ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 4, April 2012

# Improved Protection In Video Steganography Using DCT & LSB

Poonam V Bodhak, Baisa L Gunjal

***Abstract- Computer Technology and the Internet have made a breakthrough in the existence of data communication. This has opened a whole new way of implementing steganography to ensure secure data transfer. Steganography is the fine art of hiding the information. Hiding the message in the carrier file enables the deniability of the existence of any message at all. This paper designs software to develop a steganographic application to hide data containing text in a computer video file and to retrieve the hidden information. This can be designed by embedding the text file in a video file in such a way that the video does not lose its functionality using DCT & LSB Modification method. This method applies imperceptible modification. This proposed method strives for high security to an eavesdropper's inability to detect hidden information.***

***Keywords*- Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Steganography, Stego Image.**

## I.INTRODUCTION

### *A) Motivation*

The word steganography derives from the Greek word steganos, which means covered or secret, and graphy which means writing or drawing. Steganography is also referred to as Stego. The concept of steganography has existed for thousands of years. The Greek used to pass secret information by writing in wax-covered tablets: wax was first scraped off a tablet, the secret message was written on the tablet, and then the tablet was covered again with the wax. Another technique was to shave a messenger's head, tattoo a message or image on the bald head, and let hair grow again so that the tattoo could not be seen. Shaving the head again revealed the tattoo. The use of invisible ink was also used extensively during the World War II. The invisible ink method and other traditional stego methods were extensively used but the invisible secret message gets revealed when heated. Then the image files are used to hide messages. But image files are not thonly Secret information can be hidden in computer image files (JPEG, GIF, BMP), audio files (WAV, MP3), video files (MPEG, AVI), or even text files. Provided the steganographic algorithm is good enough and a Stego'd video along with the original video, even an adept steganography expert would be unable to detect the hidden information from the image. Making use of the Internet, secret information hidden in the carrier can be transmitted quickly, secretly, and securely.

### *B) Existing System*

Over the past few years, numerous Steganography techniques that embed hidden messages in multimedia objects have been proposed. This is largely due to the fact of significantly large amounts of stego-data by means of simple and subtle modifications that preserve the perceptual content of the underlying cover object. Hence they have been found to be perfect candidates for use as cover messages. A message, either encrypted or unencrypted, can be hidden in a computer video file (containing the picture of, for instance, an innocent 2 year old baby) and transmitted over the Internet, a CD or DVD, or any other medium. The image file, on receipt, can be used to extract the hidden message.Steganographic Techniques

**1) Physical Steganography**

Physical Steganography has been widely used. In ancient time people wrote message on wood and then covered it with wax. Message was written on the back of postage stamps. Message was written on paper by secret inks.

**2) Digital Steganography**

Digital Steganography is the art of invisibly hiding data within data. It conceals the fact that message exists by hiding the actual message. In this, secret data can be hidden inside the image, text, sound clip which can be represented in binary.

**3) Printed Steganography**

Digital Steganography output can be in the form of printed documents. The letter size, spacing and other characteristics of a cover text can be manipulated to carry the hidden message. A recipient who knows the technique used can recover the message and then decrypt it.

***C) Concept of proposed system:*** This design incorporates the most powerful modified LSB & DCT algorithm to encode the message into video file. Steganography Vs Cryptography -Steganography is not an alternative to cryptography. Steganography is the dark cousin of cryptography. While cryptography provides privacy, steganography is intended to provide secrecy. In other words, cryptography works to mask the content of a message; steganography works to mask the very existence of the message.

## II. LITERATURE SURVEY

The existing systems lack good user interface, nonprovision of choosing the key and more encode-decode time consumption. There are lots of steganographic programs available. A few of them are excellent in every respect; unfortunately, most of them lack usable interfaces, or contain too many bugs, or unavailability of a program for other operating systems. The proposed application will take into account these shortcomings, and since it will be written in Java,

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 4, April 2012

operability over multiple operating systems and even over different hardware platforms would not be an issue. This proposed Software provides easy way of implementing the methods. The idea behind this design is to provide a good, efficient method for hiding the data from hackers and sent to the destination securely. This proposed system is based on video Steganography for hiding data in the video image, retrieving the hidden data from the video using LSB (Least Significant Bit) DCT (Discrete Cosine transform) modification method. This design looks at a specific class of widely used image based steganographic techniques, under what conditions can an observer distinguish between stego images (images which carry a secret message) and cover images (images that do not carry a secret message).Fig.1 shows two video images, one- carrier image of the message and the other - the image labeled Stego'd image contain the hidden message. It is not viable to identify the difference between the original video and the Stego'd video image.


