Journal of Network and Information Security
9 (1) 2021, 23-27
http://www.publishingindia.com/jnis

Steganography Model Techniques, Taxonomy with Deniable Methodology and Data Concealing in Image using Steganography

Abhay Verma[1*] and Vinay Verma[2]

[1]Student, Department of Computer Science and Engineering, Vivekananda Institute of Technology, Jaipur, Rajasthan, India. Email: verma.abhay2420@gmail.com

[2]Independent Researcher, Jaipur, Rajasthan, India. Email: vnverma03@gmail.com

*Corresponding Author

Abstract: The radical enhancements in the technology and internet has led information to be shared in just single click. As a result, it really became important to worry about the intellectual property protection on the internet. Steganography and cryptography could be very much useful in achieving the secure transfer of the information. Steganography is a practice that prevent unauthorized user from accessing and reading the secret data. It is a scientific art of covering the information so that it remains undetected to everyone except the intended receiver. In this technique, carrier plays an important role and must be selected in such a way that it does not leave behind any trace of the hidden message. There is always a threat that any person can detect the hidden object and could reveal the secret, but there is also a concept of deniable strategy in steganography which in such cases reveals the secondary data instead of primary one and keep that secure. The paper is meant to introduce with the introductory concept of steganography, classification of steganography centered on various file formats support (images, videos, protocols, text, etc.), deniable steganography which is providing additional layer of security and analysis of the noticeable changes created in stego-object as compared to original carrier..

Keywords: Cryptography, Deniable steganography, Image steganography analysis, Steganography, Steganography model.

I. Introduction

Cryptography, the method of encrypting the original message by converting it into a cipher text at the sender's end using decryption key and then decrypting the data at the receiver's end using decryption keys, and many different methods were created so as to keep messages secret. Since it is not abundant to keep the content of message secret, it is also necessary to keep the presence of message secret. This was achieved by the technique called steganography. Steganography techniques are ascertaining very beneficial in hiding the surreptitious data from any unauthorized person [1].

Steganography scheme includes embedding the secret message in the desired carrier. A stego-object is created which is basically the carrier with embedded message. This stego-object is then transmitted through a media. At the receiver's side, the extraction of the message out of the stego-object takes place, which is reverse process of embedding. This process recovers the hidden message from the stego-object. Fig. 1 portrays the model of steganography.

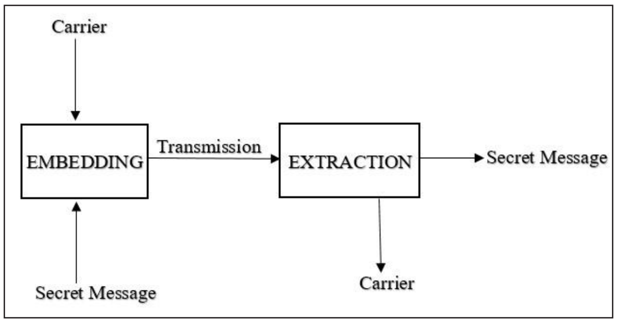


Fig. 1: Steganography Model

For hiding information, there are large number of steganography techniques which enables information hiding in images, videos and even protocols without any noticeable change. The main motive of the technique is to hide a form of information in other form of information without creating any change in the base information [1]. The word steganography is derived from Greek steganographia, where steganos meaning "covered" or "reticent", and graphia means "writing", which together forms "covered writing".

Both steganography and cryptography techniques are complement to each other, and neither technology unaided is perfect and can be compromised [2]. Once the hidden data is exposed or suspected by any unwanted person, then the tenacity of steganography is defeated. Thus, the potency of steganography technique can be intensified by combining it with cryptography applications.

II. Steganography Classification

Steganography technique supports application on images, text, audios, videos, network protocols, and many other cover medium, like email, hidden OS, folder, etc. Fig. 2 shows the major categories file formats which are supported by steganography.

