Matrix Academic International Online Journal Of Engineering And Technology
ISSN: 2348-3326, SJIF 2013 3.9
www.maioj.org © MAIOJET
Volume 4, Issue 1

A Comparative Study of Various Security and Issues in Steganography Techniques

Sukrati Jain[1], Ashendra Kumar saxena[2]

[1]*CCSIT Teerthanker Mahaveer University Moradabad*
[2]*CCSIT Teerthanker Mahaveer University Moradabad*

[1]sukratijain0918@gmail.com
[2]ashendrasaxena@gmail.com

Abstract - **In today's era, Most of the persons anxious about the security of confidential information because confidentiality is an energetic part. Sensitive information should be confidential because data can be accessed by intruders. Secrecy of message has always been a challenging task. For securing our communication, we use several types of steganography techniques. Steganography is the most popular technique to hide the data from intruders and none other than observer can recognizes the existence of content. The existence of content cannot be presumed out by the smart reader. Steganography is the technique by which we can share sensitive information surreptitiously and securely. For researchers, it has ever been an attracted subject to improve protect procedures to share message with authorized person only. In this review paper, we have premeditated several approaches proposed by research scholars in the field of steganography and analyse various steganography techniques, security issues and compare these techniques with their features and limitations. The major contribution of our paper is to represent comparative study of some existing steganography techniques.**

Keywords— **Steganography, Techniques, Confidentiality, Communication.**

I. INTRODUCTION

The main mottos of steganography will be the content should not be perceptible to anyone. Steganography means "Masking of message" so that others will have no ability to recognize it. While cryptography is a way of keeping and conducting data in a specific form so that only those who are authorized recipient can recognize it. Steganography takes a step further by modification of cryptography in the field of hiding encoded information, instead of observer nobody can suspects its presence. Whoever detecting your documents will fail to recognize it. It consists encrypted data key concept behind steganography. Rumour has it that terrorists used steganography to transmit messages to one another [1]. Steganography can also be defined as 'Stego-medium is a combination of Cover medium, secret message and Stego key'. A stego-key, for controlling the concealing procedure so as to confine retrieval of the inserted information to the third party who identify it [2]. Imperceptibility and robustness are the characteristics estimated of a stego-medium, in order that the sensitive information is recognizable by the deliberated recipient only and furthermore the stego-medium having ability to prevent content from opponents.

The quantity of confidential information inserted would be like that it does not diminish the excellence of stego-image [3]. Some Steganography software that we use to secure our communication are EZStego (Stego Online, Stego Shareware, Romana Machado),Gif-It-Up v1.0 (Lee Nelson),Hide and Seek (Colin Maroney),JPEG-JSTEG (Derek Upham) etc. Steganography will be the technique in which a individual should not be able to discriminate the existing and the stego-image(imperceptibility). The technique should be the volume of sensitive message that can be inserted without

distortion of the quality of the image (capacity) and even to the receiver the grade of effort, necessary to alteration of inserted information deprived of destroying the mask image (robustness) [4]. This paper organized in to 5 sections: Section 1 presents a study of steganography and the types of Steganography. Section 2 designates the summary of several steganography methods along with their advantages and disadvantages. Section 3 provides reviews and study of different existing methods of Steganography drawn from literature survey. Section 4 represented a comparative study of several steganography methods. Finally, conclusion is presented in Section 5.

TYPES OF STEGANOGRAPHY:

There are several types of steganography which are as follows:

A. Text steganography
B. Image steganography
C. Audio steganography
D. Video steganography
E. TCP/IP packets

A. *Text steganography:* In this technique of steganography, the secret data is embedded in text form by altering certain properties of the text document. This technique is not widely used [12]. It can be broadly categorized into 3 types:

1. *Format-based methods:* This method includes physical alteration of the format of text to hide the information. But if stego-file is opened by using word processor, spelling errors and unusable tabs will get detected. Different font's sizes can stimulate doubt to a smart reader. Additionally, if the original plaintext is available, comparing this plaintext with the suspected stenographic typescript would make operated portions of typescript quite observable [14]. However, Bennett has specified that this technique accomplished to trick most of the smart readers but it can't trick once processors have been used.
2. *Random & statistical generation:* Random and statistical generation is producing mask text according to the statistical properties. One technique is to cover message in random observing order of fonts. In alternative technique, the numeral characteristics of letter rates and word size are used in the way to generate words which will perform to have identical statistical characteristics as authentic words in known semantic [15, 16].
3. *Linguistic method:* This technique definitely deliberates the linguistic characteristics of improved & produced text, & in various procedures, works through linguistic construction like tab where contents are concealed [14].

