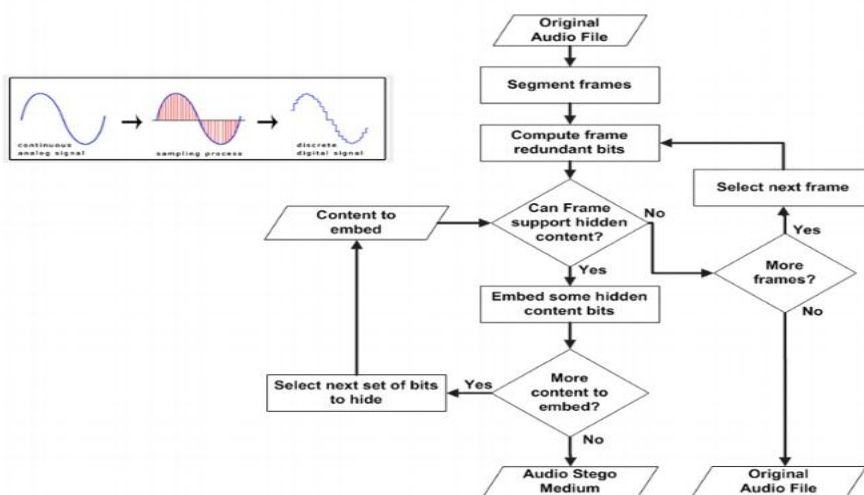


Figure 2 Audio steganography system (Adopted from [9])

2.2 Video Steganography

Video files represent another kind of steganography. This type refers to a collection of sounds and images. As such, any technique that uses images and sounds can utilise video steganography. This media can embed a lot of data. Moreover, the chances of sensing these data can be very low as stated in [11, 12, 13]. One of video steganography's advantages is that it has a continuously moving stream of sounds and images. Thus, noticeable distortions will go unnoticed because

information can be concealed by the moving stream as mentioned in [12, 13]. The figure 3 shows the video steganography system

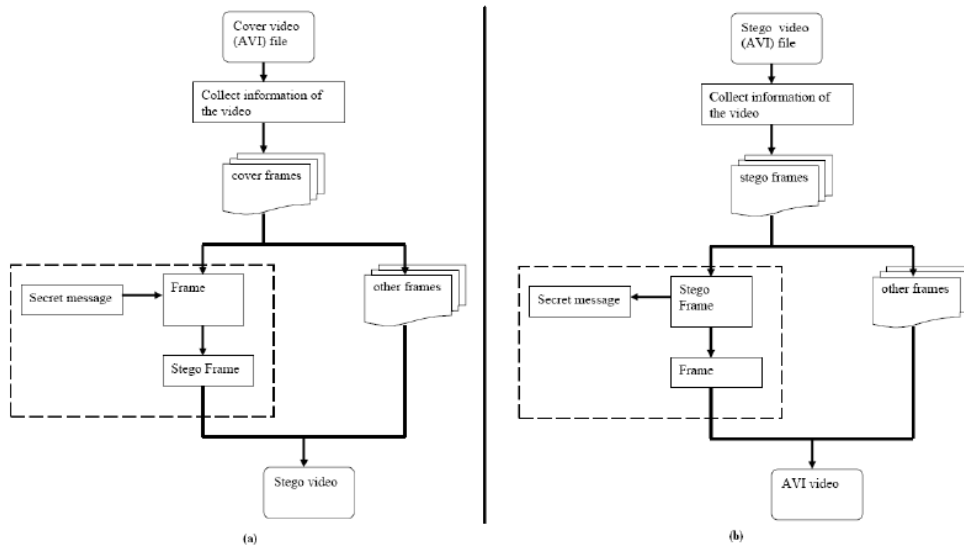


Figure 3 Video steganography system (Adopted from [11])

2.3 Text Steganography

This technique involves a text to embed a secret message. It performs a simple alteration on the characters or the text's formatting. It is still not completely known if a robust and secure steganography is possible using text messages as stated in [14, 15, 16]. Text steganography techniques include word-shift coding protocol, line-shift coding protocol, whitespace manipulation, XML, semantic, syntactic, text content, and cover generation techniques. Utilisation of text steganography does not occur often because it has a small amount of redundant data.

