A Survey of Image Steganography Techniques

Mehdi Hussain and Mureed Hussain

Shaheed Zulfiqar Ali Bhutto Institute of Science & Technology, (SZABIST), Islamabad, Pakistan.
mehdi141@hotmail.com, mhussain@szabist-isb.edu.pk

Abspract

Steganography is going to gain its importance due to the exponential growth and secret communication of potential computer users over the internet. It can also be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. Generally data embedding is achieved in communication, image, text, voice or multimedia content for copyright, military communication, authentication and many other purposes. In image Steganography, secret communication is achieved to embed a message into cover image (used as the carrier to embed message into) and generate a stego-image (generated image which is carrying a hidden message). In this paper we have critically analyzed various steganographic techniques and also have covered steganography overview its major types, classification, applications.

Keywords: *Data hiding, Steganography, Cover writing*

1. Introduction

Steganography word is originated from Greek words Steganós (Covered), and Graptos (Writing) which literally means “cover writing” [22]. Generally steganography is known as “invisible” communication. Steganography means to conceal messages existence in another medium (audio, video, image, communication). Today’s steganography systems use multimedia objects like image, audio, video etc as cover media because people often transmit digital images over email or share them through other internet communication application. It is different from protecting the actual content of a message. In simple words it would be like that, hiding information into other information.

Steganography means is not to alter the structure of the secret message, but hides it inside a cover-object (carrier object). After hiding process cover object and stego-object (carrying hidden information object) are similar. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as Steganalysis.

1.1. Steganography in Digital Mediums

Depending on the type of the cover object there are many suitable steganographic techniques which are followed in order to obtain security. It can be shown in Figure 1.

1.1.1. Image Steganography: Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information.

1.1.2. Network Steganography: When taking cover object as network protocol, such as TCP, UDP, ICMP, IP *etc*, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields [24].

1.1.3. Video Steganography: Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (*e.g.*, 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats.

1.1.4. Audio Steganography: When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or *etc* for steganography.

1.1.5. Text Steganography: General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code [21] and *etc* is used to achieve information hiding.

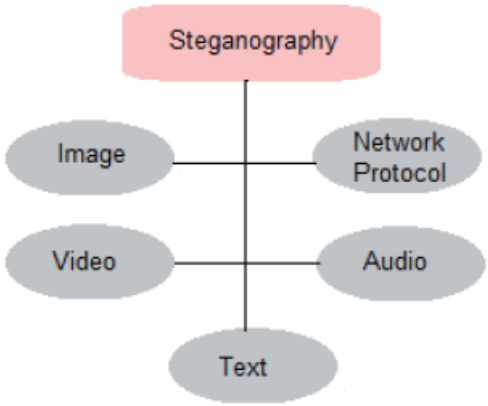

Figure-1. Digital Medium to Achieve Steganography

1.2. Image Steganography Terminologies

Image steganography terminologies are as follows:-

- **Cover-Image**: Original image which is used as a carrier for hidden information.
- **Message**: Actual information which is used to hide into images. Message could be a plain text or some other image.
- **Stego-Image**: After embedding message into cover image is known as stego-image.
- **Stego-Key**: A key is used for embedding or extracting the messages from cover-images and stego-images.