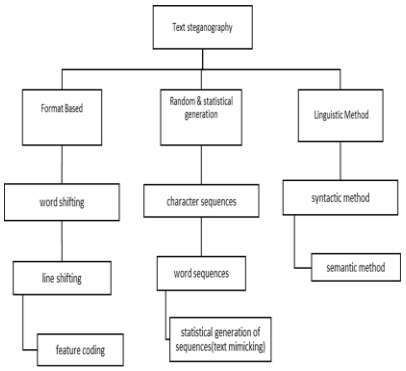

Fig. 1: Model of Text Steganography

There are number of techniques that can be employed in text steganography which are as follows [17]:

- *Word shifting coding:* Confidential information is concealed by shifting the position of words horizontally.
- *Feature coding:* Confidential information is concealed by modifying one or more features of the text.
- *Open space method:* Trailing spaces of each line of text for concealing secret information.
- *Line shift coding:* Confidential information is concealed by shifting the position of text lines vertically.
- *Semantic/Syntactic methods:* For altering the document uniquely uses synonyms of certain words in semantic methods and in syntactic methods uses punctuation marks.
- *Character sequences:* The secrecy of information within character an order is inserting the information to be seemed in frequent sequence of characters. This sequence must seem to be frequent to anybody who captures the message.
- *Word sequences:* The secrecy of information within word sequences, the definite dictionary substances is used to encrypt one or more bits of information per word through a code-book mappings between bit orders and lexical objects.
- *Statistical generation of sequences:* In addition, using the numeral frequency of letters or words in the way to create cover text.

B. *Image Steganography:*

One of the most significant techniques of steganography can embed the confidential information in the image. This

is achieved by adjusting the pixels values. Various terms that are contained in Image Steganography are [19]:

1. *Cover Image:* An importer of confidential information.
2. *Stego Image:* When secret information is embedded in to the mask image, the resulting image is known as stego image.
3. *Message:* The original data which is to be concealed.
4. *Stego key:* To embed and retrieve the original data through embedding and retrieving algorithm respectively, the stego key is required.

There are no. of techniques that can be employed in image steganography which are as follows [18]-

- *Spatial domain method:* In this method, the confidential information are inserted in cover image directly. In this scheme, the most general and easiest Steganography technique is LSB substitution method. In this scheme, LSB bits (pixels) are changed by the secret bits [21]. Hiding the data through BPCS (Bit Plane Complexity Segmentation) method has restricted data hiding capability that can keep secret up to 10-15% (vessel data amount) & can keep secret up to 50-60% (data) [20]. The baseline standard of BPCS procedure is that, the binary image is decomposed into "informative region" and noise region. Hiding the data through MBPIS (Multi Bit Plane Image Steganography) includes 2 algorithms pixel difference histogram analysis and RS steganalysis which identify the infrequent alterations affected by inserting confidential information into mask image and avert the human visual system analysis [18].
- *Transform Domain method:* It is the most complex technique for concealing data in an image. Several algorithms and alterations which are used for concealing data that are embedded in image. This type of domain embedding also known as a domain of embedding procedures for which various procedures have been proposed [22].Transform domain techniques have an plus point in comparison to spatial domain techniques i.e. they cover up message in zones of the image which are fewer uncovered to inflexibility, cropping, and image processing. Several transform domains procedures are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT). Through these transform techniques, we can concealing message in cover image transform constants [18].
- *Spread spectrum technique:* The information is blowout over a wide-ranging frequency bandwidth in comparison to the least bandwidth needed for sending the data [18].
- *Statistical technique:* In this technique, blocks and the message bits are the two portions of cover that are veiled in all blocks. By altering several numeral features of stego image, encrypt the information. The cover block remains unaffected, if message block is zero [18].
- *Distortion technique:* This method need information of original mask image, during decrypting process where decrypting functions observes variances between the original and distorted image for restoring the confidential message. The encrypted individual enhances a series of alterations to the mask image. Thus, data is defined as being warehoused by signal alteration [23]. In this procedure, a stego item is generated by applying a series of alterations to mask image. This series of alterations is compared with the confidential information desired to conduct [24]. The statistical features of the image are not distorted. Though, the requirement for transferring the cover image restricts the profits of this method.