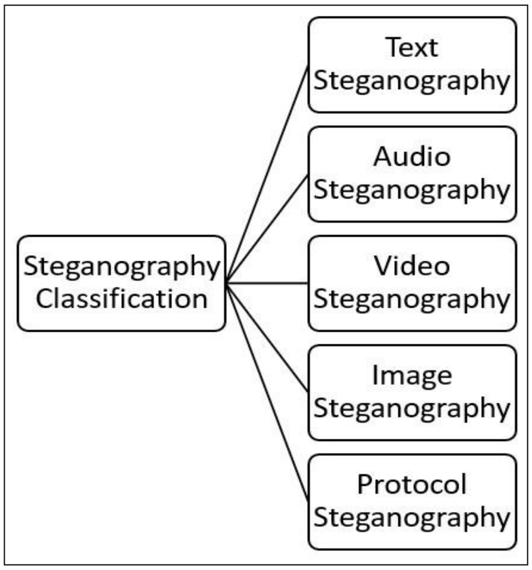


Fig. 2: Classification of Steganography Supported File Formats

- *Text Steganography:* It is the most historic steganography technique which was something like concealing the secret message in the n^{th} position of every n^{th} word, or similar technique. Although, it is difficult to achieve complete secrecy due to limited places to hide text in the carrier.
- *Audio Steganography:* Audio steganography deals with covering message in audio stream and it is a difficult technique to implement, as human ear can easily find any changes made in audio. Also, the digital signal processing's knowledge is required.
- *Video Steganography:* This steganography technique hides the message in forms of frames in between the actual video frames or every frame contains a secret message [3]. Since the video play at speed of 24 frames per second, then any hidden frame can't be detected easily. But the conditions, like playing video in slow motion or pausing it may reveal the hidden message.
- *Image Steganography:* Images have become most popular covering objects for steganography due to their small size, easy sharing and human eye cannot detect a very minute change done in the image [4].
- *Protocol Steganography:* Network Protocol Steganography is the newest approach towards steganography development. Various protocols of the OSI layer model supports this mechanism and the unused bits protocol or header bits are used to achieve the motive [5].

The major advantage that steganography offers and the purpose for what it was introduced is that the hiding of the secret message does not affect the outer appearance of the file. The support of the method with wide range of file formats especially with network protocols is creating a new benchmark in the network security [6].

III. Deniable Steganography

Deniable steganography is a deny-based technique that steganography offers. The technique allows the authorized person to deny credibly the fact that any sensitive data is being embedded in the carrier. This includes embedding an extra expendable decoy data that is need to be kept confidential and which will be revealed to the attacker in case he/she finds out presence of secret message [7]. This decoy data could be any less confidential or secret data which when revealed in front of attacker must claim like that is all there hidden inside the carrier.

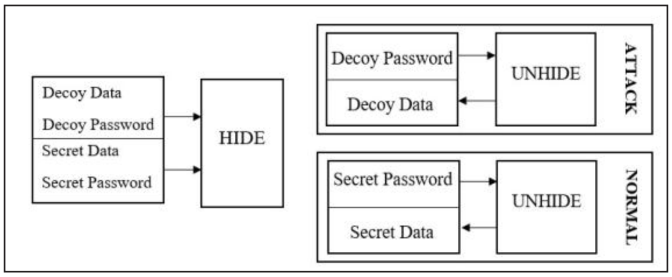


Fig. 3: Deniable Steganography

This type of techniqueis useful when a man in the middle finds out the presence of the hidden message and could extract information by means of forcing the sender to provide valid password or by using the same technique used in embedding process. It provides an additional layer of security to the stego-object and prevent disclosure of the actual hidden message.

