ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Robust and Secure Text Transmission through Video Steganography Using Pixel Mapping

K. Keerthi
M.Tech in CESP,
RVR & JC College of Engineering,
Chandramoulipuram, Chowdavaram, Guntur Dist.
Andrapradesh, India

P. Sailaja
Assistant Professor, Dept. of ECE
RVR & JC College of Engineering,
Chandramoulipuram, Chowdavaram, Guntur Dist.
Andrapradesh, India

Abstract- ***In Recent years there is a rapid growth in wireless technologies, Gega bytes of information has been exchanging over many communication channels. However, few applications like military, medical, multimedia, web and civil etc. need to provide the security to the information sending over. Hence, secure transmission is a highly challenging task. Here in this, we supposed to introduce a new secure text image transmission scheme by using pixel mapping through video steganography, which is based on the very simple easy method called as pixel mapping. In the proposed scheme, the video is divided into number of frames then after number of images afterwards the secret message will be kept into the video sequences. The simulation results have been shown both the image and video steganography outputs and the performance comparison done in terms of Peak Signal to Noise Ratio (PSNR), MSE and Structural Similarity Index (SSIM).***

Keywords: ***Stegnography, Video, Noise, Frames, Cryptography, SSIM, MATLAB.***

I. INTRODUCTION

Recent years there is a rapid growth in digital information sharing such as digital images or digital videos. Digital information sharing will be done in various applications, each of them need to transmit the information securely without knowing to the unauthorized person or party. Most of the media services and wireless network technologies were providing omnipresent conveniences for sharing, collecting or distributing images or videos over cellular mobile networks, social networks such as wechat, whatsapp, facebook etc., wireless public channels and multimedia networks for many organizations and individuals. For the applications like storage and transmission securing an image is a challenging task. For example, many strategic places like commercial centers, financial centers and public transportations will be monitored by digital video surveillance systems for the purpose of homeland security. Every day there is a large amount of images and videos with secure information, which does not known by unauthorized persons have been generated, transmitted or restored. Many applications such as medical, military, construction industries, fashion design industries and automobile industries require scanned information, blue prints and designs to be protected against espionage. In addition to this, patient's records in medical images such as Magnetic Resonance (MR) or Computed Tomography (CT) and medical signal reports such as electro cardiogram (ECG) or electro encephalogram (EEG) will be shared among the most of the doctors from different branches of health service organizations (HSO) over wireless networks for diagnosis purpose. All these medical images, signals and digital videos may contain some private information, which is more confidential. Hence, it is an important task to provide security for this sort of images and videos. Developing and employing schemes to enhance the lifetime of digital images or videos is an important, imperative and challenging task, which protects the content of original data for many years [1]. To protect an image or video encryption is an effective approach [1], which transforms the image or video into different format.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message[1]. Technically in simple words "steganography means hiding one piece of data within another". Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements. The cover media(C) that will hold the hidden data

- The secret message (M), may be plain text, cipher text or any type of data
- The stego function (Fe) and its inverse (Fe-1)
- An optional stego-key (K) or password may be used to hide and unhide the message [3].

Steganography is the art or study of hiding information by inserting secret messages in other messages. Medium where information is inserted can be anything. This medium is called the cover object. Steganography that is applied to hide information on the cover of digital objects is called Digital Steganography [3]. Cover objects that are used in digital steganography can vary, for example in the image archive. Steganography algorithms in the image archive have been widely developed. Meanwhile, steganography algorithms in audio archive are relatively few. In recent years there are so many algorithm have been developed to provide more security, enhanced quality with easy implementation and faster calculations. Among them all of the techniques have their own drawbacks like computational complexity, time consumption and reconstruction of secret information etc., Here, in this proposal we implemented pixel mapping based video steganography, which is a very simple and easy calculations and also provide more security.