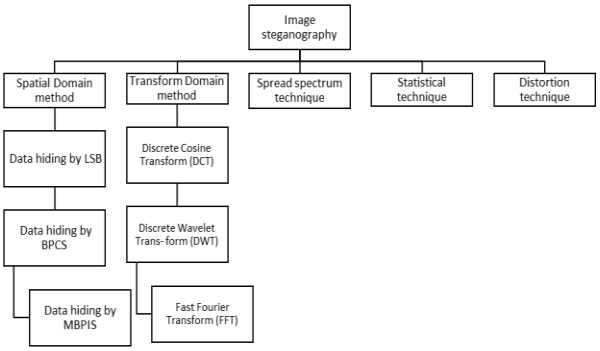

Fig. 2: Model of Image Steganography

C. *Audio Steganography:* It is the technique where the confidential information is inserted in the audio form means digital sound. Various audio formats which can be used to create a stego image are MPEG, AVI etc.

There are no. of techniques that can be employed in audio steganography which are as follows-

- LSB coding
- Parity coding
- Phase coding
- Echo coding
- Spread spectrum

- *LSB coding:* A most common approach is LSB algorithm, which substitutes the bits in certain bytes of the hidden file for hiding a series of bytes that contains the secret data [25]. It is used in audio communications like mobile communications. It transforms an analog audio signal to digital audio signal of hidden message [26].
- *Parity coding:* It is the most vigorous steganographic methods in audio steganograhy. In this technique, a signal divided into separate samples rather than divided into individual samples and inserts each bit of hidden message from a p-bit [25]. If the p-bit of a particular section doesn't equivalent to the secretive bit to be encrypted, the procedure reverses the LSB of samples in the section. Hence, the dispatcher has additional choice in encrypting the secret bit.

- *Phase coding:* It is the most popular encoding technique in comparison to other techniques. It is divided the original audio file into blocks and replaces phase of initial audio block with the phase that embodies confidential information. One shortcoming of this technique is that less capability because message is stored in initial block only. In fact, the phase constituents of audio are not as noticeable to the mortal ear as noise is [26].
- *Echo coding:* In this technique, confidential information embeds in an audio file by presenting an echo into the distinct signal. Echo of the mask signal has 3 parameters which are capability, decay rate and offset from the actual signal i.e. diverse to signify encrypted the confidential binary message [27]. It has several features in comparison to other techniques are of providing a high data transmission rate and higher robustness. One bit of confidential information could be encrypted only if not more than one echo was created from the actual signal. Thus actual signal is decomposed into blocks previously the encrypting procedure initiates.
- *Spread spectrum:* This technique is just like a radio frequency communication. Using the technique information is delivered, spread spectrum is deliberately spread across as more of the frequency spectrum like feasible using through a code which is autonomous of the original signal. Spread spectrum has two methodologies, the Direct Sequence Spread Spectrum (DSSS) which is an inflection method used in communication through transmission media and Frequency Hopping Spread Spectrum (FHSS) [27]. In some regions this technique contributes a better presentation in comparison to other techniques such as LSB encoding, phase encoding, and parity encoding in that it proposes a sensible data transmission rate, higher robustness against elimination techniques. But it has drawback also i.e. it can introduce noise into an audio file [22].

