International Journal of Intelligent Computing and Information Science

VIDEO STEGANOGRAPHY USING LEAST SIGNIFICANT BIT IN FREQUENCY DOMAIN

A.. E. Ibrahim M. A. Elshahed T. I. Elarif

Physics department, Faculty of Women for Arts, Sciences and Education, Ain Shams University-Egypt
anwarelbayomi@yahoo.com m_3li4@yahoo.com

Computer Science Department, Faculty of Computer and Information Sciences, Ain Shams University-Egypt
taha_elarif@yahoo.com

Abstract: *Video steganography is a technique to hide different types of files (secret massages) into a carrying video file. Video files contain a collection of images (frames) and sounds, so most of techniques that apply on images and audio files can be applied to video files also. The large amount of data that can be hidden inside the video and the fact that it is a moving stream of images and sounds gives the cover video files great advantages. In this paper, we present a proposed video steganography algorithm in the frequency domain. It was applied to two datasets to study the effect of selecting red, green and blue band on the quality of stego images. From the results we found, the quality of the stego images after data embedding into red channel, green channel and blue channel depends on the nature of the dataset.*

Keywords**:** Video Steganography, Characterization of Steganography Systems, General Steganography System

1. Introduction

Most of the time, users on the internet have to send, share or receive secret information. Because of rapid development in both computer technologies and internet, the security of information is considered one of the most important factors of information technology and communication. Cryptography is a technique for securing the secrecy of communication. Many different encrypt and decrypt methods have been implemented to maintain the secrecy of the message. Steganography is the art and science of invisible communication of messages. It is done by hiding information in other information. The difference between Steganography and Cryptography is that the cryptography focuses on keeping the message content secret whereas in steganography focus on keeping the existence of a message secret.

The primary goal of steganography is to hide a secret massage within a carrier. The carrier can be a text, image, audio and video file. On the other side steganalysis is the science of detecting hidden message (the objective of steganalysis is to break steganography system).
The term steganography comes from the Greek words stegos (cover) and graphy (write). As result a steganography literally means covered writing [1,2,3,4, 5].

Steganography dates back to Golden age of Greece when people at that time had different ways to hide writing such as writing on a wooden tablet and then covering it by wax, making a tattoo on a messenger head after shaving his hair and let his hair grows up again and then send him to the receiver where his hair was shaved there again to get the message. Other steganography techniques like using invisible ink for writing between lines, microdots and using character arrangement are also used.

There are many applications for steganography in our life. When sensitive data is transmitted from one place to another they have to be protected from modifying, copying and claiming their ownership. There must be a way to provide availability, integrity, confidentiality services to the information exchanged. Steganography will provide these services [6].

2. Characterization of Steganography Systems

The aim of Steganographic techniques is to embed a message inside a cover. Various features characterize the strength and weaknesses of the methods.

2.1 Capacity: The notion of capacity in data hiding refers to the total number of bits hidden and successfully recovered by the stego system, or measures the amount of hidden information compared to the amount of carrier information, without breaking any other requirement (invisibility, robustness...). In audio, it measures the rate of hidden bits per second.

2.2 Robustness: Robustness refers to the ability of the embedded data to remain intact if the stego-system undergoes transformation, such as linear and non-linear filtering, addition of random noise, scaling, rotation, and loose compression.

2.3 Undetectability: Undetectability means that the unwanted parties can not detect the foundation of the secret data inside the cover file also he can not detect the position of the hidden data. Undetectability is directly affected by the size of the secret message and the format of the content of the cover image.

2.4 Invisibility (Perceptual Transparency): This concept depends on the properties of the human visual system or the human audio system. The embedded information is imperceptible if the human is unable to distinguish between carriers that contain hidden information and those that do not. It is important that the embedding occurs without a significant degradation or loss of perceptual quality of the cover.

2.5 Security: It is said that the embedded algorithm is secure if the embedded information can not be removed after the attacker discovers it, and it depends on the total information about the embedded algorithm and secret key. It measures the degree of difficulty/ease of deletion or extraction of the hidden information, for an attacker who believes there is hidden information but does not have the stego-key [7,8].