II. VIDEO STEGANOGRAPHY

For normal human being the ability to perceive the motions of other animate frames or video has been extensively studied and it is shown that for the movements created in the running video only the small amount of the pixels are modified and rest all the pixels remain static if we compare the pixels of any consecutive frames in a video. So by the changes made in the smaller number of pixels in a sequence of images all the movements are described perfectly in a video file. This is very simple and easy method for visualizing any process under study. Research shows that among the consecutive images having million numbers of pixels only few hundred pixels are modified for showcasing the movements happening in the particular video. Any video is basically a combination of different frames and all the frames constituting a video has a fixed frame rate. Generally the frame rate is 25 so we can say that 25 frames are captured within one second time. For the efficient and successful implementation of this particular algorithm there is a requirement that the video needs to be segmented. For a particular case if we suppose that the video is of 5 minutes duration than this video majorly contains 7500 frames in it. These frames are vital building block for the video as well as for video encryption process. We can insert and send the text along with the frame by using various available watermarking techniques. There are various different watermarking techniques available like visual watermarking, discrete cosine transform, discrete Fourier transform and lossless watermarking method. All the watermarking techniques recently available have certain drawbacks and also these methods are a little bit time consuming. Also the watermarking techniques can be modified using more advanced techniques for image processing. To get over the drawbacks of the watermarking techniques stenography method can be used for the encryption of the video files. Stenography is mainly useful in terms of efficient and accurate data processing for the case of the real time applications. In the proposed work also the stenography technique can be generated by using a pixel mapping algorithm. Also the stenography technique is faster and efficient in terms of time required for marking the particular set of images.

i. Cryptography

Cryptography is an art of protecting the information by transforming it into an unreadable and untraceable

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

format known as cipher text. Only the person who possess the secret key can decipher or we can say decrypt the message into the original form. Cryptography is the technique by which one can send and share the information in a secret manner. Due the cryptography the information seems to be appearing like a garbage value and it is always almost impossible to find the information content lying under the image or a video file. The information looks like hidden inside the image or the video file. A very simplest and well known algorithm for cryptography is as shown in figure 1. The encryption key generator is used to generate the encryption key as well as the public key as shown in the block diagram below. By using the encryption key the information content to be sent gets encrypted by the encryptor. The encrypted information is then transmitted to the particular receiver. At the receiver end the Cryptography Decryptor is used which extracts the original information content mapped onto the image or a video file with the help of a public key provided by the transmitter section. So by the use of the cryptography method only the receiver which has the knowledge of the public key can retrieve the original information content from the image or a video file. So even if any unwanted person or a source gets the image or a video file with information content hidden in it, it cannot be extracted without proper public key. So public key plays a vital role in the whole cryptography process

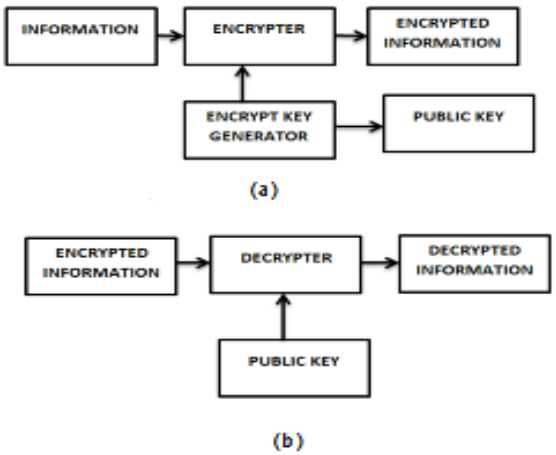


Fig.1 (a) and (b) Block diagram of Encryptor and Decryptor

ii. Steganography

Stenography is the art of hiding information by embedding message within each other. It works by replacing the very useless bits by the information content to be transmitted. It works by hiding information inside a cover. The cover may be an image file or a video file as per the user requirement. Even though the cover looks very simple and unchanged but it has information contained in it. Figure 2 describes the simplified process of steganography.

First of all, the video file in converted into sequence of frames of equal size. The information content which is to be transmitted by mapping onto the video file is distributed into small portion depending on the size of the frames in the video file. From each frame a smaller region is modified depending upon the private key. Due to this the selected groups looks very random to the third party who does not have the private key with them.

