Steganography and Classification of Image Steganography Techniques

Sumeet Kaur[1]
Asstt. Prof., YCOE, Punjabi Univ. Guru Kashi Campus
Talwandi Sabo, Distt: Bathinda, India
Email: purbasumeet@yahoo.co.in

Savina Bansal[2], R. K. Bansal[3]
Professor(s) GZSPTU Campus,
Bathinda, India

Abstract— **Information is wealth of any organization and in present era in which information transferred through digital media and internet, it became a top priority for any organizations to protect this wealth. Whatever technique we adopt for the security purpose, the degree and level of security always remains top concern. Steganography is one such technique in which presence of secret message cannot be detected and we can use it as a tool for security purpose to transmit the cofidential information in a secure way. It is an ongoing research area having vast number of applications in distinct fields such as defense and intelligence, medical, on-line banking, on-line transaction, to stop music piracy and other financial and commercial purposes. There are various steganography approaches exist and they differs depending upon message to be embedded, use of file type as carrier or compression method used etc. The focus of this paper is to classify distinct image steganography techniques besides giving overview, importance and challenges of steganography techniques. Other related security techniques are also been discussed in brief in this paper. The classification of steganography techniques may provide not only understanding and guidelines to researchers in this field but also provide directions for future work in this field.**

Keywords— Confidential; information; Cover Object; Data Security; Stego Object; Steganography; Steganalysis etc

Layout of the paper: Section I includes concepts related to steganography, objectives of this paper and introduction; Section II covers classification of commonly used steganography techniques, comparisons of spatial domain and transform domain techniques; Section III highlights factors affecting level of security for steganography, various challenges and issues that steganography is currently facing. Section IV covers conclusion and references part of this paper.

I. SECTION

A. Introduction

Digital media is most preferred source for transfer of information and communication now days. With the growth and access of internet to everyone, it became easier and possible to copy and to distribute the digital information illegally [1]. Digitally transferred data can be copied without any loss of content and quality as well, which is a big problem to the security, authenticity and copyright to the owner of the data [2] [3]. To keep secrecy of data has become an important issue and steganography offer a very reliable solution for such problems. Steganography is an art and science of embedding secret message into cover medium. In steganography, secret message is embedded in an appropriate carrier object that may be image, video, sound or other file to be transmitted over internet and embedding is parametrised by a key that makes difficult to even detect the presence of data and further to find a key to access it. Once cover object is embedded, it is known as stego object [3]. Steganography had been in use from historical times. Simmon stated that steganography also commonly known as 'Prison's Problem' because in earlier times prisoners used it in prisons for communication purposes [4]. Most basic method of steganography is to utilize the redundant information available in digital medium [5]. There is an increasing interest in using images as cover media for steganographic communication and detection of covert communications that utilize images has become an important issue [2].

There are many techniques to embed data in a carrier and each technique uses its own mathematical approach. It is therefore difficult to classify the techniques. The issue has already arisen earlier by R. Chandramouli, wherein it states that it is big challenge and question that- "Can the current and future steganography algorithms be categorized into distinct classes of mathematical techniques?" [6], as each method uses a distinct approach.

In this paper, an effort is made to classify various image steganography techniques alongwith overview, importance and challenges to steganography techniques. An attempt also been made to classify currently available steganography techniques into limited set of categories based on related literature survey and their qualitative analysis. The focus is more on image steganography as images are most popular and widely used medium over internet.

There are various other data hiding techniques for different purposes and applications. These techniques are collectively known as 'information hiding' techniques [2]. Some of these are namely steganography, cryptography; watermarking and fingerprinting are inter-linked to each other as well. Steganography also called 'Covered Writing' [7] conceals very existence of hidden secret data in cover object [8] whereas cryptography scrambles the data to prevent the attacker from

978-93-80544-12-0/14/$31.00 ©2014 IEEE

understanding the contents [9]. Steganography also used where cryptography is either not allowed or not to be used. Steganography and cryptography are complementary and orthogonal to each other and both can be used in combined form provide higher level of security. Watermarking is the process of embedding watermark signal into multimedia data to generate watermarked object to protect authenticity of owner on that digital object and mainly focuses on the robustness of embedded message rather than capacity or concealment. Since increasing capacity and robustness at the same time is not possible [10] therefore watermarking can be used for copyright protection and tracking legitimate use of a particular software or media. In fingerprinting, on the other hand, separate marks are embedded in the copies of the object that are supplied to different customers such as hidden serial numbers which enables the intellectual property owner to identify individuals who break their license agreement and supply the property to third parties [3].