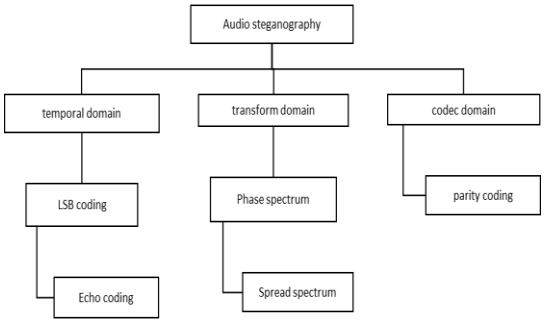

Fig. 3: Model of Audio Steganography

D. *Video steganography:* The video was then divided into several slow speed and single scene video sub-sequences. After the scene detection process, they embedded the secret message in the video file without any distortion. Finally the embedded video was tested for Steganalysis to check the presence of hidden data in the video.

1. LSB method
2. Non uniform rectangular partition
3. Compressed video steganography
4. Anti – forensic technique
5. Masking and filtering

1. *LSB method:* This technique is one of the most popular techniques for the security of data due to its effortlessness and frequently used approach. For embedding the data, It is the most simplest and effective approach. In this technique, the pixel values (bytes) of cover videos are removed, and then its least significant bits are substituted by the secret bits that we will insert. Now since we alter the LSB bits of the host video only, it doesn't get distorted and virtually looks alike as the actual video [28].
2. *Non-uniform rectangular partition:* This technique is used steganography for uncompressed domain. In this technique, by hiding an uncompressed secret video file in the host video file we can hide the data. But we have to ensure that both the secret and the cover file must be of the equal size. The secret video will be concealed in the leftmost 4 LSB bits of all frames of the source video [28].
3. *Compressed video steganography:* This technique is for the compressed videos only. Data can be inserted in the block of frame with extreme part alteration and in P and B block with extreme enormousness of signal directions [3].
4. *Anti-forensics technique:* These techniques are the activities which are occupied to damage, conceal and operate the data to attack the computer forensics. It offers security for protecting from unofficial individuals. Steganography is like anti-forensic where we attempt to conceal data under host file. Steganography and anti- forensics simultaneously makes the system more protected from unauthorized access [28].
5. *Masking and filtering:* This procedure is worked on 24 bits/pixel images and is valid for both colored and gray scale images. It looks alike as watermarking over an image and doesn't distorting the excellence of that image. In contrasting to other techniques, in data masking the secret message is so processed such that it looks like a multimedia file. Data masking cannot simply be sensed by predefined steganalysis [28].

E. *Protocol Steganography:* In this technique of steganography, communication protocol control elements are used to hide the secret data i.e. when mask object taking as a network protocol like TCP, UDP, and IP etc. In this, protocol is used as transferor. This domain is referred to as the network steganography. In the OSI model there is the existence of hidden channels where steganography can be found in new header bits of TCP/IP fields [13].

II. SUMMARY OF SEVERAL STEGANOGRAPHY METHODS

In this section, we represent several steganography methods along with their descriptions, features, disadvantages.

TABLE I

S. No.	Text steganography Techniques	Descriptions	Features	Disadvantages
1.	Word shift coding	For altering the document, horizontally shift the locations of words within text lines.	Less Identification because of variation of span between words.	Word shifted distance related algorithm can easily be detected.
2.	Feature coding	Altering one or more features of text.	Enormous data can be concealed in text.	If OCR program is used, the covert content would get distorted.
3.	Open space method	For altering the document uniquely, trailing spaces of each line of text.	Tabs in a document can't easily be noticed by the reader.	Erratic use of tabs is not transparent.
4.	Line shift coding	For altering the document uniquely, vertically shift the locations of text lines.	It is suitable for printed text.	Not suitable for OCR (Hidden content gets destroyed).
5.	Semantic/syntactic method	For altering the document uniquely uses synonyms of certain words / uses punctuation marks.	Can't detect by retyping or using OCR programs, Amount of information to hidden the method is insignificant.	Easily detect by smart readers/ It requires identification of correct places to insert punctuation marks.

