A REVIEW PAPER ON TRANSFORM DOMAIN TECHNIQUES OF IMAGE STEGANOGRAPHY IN TEXT AND IMAGE

[1]Mandavilli Kavya, [2]RamBabu M
[1]Assistant Professor, [2] Assistant Professor
[1]Computer Science Department
[1]KG Reddy College of Engineering and Technology, Hyderabad, India

ABSTRACT: Now a day's Steganography is becoming an significant area of research. So this paper is focusing on giving the overview of general types of steganography which includes text , image, audio, video steganography. Steganography is one of the most secured technique in an information security, here different authors are used various techniques. We are focus on image steganography. Image steganography is broadly categorized into two type's spatial steganography and transform domain steganography. This focuses only on transform domain steganography techniques. Steganography is the powerful tool for hiding information inside useful cover medium in ways such that the hidden message is undetectable. In Greek language, stego means covered or secret and graphy means to write. Hence, steganography means covered writing. Transform domain steganography is one of the techniques used for hidden exchange of information in frequency domain and it can be defined as the study of invisible communication that deals with the ways of hiding the existence of the communicated message. In this way, if successfully achieved, the message does not get attention of attackers and eavesdroppers. In steganography, information can be hidden in different cover carriers. Cover media can be a text, image, audio or video files. In this paper, the process of embedding the message in the image and generating a stego-image from the cover image which will be in an unpredictable format.

Keywords: **Image Steganography, DCT, DWT, IWT, DCVT**

I. INTRODUCTION:

Steganograpghy:

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows that a message has been sent. In steganography secret communication can be done in either of the following cover media i.e. text, image, audio or video. The goal of steganography is always to conceal the very existence of the secret message. Steganography is useful in many applications. Here the recipient receives a secret message in a hidden form in any of the cover media which is invisible to the human visual system. Steganography"s ultimate objectives are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data that separates it from related techniques such as watermarking and cryptography. Depending on the media used for cover, steganography can be classified as text, image, audio and video steganography.

An image is a picture that has been created or copied and stored in digital form. An image can be described in terms of vector or raster graphics. An image stored in raster form is sometimes called a bitmap. A pixel is the fundamental building block of any image. Gray images have pixels of 8 bits while colour images have pixels of 24 bits. So gray images can vary their pixel colours in 256 different shades of gray. Colour images have red, green, and blue as primary colours. Different percentage of this primary colour in this 24 bits constitute the coloured pixels which are also called as true colour pixels.

II. RELATED WORK

2.1 TYPES OF STEGANOGRAPHY:

Text Steganography: This method is used to hide the text in a text file to make it as a secret message. This is one of the tedious form of steganography methods as the same amount of text will be used to hide the message which we want to hide . A message is inserted in the cover text i.e., plain text through an embedded algorithm then the resulted cipher text i.e., stego text which is broadcasted over a channel to the receiver. Now ,the process of extraction taken place using exraction algorithm using a secret key. During the broadcasting of the stego text this text can be viewed by unauthenticated viewers who can observe only the text present in the file irrespective of the presence of the hidden text in that particular text file. The secret text is hidden behind every nth letter of every words of text message. This is broadly classified into three categories :

- Format based
- random and statistical generations
- linguistic method

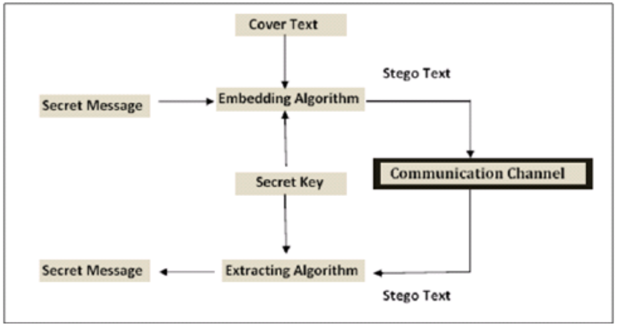


Fig 1: Model of text steganography

Types of steganography :