Example: Susan eats truffles. Under pressure that helps everything before Owing Major Bullwinkle. Real or secret message "Set Up the b0MB"

2.4 Image Steganography

Image steganography is considered the most common form of data secretion technique since it is able to firm large data within the cover image without compromising the cover image's quality. It generally uses a grey scale image because it has a pixel value of 8 bits and because its hiding capacity is greater compared to other image formats. Images can exist in grey scales, monochrome, or in other colour schemes. Generally, grey scale images are more appropriate for image steganography because any changes on the colour components can expose the presence of embedding as mentioned in [17, 18, 19]. The figure 4 shows the system of image steganography.

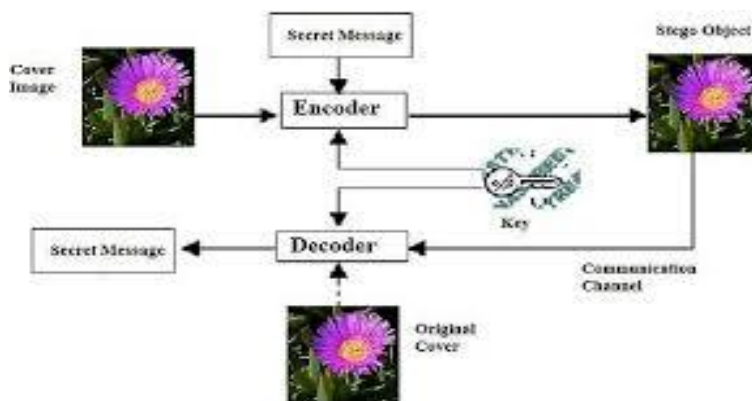


Figure 4: System of Image Steganography (Adopted from [17])

3 Steganography Protocols

To create an effective system for steganography, there are three kinds of steganography protocols. However, the researchers only have to choose one of these three protocols. These protocols are secret key steganography, pure steganography, and public key steganography as stated in [20, 21, 22].

1. **Pure Steganography:** This steganography system can ensure the hiding of data without having to exchange some secret information first, like the key. The two parties involved should have previous knowledge about the algorithms for embedding and extracting. However, this knowledge should not become public as stated in [1, 22].

2. **Secret Key Steganography:** This technique bears a similarity to a symmetric cipher. In this cipher, the sender picks a cover C where it can embed the secret message via a secret key known as K. To extract the message, the receiver should be aware of what key was utilized in the establishing of encryption operation. This key is needed to reverse the process and obtain the hidden message. Consequently, in the absence of the secret key, the encoded message cannot be detected easily by anyone as stated in [20, 22].

3. **Public Key Steganography:** This protocol utilises two keys, a private one and a public one. The public key is kept in a public database while the private key is used during the establishing procedure. Moreover, the private key is used to remake the confidential message. Furthermore, the encrypted message can hide in plain sight, while the protocol can randomly employ the public key steganography as mentioned in [23, 24].

4 Steganography Terminologies

According to Hopper [25] and Denemark [26] the steganography involves the use of certain terminologies, such as cover or host, embedding, stego-object, and extraction. Figure 5 discussed types of steganography terminologies.

- **Cover or host:** this refers to the genuine, pure message, audio, data, video, or still image.
- **Embedding:** refers to the procedure of storing the embedded or hidden information into the cover information
- **Stego-object:** refers to the data that contains both the embedded information and the cover signal.
- **Extraction:** refers to the procedure of extracting the cryptic data from the stego object.
- **Stego-key:** refers to the key that is shared between two parties (sender and receiver). This key is also used to embed and extract the secret message.