**Fig. 1. Steganography using video image**

***METHODS OF CONCEALING DATA IN VIDEO:***

***1) Least Significant Bit (LSB):*** LSB is the lowest bit in a series of numbers in binary. E.g. in the binary number: 10110001, the least significant bit is far right. The LSB based Steganography is one of the steganographic methods, used to embed the secret data in to the least significant bits of the pixel values in a cover image. e.g. 240 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
240: 011110000

RESULT:

(00100110 11101001 11001001)
(00100111 11001001 11101000)
(11001000 00100110 11101000)

Here number 240 is embedded into first eight bytes of the grid and only 6 bits are changed.

***2) Discrete Cosine Transform (DCT):*** DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. 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.

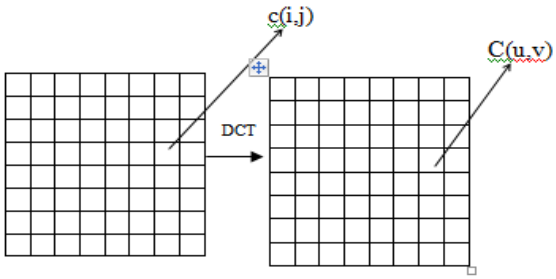


**Fig. 2. Discrete Cosine Transform of An Image**

The general equation for a 1D (N data items) DCT is defined by the following equation:

$$C(u) = \alpha(u)\sum_{x=0}^{N-1} f(x)\cos\left[\frac{(2x+1)u\pi}{2N}\right] \quad (1)$$

*for u = 0, 1, 2, . . . , N-1.*

The general equation for a 2D (*N* by *M* image) DCT is defined by the following equation:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (2)$$

For u,v = 0, 1, 2, . . . , N-1

Here, the input image is of size N X M. c(i, j) is the intensity of the pixel in row i and column j; C(u,v) is the DCT coefficient in row u and column v of the DCT matrix. Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT. Compression can be achieved since the lower right values represent higher frequencies, and generally small enough to be neglected with little visible distortion. DCT is used in steganography as: Image is broken into 8×8 blocks of pixels. Working from left to right, top to bottom, the DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

## III. BLOCK DIAGRAM

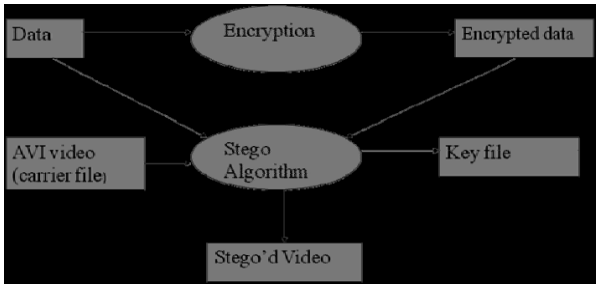


**Fig. 3. Block Diagram of VIDEO steganograpy**

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 4, April 2012

## IV. ALGORITHMS OF VIDEO STEGANOGRAPHY:

***A) DCT Algorithm***

Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8×8 block of pixels.
Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels. Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
Step 8: Write stego image. Algorithm to retrieve text message:-
Step 1: Read stego image.
Step 2: Stego image is broken into 8×8 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels. Step 4: DCT is applied to each block. Step 5: Each block is compressed through quantization table.
Step 6: Calculate LSB of each DC coefficient.
Step 7: Retrieve and convert each 8 bit into character.

***B) LSB Algorithm***

Algorithm to embed text message:-
Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego image Algorithm to retrieve text message:-
Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image. Step 3: Retrieve bits and convert each 8 bit into character

## V. DETAILED DESIGN

The video steganography software performs the process of conceal and reveal in following modules. The modules of Video Steganography are.

- Video Header Information
- File Handling
- Encryption
- Steganography – Conceal data
- DeSteganography - Reveal original data
- Decryption
- Graphical User Interface

***A) Video Header Information:*** The video header module collects the header information of an AVI (Audio/visual interleaved) file which is based on the RIFF (resource interchange file format) document format which it is used to verify the AVI format of the carrier file. This module is used to store the information about AVI Main Header, AVI Stream Header, Audio, and BITMAP. This information is used to verify whether the carrier file is in AVI format and to check whether it is a Video, Audio, or any other format.