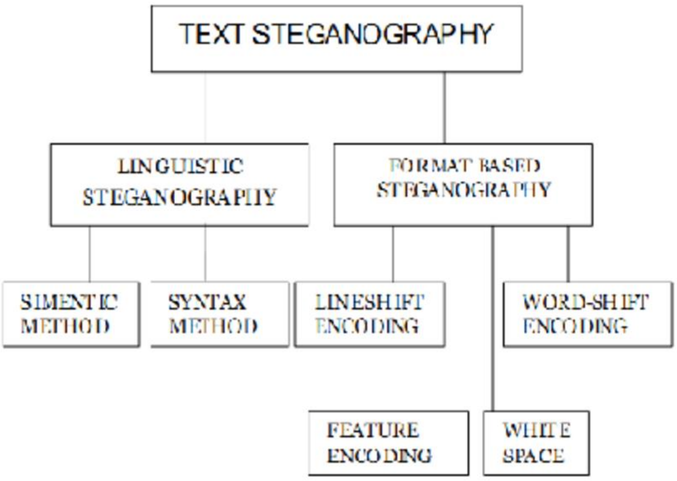


Fig 2: Image steganography types

Format-based methods : This method uses the physical formatting of text as a space in which to hide information. Insertion of spaces or non-displayed characters, careful errors tinny throughout the text and resizing of fonts are some of the many format-based methods used in text steganography. Some of these methods, such as deliberate misspellings and space insertion, might fool human readers who ignore occasional misspellings, but can often be easily detected by a computer.

Random and statistical generation method : Random and statistical generation methods are used to generate cover-text automatically according to the statistical properties of language. These methods use example grammars to produce cover-text in a certain natural language. A probabilistic context-free grammar (PCFG) is a commonly used language model where each transformation rule of a context- free grammar has a probability associated with it .

Linguistic methods : Linguistic steganography specifically considers the linguistic properties of generated and modified text, and in many cases, uses linguistic structure as the space in which messages are hidden .

Comparison of text steganography methods:

Table 1: overview of steganography

Text Steganography methods	**Advantage**	**Dis-Advantage**
Line shifting	This concept will be suited only for printed text.	When OCR (character recognition program) applied the hidden information gets destroyed.
Word shifting	Word shifting method identify less because of change of distance between words to fill line is quite common.	The algorithm that related to word shifted distance, easily can get hidden data.
Synactic Method	The amount of information to hidden the method is trivial.	Smart reader can find hidden data easily.

Semantic based Hiding	This method is better than above methods, syntactic, line shifting and word shifting because that cannot detect by retyping or using OCR programs.	Smart reader which has huge knowledge of words their synonyms or antonyms can discover it.
Abbreviation Based Hiding	This method is because it's a kind of any abbreviation present and we built also.	It is limited only for small data means out of large data. Only small part of data can be hidden.
Hiding Data Using white spaces	One way of hiding data in text is to use white space. Due to the fact that in practically all text editors, extra white space at the end of lines is skipped over, it won't be noticed by the casual viewer.	In a large piece of text, this can result in enough room to hide a few lines of text or some secret codes.
Hiding Data In Paragraphs	The approach works by hiding a message using start and end letter of the words of a cover file. A word having same start and end letter is skipped. Since no change is made to the cover, the cover file and its corresponding stego file are exactly the same.	The volume of data hiding in the paragraph would be very less. The capacity of hiding the large volume of data leads to the Challenge

Image steganography:

In the method of image steganography the information is inserted into a cover image i.e., normal image and the image in which we are inserting the message is called as stego image. This is the concept in which confidential communication is happened through digital images. This technique is used in military,personal and inteelectual property applications. This image is transmitted through a known channel but the unauthorized users does not know that the image is a stego image which means it consists of some message. Once the receiver gets the image reciver extract the image using the stego-key using the process of embedding algorithm used.