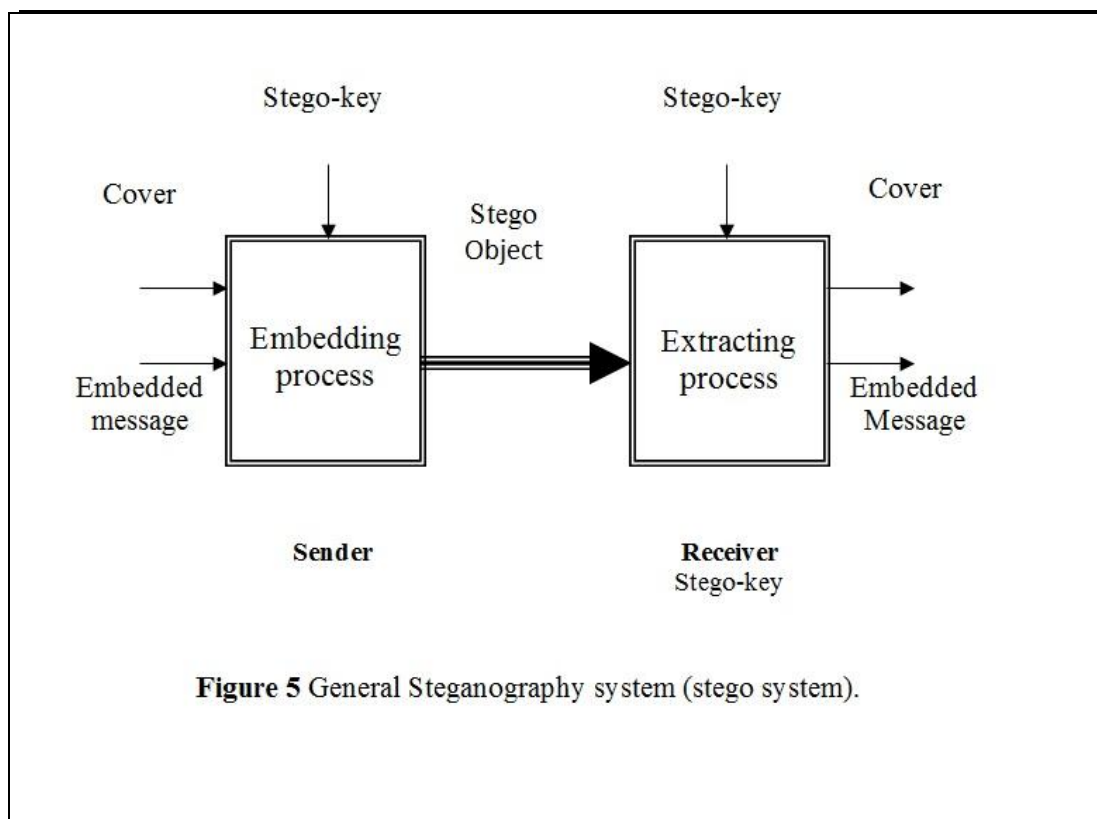


Figure 5: General Steganography System (Adopted from [25])

5 Steganography Properties

According to Ali in [27] suggested that for the data hiding technique to have an effective scheme, it should possess security, robustness, imperceptibility, invisibility, and payload. The following subsections will explain the main properties.

Robustness: An embedding algorithm is considered secure if one cannot remove the embedded information beyond credible revelation using targeted assaults that depend on a perfect knowing of the detector (except the secret key) and the embedding algorithm, and knowing at least one carrier carrying a hidden message as stated in [28, 29].