TABLE II

S. No.	Image steganography techniques	Descriptions	Features	Disadvantages
1.	Least Significant Bit Technique	Total no. of bytes of the bytes of LSB into an image can be replaced with secret message bits.	Changes can't be recognize by the human eye, simple to implement.	Integrity of hidden content can easily be destroyed.
2.	Hiding gray images using blocks technique	Comparison of every pixel in inserting image to all the corresponding block pixels (cover image).	Hide the gray images and not easily detected by unauthorized individual.	Cover is decomposed into blocks of equivalent sizes.
3.	JPEG image steganography technique	The color of array is vast which makes it the best choice for tamping graphic imagery.	Uses lossy compression algorithm, popular for all imaging devices, low visibility and high robustness.	Low data capacity, medium payload capacity.
4.	Spread spectrum technique	Conceals and improves a message of considerable distance within digital imagery.	Can't detect easily by intruder, easy to extract, high data transmission rate, and high robustness.	Synchronizing long codes can be time consuming and codes need to be exactly orthogonal.

TABLE III

S. No.	Audio steganography Techniques	Descriptions	Advantage	Disadvantages
1.	LSB method	Digital audio file is changed with binary correspondent of private content.	Huge amount of data to be encrypted.	Easy to extract.
2.	Parity coding	Decompose a signal into distinct trials and embeds each bit of the hidden message from a P- bit	More robustness	Loss of embedded information
3.	Phase coding	Change primary audio fragment phase with a	Robust against signal processing operation	Low data transmission rate, only used for minor data.

		reference phase that signifies secret message.		
4.	Echo coding	Confidential message is inserted into covert audio signal like an echo.	Difficult to determine.	Low data security and less data capability.
5.	Spread spectrum	Spread the information overall signal frequencies.	Provides better robustness and increase transparency.	Susceptible to time scale variation & requires more bandwidth.

TABLE IV

S. No.	Video steganography Techniques	Descriptions	Advantage	Limitations
1.	LSB method	The cover video's pixel values are extracted which are in bytes, then its LSB are substituted by the secret message bits that we will embed.	Easy to embed the data & implement & high message payload.	Data may be destroyed by simple attacks or image compression, less robust.
2.	Non uniform rectangular partition	Hiding an uncompressed confidential video file in the source video stream with most similar size.	Conceal a source video without any alteration in source video.	Both the secret as well as cover file should be of almost the same size.
3.	Compressed video steganography	Data hiding operations are executed entirely in the compressed domain.	Extraction of data without requiring original video.	Useful only for compressed videos.
4.	Anti-forensics technique	Hide data under some host file.	Prevent data from unauthorized access.	Mainly used to attack the computer forensics.
5.	Masking & filtering	Hide a signal by different signal	Can't easily detected, applicable for both colored and gray scale images, more robust	It can be detected by simple statistical analysis and tools & apply only to gray scale images.

III. REVIEW ON RESEARCH

This research paper signifies a comparative study on steganography techniques. The PSNR (Peak Signal-to-Noise Ratio) value is used to measure the superiority of stego images. Higher PSNR rate specifies improved the excellence of image or minor distortion and also classify some valuable, reliable and effective steganography techniques [5].

This paper proposed a new method of image steganography for preventing data from unauthorized access and for data hiding also. In this technique, using a hash function can produce a form to conceal data bits into LSB of RGB pixel amounts (mask image). The proposed method ensures that the information has been encoded before concealing it into a covert image. If there is a situation, the encoded information got publicized from the covert image, the mediator other than intended recipient can't get information that it is in encoded form. It is used to increase the safety of confidential message [6].

This research paper suggests a protected steganographic mechanism based on cellular automata. Fibonacci representation presents frequently existing bit-planes that are used to conceal the data. The hidden bits are inserted into the upper LSB layers on the mask-image with lower distortion. For increasing the robustness of secret message against attacks that modify it, the hidden bits are entrenched into the upper LSB layers. Due to this more distortion to cover image will occur. So to diminish the distortion of covert image, an adaptive amendment was applied. The suggested theorem improves the presentation of safety of secret information against graphical, statistical attacks [7].