***B) File Handling:*** In file handling, the AVI (Audio/visual interleaved) file header is skipped and its contents are opened in an ASCII format for processing. This reads the AVI file in terms of byte corresponding to the header and creates a Key file. The text file which is to be embedded is converted into binary value.
Then each bit in the binary value is then converted to 8 bit value which is done by appending zeros in front of the bit.

***C) Encryption:*** The message to be hidden inside the carrier file is encrypted along with a key to disappoint the prying eyes of nosy people. This is to enhance the security during data transmission. This strong encryption method provides robustness to the Stego machine. In this module, the input message is first converted to byte value. The key is obtained from the user which is added to the respective byte and stored in a separate byte array which is then converted to character to get the encrypted form of message. The input to this function is the plain text message and a key value to encrypt the message.

***D) Steganography – Conceal data:*** This module performs the process of steganography. Here the carrier file (AVI file) length is obtained and checked for whether it is eight times greater than that of the text file. Find the starting point of the data in the AVI file and create a key file by writing the content of the AVI file starting from the data to the end. The carrier file is converted into binary. The result is overwritten to the data part of the AVI file and as well as written into the newly created text file. The output obtained for this system is a stego'd video file, and a key file which is to be shared by a secure channel. Fig. 2 depicts the clear picture of concealing the data.

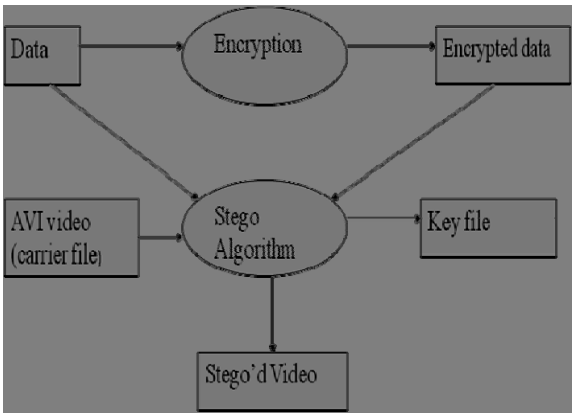


**Fig.4 .Video Steganography**

***E) DeSteganography- Reveal Original data:*** This DeSteganography module decodes the video file to retrieve the hidden data from video. Here the carrier file

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 4, April 2012

(AVI file) and the Key file are given as input. The AVI file and the Key file are opened in a Random Access Mode to find the starting point of the data in the AVI file. This reads the AVI file and Key file Byte by Byte and finds the difference between them. The output obtained is an original AVI video file, and a data file that is the message which is hidden inside the AVI video file. Fig.3 illustrates the process of revealing the original data from Stego'd video file.

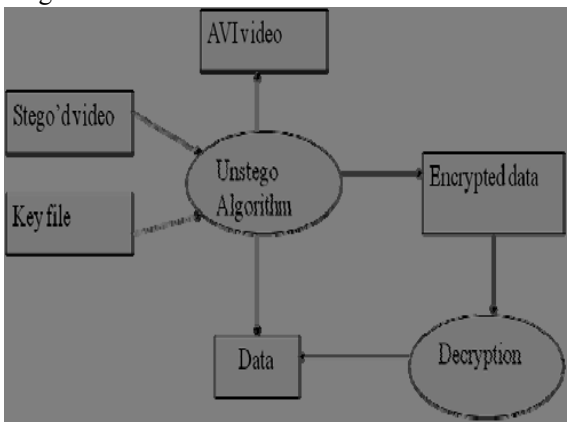


**Fig. 5 DeSteganography**

***F) Decryption:*** The hidden message is decrypted using the key, as once the algorithm gets revealed, all encrypted data with the algorithm could be decrypted. This module first converts the input message to byte value. The key is obtained from the user which is subtracted from the respective byte and stored in a separate byte array which is then converted to character to get the decrypted form of message. The input to this function is the encrypted message file and a key value to decrypt the message

***G) Graphical User Interface (GUI):*** This GUI is created as a user friendly wizard and does not need any previous training to operate it. It helps user to do steganography without encryption and encryption without steganography. This will help user with a wizard to

- Hide a message in a video file
- Retrieve the hidden message in a stego'd video
- Encrypt a text file
- Decrypt an encrypted file.