Imperceptibility: Human Visual System (HVS) or Human Audio System (HAS) is an invisibility property. Therefore, no perceptible artefacts must be left behind if humans are not able to distinguish between carriers with or without a hidden message as stated in [23, 27, 30]. The image's quality is measured via the peak signal to noise ratio (P) at the end of the embedding process. This is done to assess the diversity between the stego-image and the original image. The integrating data is considered insignificant to human sight when the acquired outcome is equal to 30 dB as mentioned in [30].

$$P = 10 \log_{10} \frac{255^2}{M} \quad (2.1)$$

Where M represents the mean square error that can be defined as

$$M = \sum_{i=1}^{r*c} \frac{(g_i - g'_i)^2}{(r*c)} \quad (2.2)$$

Where, c and r refer to the size of the image, and g'_i and g_i represent the stego-image and cover, respectively.

Payload Capacity: Capacity is used to refer to the quantity of information that could be- concealed in relation to the cover's size. There are trade-offs that exist between the degree of host signal degradation and the amount of embedded data; a data-hiding method is able to operate with either high modification resistance or high-embedded data rate, but not both. When one of these factors increases, the other should decrease as written by [1, 9, 30].

6 Image Steganography Techniques

This section discussed the most techniques that are used in image steganography. However the image steganography techniques can be categorized into three groups: Spatial domain (Substitution Technique) and Transform domain based on the following diagram.

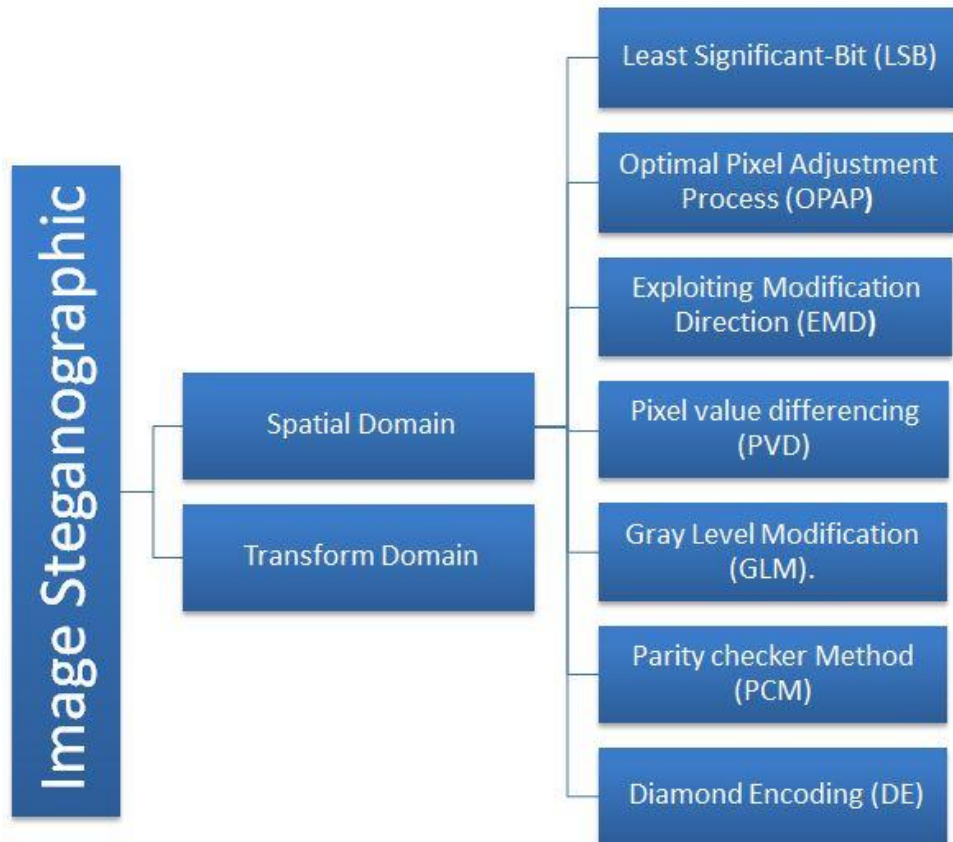


Figure 6: Image Steganography Techniques

Therefore, this paper focused on the techniques of spatial domain which is used in image steganography and these techniques are discussed in following subsections.