IV. Image Steganography Analysis

Image steganography hides the secret message in image files of different formats such as png, jpg, pcx, tga and bmp. The various techniques used for image steganography are:

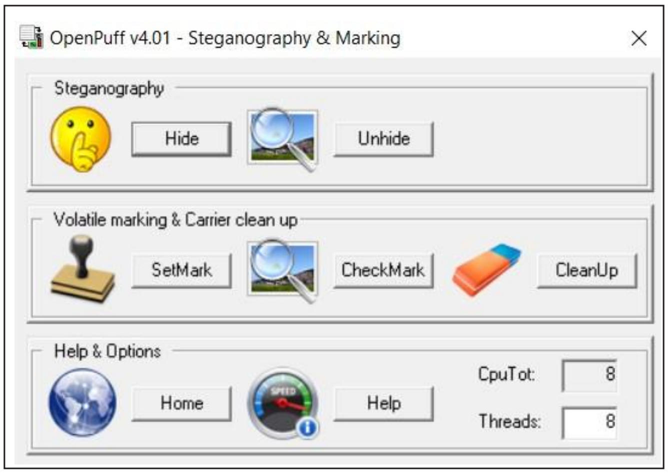
Least Significant Bit Insertion: The secret message's binary data is broken, and then inserted into the least significant bit of each pixel of the image file in a firm sequence [8].

Masking and Filtering: This technique covers data using techniques like watermarks on an actual paper; this can be ensured by altering the luminance of some part of image [9].

Algorithm and Transformation: The mathematical functions that are used in compression algorithm are used to hide data. Also, the secret message is entrenched in the cover image by changing the coefficient of transform of an image.

Metadata is the term used for the "*the data which provides information about other data.*" In general words, metadata are the properties of any file that defines the characteristics of the file.

The analysis of the image steganography is based on the comparison of metadata of the image before and after applying the steganography. The software used is *OpenPuff v4.01* to hide and unhide the secret message text file in the cover image. For metadata extraction, *EXIF & Metadata Viewer (https://exifmeta.com/index.html)* tool is used which is a web-based free tool for metadata extraction. Image is taken from the https://wallpapercave.com/w/wp2895347 source. Document file (*Message.txt*) with the content *"This is a hidden message."* is used as a secret message.


OpenPuff v4.01 - Steganography & Marking
Steganography
Hide
Unhide
Volatile marking & Carrier clean up
SetMark
CheckMark
CleanUp
Help & Options
Home
Help

CpuTot: 8

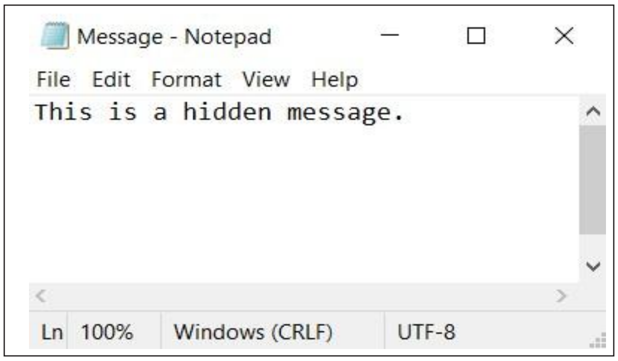
Threads: 8

Fig. 4: OpenPuff Screenshot

The process of analysis of an image includes the following steps:

- Note the metadata of the original image.
- Applying steganography on the image and embedding the text file with text "*This is a hidden message.*" written in it.
- Note the metadata of the new image created after applying steganography.
- Compare the metadata before and after applying the steganography.

Fig. 5 below demonstrate the text file that is used as a secret message.



```
This is a hidden message.
```