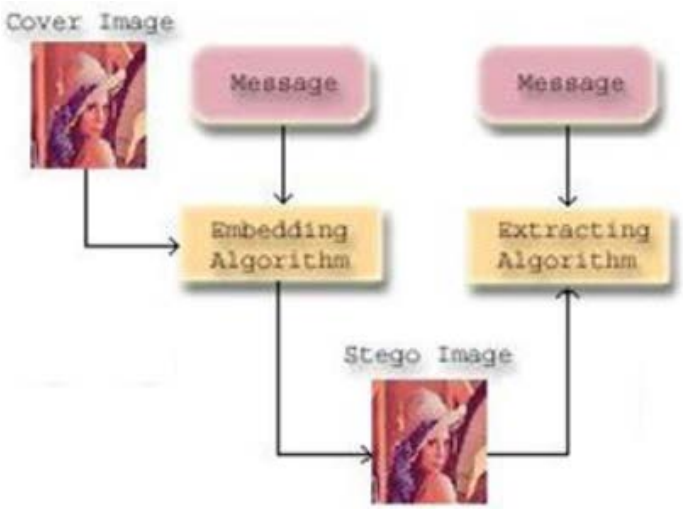

Figure 2. Image Steganography

Generally image steganography is method of information hiding into cover-image and generates a stego-image. This stego-image then sent to the other party by known medium, where the third party does not know that this stego-image has hidden message. After receiving stego-image hidden message can simply be extracted with or without stego-key (depending on embedding algorithm) by the receiving end [21]. Basic diagram of image steganography is shown in Figure 2 without stego-key, where embedding algorithm required a cover image with message for embedding procedure. Output of embedding algorithm is a stego-image which simply sent to extracting algorithm, where extracted algorithm unhides the message from stego-image.

1.3. Image Steganography Classifications

Generally image steganography is categorized in following aspects [23] and Table-1 shows the best steganographic measures.

High Capacity: Maximum size of information can be embedded into image.

Perceptual Transparency: After hiding process into cover image, perceptual quality will be degraded into stego-image as compare to cover-image.

Robustness: After embedding, data should stay intact if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise.

Temper Resistance: It should be difficult to alter the message once it has been embedded into stego-image.

Computation Complexity: How much expensive it is computationally for embedding and extracting a hidden message?

Table 1. Image Steganography Algorithm Measures

Measures	Advantage	Disadvantage
High Capacity	High	Low
Perceptual Transparency	High	Low
Robustness	High	Low
Temper Resistance	High	Low
Computation Complexity	Low	High

1.4. Image Steganographic Techniques

Image steganography techniques can be divided into following domains.

1.4.1. Spatial Domain Methods: There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. Spatial domain techniques are broadly classified into:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labeling or connectivity method
7. Pixel intensity based method
8. Texture based method
9. Histogram shifting methods

General advantages of spatial domain LSB technique are:

1. There is less chance for degradation of the original image.
2. More information can be stored in an image.

Disadvantages of LSB technique are:

1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks.

1.4.2. Transform Domain Technique: This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested [17]. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. Transform domain techniques are broadly classified into:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

1.4.3. Distortion Techniques: Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion [18].Using this technique, a stego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit [19].The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a "1." otherwise, the message bit is a "0." The encoder can modify the "1" value pixels in such a manner that the statistical properties of the image are not affected. However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered [20].

1.4.4. Masking and Filtering: These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Advantages of Masking and filtering Techniques:

1. This method is much more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image.

Disadvantages of Masking and filtering Techniques:

1. Techniques can be applied only to gray scale images and restricted to 24 bits.

2. Literature Review

In [1] authors have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels ranges (0-255) and generates a stego-key. This private stego-key has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of proposed method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitation is to hide extra bits of signature with hidden message for its integrity purpose. It also proposed a method for color image just to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity plus security of hidden message.

Yang *et al.,* in [2] proposed an adaptive LSB substitution based data hiding method for image. To achieve better visual quality of stego-image it takes care of noise sensitive area for embedding. Proposed method differentiates and takes advantage of normal texture and edges area for embedding. This method analyzes the edges, brightness and texture masking of the

cover image to calculate the number of k-bit LSB for secret data embedding. The value of k is high at non-sensitive image region and over sensitive image area k value remain small to balance overall visual quality of image. The LSB's (k) for embedding is computed by the high-order bits of the image. It also utilizes the pixel adjustment method for better stego-image visual quality through LSB substitution method. The overall result shows a good high hidden capacity, but dataset for experimental results are limited; there is not a single image which has many edges with noise region like 'Baboon.tif'.

In [3] anthers have proposed LSB based image hiding method. Common pattern bits (stego-key) are used to hide data. The LSB's of the pixel are modified depending on the (stego-key) pattern bits and the secret message bits. Pattern bits are combination of MxN size rows and columns (of a block) and with random key value. In embedding procedure, each pattern bit is matched with message bit, if satisfied it modifies the 2nd LSB bits of cover image otherwise remains the same. This technique targets to achieve security of hidden message in stego-image using a common pattern key. This proposed method has low hidden capacity because single secret bit requires a block of (MxN) pixels.

