International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015
ISSN 2091-2730

Authentication of secret data using video and audio steganography with wireless transmission

Abhilasha Ramdas Bhagat[1], Prof.Ashish B Dhembhare[2]

[1]PG Student, Dept. of Electronics & Telecomm., P.R.M.I.T & R, Badnera, Amravati, Maharashtra, India
abhilashabhagat126@gmail.com

[2] Professor, Dept. of Electronics & Telecomm., P.R.M.I.T & R, Badnera, Amravati, Maharashtra, India

Abstract— Steganography is a science of covered writing in which the data is hidden in the carrier vessel .The carrier vessel can be image, audio ,video , text .The video have more hiding capacity to store more data than the rest of the vessel media. Various algorithm are available such as LSB substitution algorithm DCT algorithm ,SLSB algorithm ,etc .All of these algorithm have less hiding capacity moreover they are less secure and easily detectable by unauthorized users. BPCS algorithm (Bit plane complexity segmentation) in which the image frame of video is decomposed into bit planes from LSB to MSB .The data is stored in complex area of the bit planes so the hiding becomes undetectable and moreover the capacity to store data increases.To increase more security the video steganography is combined with the LSB audio steganography.Both transmitting party and and receiving party is provided with the authorization key, thus the unauthorized user cannot access secret data without the authorization key .The level of hiding capacity is thus increased along with enhanced security level.

Keywords— Bit planes ,BPCS, Carrier vessel, cryptography, data or information hiding, LSB, steganography, ,stego audio, stego frame, stego image, stego video.

INTRODUCTION

In the real time digital world, steganography has produced an atmosphere of vigilance that has explored interesting applications, thus its further evolution is possible[24]. This theory makes use of terms mostly used by steganography and watermarking techniques. To our existing knowledge no prior work has discussed the combination of video and audio steganography .
All of the previous steganographic methods affects from intolerance to any kind of modification in image applied to the stego-image .If steganography is a process which do not take into account the robustness of image as it is then there is ambiguity to differentiate it from watermarking. The robustness is a essential requirement for a steganographic system. "Many of the steganographic systems are designed so as to be robust against a class of mapping." [25]. It is required to create an undetectable or unrecognizable steganography algorithm that resists common image processing modification that may occur by accident and may or may not by an attack.

RELATED WORK

A number of steganographic methods have been introduced. They can be divided into following 3 categorizes: spatial domain method ,frequency domain methods and adaptive methods or model based. In the spatial domain a steganographer manipulates the secret data and the cover vessel which encodes at the level of the LSBs (least significant bits). LSB is a method that involves modifying the least significant bit of the three colors in a pixel of a 24-bit color image .The problem with colored BMP images is that they are not mostly used on web and tend to stand out (except JPEG and PNG). S-Tools is based on LSBs in the spatial domain, considering that least significant bits of image frame of video is nothing but uncorrelated noise .[24]; it hides messages by manipulating the DCT (discrete cosine transform) coefficients. The central procedure done in F5 is matrix hiding or embedding with the aim of reduction in the changes made to the DCT coefficients. [15] uses vector quantization method known Linde-Buzo-Gray (LBG) combined with Block codes(BCH code) and 1-StageDCT Wavelet transforms. They reaffirm that manipulation of data using a wavelet transformation method preserves better quality with least perceptual changes. [16] propose a data embedding technique in the (DWT)domain. Both secret image and cover vessel images are decomposed by using DWT ,each of which are divided into 4x4 blocks. Blocks of the secret image are placed into the cover blocks for determining the match. After that , error blocks are created and hidden into coefficients of the better matched blocks in HL of cover image. The extracted payload is not perfectly identical to embed version. Adaptive steganography is special case of two above methods. It is also called as Statistics-aware embedding [17], Masking [18], Model-Based method [19] and block complexity [20]. This method explores statistical global properties of image before interacting with its LSB/DCT coefficients. The statistics will explore where to make the modification at [21, 22]. It is characterizes a random adaptive selection of pixels which depends on the cover image and the pixels are selected in a block with large standard deviation.