Steganography provides an ultimate guarantee of authentication that no other security tool can ensure. The primary goal of steganography techniques is to maximize embedding rate and minimizing the detectability of the resulting stego images against steganalysis techniques [11].

To detect the hidden text in the stego object is called Steganalysis. It has two major types of analysis: Visual Analysis and statistical Analysis. Visual analysis deals with detection of secret message with naked eyes or with the help of computer in which bit planes are analyzed separately for any unusual change in the appearance for the presence of secret message. Statistical analysis deals with checking of any change in statistical properties of stego object caused by steganographic algorithm [5]. Steganalysis can be divided into two major types: Universal steganalysis and Specific type of steganalysis techniques. Universal steganalysis techniques can detect secret message in stego objects embedded by a range of steganographic algorithms and specific steganalysis techniques, which are more sophisticated techniques and work corresponding to a particular steganographic algorithm only. In order to design a good steganographic algorithm there is need to understand steganalysis concepts and techniques as well.

B. Requirements for a Steganogrphy Algorithm

The main objectives for any steganography algorithm are capacity, undetectibility and robustness [5]. Although it is difficult for a steganography algorithm to have all the characteristics at the same time because there is generally trade-off between these characterstics.

- Capacity: The amount of data to be embedded in cover medium and can retrieved later successfully without significantly changing the cover medium.
- Undetectibility: There should be no visual difference between cover and stego object i.e. embedded message should not be visible to human eye.
- Robustness: A stego system is said to be robust if it can bear any attack and if it undergoes transformation such as scaling, rotation, filtering and lossy compression etc. it should remain intact.
- Security: An embedding algorithm is said to be secure if the embedded information could not be removed after detection by the attacker. It depends on the knowledge about the embedded algorithm and secret key.

II. SECTION

Steganography algorithms may differ from each other depending upon: type of cover object used, type of domain (spatial or transform domain), type of file format or compression used and type of embedding method used to modify the cover object etc. and can be classified accordingly as shown in Fig. 1.

A. Steganography based on type of Cover Object

Different types of cover objects like text, image, audio or video files can be used to hide secret data.

1) Image Steganography: Image steganography is most popular form of steganography. Here secret message is embedded into an image as noise, which is nearly impossible to detect by human eyes. Data hiding in still image imposes certain challenges to cope up with human visual systems (HVS). Still images further subject to various operations like ranging from simple to nonlinear transformation such as cropping, blurring, filtering and lossy compression etc. and data hiding method should be resistant to these types of transformations [12]. Images are widely used medium over internets and this expects to grow continuously as computer graphics power will grow. Images also have high degree of redundancy and provide higher capacity and distortion tolerance. Many programs are already available based on image steganography to hide text as steganography tools.

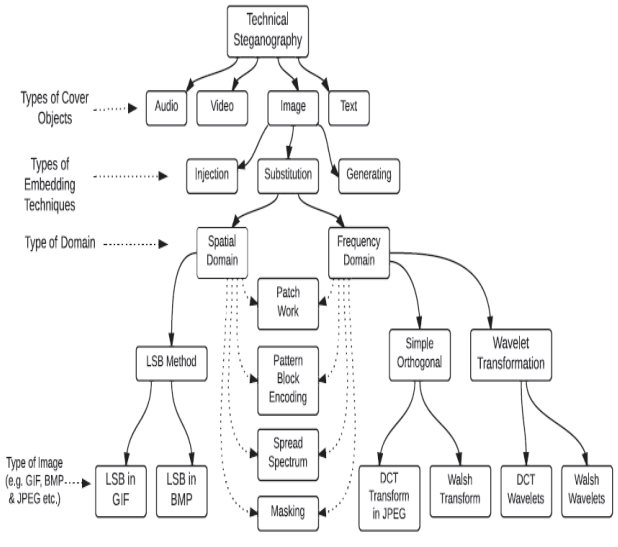

Fig. 1. Classification of various image steganography techniques

2) Text Steganography: It is one of the earliest and most difficult types of steganography. It is a method of using written natural language to conceal a secret message. Text steganography is most challenging due to the presence of lesser redundancy in text documents as compared to the images and audio files [13].

3) Audio Steganography: Audio steganography embeds the message as noise into a cover audio file at a frequency out of human hearing range. Embedding secret messages in digital sound is generally more difficult than embedding messages in other media, Sensitivity to additive random noise is also acute [12]. Commonly used methods for audio Steganography are LSB coding, parity coding, phase coding, spread spectrum, and echo hiding.