In [4] author proposed a Pixel value difference (PVD) and simple least significant bits scheme are used to achieve adaptive least significant bits data embedding. In pixel value differencing (PVD) where the size of the hidden data bits can be estimated by difference between the two consecutive pixels in cover image using simple relationship between two pixels. PVD method generally provides a good imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. Proposed method hides large and adaptive k-LSB substitution at edge area of image and PVD for smooth region of image. So in this way the technique provide both larger capacity and high visual quality according to experimental results. This method is complex due to adaptive k generation for substitution of LSB.

In [5] authors proposed a method of Multi-Pixel Differencing (MPD) which used more than two pixel to estimate smoothness of each pixel for data embedding and it calculate sum of difference value of four pixels block. For small difference value it uses the LSB otherwise for high difference value it uses MPD method for data embedding. Strength is its simplicity of algorithm but experimental dataset is too limited.

In [6] author proposed another pixel value differencing method, it used the three pixels for data embedding near the target pixel. It uses simple k-bit LSB method for secret data embedding where number of k-bit is estimated by near three pixels with high difference value. To retain better visual quality and high capacity it simply uses optimal pixel adjustment method on target pixels. Advantage of method is histogram of stego-image and cover-image is almost same, but dataset for experiments are too small.

In [7] authors have introduced a high capacity of hidden data utilizing the LSB and hybrid edge detection scheme. For edge computation two types of canny and fuzzy edges detection method applied and simple LSB substitution is used to embed the hidden data. This scheme is successful to embed data with higher peak signal to noise ratio (PSNR) with normal LSB based embedding. The proposed scheme is tested on limited images dataset. This method is not tested on extensive edges based image like 'Baboob.tif'.

Madhu *et al.,* in [8] proposed an image steganography method, based on LSB substitution and selection of random pixel of required image area. This method is target to improve the security where password is added by LSB of pixels. It generates the random numbers and selects the region of interest where secret message has to be hidden. The strength of method is its security of hidden message in stego-image, but has not considers any type of perceptual transparency.

In [9] proposed an image steganographic method of mapping pixels to alphabetic letters. It maps the 32 letters (26 for English alphabetic and other for special characters) with the pixel values. Five (5) bits are required to represent these 32 letters and authors have generated a table where 4 cases design to represent these 32 letters. According to that table, each letter can be represented in all 4 cases. It utilizes the image 7 MSB (Most Significant Bits) (27 = 128) bits for mapping. Proposed method maps each 4-case from the 7 MSB's of pixel to one of the 32-cases in that table. These 4-cases increase the probability of matching. This algorithm keeps the matching pattern of cover-image which is then used for extracting data from the stego-image. Proposed method does not required any edge or smoothness computations but secret data should be in the form of text or letter for embedding.

In [10], authors have introduced a data hiding technique where it finds out the dark area of the image to hide the data using LSB. It converts it to binary image and labels each object using 8 pixel connectivity schemes for hiding data bits. This method required high computation to find dark region its connectivity and has not tested on high texture type of image. Its hiding capacity totally depends on texture of image.

In [16] a novel lossless or reversible data hiding scheme for binary images is proposed. JPEG2000 compressed data is used and the bit-depth of the quantized coefficients are also embedded into some code-blocks. Proposed data embedding method is useful for binary images not for gray or color images.

Babita *et al.,* in [11] uses 4 LSB of each RGB channel to embed data bits, apply median filtering to enhance the quality of the stego image and then encode the difference of cover and stego image as key data. In decoding phase the stego-image is added with key data to extract the hidden data. It increases the complexity to applying filtering and also has to manage stego-key. Proposed scheme has high secret data hiding capacity.

In [12] author have proposed a pixel indicator technique with variable bits; it chooses one channel among red, green and blue channels and embeds data into variable LSB of chosen channel. Intensity of the pixel decides the variable bits to embed into cover image. The channel selection criteria are sequential and the capacity depends on the cover image channel bits. Proposed method has almost same histogram of cover and stego-image.