Then it is meant to ignore the areas of uniform or similar color, e.g., smooth areas. This behavior enable adaptive steganography get images with present or added noise and images that gives color complexity. Spatial domain algorithms are subjected to statistical attacks such as Chi-Square [23] and steganalysis . Frequency
domain, that is JPEG, method is subjected to attacks of double compression effect, statistical distributed DCT coefficients and merged statistical properties.

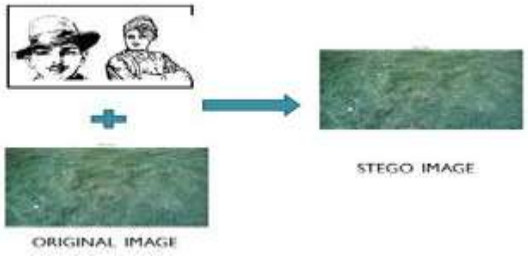

Fig 1: Generation of stego image from original image and secret image

The steganographic algorithms were initially developed for digital images frames and video clips, research and interest in audio steganography started later than above vessel media.Fig.1, represents the generation of the stego image frame from carrier vessel image frame .Few years ago , various algorithms for hiding and extraction of message in audio have been given . All developed algorithms make an advantage of the perceptual feature or properties of the HAS(human auditory system) in order to add a message into a host signal in a transparent way. Hiding additional secret data into audio sequences is a more tedious or difficult task as compared to images, due to superiority of the HAS over human visual system.
On the other hand, many treats that are malicious or harmful against image frame steganography algorithms such as spatial scaling ,geometrical distortions, etc cannot be applied to audio steganography . Consequently ,hiding information into audio seems more secure due to least steganalysis techniques for attacking to audio. The obvious advantage of substitution algorithm or the reason for selecting this technique, is its high storage capacity for hiding a data or message; the use of only one LSB of the host audio files gives a storage capacity of 44.1 kbps. The capacity of substitution algorithm is not comparable with the storage capacity of other robust algorithm like spread spectrum technique that is highly robust but has a low hiding, embedding the information capacity i.e.4 bps .

A)LEAST SIGNIFICANT BIT STEGANOGRAPHY

`The mostly used technique or algorithm to embed secret data, is the use of the LSB. Although prevalent several disadvantages in this approach, the easiness to implement this algorithm, makes it a popularly used method. To hide or embed a secret data or message inside a image frame of video , a proper cover image is required. Because this method make use of bits of pixel in the image frame , it is necessary to make use of a lossless compression , otherwise the embedded information will get lost in the transforming of a lossy compression algorithm.

While using a "24 bit color image", a bit of each of the pixels of blue,red and green color components can be used, a total of three bits is stored in each pixel. Thus, a 800 x 600 size pixel image frame can contain a total of 1.440.000 bits (180 bytes) of secret information. While using a '24 bit image' gives a large amount of storage space to hide messages, it is possible to use a eight bit image as a cover image source. Because of the small space and different properties, eight bit images requires a more careful technique. Where 24 bit color images use three bytes to represent a pixel, an eight bit image uses only one byte . Modifying the LSB of byte will result in a visible change in color, as another color in the present palette will be displayed in that place . Therefore, the cover image needs to be selected more carefully and preferred in grayscale format, as the human eye will not recognize the difference between different gray values of image as easy as with different colors .Disadvantages of using LSB substitution method, is the fact that it needs a large cover image to generate a usable amount of embedding space. Even now a days , uncompressed images frame of 800 x 600 size pixels are not used on the Internet or web, so using these may rise doubt or suspicion. Another disadvantage arises when compressing an image frame consisting of a secret data using a lossy compression algorithm. The hidden or embedded message will not
sustain or survive in this procedure and is lost after the transforming.