Fig. 5: Secret Message (Message.txt) File

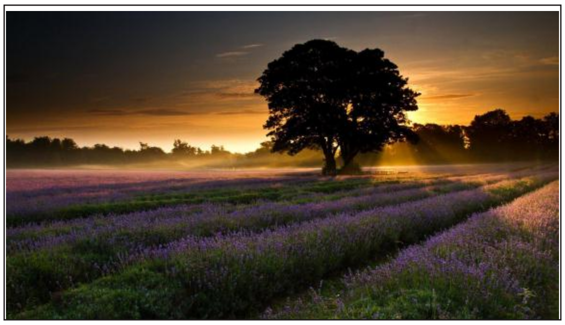


Fig. 6 (a): Original Image

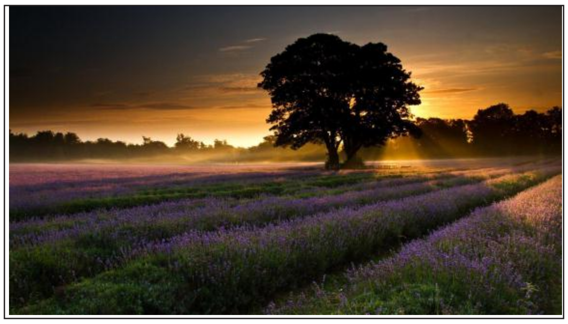


Fig. 6 (b): Stego-Object

Fig. 6 (a) is the original image before applying steganography and Fig. 6 (b) is the image after applying steganography, and it has the *'Message.txt'* file embedded in it.

When the steganography is applied on any image with any file as a secret message, a new image file in generated which has the embedded messages. This new file is then transmitted to the authorized receiver and requires a password to extract message from the cover image. Without valid password, the extraction process fails and the file is kept hidden. This password is applied by the sender at time of embedding the message in cover image.

Both the images appear to be same and not a single difference could be found. The quality of both images is the same, and there is no conciliation in the quality of the image after applying steganography.

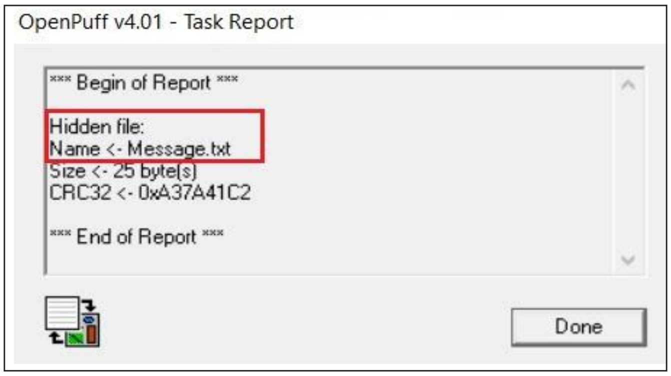
Table I: Metadata Comparison of Original and Stego-Object Image

Properties	Before Steganography	After Steganography
File Size	298182	298184
File Permission	644	644
File Type	JPEG	JPEG
Image Width	1920	1920
Image Height	1080	1080
Encoding Process	0	0

Properties	Before Steganography	After Steganography
Bits per Sample	8	8
Color Component	3	3
YCbCr Sub Sampling	2 2	2 2
JFIF Version	1 1	1 1
Resolution Unit	0	0
X Resolution	1	1
Y Resolution	1	1
Megapixels	2.0736	2.0736

The comparison of the metadata of both the images is given in Table I. It can be easily analyzed from the comparison table that there are no considerable changes created in the metadata except the file size of both files. Original image has file size of 298182 bytes, and stego-object has file size of 298184 bytes, but both forms 291 KB which makes it difficult to detect that any secret message is hidden.

At the receiver's end, when the image is extracted for the secret message, the text file that was embedded in the initial stage is recovered only by using correct and valid password by the receiver.



OpenPuff v4.01 - Task Report

```
*** Begin of Report ***

Hidden file:
Name <- Message.txt
Size <- 25 byte(s)
CRC32 <- 0xA37A41C2

*** End of Report ***
```

Fig. 7: Secret Message Extraction Report

The output after extracting the image is shown above in the Fig. 7, which names the file that was hidden and has been extracted to the defined designation folder. The extraction/unhide report mentions the name of the file hidden in the carrier (highlighted by red block).