## VI. TEST CASES

**Table I: Unit testing test Cases**

| NO | TEST CONDITION | EXPECTED RESULTS | ACTUAL RESULT |
|---|---|---|---|
| 1. | To test whether the Mp3 player is playingmp3 file | The player is running& playing the file | Same as expected. |
| 2. | To test that LZW compression is properly done | Properly getting the Compressed file. | Same as expected. |
| 3. | To test that encoding & Decoding is properly done. | Properly getting the encoded and extracted file. | Same as expected. |
| 4. | To test whether the login is done properly | We are getting negative response for incorrect login name and password. | Same as expected |

**Table II: Top Down or Bottom Up test Cases**

| NO | TEST CONDITION | EXPECTED RESULTS | ACTUAL RESULT |
|---|---|---|---|
| 1. | To test whether the all instructions are played properly. | All the instruction are played properly. | Same as expected. |
| 2. | To test whether customer select the proper option. | User should select given option only. | Same as expected. |
| 3. | To test that option handle by the user should give proper next instructions to be performed | The selected option should give further instructions to be performed. | Same as expected. |

**Table III: Regration testing test Cases**

| NO | TEST CONDITION | EXPECTED RESULTS | ACTUAL RESULT |
|---|---|---|---|
| 1. | To test whether the all instructions are played properly. | All the instruction are played properly. | Same as expected. |

## VII. ADVANTAGES OF PROPOSED SYSTEM

The advantages of the proposed stego machine are a very usable and good looking wizard based GUI (Graphical User Interface) for the system Ability to operate the system with no prior training and consultation of any help files

a) Ability to conceal and reveal the exact hidden data from video file without disturbing the running application or new application

b) Ability to encrypt and decrypt the data with the images

c) With this system, an image, after hiding the data, will not degrade in quality.

## VIII.IMPLEMENTATION AND RESULTS

Mean Square Error
a)D:\project testing\Airtelvideo\Airtel_H.avi
b)D:\project testing\ Airtelvideo\ stegoAirtel_H.avi

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 4, April 2012

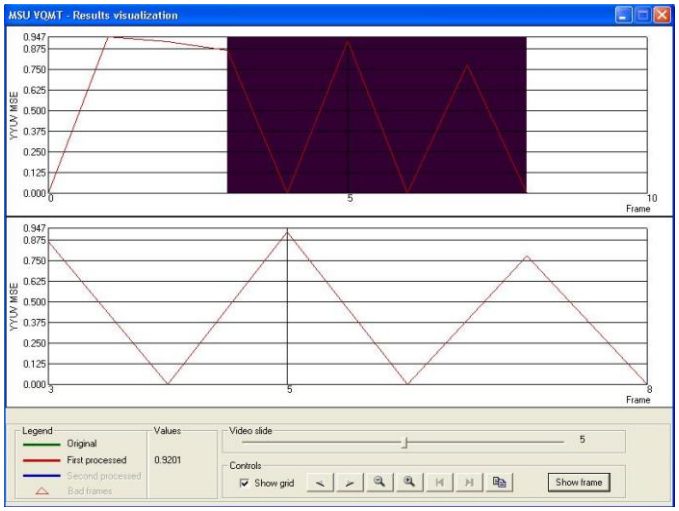


**Fig. 6 Mean Square Error**

| MSE_YYUV |
|---|
| D:\project testing\Airtelvideo\Airtel_H.avi |
| D:\project testing\Airtelvideo\stegoAirtel_H.avi |
| AVG: 0.40168 |
| 0 |
| 0.94711 |
| 0.9137 |
| 0.86241 |
| 0 |
| 0.92009 |
| 0 |
| 0.77511 |
| 0 |
| 0 |
| 0 |

PSNR :a)D:\project testing\Airtelvideo\Airtel_H.avi

b)D:\project testing\Airtelvideo\stegoAirtel_H.avi

| PSNR_YYUV |
|---|
| D:\project testing\Airtelvideo\Airtel_H.avi |
| D:\project testing\Airtelvideo\stegoAirtel_H.avi |
| AVG: 52.09036 |
| 100 |
| 48.36512 |
| 48.5211 |
| 48.77189 |
| 100 |
| 48.49081 |
| 100 |
| 49.23547 |
| 100 |
| 100 |
| 100 |