VIDEO STEGANOGRAPHY

Out of the image and audio steganography mentioned ,this steganographic technique have storage capacity. The storage capacity of secret information or data increases in video .The video is made up of audio and image .Video steganography enables to hide data in audio as well as in image and create the stego video. Other algorithm embed or hide the secret data or information in a particular band of the spatial frequency coefficient of the carrier. Some other algorithm uses the sampling error property in image digitization. However, all of those Steganographic algorithm are limited in capacity of information hiding . They can hide or embed only 5-15 percentage of the carrier vessel image frame of video efficiently. .We call this steganography as BPCS steganography which is stands termed a "Bit-Plane Complexity Segmentation" Steganography.

We made an experimental system to observe this technique in depth. The advantages of BPCS-Steganography found as follows.

1) The information hiding or storage capacity of a color image frame of video is around 50%.

2) A sharpening operation on the carrier image frame of (video) increases the embedding or hiding capacity quite a bit..

3) Randomizing of the secret information or data by a compression techniques makes the hidden data more undetectable and intangible.

4) Customizing BPCS - Steganography program for each party(user) is easy. It protects unauthenticated user from eavesdropping on the hidden information

5) It is secured technique and provides high level of security.

PROPOSED SYSTEM

In steganography, data or information is hidden or embedded inside a vessel media or container that looks like itself and contains nothing . A variety of vessels media are possible, such as executable files , sound clips, and digital images. All of the present traditional steganographic algorithm or techniques have limited data-hiding capacity. They can hide or embed only 10 percent or less of the data amount or capacity of the vessel carrier . This technique uses an image frame from video as the vessel carrier and we embed secret information in the bit-planes of the vessel. We replace all of the noise-like regions in the "bit-planes "of the vessel image frame of video with secret information or data without degrading or deteriorating the quality of image .This video is known as stego video. This steganography is called as "BPCS-Steganography,"

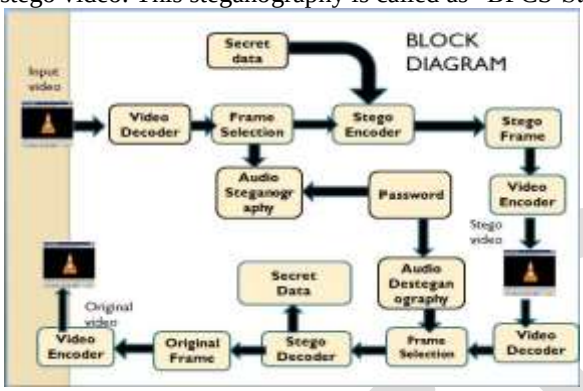

Fig 2:Video Steganography

Fig 3:Audio Steganography

Fig .2. represents the block diagram of video steganography and its linkage with audio steganography through password.Fig.3. represents the internal block diagram audio steganography.

A)Bit Plane Slicing Concept in BPCS*:* The bit plane slicing can be better understood best with the help of fig3 .The operation of splitting or decomposing the image frame of video into its binary pixel planes is called Bit plane slicing. Pixels are digital numbers composed of bits. In an eight bit image, intensity of each pixel is represented by eight bits. The eight bit image is composed of eight 1-bit plane regions from bit plane zero (LSB) to bit-plane seven (MSB). Plane "zero" contains all lowest order bits of all pixels in the image frame while plane seven contains all higher order bits of all pixels. Bit plane Slicing is very useful for image compression. Complexity of each bit–plane of pixel of image frame increases from MSB to LSB .