3. General Steganography System

A general Steganography system is shown in Figure (1). At first both the secret information and the cover media pass into the encoder. Inside the encoder, one or several process will be implemented to embed the secret information into the cover media.
In the embedding process a secret message (M) embed into an object (I). A key (K) is used in the embedding process. The result of the embedding process is a stego object (Ĩ). The resulting stego object (Ĩ) is generated by the mapping: $I \times K \times M \rightarrow \tilde{I}$.

The stego object will then be sent off via some communications channel, such as email, to the intended recipient for decoding. The stego object should be identical to the cover object as otherwise a third party attacker can see embedded information. In the decoder an algorithm will be implemented to extract the secret information embedded in the stego object using the stego key [9].

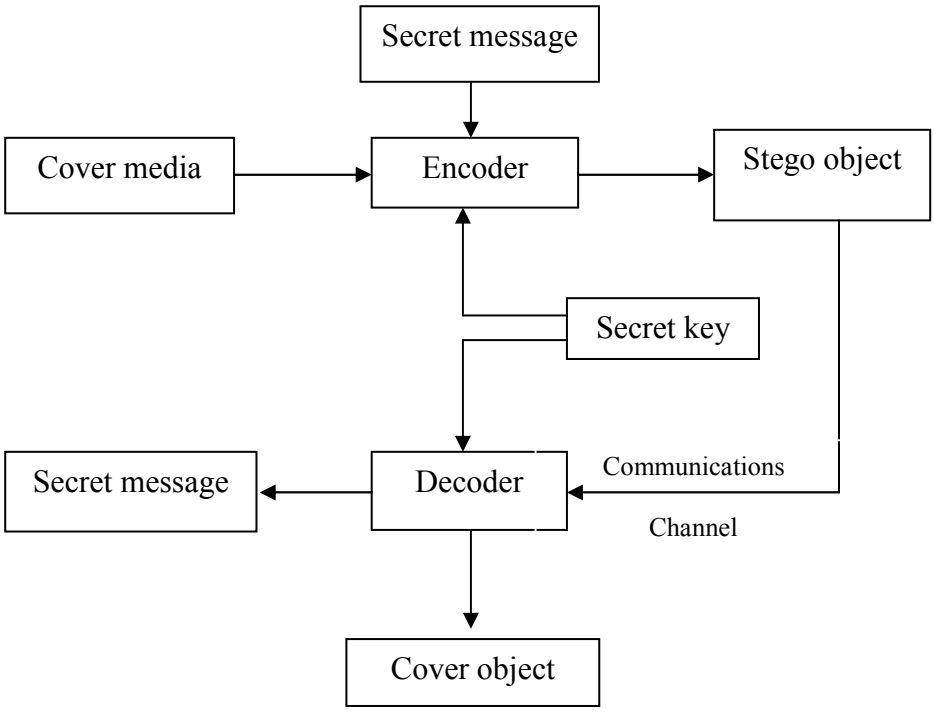


Figure (1): General Steganography System.

4. Categorization of Steganography According to Carrier Files

Depending on the media in which we hide the data, steganography is classified as text, image, audio, video or protocol. Almost all digital file formats can be used for steganography, but the files with a high degree of redundancy are more suitable. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Figure (2) shows the four main categories of cover media that can be used for steganography [10].

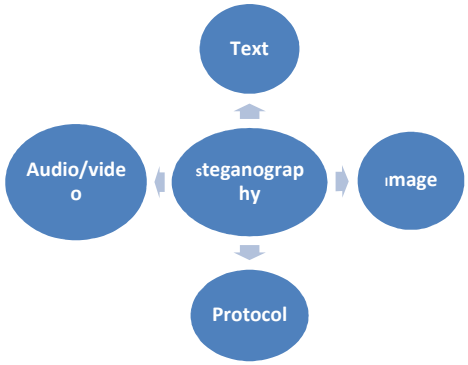


Figure (2): Categories of steganography.