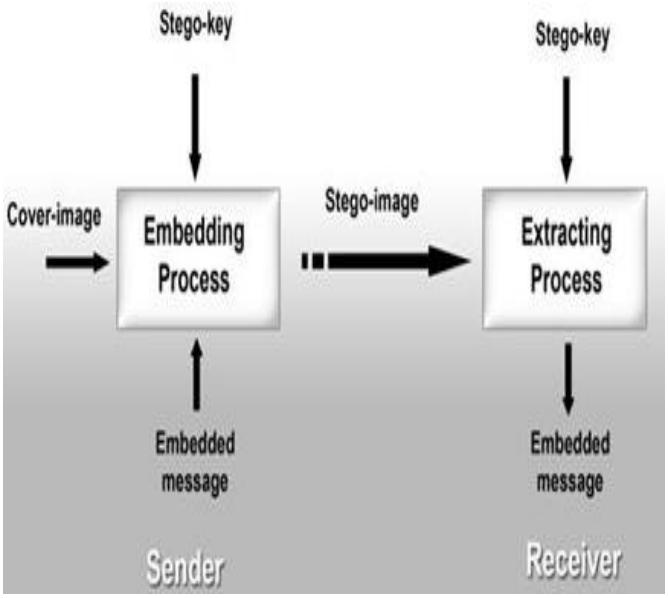


Fig2. Process of Steganography

III. PROPOSED ALGORITHM

Proposed algorithm include both embedding and extraction processes. Embedding is a process in which the message information will be inserted into the cover video by using the pixel mapping algorithm. And the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

retrieving of message information by applying inverse process of embedding is called as extraction process.

Figure 3 describes the sequence of steps to be executed for generating the embedded video file for secured text data transmission. The algorithm is briefly described in terms of block diagram for the better understanding of the whole process. The complete algorithm is coded in a Matlab code showing the detailed process involved in the video steganography and the text insertion in the video file for secured transmission. As shown in the algorithm in figure 3 the complete video is segmented into number of images using a small Matlab code module and after the processing of the video by the Matlab code module the video gets divided into different frames of same size. Then select the image to embed the message file into it. Then apply pixel mapping algorithm to embed the message bits

Pixel mapping algorithm with LSB approach

Step1: Select the cover image *'C'* from the video sequences, which had converted by using MATLAB code

Step2: Convert the image *'C'* into unsigned integer format (uint8) and divide the cover image into Red (R), Green (G) and Blue (B) components

Step3: Select the number of input bits '*n*' to be substituted in '*C*'

Step4: Now, do the logic AND operation to the number of bits in R component of *'C'* and substituted *'n'* bits

Step5: Then do the bit OR operation to the output of above step and the entire shifted message bits with '*n'* bits

Step6: Repeat the same for green and blue components also

Step7: Do the same process for all the selected frames from the video file and then convert R, G and B components into stego frame then after reconstruct all the frames into stego video, in which the message information has been embedded

LSB Approach

- Least Significant Bit (LSB) insertion is a common, simple approach to embedding information in a cover video.
- Video is converted into a number of frames, and then convert each frame in to an image.
- After that, the Least Significant Bit (in other words the 8 bit) of some or all of the bytes inside an image is changed to a bit of each of the Red, Green and Blue colour components can be used, since they are each represented by a byte.
- In other words one can store 3 bit in each pixel.
- We implemented our project such that it can accept and video of any size.