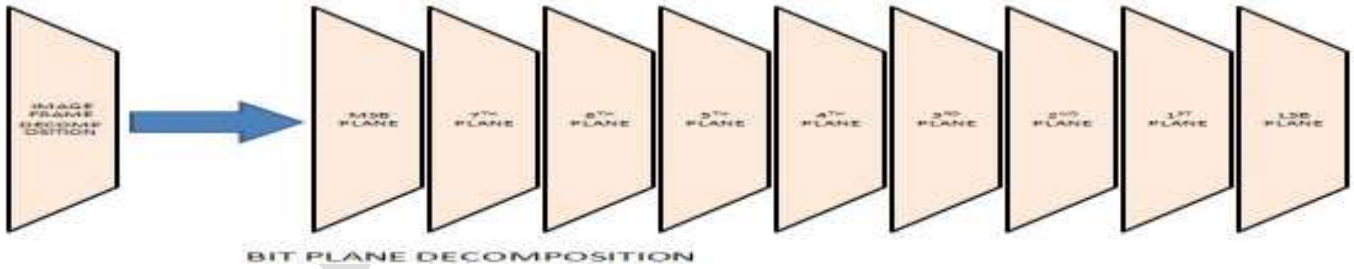

Fig 4: Binary pixel blocks on bit-planes and decomposition

The decomposing of image frame into bit planes is represented in Fig 4 .

B)The definition of image complexity

The length of black-and-white edge in a binary image frame is a good measurement of complexity of image . If the edge is long, theimage is termed as complex, otherwise it is termed simple. The sum of length of the white and black edge equals to the summation of the number of color-changes or transition along the column and rows in an image frame . For e.g., a single white pixel surrounded by black background pixels has the boarder length of 5.We will define the image complexity β by the following.

$$\Omega = \frac{l}{\text{(The max.possible B} - \text{W changes in the image)}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Where, l is the total length of black-and-white border in the image. So, the value ranges over $0 \leq \Omega \leq 1$.

β is calculated over the whole image frame area. It gives us complexity of a binary pixel image.

C)Conjugation of a binary image

Let R be an 8X8 size white and black image with black as the foreground area and white as the background area. We have introduce a two Checker board patterns Wc and Bc, where Wc is a white pixel at the upper left position, and Bc is its complement, the upper-left pixel is black. We termed black and white pixels as having a binary value of '1' and '0', respectively represented in Fig 5.
R is interpreted as follows. Pixels in the background area have the W pattern and pixels in the foreground area have the B pattern .
Now we define R* as the conjugate of R. The most important property about conjugation is the as follows:.
Let Ω(R) be the complexity of a given image R, then we have, $\Omega(R^*) = 1 - \Omega(R)$……………………………………………………..…..(2)
The complexity value of R* is always symmetrical against R regarding Ω = 0.5. For example, if R has a complexity of 0.7, then R* has a complexity of 0.3.Replace complex image-data information block to message block

Fig .5. Illustration of binary pixels

SYSTEM ARCHITECTURE

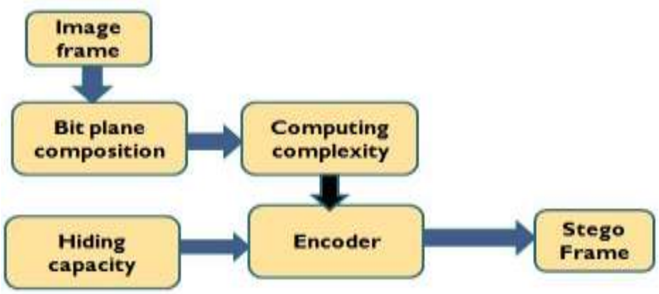

Fig 6.Stego Encoder

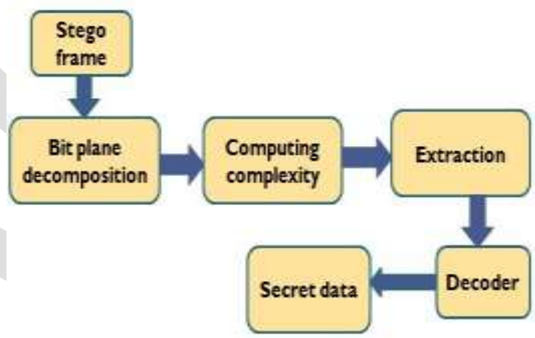

Fig 7:Stego Decoder

Fig.6. represents the block diagram of stego encoder in which the image frame is decomposed or splitted into planes and complexity of each plane is calculated using (1). If more is complexity of frame more data can be hidden in carrier. Thus the frame created is called as stego frame.Fig.7.represents the block diagram of stego decoder in which the stego image frame is decomposed or splitted into bit plane and complexity of each bit plane is calculated using (1) and the secret data or information can hidden in frame is extracted.