6.1 Least Significant-Bit (LSB)

The Least Significant-Bit (LSB) utilises one of the most prevalent methods as stated in [9]. For this method, the immediate dealing takes place with a cover-image once a confidential image is hidden inside it. It commonly uses bit-mapped images. Every single image is made up of a set of pixels. Furthermore, one colour

is represented by every pixel. Grey-scale images have a value that ranges from 0 to 255. If the pixel value is equal to (0), darkness is signified. When the pixel value is equal to (255), it indicates lightness. Therefore, adjusting the values can adjust a grey level image. To represent these values, at least 8 bits are needed. These values are stored by the binary system from bit b_1 , b_2 ... b_8 . The LSB substitution is altered in the last bit (b_1) in order to produce an insignificant adjustment that cannot be perceived by the human vision system. For example, if the pixel has a value of 100 and we aim to embed a 1, the value of the pixel becomes 101. This difference is not perceived by human vision. However, LSB can embed secret data into an image easily while having an imperceptible effect on the image as written by [15, 31, 32].

6.2 Optimal Pixel Adjustment Process (OPAP)

Chan and Cheng [33] proposed the Optimal Pixel Adjustment Process (OPAP) to address the drawbacks of the LSB method. It does this by embedding each pixel with more than one bit in the cover image and reducing image distortion by adding complex computation. This algorithm was able to reduce image distortion effectively. The OPAP embeds data using the last n bits while it toggles the $n+1$ bit at the same time. It does this while it compares the toggle with the least distortion. However, the efficacy of OPAP is only exhibited when establishing two or more bits as written by [34, 35].

6.3 Exploiting Modification Direction (EMD)

Xinpeng and Shuozhong [36] proposed the Exploiting Modification Direction (EMD) in order to lessen the stego image's distortion. EMD is used n pixels as a group so that it could establish hidden digits to a $(2n+1)$ array notational system. Furthermore, embedding needs a decrease or an increase from a specific pixel's value within the set. For this method, it is necessary to compute for the value of n before embedding. The image's highest quality is achieved when the value of n is equal to 2, where the embedding is represented by only one secret digit within each two pixels.

6.4 Pixel Value Differencing (PVD)

Wu and Tsai [38] proposed Pixel value differencing (PVD) steganography with a thought that pixels at edge ranges can conceal more number of bits contrasted with

the pixels at smooth areas. An area means a block with two continuous pixels. The quantity of bits installed in a block relies on the distinction esteem between the two pixels. Besides, PYD techniques utilizing four pixel blocks are proposed to build the inserting capacity.

6.5 Gray Level Modification (GLM)

The grey level values of those pixels are checked and contrasted to the bit stream that is to be mapped in the image. At first, the gray level values of the chosen pixels (odd pixels) are made even by changing the grey level by one unit. When all the chosen pixels have an even grey level, it is contrasted to the bit stream, which must be mapped. The principal bit from the bit stream is contrasted to the initial chosen pixel. When, the primary bit is even (i.e. 0), then the primary pixel is not altered as all the chose pixels have an even grey level value. Whenever the bit is odd (i.e. 1), then the grey level value of the pixel is decremented by one unit to make its esteem odd, which then would represent an odd bit mapping. This is done for all bits in the bit stream and every single bit is mapped by changing the grey level values consequently. [37]

6.6 Parity checker Method (PCM)

In this method the image steganography process by improved the data storing or pay load capacity then making use of modification direction. This scheme had provided robustness to communication system to communicate over secure or unsecure channel. This full Technique works on pixel pairing. [39]

6.7 Diamond Encoding (DE)

In this method the image steganography process by improved the data storing or pay load capacity then making use of modification direction. This scheme had provided robustness to communication system to communicate over secure or unsecure channel. This full Technique works on pixel pairing

7- Conclusions

This paper offered a background discussion on the concepts related to our study. This was done in order to reinforce the idea of steganography and to obtain a better grasp about this research area, as well as the problem itself. Specifically, we first provided some general information about steganography and the concept of hiding information. Then, the steganography concept was reviewed, as well as the steganographic Protocols and types. Furthermore, there was a discussion of the current methods. Some efforts were also surveyed through the improvement of their methods. Afterwards, the formulas for steganography evaluation were described. Finally, an overview of the steganography methods and the steganography encryption attacks was presented.