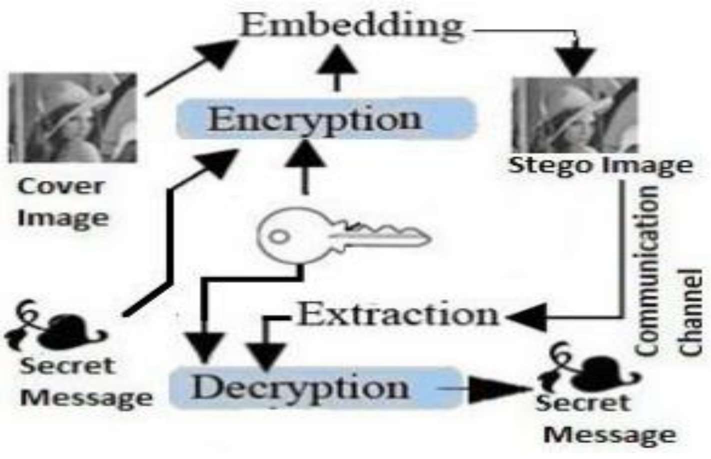
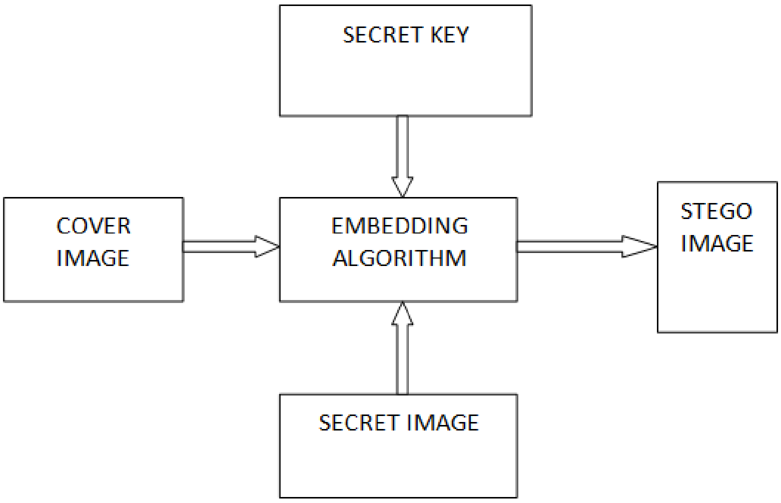


Fig 3: Image steganography procedure

In the below figure the process of image is hiding in another image is being shown. Original image/ cover image is taken and using secret key secret image is embedded using embedding algorithm and the pixels are replaced with out changing the outlook of original image so that stego image is being generated.



Types of image steganography:

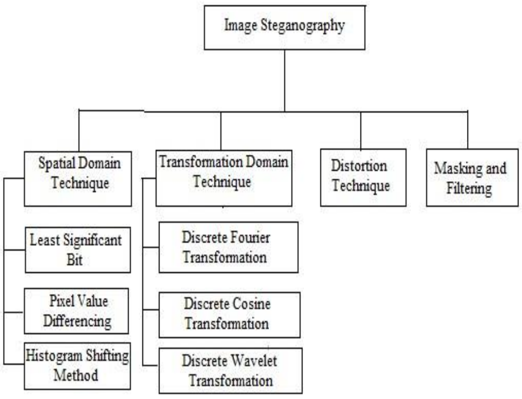


Image Steganography
Spatial Domain Technique
Transformation Domain Technique
Distortion Technique
Masking and Filtering
Least Significant Bit
Pixel Value Differencing
Histogram Shifting Method
Discrete Fourier Transformation
Discrete Cosine Transformation
Discrete Wavelet Transformation

Fig 4: Image steganography types

Audio Steganography: In the concept of audio Steganography , confidential messages are inserted into digitized audio signal which will be resulting the altering binary sequence of corresponding audio file which is inserted. The various formats using this steganography are MPEG,WAVE,AVI etc.this is one of the tedious process compared to inserting the messages /text in other media files. This concept provides more security and less malicious attacks because other media steganograpghy techniques are error prone. As mentioned this provides more security even when the information is transmitted through insecure channels ,the secrecy of information is maintained.