MECHANISM

A. Histogram
B. Size estimation.
C. BPCS video steganography
D.LSB audio steganography
E. Wireless transmission
F. De-steganography.
G.Error analysis

A. Histogram:

Histograms are functions defining information extracted from the image .The histogram function is described over all intensity levels. For each level of intensity, its value is equal to the number of the pixels with that present intensity.

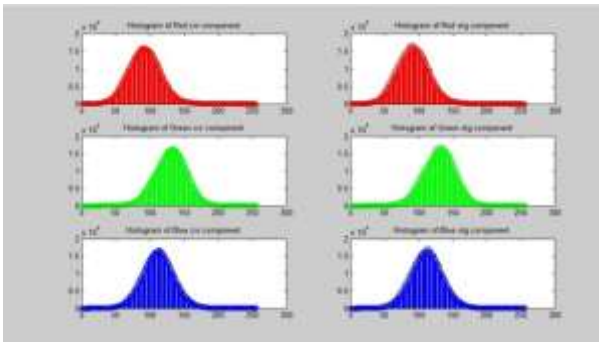

Fig.7.Graph of the histogram function of images

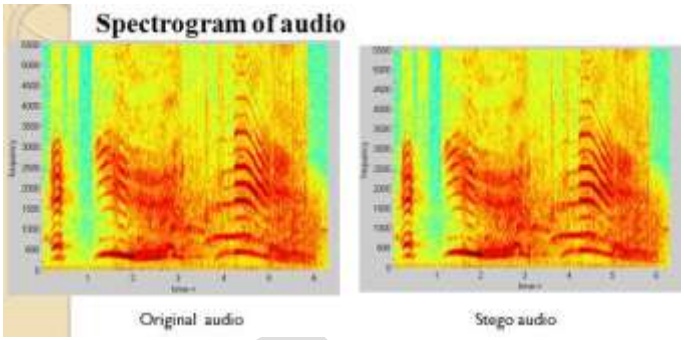

Fig 8.Spectrogram of original and stego audio

B. Size estimation:

In size estimation we have to calculate the regions where maximum color transition or variations are observed. After this we have to insert pixel value of secret image at that variation regions ,we do so using the concept of embedding capacity. For a image frame , embedding capacity can be traded with quality of image by changing the complexity threshold. If image used has a threshold of twenty four border or edge pixels per "8 × 8 "region; so regions having more border pixels value than this are eligible for hiding or embedding.

C.. BPCS Steganography: .

1) Convert the carrier image from PBC format to CGC format system i.e. convert file into png format.
2) Segmentation process on carrier image is performed i.e. each bit-plane of the carrier image is represented in form of informative and noise-like regions by using a threshold value (β0).This means complexity of image is calculated.
3) Group the bytes of the secret data file into a series of secret blocks.
4) If a block is less complex as compared to the threshold (β_0), then take its conjugate making it a more complex block .
5) The conjugate block must be more complex than β0.
6) Replace all the noise like regions with a series of secret information blocks where more color changes are observed.
7) Convert the embedded image from CGC back to PBC format.

D. LSB Audio steganography

Least significant bit (LSB) coding is the easiest way to store information in a digital audio file format. With substituting the least significant bit of each sampling point with a binary message, LSB enables for a large quantity of data to be encoded but less than BPCS method . This increases the amount of data that can be embedded but also increases the resulting noise in the audio file .The image frame number of video is stored in binary format in LSB bits of audio file. The authorization key is given to both transmitter and receiver side the image frame number used in bpcs steganography is stored in binary format in LSB bit of audio file.

To extract a secret message from an LSB encoded sound file, the receiver needs access to the authorization key used in the embedding process

E. Wireless transmission

In mailing we create an environment just like Bluetooth, drop box , cloud and send video from one user to other. After receiving the stego video and password from server the authenticated user can get image frame containing secret information from video and extract the hidden data from it by performing de-steganography.