Reference

- [1] Katzenbeisser, S. and Petitcolas, F. (2000). Information Hiding Techniques for Steganography and Digital Watermarking: Artech House, Inc.
- [2] Hussain, Mehdi, and Mureed Hussain. "A survey of image steganography techniques." (2013).
- [3] Subhedar, Mansi S., and Vijay H. Mankar. "Current status and key issues in image steganography: A survey." Computer science review 13 (2014): 95-113.
- [4] Pandit, Anuradha S., S. R. Khope, and Faculty Student. "Review on Image Steganography." International Journal of Engineering Science 6115 (2016).
- [5] Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J. and Kalker, T. (2006). Digital and watermarking (2nd ed.). USA: ELSEVIER.
- [6] Atkins, John F., et al. "Ribosomal frameshifting and transcriptional slippage: From genetic steganography and cryptography to adventitious use." Nucleic acids research (2016): gkw530.
- [7] Johnson, N.F., Duricn, Z. and Jajodia, S. (2001). Information Hiding: Steganography and Watermarking Attack and Countermeasurments. Journal of Electronic Imaging, 10(3), 825-826.
- [8] Roy, Souvik, and P. Venkateswaran. "Online payment system using steganography and visual cryptography." Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on. IEEE, 2014.
- [9] Bender, W., Gruhl, D., Morimoto, M. and Lu A. (1996). Techniques for data hiding. IBM Systems Journal, 35(3-4), 313-336.
- [10] Bilal, Ifra, and Rajiv Kumar. "Audio steganography using QR decomposition and fast Fourier transform." Indian Journal of Science and Technology 8.34 (2015).
- [11] Cummins, J., Diskin, P., Lau, S. and Parlett, R. (2004). Steganography and Digital Watermarking. School of Computer Science, University of Birmingham., 1(2), 1-24.

- [12] Sadek, Mennatallah M., Amal S. Khalifa, and Mostafa GM Mostafa. "Video steganography: a comprehensive review." *Multimedia tools and applications* 74.17 (2015): 7063-7094.
- [13] Mstafa, Ramadhan J., and Khaled M. Elleithy. "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes." *Multimedia Tools and Applications* 75.17 (2016): 10311-10333.
- [14] Mathkour, H., Al-Sadoon, B. and Touri, A. (2008). A New Image Steganography Technique. *Proceedings of the 2008 Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on.* 12-14 Oct. 2008. 1-4.
- [15] Vidhya, P. M., and Varghese Paul. "A Method for Text Steganography Using Malayalam Text." *Procedia Computer Science* 46 (2015): 524-531.
- [16] Yadav, Virendra Kumar, and Saumya Batham. "A novel approach of bulk data hiding using text steganography." *Procedia Computer Science* 57 (2015): 1401-1410.
- [17] Li, B., He, J., Huang, J. and Shi, Y. Q. (2011). A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing*, 2(2), 142-172.
- [18] Agarwal, Anshit. "Stretching the Limits of Image Steganography." *International Journal of Scientific and Engineering Research* 5.2 (2014): 1253-1256.
- [19] Zielińska, Elżbieta, Wojciech Mazurczyk, and Krzysztof Szczypiorski. "Trends in steganography." *Communications of the ACM* 57.3 (2014): 86-95.
- [20] Lucena, N., Chapin, S., Pease, J. and Yadollahpour, P. (2004). Syntax and Semantics-Preserving Application-Layer Protocol Steganography. Paper presented at the 6th Information Hiding Workshop IH, Canada :Toronto- Ontario.
- [21] Sedighi, Vahid, Rémi Cogranne, and Jessica Fridrich. "Content-adaptive steganography by minimizing statistical detectability." *IEEE Transactions on Information Forensics and Security* 11.2 (2016): 221-234.
- [22] Trivedi, Munesh Chandra, Shivani Sharma, and Virendra Kumar Yadav. "Analysis of Several Image Steganography Techniques in Spatial Domain: A Survey." *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies.* ACM, 2016
- [23] Michael, B. and Cachin, C. (2004). Public-Key Steganography with Active Attacks. *IBM Research*, 1-16.
- [24] Le, T. V. and Kurosawa, K. (2006). Efficient Public Key Steganography Secure Against Adaptive Chosen Stegotext Attacks. Paper presented at the 8th Information Hiding Workshop IH, USA : Old Town Alexandria-Virginia.
- [25] Hopper, N. (2004). Toward a theory of Steganography. Ph.D, Carnegie Mellon University, Pittsburgh.
- [26] Denmark, Tomáš Denmark, Mehdi Boroumand, and Jessica Fridrich. "Steganalysis features for content-adaptive JPEG steganography." *IEEE Transactions on Information Forensics and Security* 11.8 (2016): 1736-1746.