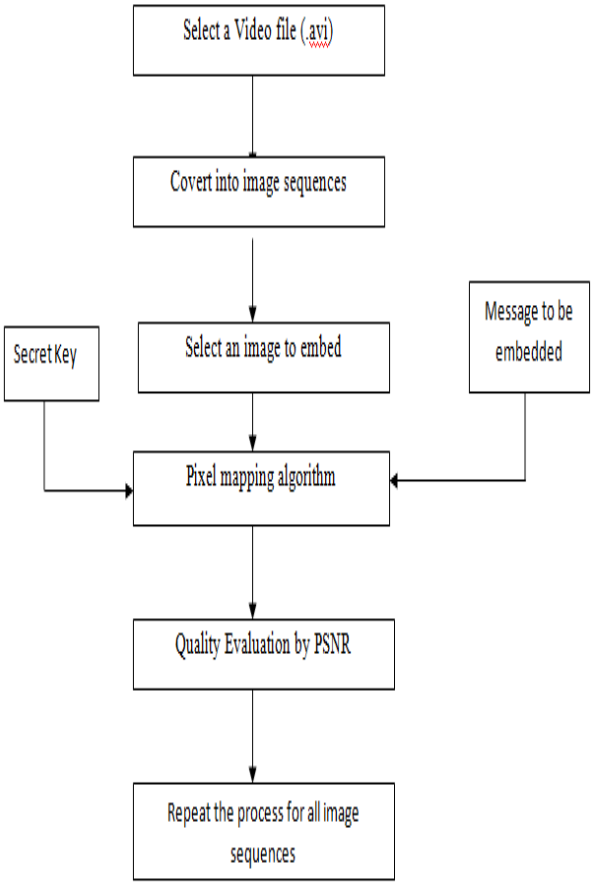


Fig3. Proposed Embedding algorithm

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

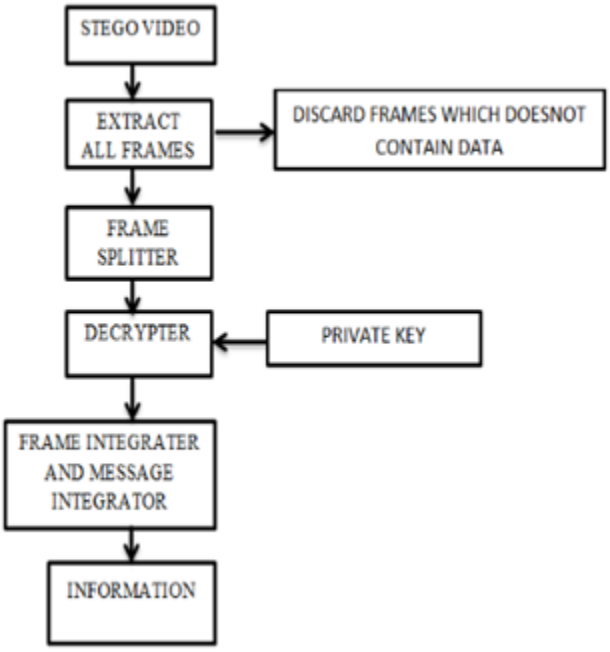


Fig4. Proposed Extraction process

IV. SIMULATION RESULTS

Experimental results has been shown in this section, all the experiments have been done in MATLAB 2014a. We had tested the proposed algorithm for both images and videos for different number of bits substitutions. The histogram approach is used to compare the extracted message with the original message.

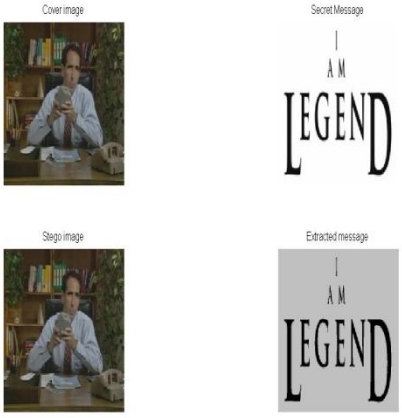


Fig5. Simulation results of proposed scheme for N=2 bits

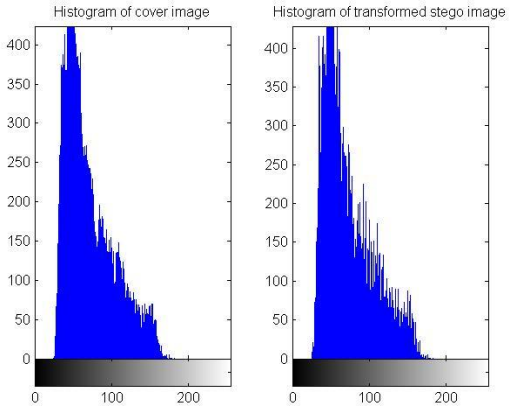
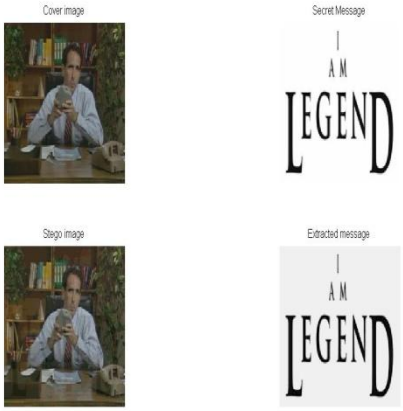
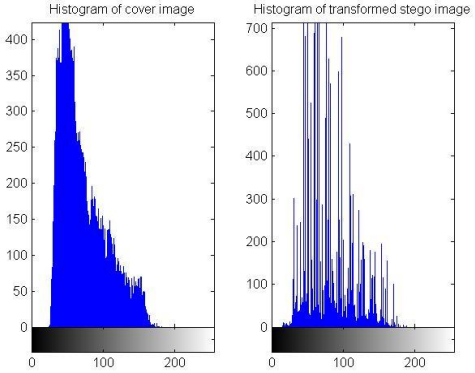


Fig6. Comparison of cover and stego image for N=2 bits

In fig.5, the embedding and extraction results has given for N=2 bits i.e., the number message bits insertion is in LSB range that's why the original and stego images are almost same and we can found that even in the histogram graph in fig.6.