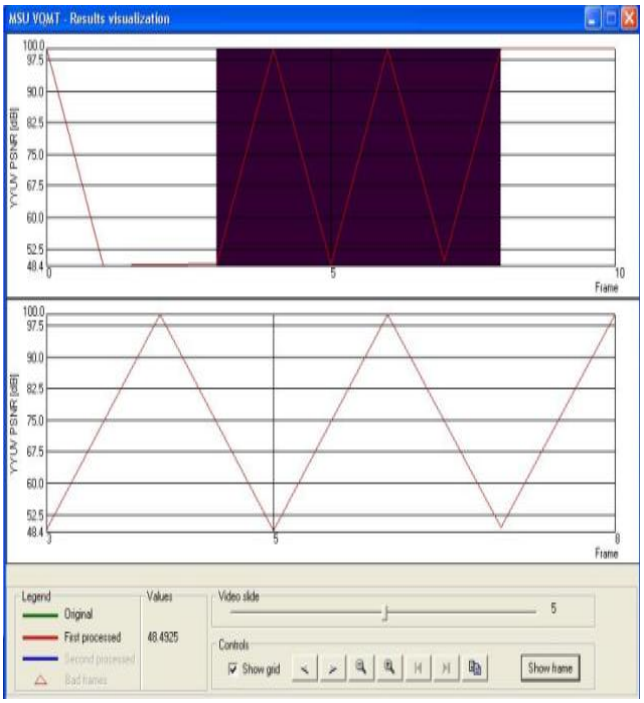


**Fig. 7. PSNR**

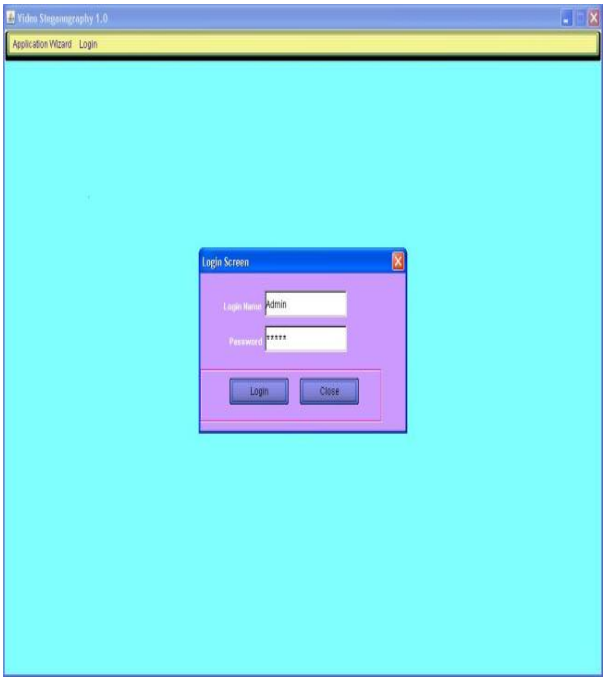


**Fig 8 Login Screen**

Choose Option:

Embed

Extract

Video Extractor:

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 4, April 2012

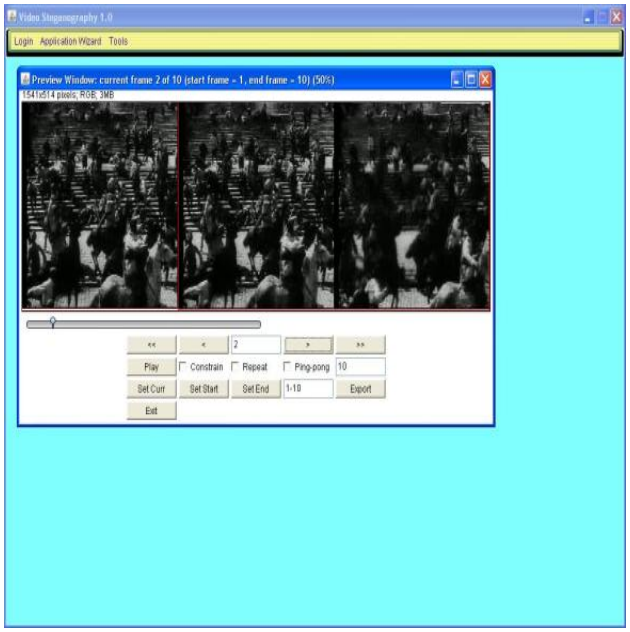


**Fig .9. Video Extractor**

Main Panel (Transmitter Receiver):