F. De-steganography:

De-steganography is exactly opposite of steganography. Here we will extract secret image frame from vessel or carrier image frame of video. In this way we will get the secret image/information from stego video hiding it from the third person.

G:Error analysis

i)Bit Error Rate: For the successful recovery of the hidden information or data communication channel must be ideal but for the real communication channel , there will be error while retrieving or extracting hidden information and this is measured by BER cover image as "cov "and stego image as "steg" in the given equation.

$$BER= \frac{1}{|imagecov|}\sum_{I=0}^{all\ pixels}|imagecov - imagesteg| \quad \text{.....(3)}$$

ii) Peak Signal to Noise Ratio: It is the ratio of the maximum signal to noise in the stego image.

$$PSNR = 20 \log10 \frac{255}{\sqrt{MSE}} \quad \text{.....(4)}$$

ADVANTAGE/SCOPE . Less prone or subjected to attacks, worms, viruses, vulnerabilities ,unmatched clients Sensitive data stored on secure servers 4) Encrypted transmission of all data between server and clients.

RESULT

We have discussed the following points and showed our experiments. We can decompose the bit-planes of a natural image in terms of informative areas and noise-like areas by the complexity thresh holding. We can replace complex regions with secret information in the bit-planes of a natural image without changing the image/video quality. This leads to our BPCS-Steganography. Gray coding provides a better means of identifying which regions of the higher bit planes can be embedded Gray coding provides a better means of identifying which regions of the higher bit planes can be hidden. Combining least bit audio steganography with BPCS video steganography has enhanced the level of security .The histogram of original and stego image frame of video are same as shown in Fig.7.The spectrogram of original and stego audio is almost similar as shown in Fig 8..The original video and stego video were equal in terms of size, frame rate, quality.

CONCLUSION

The objective of this paper was to combine our BPCS- video Steganography, which is dependent on a property of the human visual system with LSB audio steganography ,which is based on human auditory system.. The most important point for this BPCS technique is that humans cannot see any information in the bit-planes of a color image if it is very complex, We have hidden the frame number as message bit in audio's LSB bit .So the storage capacity increases with using video steganography. We are transmitting this stego video so generated through wireless media like Bluetooth, drop box, cloud etc to receiver along with authorization key without which the data cannot be retrieved from both audio and video. Thus combination of audio video steganography further enhances the security level. The histogram of both original and stego image frame of video is same. The spectrogram of original and stego audio are same .So, there is no change in original video and stego video.

ACKNOWLEDGEMENT

I would like to present my honest gratitude to Prof. Ashish .B. Dhembhare for his guidance and immense support throughout the work.

REFERENCES

1. K. Jung, K. I. Kim, and A. K. Jain, "Text information extraction in images and video: A survey," Pattern Recognit., vol. 37, no. 5, pp. 977–997, 2004.
2. X. Zhao, K.-H. Lin, Y. Fu, Y. Hu, Y. Liu, and T. S. Huang, "Text from corners: A novel approach to detect text and caption in videos," IEEE Trans. Image Process., vol. 20, no. 3, pp. 790–799, Mar. 2011.
3. W. Kim and C. Kim, "A new approach for overlay text detection and extraction from complex video scene," IEEE Trans. Image Process., vol. 18, no. 2, pp. 401–411, Feb. 2009.
4. Jing Zhang and R. Kasturi, "A noval text detection system based on character and link energies" in IEEE Trans. Image Processing, Vol. 23, No. 9, Sep 2014.
5. Y.-F. Pan, X. Huo, and C.-L. Liu, "A hybrid approach to detect and localize texts in natural scene images," IEEE Trans. Image Process., vol. 20, no. 3, pp. 800–813, Mar. 2010.
6. Z. Tu, X. Chen, A. L. Yuille, and S.-C. Zhu, "Image parsing: Unifying segmentation, detection, and recognition," Int. J. Comput. Vis., vol. 63, no. 2, pp. 113–140, 2005.
7. C. Yi and Y. Tian, "Text string detection from natural scenes by structure-based partition and grouping," IEEE Trans. Image Process., vol. 20, no. 9, pp. 2594–2605, Sep. 2011.
8. K. I. Kim, K. Jung, and J. H. Kim, "Texture-based approach for text detection in images using support vector machine and continuously adaptive mean shift algorithm," IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 12, pp. 1631–1638, Dec. 2003.