Steganography in Audio:

Table 2: overview of audio steganography

Methods	Embedding Techniques	Strengths	Weakness	Hiding Rate
Least Significant Bit	LSB of each sample in the audio is replaced by one bit of hidden information	Simple and easy way of hiding Information with high bit rate	Easy to extract and to destroy	16 Kbps
Echo Hiding	Embeds data by introducing echo in the cover signal	Resilient to lossy data Compression algorithms	Low security and capacity	40-50 Bps
Phase Coding	Modulate the phase of the cover signal	Robust against signal processing manipulation and data Retrieval needs the original signal	Low capacity	333 Bps

Parity Coding	Break the signal into separate samples and embeds each bit from secret message in sample region parity bit	Sender has more of a choice in encoding the secret bit.	Not Robust	320bps
Spread Spectrum	Spread the data over all signal frequencies	Provide better robustness	Vulnerable to time scale modification	20 Bps

Video Steganography: This concept deals with the embedding of information in each of a particular video. The video in which the message is inserted is called as stego video which is received by the receiver. The best technique in which we can embedd the message in the video so that original quality of the cover video can't be changed. Many video steganography techniques are used now a days to secure the confidential information. Some of the techniques are:

LSB (Least Significant Bit) : method LSB is said to be the best method for protecting the data because of its simplicity in nature , easier and effective. In this concept of LSB the original/ cover video pixel values which are in the form of bytes are extracted and then the LSB of this video are replaced with the bits of the confidential/secret message will be embedded into it. As we are changing only the LSB values of the original/ cover video the pixels does not get disfigured and almost views like the original/cover video.

Non-uniform rectangular partition : This method is used for uncompressed videos , hiding of the data is done by hiding an uncompressed secret video file in the original video stream in each and every frame. Only one thing need to be crosschecked that the secret file as well as the original/cover file should be of the same size and each and every frame of the original and secret video will be applied with some image steganograph techniques. The secret video file will be hidden in the leftmost four least significant bits of the frames of the original / cover video.

Compressed video Steganography : This method is done entirely on the compressed domain. Data can be embedded in the block of I frame with maximum scene change and in P and B block with maximum magnitude of motion vectors. The AVC encoding technique yields the maximum compressing efficiency.

Anti- forensics techniques: This is the concept in which actions are taken to destroy,hide and manipulate the data to attack on computer forensics. This provides security by stopping the unauthorized access to the users and also can be used for the criminal purpose also , this technique will hide the data under original file with all these features this technique will be more secured.

Masking and filtering techniques : These are applicable for both colored and gray scale images.this acts like a watermarking on the image and will not effect the quality of the original image. Unlike other methods of steganography in this data masking the confidential message is processed which looks like a multimedia file. The security is more than the other traditional steganalysis.

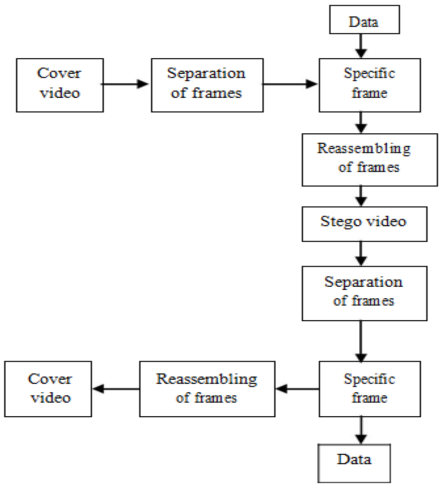


Fig 5: overview of video steganography

III. PROPOSED METHODS OF STEGANOGRAPHY

TRANSFORM DOMAIN TECHNIQUES The transform based techniques utilizes the domain specific characteristics of image to embed data on it and for performing it the image firstly transformed to that domain like frequency domain (DCT, DFT), wavelet domain (DWT), curvelet domain etc. in these techniques the data is embedded on the transformed image instead of direct pixels (as in spatial domain) and then the image is retransformed to spatial domain the advantage of the algorithm is that the information can be embedded in are as of the image that are less exposed to compression, cropping, and image processing also the information in one component of transformed domain spreads over larger number of pixels or even in whole image. This reduces the possibility of removal of information by any attack or operation. Although this is a more complex way of hiding information in an image. Transform domain techniques are broadly classified into:

A. Discrete Cosine transform (DCT) based technique
B. Discrete Fourier transform (DFT) based technique.
C. Discrete Wavelet transform (DWT) based technique.
D. Integer Wavelet Transform (IWT) based techniques.
E. Discrete Curvelet Transform (DCVT) Based techniques.