Hamid *et al.,* in [13] have proposed a texture based image steganography. The texture analysis technique divides the texture areas into two groups, simple texture area and complex texture area. Simple texture is used to hide the 3-3-2 LSB (3 bits for Red, 3 bits for Green, 2 bits for Blue channels) method. On the other hand over complex texture area 4 LSB embedding technique is applied for information hiding. The above method used the both (2 to 4 LSB for each channel) methods depending on texture classification for better visual quality. Proposed method has high hidden capacity with considering the perceptual transparency measures e.g PSNR etc.

M. Chaumont *et al.,* in [14] have proposed a DCT based data hiding method. It hides the color information in a compress gray-level image. It follows the color quantization, color ordering and the data hiding steps to achieve image steganography. The purpose of method is to give free access to gray-level image to everyone but restricted access of same color images to those who have its stego-key. It has high PSNR plus with noticeable artifact of embedding data.

K. S. Babu *et al.,* in [15] proposed hiding secret information in image steganography for authentication which is used to verify the integrity of the secret message from the stego-image. The original hidden message is first transformed from spatial domain to discrete wavelet transform (DWT); the coefficients of DWT are then permuted with the verification code and then embedded in the special domain of the cover image. The verification code is

also computed by special coefficient of the DWT. So this method can verify each row of the image of modified or tampered by any attacker.

3. Critical Analysis

Lit. Ref	Domain	Technique	Target to					Advantage	Disadvantage
			Capacity	Perceptual	Robustness	Temper	Computatio		
[1]	Spatial	Adaptive LSB	Y	N	N	N	N	Integrity of secret hidden information with High Capacity	Hide extra bits of signature with hidden message
[2]	Spatial	Texture, Brightness and Edge based Adaptive LSB	Y	Y	N	N	N	High Hidden Capacity with Considering of Good Visual Quality	Experimental Dataset is limited
[3]	Spatial	Combine Pattern bits (Stego-Key) with Secret Message using LSB	N	N	N	N	N	Security of Hidden Data	Hidden Capacity is Low
[4]	Spatial	PVD (on edges) with Adaptive LSB (smooth)	Y	Y	N	N	Y	High Hidden Capacity with Considering of Good Visual Quality	Computationally Complex
[5]	Spatial	MPD with LSB	Y	Y	N	N	N	Better than general PVD methods	Experimental Dataset is limited and Threshold (Stego) Key Required for Both ends
[6]	Spatial	PVD with	Y	Y	N	N	N	Histogram of	Dataset for

		Adaptive LSB						cover and stego image is almost same	Experiments is too small.
[7]	Spatial	Hybrid (canny + fuzzy) edge detection with LSB	Y	Y	N	N	N	High PSNR with high hidden capacity	Limited Dataset with ideal images and Extensive edge based images may failed
[8]	Spatial	LSB substitution with Random pixel selection	N	N	N	N	N	Security of hidden message in Stego-image	Embedding data without considering Visual Quality in Random pixel selection
[9]	Spatial	Mapping pixel to hidden alpha-numeric letters	N	Y	N	N	N	Just Mapping of pixel with letter no need of image processing (edge etc.) required.	Have to keep Matching Pattern for Extracting procedure plus Only useful for Letter based hidden data
[10]	Spatial	LSB substituting on Dark region of Image	N	Y	N	N	N	Useful for smooth region with solid boundary of object based dataset	High computation required and not tested on high texture areas
[11]	Spatial	LSB substitution with Median Filtering	Y	N	N	N	N	High hidden capacity	Computationally complex (filtering) plus Stego-key requirement
[12]	Spatial	Pixel indicator with variable LSB substitution	Y	N	N	N	N	Almost Same histogram of stego-image against cover image	Hidden capacity depended on Cover image pixel intensities
[13]	Spatial	Simple	Y	Y	N	N	N	High hidden	High hidden

		and Complex Texture based LSB substitution						capacity	capacity degrade the visual quality PSNR
[14]	Transform	DCT Coefficient based	N	Y	N	Y	N	High PSNR	Noticeable artifact of hidden data
[15]	Transform	DWT Coefficient permuted and embedding in Spatial domain	N	N	N	N	N	Integrity of hidden data in stego-image	Computationally complex
[16]	Transform	Secret bits plus Bit-depth embedded into coded-block	N	Y	N	Y	N	Useful for binary image	Not for Color image support

4. Conclusion and Future Work

This paper gave an overview of different steganographic techniques its major types and classification of steganography which have been proposed in the literature during last few years. We have critical analyzed different proposed techniques which show that visual quality of the image is degraded when hidden data increased up to certain limit using LSB based methods. And many of them embedding techniques can be broken or shows indication of alteration of image by careful analysis of the statistical properties of noise or perceptually analysis.