4) Video Steganography: It pertains to hide information in video files, which are generally collection of sound and images. Steganography methods that are applicable to sound and images are also applicable to video files. Advantage of this method is that large amount of data can be hidden inside video with smaller amount of distortion because of continuous flow of information and that might go unobserved by observer [14].

5) Protocol Steganography: It pertains to hiding information in unused or optional fields of network control protocols used in transmission over a network [15]. In the layers of the OSI network model, there exist covert channels where steganography can be used [16]. Information can also be hidden in the header of a TCP/IP packet in some fields that are either optional or are never used. Advantage of hiding information in header is that human beings read some fields rarely and these fields serve as an ideal place for hiding data but there is disadvantage that when we configure firewalls for safety purpose to filter out packet where reserved fields contain unusual information then hidden information may also got lost [8].

As image steganography is mostly used, hence basis for next level of classification is image steganography only as shown in Fig. 1.

B. Steganography based on Domain Type

Based upon domain type, spatial domain and transform domain techniques are commonly used steganography techniques.

Spatial Domain Techniques: Spatial domain techniques include bitwise manipulation of intensity of pixels and noise manipulation. There are various approaches to embed data in spatial domain. Most commonly used and simple techniques for spatial domain are Least Significant Bit (LSB) Methods.

LSB Method: It replaces least significant bits of cover object with secret message. It is most popular and simple technique when dealing with images. It has low computational complexity and high embedding capacity [5]. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small. Therefore, to the human eye, the resulting stego-image will look identical to the cover-image. This allows high perceptual transparency of LSB. Although it is very simple technique but it is susceptible to lossy compression and image manipulation such as scaling, rotation, cropping etc, and in addition, of noise or lossy compression the stego-image will destroy the message as well. It works best when the image file is larger than the message file and if the image is grayscale with gradual changes in shades. LSB can be of fixed type bit and variable bit.

Transform Domain Techniques: Transform domain techniques are also known as frequency domain techniques. Transform domain techniques first convert image from spatial domain to frequency domain and then secret message is embedded. These techniques hide data by using mathematical functions. We oftenly use these techniques in compression algorithms and transformation involve hiding secret message in transform space of the cover object. In Frequency domain schemes, the secret data will be embedded into transform coefficients which are transformed first into frequency domain by various frequency domain methods like Discrete Cosine Transformation (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT) etc then secret data will be embedded into transform coefficients [10].

A transform maps image data into a different mathematical space via a transformation equation. Discrete transformations are performed, which are based on specific functions called the basis functions. The discrete version of 1-D basis function is called basis vectors. The discrete version of 2-D basis function is called basis images (or basis matrices). Difference between the different types of transform is the basis image used. Each type of transform has its own equation to generate the basis images. 2D Walsh-Hadamard transform is the tensor of the 1D transform.

DCT: Most commonly used transformation domain technique is DCT. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components. Embedding in DCT domain is simply did by altering the DCT coefficients. DCT transformation and compression using quantization and run-length coding on raw images can be used to obtain secure stego images. DCT is a lossy compression transform because its cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors in results. Variances between original data values and restored data values depend upon the method used to calculate DCT [18].

DFT: The Fourier transform is the well-known and widely used transform. Fourier transform decomposes an image into a weighted sum of 2-D sinusoidal term. Once all the required basis images have been obtained, we can perform the transform operation. After performing the transform, we can get back the original image by applying the inverse Fourier transform.

TABLE1. COMPARISONS BETWEEN SPATIAL DOMAIN TECHNIQUES AND TRANSFORM DOMAIN TECHNIQUES

Criteria	Spatial Domain Techniques	Transform Domain or Frequency Domain Techniques
Embedding Process	In spatial domain steganography methods secret messages are embedded by manipulation of pixel values i.e. intensity of pixel values.	Transform domain techniques, first convert image from spatial domain to frequency doamin and then message is embeded.
Robustness Against Attacks	Data embedding in the spatial domain is more robust to geometrical attacks, such as cropping and down sampling.	Data embedding in the frequency domain usually has more robustness to signal processing attacks, such as addition of noise, compression and low pass filtering [20].
Capacity	Data embedding in spatial domain category provides higher capacity.	Data embedding is lower as compare to transform domain [10].
Comlexity	Spatial domain techniques are quite simpler.	These techniques are complex.
Examples	Commonly used techinques for spatial domain are LSB techniques.	Masking and filtering techniques are more commonly used with frequency domain techniques.