A. DISCRETE COSINE TRANSFORM (DCT) BASED TECHNIQUE:DCT is a general orthogonal transform for digital image processing and signal processing. It is having a advantage of high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity. DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands thus making it easier to choose the band in which the watermark is to be inserted . The literature survey reveals that mostly the middle frequency bands are chosen because embedding the information in a middle frequency band does not scatter the watermark information to most visual important parts of the image i.e. the low frequencies and also it do not overexpose them to removal through compression and noise attacks where high frequency components are targeted. Numerous watermarking techniques based on DCT are proposed. Although some of the watermarking techniques embed the watermark in the DC component, most techniques utilize the comparison of middle band DCT coefficients to\ embed a single bit of information into a DCT block.

B. DISCRETE FOURIER TRANSFORM (DFT) BASED TECHNIQUE: The DFT based technique is similar to the DCT based technique but it utilizes the Fourier transform instead of cosine which makes it lack resistance to strong geometric distortions. Although it increases the overall complexity of the process.

C. DWT BASED: A wavelet is a small wave which oscillates and decays in the time domain. The Discrete Wavelet Transform (DWT) is a relatively recent and computationally efficient technique in computer science. Wavelet analysis is advantageous as it performs local analysis and multi-resolution analysis. To analyze a signal at different frequencies with different resolutions is called multi-resolution analysis (MRA). This method transforms the object in wavelet domain, processes the coefficients and then performs inverse wavelet transform to represent the original format of the stego-image object. Wavelet analysis can be of two types: continuous and discrete. Analyzing the signal at different frequencies with different resolutions is Called multi-resolution analysis (MRA). The DWT divides an image into four parts namely a lower resolution approximation component (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The LL sub band is obtained after low-pass filtering both the rows and columns and contains a rough description of the image. The HH sub-band is high-pass filtered in both directions and have the high-frequency components along the diagonals. The HL and LH sub bands are the results of low-pass filtering on one direction and high-pass filtering in the other direction. After the image is processed by the wavelet transform, most of the information contained in the host image is concentrated into the LL image. LH sub band contains mostly the vertical detail information which corresponds to horizontal edges. HL band represents the horizontal detail information from the vertical edges. The process can be repeated to obtain multiple scale‟ wavelet decomposition"

D. IWT BASED: Since the discrete wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them, hence it is expected to make the process of imperceptible embedding more effective. However, the used wavelet filters (and also the other filters like DCT, FFT) have floating point coefficients. Thus, when the input data consist of sequences of integers (as in the case for images), the resulting filtered outputs no longer consist of integers, which doesn't allow perfect reconstruction of the original image. However, with the introduction of Wavelet transforms that map integers to integers the output can be completely characterized with integers .

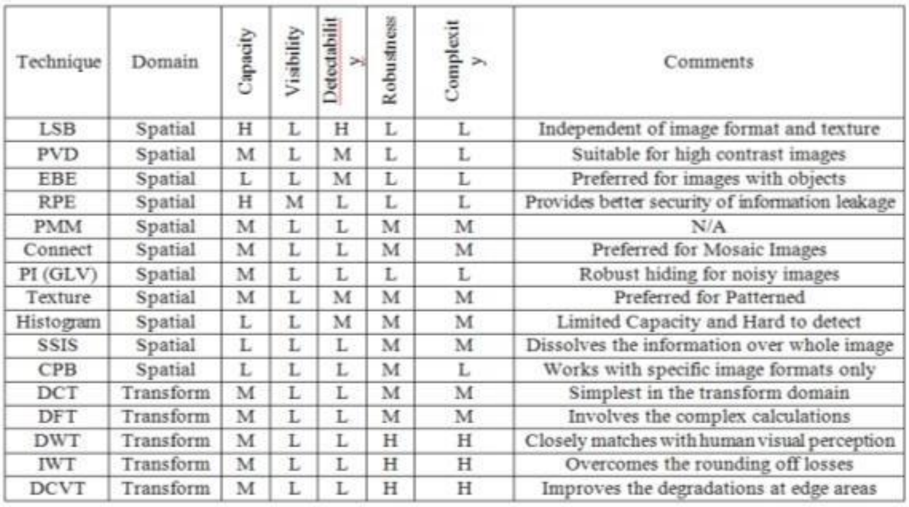
E. DCVT BASED: This curvlet transform is one of the new form / member of this family of multiscale geometric transforms. This concept is used for showing edges better than the forms of wavelet, Curvelet transform offers an effective solution to the problems associated with image steganography using Wavelets and DCT (Discrete Cosine Transform).