- [27] Ali, D. B. (2004). Digital Image Watermarking Techniques for Copyright Protection. Ph. D., University of Mosul, Mousl.
- [28] Michaud, E. (2003). Current Steganography Tools and Methods. GSEC Practical as part of GIAC Practical Repository, 1(4), 1-11.
- [29] Atoum, Mohammed Salem. "A Comparative Study of Combination with Different LSB Techniques in MP3 Steganography." Information Science and Applications. Springer Berlin Heidelberg, 2015. 551-560.
- [30] Jung, H. K. and Yoo, K. Y. (2009). Improved Exploiting Modification Direction Method by Modulus Operation. International Journal of Signal Processing, Image Processing and Pattern, 2(1), 79-88.
- [31] Shjul, A. A. and Kulkarni, U. L. (2011). A secure skin tone based steganography Using wavelet transform. International Journal of computer theory and Engineering, 3(1), 16-22.
- [32] Holub, Vojtěch, and Jessica Fridrich. "Digital image steganography using universal distortion." Proceedings of the first ACM workshop on Information hiding and multimedia security. ACM, 2013.
- [33] Chan, C.K. and Cheng, L.M. (2004). Hiding data in images by simple LSB substitution. Pattern Recognition, 37(3), 469-474.
- [34] Kai Yung, L., Wien, H., Chen, J., Tung Shou, C. and Wen Chin, C. (2010). Data hiding by Exploiting Modification Direction technique using optimal pixel grouping. Proceedings of the 2010 Education Techno+logy and Computer (ICETC), 2010 2nd International Conference on. 22-24 June 2010. V3-121-V123-123.
- [35] Garg, Shalu, and Monika Mathur. "Chaotic map based steganography of gray scale images in wavelet domain." Signal Processing and Integrated Networks (SPIN), 2014 International Conference on. IEEE, 2014.
- [36] Xinpeng, Z. and Shuozhong, W. (2006). Efficient Steganographic Embedding by Exploiting Modification Direction. Communications Letters, IEEE, 10(11), 781-783.
- [37] W. Hong and T.S. Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching," IEEE Transactions on Information Forensics and Security, vol.7, Feb. 2012
- [38] D. Wu and W. Tsai., "A steganographic method for images by pixel value differencing," Pattern Recognition Letters, vol.24, pp. 1613-1626, Jul. 2003
- [39] X. Zhang and S. Wang, "Efficient Steganographic embedding by exploiting modification direction," IEEE Commun. Lett. , vol. 10, no.2, pp. 781-783, Nov. 2006.