Comparisons between spatial domain and transform domain techniques can be based upon various criteria like robustness, payload capacity, complexity of technique etc. as shown in table 1.

Wavelets: For image processing applications, we need wavelets that are two-dimensional. Wavelets are functions that "wave" above and below the x-axis, have (1) varying frequency, (2) limited duration, and (3) an average value of zero. This is in contrast to sinusoids, used by FT, which have infinite energy. Like sines and cosines in FT, wavelets are used as basis functions. The location of the wavelet allows to explicitly representing the location of events in time. The shape of the wavelet allows representing different detail or resolution [17]. Now a days, wavelet transform is being increasingly used not only in the field of image and signal processing applications but also in many other different areas ranging from mathematics, physics, astronomy to statistics and economics [14,19].

C. Steganography based on File Format and type of Compression used

The Most commonly used image format on internet are Graphic Interchange Format (GIF), Joint Photographic Expert Group (JPEG), and to lesser extent – the Portable Network Graphics (PNG). Most of the steganography techniques exploit these image formats and some of the techniques are based on Bitmap format (BMP) [10]. To transmit and store large image files in a reasonable amount of time, image compression is used. There are two types of compression methods for images: lossy and lossless compression. Although both methods save space but has different effect on uncompressed hidden data.

GIF files and Steganography: In 8-bit GIF files, each pixel is represented as a single byte and merely points to a color index table (a palette) with 256 possible colors. Therefore, pixel's value lies in between 0 and 255. Embedding in palette is done normally with GIF formatted images. Palette image consists of three parts-- a header, a palette and an image data. The palette contains RGB triplets of all colors that occur in image. Secret message can be embedded in palette or in image data but palette-based images leave easily detected distortions [5] [21].

BMP Images and Steganography: Bitmap images were introduced by Microsoft as standard image file format between users of windows operating system but it is used less often due to large size. Large size of bmp files is due to poor compression that makes this format useful for steganography. BMP files use a type of compression called "run length encoding", which is lossless compression. This file format contains some unique properties, which can be used for steganography purposes like image is stored in reverse order i.e. first blue byte, followed by green and then red byte. Pixels are written explicitly in the file, which allows easy identification and modification for steganography. Identifying bit planes and how these are accessed is important in understanding and using steganography techniques. One common method is to use single plane to modify rather than disrupting entire image.

JPEG Images and Steganography: Earlier it was believed that steganography cannot be used with JPEG images due to lossy compression and their compression algorithm does not support a direct LSB embedding into spatial domain [10]. Nowdays steganographic systems for the JPEG format seem more interesting because now the system operate in a transform space and is not affected by visual attacks [22]. JPEG image uses DCT to achieve compression. JPEG compression uses two stages: (i) DCT and quantization, which form the part of lossy stage (ii) Huffman coding, which compresses lossless data. Embedding data with JPEG image can take place between these two stages [23]. By embedding the information at this stage, in the transform domain, it becomes extremely difficult to detect, since it is not in the visual domain.

While working with steganography, it is very important to understand the compression and type of compression used in cover object. Uncompressed formats (GIF & BMP) have larger file size than any other format and have more visual redundancy hence can accommodate higher volume of secret data and are more convenient for data hiding algorithms.

D. Embedding Methods

Some of commonly used methods based upon some specific approach to manipulate the cover object to hide secret data are considered here:

Spread Spectrum: This technique is based on spread spectrum communication that is spreading the bandwidth of a

narrow band signal. In spread spectrum steganography secret message is embedded in noise and then combined with cover image to generate stego image where power of embedded signal is much lower than cover image and stego image is not perceptible to HVS [23][24].

Masking: This technique masks secret data over original data by changing the luminance of particular areas. It embeds the message within significant bits of the cover image. Unlike LSB, masking is not susceptible to lossy techniques because image manipulation does not affect the secret message because masking adds redundancy to the hidden information. This makes the masking technique more suitable than LSB with lossy JPEG images. It may also help to protect against some image processing operations such as cropping and rotating.

Statistical: Here hiding and extracting the data are based on certain statistical properties of cover object. It uses existence of "1-bit" steganography and modifies cover in such way that "1" is transferred by changing certain statistical properties of cover otherwise, cover remains unchanged [25].