This research paper gives a suggestion of hidden steganographic frequencies. The technique is based on the alteration of cyclic prefixes in OFDM (Orthogonal Frequency-Division Multiplexing) ciphers. The proposed technique affords the utmost covert conduction and includes hypothetical study and imitation outcomes of the existed steganographic system presentation. The vital feature of the concealed channel's safety is covert secretive keys, presented in the procedure, which create frequent tabs between conducted secret message factors. But there is the requirement to fix an extra signal channel which would be used to approve the rate of secretive keys and deliver information related to conduction [8].

This research paper represents statistical methods which have been used for viral code detection. Such type of detection method is known as spectral analysis, because of its working with statistical distributions (bytes, instructions). This algorithm verifies the simulability of the equivalent statistical tests [9].

This research paper presents some particular Image based Steganography methods, which represents that an spectator can differentiate between images that carry secret information and images which do not carry information. Hence originates a

highly similar form appearance of the possibility of revealing of the images after that recognizes as how many bits can be inserted in the way to secure the covert image. A criminal's difficulty is assumed in the research paper in which Alice and Bob are two individuals who desire to interconnect with each other in the way to deliberate an escape plan. All inclusive transmission between them is inspected by a supervisor [10].

The research scholar presented LSB based hybrid approach which is used in AVI videos. Video is transformed into 20 equivalent gray scale images. Data hiding is complete in the host video by using 1 bit, 2 bit and 3 bit LSB substitution and after that Advanced Encryption Standard Algorithm is applied. When the source video is processed by using the data hiding techniques, the encoded AVI Video is sent by the sender and decoding is performed by the receiver. They got the PSNR and correspondence factor between existing and inserted image for 1 bit & 2 bit & 3 bit LSB Substitution and AES technique. It is observed that PSNR value decreases and security increases with the increase of LSB substitution bit. In this paper they have found no correlation relation between existing image and encoded image for altered frames [11].

IV. COMPARISON TABLE

In this section, we are comparing the study of several steganography methods presented in this paper to present in other research papers.

Authors	Text steganography					Image steganography			
	Word shift coding	Feature coding	Open space method	Line shift coding	Semantic/syntactic method	LSB Method	HGI using blocks	JPEG	Spread spectrum
Mr. Falesh M. Shelke (2014)	-	-	-	-	-	✓	✓	✓	✓
Vidhya saraswathi (2014)	✓	-	-	✓	✓	-	-	-	-
Monika Agrawal (2013)	✓	✓	✓	✓	✓	-	-	-	-
Masoud nosrati (2011)	✓	✓	-	✓	-	✓	-	-	-
In this paper (2016)	✓	✓	✓	✓	✓	✓	✓	✓	✓

Authors	Audio steganography				video steganography				
	LSB coding	Parity coding	Echo coding	Phase coding	LSB Method	Non uniform rectangular partition	Compressed	Anti-forensic	Masking & Filtering
Syeda Musfia Nasreen (2015)	-	-	-	-	✓	✓	✓	✓	✓
Gunjan Nehru (2012)	✓	-	-	✓	-	-	-	-	-
Burate D.J. (2013)	✓	✓	-	✓	-	-	-	-	-
Jayaram P (2011)	✓	✓	✓	✓	-	-	-	-	-
In this paper (2016)	✓	✓	✓	✓	✓	✓	✓	✓	✓

V. CONCLUSION

In this research paper, we discussed about various types of steganography techniques which help to protect confidential information without any distortion from intruders. We also talking about comparative study and reviews various research papers that are related to steganography. There are several different elements available which supports to improve in security like phase encoding, Least Significant Bit, spread spectrum. This research paper represented comparative study of text, image and audio, video steganography techniques so that individual can select the most secure technique for securing the secret message. The goal of this analysis is to isolate the consistent and best method.