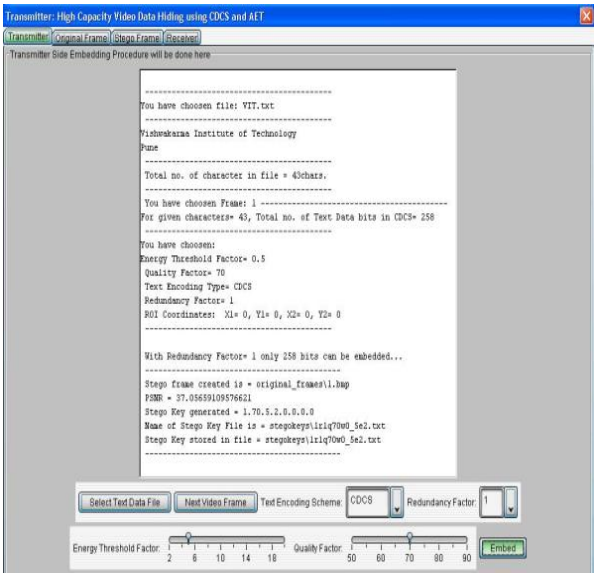


**Fig.10. Main Panel (Transmitter Receiver)**

## IX. CONCLUSION

The proposed System is based on the research findings developed an application which would be able to hide data into video images (AVI) that provides a robust and secure way of data transmission. This Stego system implements steganography in video image and reveal process without restarting a different application. Also this system is Platform Independent application with high portability and high consistency.

## ACKNOWLEGEMENT

Thanks To IJEIT for accepting this paper. We are very thankful to Amrutwahini College of Engineering, Sangamner, and Ahmednagar, India for providing us the opportunity to work on this project.

## REFERENCES

[1] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding—A Survey," Proc. IEEE, 1999.

[2] Niels Provos and Peter Honeyman, "Hide and Seek: An Introduction to Steganography", University of Michigan, IEEE 2003.

[3] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia,"Application of LSB Based Steganographic Technique for 8-bit Color Images", WASET 2009.

[4] Sutaone, M.S.; Khandare, "Image based Steganography using LSB insertion technique", IET, 2008.

[5] Mazdak Zamani, Azizah A. Manaf, and Shahidan Abdullah, "A Genetic- Algorithm-Based Approach for Audio Steganography" WASET 2009.

[6] Neeta Deshpande, Kamalapur Sneha, Daisy Jacobs, ―Implementation of LSB Steganography and Its Evaluation for various Bits_ Digital Information Management, 2006 1st International Conference on. 06/01/2007; DOI: 10.1109/ICDIM.2007.369349.

[7] Kharrazi, M., Sencar, H. T., and Memon, N. (2004). Image steganography: Concepts and practice. In WSPC Lecture Notes Series.

[8] Neil F. Johnson, Duric, Z., Jajodia, S. Information Hiding Steganography and Watermarking Attacks and Countermeasure. Kluwer Academic Press. Norwrll, MA, New York, The Huague, London vol 32.8(2010) 79-94.

[9] Neil F. Johnson and S. Jajodia Exploring Steganography. Seeing the Unseen, IEEE Computer, vol. 31.2 (2009) 26 - 34.

[10] Min. Wu Joint Security and Robustness Enhancement for Quantization Embedding. IEEE Transactions, vol 0-7803-7750-8/03 (2009) 483-486.

[11] C. E. Shannon A mathematical theory of communication. Bell System Technical journal, vol. 27 (1948) 379-423.

[12] G. J. Simmons The prisoners' problem and the subliminal channel, in Advances in Cryptology. Proceedings of Crypto 83 (D. Chaum, ed.), Plenum Press vol 12.9(2010)51-67.

## AUTHOR BIOGRAPHY

.

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 4, April 2012

Poonam V Bodhak completed her Diploma From MIT Polytechnic, BE in Computer Engineering from GSMCOE, ,Balewadi,Pune.Presently work ing as a HOD of Computer Technology in Ajitd ada Pawar College Of polytechnic,Shrirampur, A'Nagar,Maharashtra. Pursuing in Second year of ME Computer Engineering.

Baisa L Gunjal completed her BE Computer From University of pune and Mtech in I.T from Bharti Vidhyapeth India.Working as PG Co-coordinator in AVCOE College of Engineering, Sangamner, India. Presentl working on research project on "Image Water marking" fund BCUD, University of Pune.