9. X. Chen and A. L. Yuille, “Detecting and reading text in natural scenes,” in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2. Jun./Jul. 2004, pp. II-366–II-373.

10. D. Chen, J.-M. Odobez, and H. Bourlard, “Text detection and recognition in images and video frames,” Pattern Recognit., vol. 37, no. 3, pp. 595–608, 2004.
11. J. Zhang and R. Kasturi, “Extraction of text objects in video documents: Recent progress,” in Proc. 8th IAPR Int. Workshop Document Anal. Syst., Sep. 2008, pp. 5–17.
12. H. Tran, A. lux, T. H. L. Nguyen, and A. Boucher, “A novel approach for text detection in images using structural features,” in Proc. 3rd Int. Conf. Adv. Pattern Recognit., 2005, pp. 627–635.
13. J. Zhang and R. Kasturi, “Text detection using edge gradient and graph spectrum,” in Proc. 20th Int. Conf. Pattern Recognit., Aug. 2010, pp. 3979–3982.
14. P. F. Felzenszwalb and D. P. Huttenlocher, “Pictorial structures for object recognition,” Int. J. Comput. Vis., vol. 61, no. 1, pp. 55–79, 2005
15. N.K. Abdulaziz and K.K. Pang, “Robust data hiding for images,” in Proc. IEEE International Conference on Communication Technology, vol. 1, pp. 380-383, 21-25 Aug. 2000.
16. A. A. Abdelwahab and L.A. Hassan, “A discrete wavelet transform based technique for image data hiding,” in Proc. 25th National Radio Science Conference, Egypt, pp.1-9, 18-20 March. 2008.
17. N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” *IEEE Security and Privacy*, vol.1, no. 3, pp.32-44, May-June 2003.
18. N.F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” *IEEE Computer*, vol. 31, no. 2, pp.26- 34, Feb. 1998.

19. P. Sallee, "Model-based methods for steganography and steganalysis," *International Journal of Image and graphics*, vol. 5, no. 1, pp. 167-190, 2005.
20. H. Hioki, “A data embedding method using BPCS principle with new complexity measures,” in Proc. Pacific Rim Workshop on Digital Steganography, pp.30-47, 2002.
21. R. Tzschoppe, R. Baum, J. Huber and A. Kaup, “Steganographic system based on higher-order statistics,” in Proc. SPIE, Security and Watermarking of Multimedia Contents V, Santa Clara, California, USA, vol. 5020, pp. 156-166, 2003.
22. E. Franz, “Steganography preserving statistical properties,” in Proc. of the 5th International Workshop on Information Hiding, Noordwijkerhout, The Netherlands, *LNCS*, vol. 2578/2003, pp. 278-294, 2003.
23. A. Westfeld and A. Pfitzmann, “Attacks on steganographic systems,” in Proc. of the 3rd Workshop on Information Hiding, Dresden, Germany, LNCS 1768, pp. 61-76 , 2000.
24. N.F. Johnson, D. Zoran and J. Sushil, Information Hiding Steganography and Watermarking - Attacks and Countermeasures, Kluwer Academic Publishers, 2001.
25. G.J. Simmons, “The prisoners’ problem and the subliminalchannel,” in Proc. of Advances in Cryptology, pp. 51-67,22-24 August. 1984
26. S.C. Katzenbeisser, Principles of steganography, In: S. Katzenbeisser and F.A.P Petitcolas, (ed.), Information hiding techniques for steganography and digital watermarking, Norwood: Artech House, INC, 2000.
27. L. Siwei, "Natural Image Statistics for Digital Image Forensics," Thesis of Doctor of Philosophy, Dartmouth College, Hanover, New Hampshire, pp. 67, August, 2005