REFERENCES

[1] (http://www.wired.com/news/politics/0,1283,41658,00.html)
[2] Fabien A.P.Petitcolas, Ross J.Anderson and Markus G.Kuhn, (1999) "Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, pp.1062-1078.
[3] C.P.Sumathi1, T.Santanam2 and G.Umamaheswari A Study of Various Steganographic Techniques Used for Information Hiding International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013
[4] rengarajan amirtharajan and J. B. B. Rayappan research journal on information technology 5(2):53-66,2013
[5] Ekta Dagar, Sunny Dagar Comparative Study of Various Steganography Techniques International Journal of Emerging Engineering Research and Technology Volume. 2, Issue 2, May 2014,
[6] Anil Kumar *, Rohini Sharma A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013 ISSN: 2277 128X
[7] Tuan Duc Nguyen , Somjit Arch-int A secure steganographic algorithm based on Cellular Automata using Fibonacci representation
[8] Szymon Grabski, Krzysztof Szczypiorski Steganography in OFDM Symbols of Fast IEEE 802.11n Networks
[9] Eric Filiol,Sébastien Josse New Trends in Security Evaluation of Bayesian Network-based Malware Detection Models

[10] R. Chandramouli, Nasir Memon,"Analysis of LSB Based Image Steganography Techniques", Computer Science Department, Brooklyn, NY 11201
[11] Hemant Gupta and Dr. Setu Chaturvedi,"video steganography through LSB based hybrid approach", International Journal of Engineering Research and Development, Volume 6, Issue 12 (May 2013), PP. 32-42
[12] Latika, Yogita Gulati A Comparative Study and Literature Review of Image Steganography Techniques IJSTE - International Journal of Science Technology & Engineering | Volume 1 | Issue 10 | April 2015
[13] Handel,T.& sandford, M., Hiding data in the OSI network model,proceedings of the 1st international workshop on information hiding ,june 1996
[14] K. Benett, "Linguistic steganography- survey, analysis and robustness concerns for hiding information in text," Purdue University, CERIAS Tech. Report 2004-13, 2004.
[15] L. Y. Por, and B. Delina, "Information hiding- a new approach in text steganography," 7th WSEAS Int. Conf. on Applied Computer and Applied Computational Science, 2008, pp. 689-695.
[16] L. Y. Por, T. F. Ang, and B. Delina, "WhiteSteg- a new scheme in information hiding using text steganography," WSEAS Transactions on Computers, vol.7, no.6, pp. 735-745, 2008
[17] Ronak Karimi ,Mehdi Hariri, Masoud Nosrati An introduction to steganography method World Applied Programming, Vol (1), No (3), August 2011,
[18] Preeti Singh, Charu Pujara Comparative study of various Techniques Employ in Image Steganography International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012
[19] Mehdi Hussain and Mureed Hussain A Survey of Image Steganography Techniques International Journal of Advanced Science and Technology Vol. 54, May, 2013
[20] ShrikantS.Khaire,Dr.BabasahebAmbedkand Dr Sanjay L Nalwarbar Steganography," Bit Plane Complexity Segmentation Technique , International Journal of Engineering Science and TechnologyVol. 2(9), 2010, 4860-4868.
[21] Johnson, N.F and Jajodia, S., "Exploring Steganography:Seeing the Unseen", Computer Journal, February 2008.
[22] N. F. Johnson and S. Katzenbeisser, "A Survey of steganographic techniques. in Information Hiding Techniques for Steganography and Digital Watermarking,S.Katzenbeisser and F.Petitcolas, Ed. London: Artech House, (2000), pp. 43-78.
[23] H. S. Majunatha Reddy and K. B. Raja, (2009) High capacity and security steganography using discrete wavelet transform. International Journal of Computer Science and Security. pp. 462-472.
[24] S. C. Katzenbeisser. Principles of Steganography. in Information Hiding Techniques for Steganography and Digital Watermarking", S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, (2000), pp. 43-78
[25] Jayaram P1, Ranganatha H R2, Anupama H S3 INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY
[26] Approach Gunjan Nehru1, Puja Dhar2 A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm
[27] Steganography Techniques - Data Security Using Audio and Video Hilal Almara'beh International Journal of Advanced Research in Computer Science and Software Engineering, volume 6, Issue 2, February 2016 ISSN: 2277 128X Research Paper Available online at: www.ijarcsse.com
[28] https://edupediapublications.org/journals/index.php/ijr/article/view/678/309