Distortion: Here secret message is embedded by distortion of cover and measuring deviation between original cover and stegos at decoding stage. Distortion techniques are less secure and are not used in various applications because original cover object may available to steganalyst for comparison. Text based steganography techniques generally use distortion type for embedding [25].

III. SECTION

A. Factors affecting security level of a Steganography Algorithm

As per literature there are various factors affecting the level of security of a steganography algorithm. Choice of cover object and length of embedded secret message is important factors that may affect the security of ebedding algorithm as lesser the embedded information lesser will be the detectable artifacts introduced by embedding process. Gray scale images are generally the best cover objects for embedding secret data. Uncompressed scan images as obtained from digital cameras containing large no of colors are also preferred for steganography. Choice of compression method also plays a significant role. JPEG images using transform domain results in more secure embedding and these also cannot detected visually. Computerized images or images with unique semantics such as fonts should be avoided in steganography. Further contrast, brightness, presence of noise and various other factors are also needed to consider making communication secure using steganography etc.

B. Challenges and Issues with Steganography

After studying and analyzing available literature and existing techniques, it was observed that steganography algorithms are facing various challenges and issues that demand further exploring and investigations. Some of the prominent issues and areas are as follows-

- Data hiding in still image poses various challenges as these provide less redundancy and imperceptibility as compared to audio and video files [10][12].
- It is also a challenge to embed message into group images, which are highly inter correlated and often manipulated in compressed form [10][26].
- Steganography algorithms generally struggle for providing high data rate and imperceptibility. If a technique provides high payload capacity then it may become less robust and vice versa. Requirements for higher capacity and secure communication are often contradictory [12]. Depending upon the specific application this trade off needs to seek out and at the same time there is also need to produce high quality stego algorithm by achieving high value of PSNR (Peak Signal to Noise Ratio).
- Steganographic techniques are very sensitive to various modifications in cover medium like Image processing operations (smoothing, filtering, image transformations etc.) compression techniques, removing and filtering digital noise techniques because these techniques lead to removal or modifications of secret embedded information too. There is also need to design steganographic algorithms capable of bearing image processing operations.
- Hidden message must be secure both from perceptual and statistical attacks. There is requirement to design more robust steganography algorithms and there is need to pay special attention for the presence of active and malicious attacks.
- Steganography has various useful applications but like other technologies, criminals and terrorists can also misuse it for ill purposes. There is need to understand all steganography as well as steganalysis are concepts, practices and its applications for social purposes rather then ill purposes.

IV. SECTION

CONCLUSION

With the development, growth, ease and access of internet to everyone and use of digital media for transfer of information, there is need to communicate secret and confidential data over the internet securely [9]. Steganography provides a reliable solution by hiding the very existence of message and hence used as a security tool. The technical challenge of data hiding is finding redundant bits in carrier signal that cannot be statistical and perceptually attacked [26]. Uncompressed file formats (BMP, GIFF, TIFF) based on lossless compression provides high data capacity and are more convenient for data hiding algorithms. There are various steganography approaches depending upon type of cover

object used, type of domain, type of file format or compression used and type of embedding method used to modify the cover object etc. There is also need to decide characteristics to compromise in order to ensure high performance. Steganography has applications in various fields such as confidential transmission, video surveillance; military and medical applications [27], band captioning, integration of multiple media for convenient and reliable storage, management, transmission, embedding executables for function control, error correction, and version upgrading etc. [9].

In earlier work, researchers emphasized on specific steganography techniques and only little research work has been done in classification direction. Steganography is an ongoing research area and without classification or categorization, it becomes difficult for new researchers to follow a direction and enhance their research. Through this paper, an effort has been made to classify the various steganography techniques based on available literature and qualitative aspects of techniques. The basic concepts and classification given in this paper may provide the researchers with a direction to follow so that advancements can be made in the field of steganography.

Like any other science this can also be used for ill purposes by criminal and terrorists, it is therefore necessary to understand steganography and steganalysis concepts. Researchers need to pay special attention toward this challenging but valuable area.

REFERENCES

[1] S. K. Wajid, M. Arfan Jaffar, Wajid Rasul, and Anwar M. Mirza, "Robust and imperceptible Image Watermarking using Full Counter Propagation neural Networks" 2009 International Conference on Machine Learning and Computing, IPCSIT vol.3, 2011, IACSIT Press, Singapore , pp 385-391.

[2] R. Chandramouli, M. Kharrazi, and N. Memon, "Image Steganography and Steganalysis: Concepts and Practice", T. Kalker et al. (Eds.): IWDW 2003, LNCS 2939, Springer-Verlag Berlin Heidelberg, 2004, pp. 35–49.