(a)



(b)

Fig7. Embedding and extraction results for N=4 bits

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

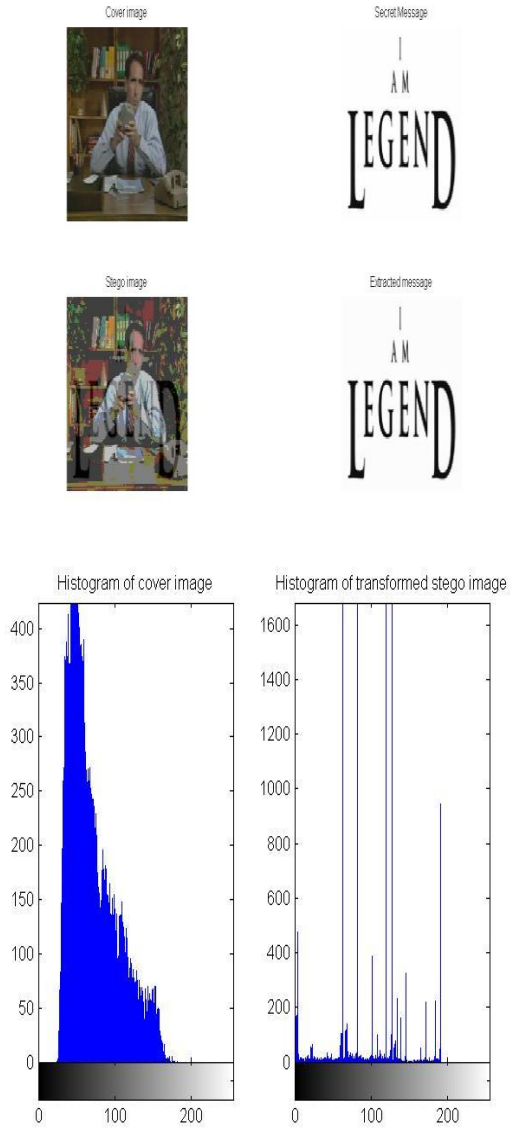


Fig8. Embedding and extraction results for N=6 bits

Fig 7(a) shows the results of proposed steganography for N=4 bits, in which the total four LSB bits has been modified by the message bits insertion and the stego image also changed slidely that is the message is visible to the naked eye. It has shown in fig.7 (b) by its histogram representation. Fig.8 shows for N=6 bits, in which the stego image is completely changed and the message bits were visible to the unauthorized person. This observation give us a conclusion that, by increasing the N the quality of stego image was degrading and secure concern also reducing.