References

[1] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, **(2010)** March 1.

[2] H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal: Radioengineering, vol. 18, no. 4, **(2009)**, pp. 509-516.

[3] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, **(2009)**.

[4] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. **(2008)** September 3, pp. 488-497.

[5] K.-H. Jung, K.-J. Ha and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), **(2008)** August 28-30, pp. 355-358.

[6] H. Zhang, G. Geng and C. Xiong, "Image Steganography Using Pixel-Value Differencing", Electronic Commerce and Security, ISECS '09. Second International Symposium on **(2009)** May.
[7] W. J. Chen, C. C. Chang and T. H. N. Le, "High Payload Steganography Mechanism Using Hybrid Edge Detector", Expert Systems with Applications (ESWA 2010), vol. 37, pp. 3292-3301, **(2010)** April 4.
[8] V. Madhu Viswanatham and J. Manikonda, "A Novel Technique for Embedding Data in Spatial Domain", International Journal on Computer Science and Engineering, IJCSE, vol. 2, **(2010)**.
[9] M. A. Al-Husainy, "Image Steganography by Mapping Pixels to Letters", Journal of Computer Science, vol. 5, no. 1, **(2009)**, pp. 33-38.
[10] H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", World Academy of Science, Engineering and Technology, France, **(2007)**.
[11] B. Ahuja, M. Kaur and M. Rachna, "High Capacity Filter Based Steganography", International Journal of Recent Trends in Engineering, vol. 1, no. 1, **(2009)** May.
[12] M. Tanvir Parvez and A. Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography", IEEE Asia-Pacific Services Computing Conference, **(2008)**, pp. 1322-1327.
[13] A. M. Hamid and M. L. M. Kiah, "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis", International Journal of Engineering and Technology (IJET): 0975-4042, **(2009)**.
[14] M. Chaumont and W. Puech, "DCT-Based Data Hiding Method To Embed the Color Information in a JPEG Grey Level Image", 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, copyright by EURASIP, **(2006)** September 4-8.
[15] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, "Authentication of secret information in image steganography", IEEE Region 10 Conference, TENCON-2008, **(2008)** November, pp. 1-6.
[16] S. Ohyama, M. Niimi, K. Yamawaki and H. Noda, "Lossless data hiding using bit depth embedding for JPEG2000 compressed bit-stream", Journal of Communication and Computer, vol. 6, no. 2, **(2009)** February**.**
[17] 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.
[18] 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.
[19] 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
[20] P. Kruus, C. Scace, M. Heyman, and M. Mundy., A survey of steganography techniques for image files . Advanced Security Research Journal. [On line], 5(1), **(2003),** pp. 41-52.
[21] N. Johnson and S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer, pp. 26-34, February **(1998)**.
[22] Pfitzmann, B., Information hiding terminology - results of an informal plenary meeting and additional proposals. In: Proceedings of the First International Workshop on Information Hiding. Springer-Verlag, London, UK, pp. 347–350. **(1996)**.
[23] E Lin, E Delp, A Review of Data Hiding in Digital Images. Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS'99), Savannah, Georgia, April 25-28, **(1999)**.
[24] Handel, T. & Sandford, M., Hiding data in the OSI network model, Proceedings of the 1st International Workshop on Information Hiding, June **(1996)**.

Authors

Mehdi Hussain is currently working as a Senior Software Engineer in Private Software House. He received his B.S degree in Computer Science from Islamia University of Bahawalpur (2006) and also M.S in Computer Science from SZABIST Islamabad (Pakistan) 2011. Research areas of interest are Image steganography, Image Compression, Information Security and so on.