[3] F. A.P. Petitcolas, R. J. Anderson, "On the Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 98, Special Issue on Copyright & Privacy Protection. ISSN 0733-8716, pp 474-482.

[4] G.J. Simmons, "The Prisoner's Problem and the Subliminal Channe". In: Proceedings of CRYPTO '83. Plenum Press, 1984, pp 51-67.

[5] N. Provos and P. Honeyman, "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003, pp 32-44.

[6] R. Chandramouli, "Mathematical approach to steganalysis". In: Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV, vol. 4675. International Society for Optical Engineering, San Jose, California, January 21-24, 2002, pp. 14-25.

[7] P. Salee, "Model–based Steganography", In: Proceeding of the 2nd International workshop on digital water marking, Seoul, Korea, October 20-22 2003 , LNCS , vol.2939, pp. 254-260.

[8] J. Silman, "Steganography and Steganalysis: An Overview", SANS Institute, 2001.

[9] W. Huaiqing and W. Shouzhong, "Cyber Warfare: Steganography vs. Steganalysis", October 2004, Vol. 47, No. 10 communication of ACM, pp. 76-82.

[10] A. Cheddad, J. Condell, K. Curran, & P. Mc Kevitt, (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, Vol 90, Issue 3, March 2010, pp. 727-752.

[11] M. Kharrazi, H.T. Sencar and N. Memon, "Cover Selection for Steganographic Embedding", IEEE International Conference on Image processing, 8-11 oct 2006, Atlanta USA, pp. 117-120.

[12] W. Bender, D. Gruhl, N. Morimoto, and A.Lu, "Techniques for data hiding", IBM Systems Journal, Vol 35, No. 3-4, pp 313-316.

[13] Lee, Y.K. and Chen, L.H., "High capacity image steganographic model", Visual Image Signal Processing, 147:03, June 2000.

[14] R. Krenn, "Steganography and steganalysis" Internet Publication, March 2004. Available at: http://www.krenn.nl/univ/cry/steg/article.pdf

[15] K. Ahsan, K. Deepa "Practical Data hiding in TCP/IP", in: Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002.

[16] T. Handel, M. Sandford, "Hiding data in the OSI network model", In Anderson, R.,ed: Information Hiding: Proceedings of the 1st International Workshop on Information Hiding, Cambridge, U.K., Springer June 1996, pp 23-38.

[17] S. Mallat, "A Theory for Multi Resolution Signal Decomposition: The Wavelet Representation", IEEE Transactions on Pattern Analysis and Machine Intelligence, July 89, Vol.11, No.7, pp. 674-693.

[18] N.F. Johnson and S. Jajodia, George Mason University, "Exploring Steganography: Seeing the Unseen Steganography", Feb 1998, IEEE, pp 26-34.

[19] Toufik, Bouden, and M. Nibouche, "The Wavelet Transform for Image Processing Applications", The Wavelet Transform for Image Processing Applications in Engineering, Physics and Technology, Publisher InTech, ISBN 978-953-51-0494-0, April 2012, pp 395-422.

[20] F. A.P. Petitcolas, R. J. Anderson, and M. G. Kuhn," Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of mutimedia contens, July 1999, pp 1062-1078.

[21] N.F. Johnson and S. Jajodia, "Steganalysis of Images Created Using Current Steganographic Software," Proc. 2nd Int'l Workshop in Information Hiding, Springer-Verlag, 1998, pp. 273–289.

[22] A.Westfield and A.Pfitzmann, "Attacks on Steganographic Systems," Proc. Information Hiding 3rd Int'l Workshop, Springer Verlag, 1999, pp. 61–76.

[23] T. Morkel, J.H.P. eloff and M.S. Olivier "An overview of image Steganography" information and computer security architecture (icsa) research group.

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

[25] N. F. Johnson and Stefan C. Katzen Beisser, "Information hiding techniques for steganography and digital watermarking", Artech House 2000, ISBN 1-58053-035-4, pp 67-71.

[26] Z. Zhao, N. Yu, and X. Li, "A novel video watermarking scheme in compression domain based on fast motion estimation", In: Proceedings of IEEE International Conference on Communication Technology, 2003, pp. 1878-1882.

[27] P. Amat, W. Puech, S. Druon and J.P. Pedeboy, "Lossless 3D Steganography based on MST and Connectivity modification", Signal Processing: Image communication 25(2010) , Elsevier, pp 400-412.