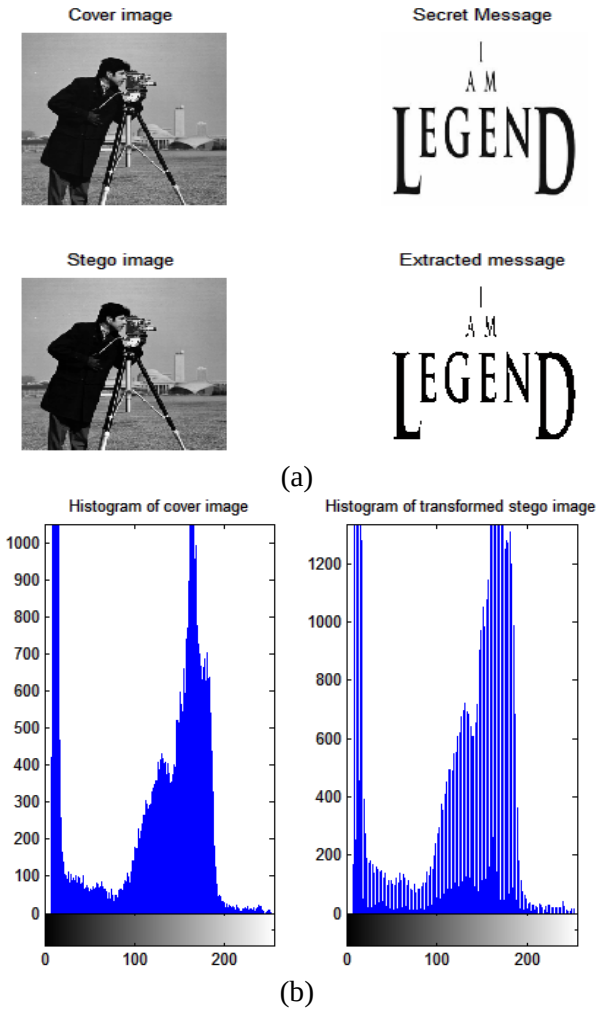


Fig9. Simulation results for image steganography

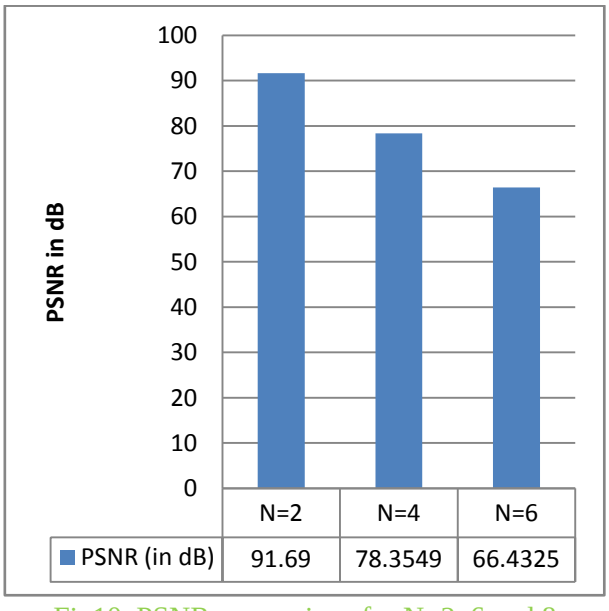


Fig10. PSNR comparison for N=2, 6 and 8

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

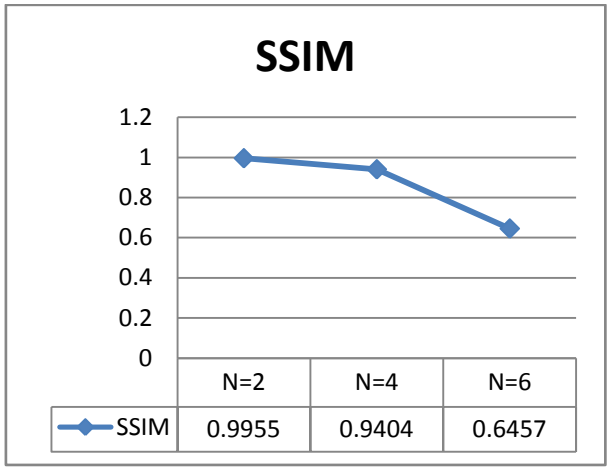


Fig11. SSIM comparison for N=2, 6 and 8

Inn fig 10 and 11, the quality metrics Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM) has been calculate for original and stego images and the performance graph has been displayed. We can see that the quality of image has been degrading while increasing the *N* value.

V.CONCLUSIONS

One of the important features of the proposed work is it plays a vital role in transmitting the information mapped on an either image or a video file very effectively and efficiently. The information underlying the image or a video is not visible to the naked eye when we embed the message information into LSB. Only the person having the private key and the rule list can identify and decode the original information into its original form. This method simplifies the task of securing the vital information from the misuse and protects it from the unwanted user. With the use of the cryptography and steganography combination the information security can be increased.

REFRENCES

1. http://en.wikipedia.org/wiki/Time-lapse.
2. Handbook of image and video processing by Alan Conrad Bovik, Elsevier Inc., ISBN 0-12-119192-1.
3. R.Asha & M.Raja babu, Discrete Wavelet Transform Based Steganography for Transmitting Images, IJMETMR, http://www.ijmetmr.com/oldecember2014/RAsha-MRajababu-108.pdf, Volume No: 1(2014), Issue No: 12 (December)
4. Digital Video Processing by A. Murat Tekalp, Prentice Hall Signal Processing Series.
5. R. Schaphorst, Videoconferencing and video telephony, Boston, MA: Artech House Publishers, 1996.
6. Adnan M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Trans. On Image Processing, vol. 13, no.8, Aug, 2004.
7. Avcibas, N. Memon, and B. Sankur Steganalysis using image quality metrics, IEEE Trans. IP, VOL. 12, PP.221-229, Feb. 2003.