General advantages of transform domain technique are:
1. There is less chance for removal or loss of the hidden data.
2. Information is distributed over all whole image.
3. Provides much higher flexibility for hiding data.
4. Typically independent of the image format.

Disadvantages of transform technique are:
1. Greater understanding of the embedding domain required.
2. Careful selection of embedding coefficients required otherwise it can cause degradation of image.
3. Higher Mathematical Complexity.
4. Relatively Low embedding capacity.

IV. PERFORMANCE METRICS:

Table 3: performance analysis



Technique	Domain	Capacity	Visibility	Detectability	Robustness	Complexity	Comments
LSB	Spatial	H	L	H	L	L	Independent of image format and texture
PVD	Spatial	M	L	M	L	L	Suitable for high contrast images
EBE	Spatial	L	L	M	L	L	Preferred for images with objects
RPE	Spatial	H	M	L	L	L	Provides better security of information leakage
PMM	Spatial	M	L	L	M	M	N/A
Connect	Spatial	M	L	L	M	M	Preferred for Mosaic Images
PI (GLV)	Spatial	M	L	L	L	L	Robust hiding for noisy images
Texture	Spatial	M	L	M	M	M	Preferred for Patterned
Histogram	Spatial	L	L	M	M	M	Limited Capacity and Hard to detect
SSIS	Spatial	L	L	L	M	M	Dissolves the information over whole image
CPB	Spatial	L	L	L	M	L	Works with specific image formats only
DCT	Transform	M	L	L	M	M	Simplest in the transform domain
DFT	Transform	M	L	L	M	M	Involves the complex calculations
DWT	Transform	M	L	L	H	H	Closely matches with human visual perception
IWT	Transform	M	L	L	H	H	Overcomes the rounding off losses
DCVT	Transform	M	L	L	H	H	Improves the degradations at edge areas

V. CONCLUSION

On transform domain steganography techniques is found to be best in image steganography, which provide high secured Stego-image and it gives lowest bit error rate. So the quality of the stego-image obtained in this method is high. Further these steganographic methods can be made more secure by encrypting them using strong encryption algorithms.

VI. REFERENCES:

[1] Dulce R. Herrera-Moro, Raúl Rodríguez-Colín, Claudia Feregrino-Uribe "Adaptive Steganography based on textures",17th International Conference on Electronics, Communications and Computers (CONIELECOMP'07).

[2] YildirayYalman 1 , FeyziAkar 2 and Ismail Erturk "Contemporary Approaches to the Histogram Modification

[3] Blossom Kaur, Amandeep Kaur, Jasdeep Singh "STEGANOGRAPHIC APPROACH FOR HIDING IMAGE IN DCT DOMAIN", International Journal of Advances in Engineering & Technology, July 2011.

[4] Xuefeng Wang Zhen Yao Chang-Tsun Li "A PALETTE-BASED IMAGE STEGANOGRAPHIC METHOD USING COLOURQUANTISATION", Image Processing, 2005. ICIP 2005. IEEE International Conference on 11-14 Sept. 2005

[5] Souvik Bhattacharyya, Gautam Sanyal "Study and analysis of quality of service in different image based steganography using Pixel Mapping Method (PMM)", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 2– No.7, May 2012 – www.ijais.org

[6] Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., *"Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography*", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[7] Swati malik, Ajit "Securing Data by Using Cryptography with Steganography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[8] Ishwarjot Singh ,J.P Raina," *Advance Scheme for Secret Data Hiding System using Hop field & LSB*" International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[9] G. Manikandan, N. Sairam and M. Kamarasan *"A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme* ", Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012

[10] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, *"Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique",* International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012.