V. Result

After the analysis of original and stego-image on basis of metadata comparison, it has been logged that there are no such considerable changes that took place in the metadata before and after applying steganography that could easily help in detecting whether the image is embedded or not. The major change takes place in the file size which just increases by 2 bytes and could vary based on the message size. All other metadata remains the same and it does not affect the resolution and quality of the image. With bare human eyes, it becomes almost unfeasible to detect the changes in the carrier made due to the steganography application.

VI. Conclusion

Steganography with the provision of cryptography is creating a new secured way for the digital communication in the high risk cyber world. The techniques are becoming quite useful in various fields, especially in defense or where data privacy means a lot. Both technologies are backbone of each other and the complement of one strengthens the other. The support of steganography technique with a wide variety of file formats which includes, text, folder, images, protocols, mails, and various others are another boon for the technology. The data can be embedded without creating any visible changes in the carrier convinces the data security from unauthorized person. On the other hand, deniable steganography provides an extra privilege to the sender to keep the hidden message secure even when an attacker finds such presence by uncovering the decoy data. Steganography has wide set of algorithms and techniques for different types of carriers and hidden message which are more difficult to crack. Images have some insignificance regions that the human visual structure cannot recognize, and by replacing, or adding other information in these regions does not deploy any noticeable changes which makes image steganography more reliable, secure, and effective [10].

References

[1] C. Cachin, "An information-theoretic model for steganography," in D. Aucsmith, Ed., Information Hiding, IH 1998, *Lecture Notes in Computer Science,* vol. 1525, Springer, Berlin, Heidelberg, 1998. [Online]. Available: https://doi.org/10.1007/3-540-49380-8_21

[2] R. J. Anderson, and F. A. P. Petitcolas, "On the limits of steganography," in *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 474-481, May 1998, doi: 10.1109/49.668971.

[3] S. D. Hu, and K. Tak U., "A novel video steganography based on non-uniform rectangular partition," *2011 14th IEEE International Conference on Computational Science and Engineering*, Dalian, 2011, pp. 57-61, doi: 10.1109/CSE.2011.24.

[4] A. Yahya, "Introduction to steganography," in *Steganography Techniques for Digital Images*, 2019, Springer, Cham, 2019. [Online]. Available: https://doi.org/10.1007/978-3-319-78597-4_1

[5] A. Dhamade, and K. Panchal, "Network protocols for steganography: A glance," *International Journal of Innovative Research in Technology*, vol. 1, no. 7, pp. 31-35, 2014.

[6] B. Jankowski, W. Mazurczyk, and K. Szczypiorski, "PadSteg: Introducing inter-protocol steganography," *Telecommun Syst*, vol. 52, pp. 1101-1111, 2013. [Online]. Available: https://doi.org/10.1007/s11235-011-9616-z

[7] P. H. Che, S. Kadhe, M. Bakshi, C. Chan, S. Jaggi, and A. Sprintson, "Reliable, deniable and hidable communication: A quick survey," *2014 IEEE Information Theory Workshop (ITW 2014*), Hobart, TAS, 2014, pp. 227-231, doi: 10.1109/ITW.2014.6970826.

[8] R. Chandramouli, and N. Memon, "Analysis of LSB based image steganography techniques," *Proceedings 2001 International Conference on Image Processing (Cat. No.01CH37205),* Thessaloniki, Greece, 2001, pp. 1019-1022, vol. 3, doi: 10.1109/ICIP.2001.958299.

[9] R. Chandramouli, M. Kharrazi, and N. Memon, "Image steganography and steganalysis: Concepts and practice," in T. Kalker, I. Cox, and Y. M. Ro, Eds., Digital Watermarking, IWDW 2003, *Lecture Notes in Computer Science*, vol. 2939, Springer, Berlin, Heidelberg, 2004. [Online]. Available: https://doi.org/10.1007/978-3-540-24624-4_3

[10] A. A. J. Altaay, S. B. Sahib, and M. Zamani, "An introduction to image steganography techniques," *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT),* Kuala Lumpur, 2012, pp. 122-126, doi: 10.1109/ACSAT.2012.25.