4.1 Text Steganography

Text steganography uses the text media as a cover to embed a secret message. Embedding secret messages in text is considered a very challenging task because text files have a very small amount of redundant data to replace with a secret message. Another disadvantage of text steganography is that unwanted parties can alter the text itself or reformate the text to some other form (from .TXT to .PDF, etc.) [11].

4.2 Image Steganography

Steganography that uses image files to hide the secret information is called image steganography. In Image steganography, the secret message is embedded into an image as noise to it, which is nearly impossible to differentiate by human eyes.

Image steganography techniques can be divided into two groups shown in figure (3): the first is the image domain which is also known as the spatial domain technique in which secret messages embed directly in the intensity of the pixels, the second is the transform domain which is also known as the frequency domain in which images are first transformed to the frequency domain and then the message is embedded in the image.

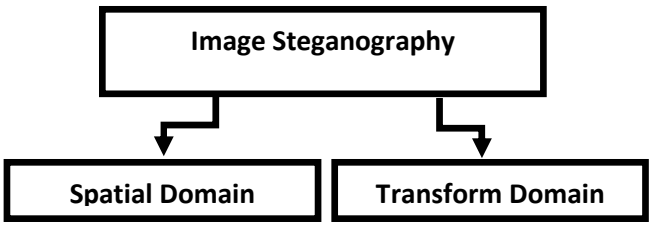


Figure (3): Image Steganography techniques Classification.

4.3 Audio Steganography

Embedding secret messages into audio files (digital sound) is called audio steganography. Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range [12,13].

4.4 Protocol Steganography

Protocol steganography means embedding secret information within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist covert channels where steganography can be used, for example embedding information in the header of a TCP/ IP packet in some fields that are either optional or are never used [14].

5. Previous Work

In [15], video steganography by Least Significant Bit (LSB) substitution using different polynomial equations was proposed. In this paper, a data hiding scheme will be developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation.

In [16], improved protection in video steganography using Discrete Cosine Transform (DCT) & LSB was proposed. 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.

In [17], a Hash based least significant bit technique for video steganography was proposed whose main goal is to embed a secret information in a particular video file and then extract it using a stego key or password. In this Least Significant Bit insertion method is used for steganography so as to embed data in cover video with change in the lower bit. A hash function is used to select the particular position for insertion of bits of secret message in LSB bits.

In [18], Video Steganography Using Pixel Intensity Value and LSB Technique was proposed. In this paper, a new idea in video based steganography was introduced, where secret message bits are embedded in the cover file by using LSB technique. For embedding, the selection of cover file RGB pixels is done on the basis of its color intensity value.

In [19], an improved technique for video steganography was proposed. The technique is based on hash based round LSB method. In this paper secret text message is embedded in the video file using proposed hash based round Least Significant Bit technique. The proposed technique hash based round Least Significant Bit was compared with the hash based Least Significant Bit. The results obtain for the proposed technique H- Round LSB are improved in comparison to H-LSB.

6. The Proposed Embedding Algorithm

In our proposed algorithm, at first the input video is separated into frames, certain frames are selected then separate the frames into three bands (red, green and blue), then select the band and apply the discrete cosine transform (DCT), apply the ZigZag Scan that aims to convert the two dimensional array into one dimensional array and arrange the low frequencies then the high frequencies, convert the secret message into binary, embed the secret data using Least Significant Bit (LSB) into the one dimensional array selecting a certain skip to hide data into the high frequencies to obtain little distortion , apply the inverse operations, the inverse ZigZag Scan, the inverse discrete cosine transform, return the modified frames to get the output video. Figure (4) shows the proposed embedding algorithm.

7. Experimental results

In the experiment we used two datasets each dataset contains 300 frames, the frame size is 288*352. We use the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and correlation to measure the quality of the stego after data embedding. We studied the effect of selecting the red channel, green channel and blue channel on the quality of the of the stego images after data embedding.

For the first dataset we found when we embed the secret message in red channel the average PSNR= **58.35497766,** when we embed data in green channel the average PSNR= **58.7778769** and when we embed data in blue channel the average PSNR= **57.7651502**. Figure (5) shows the PSNR of the stego frames.

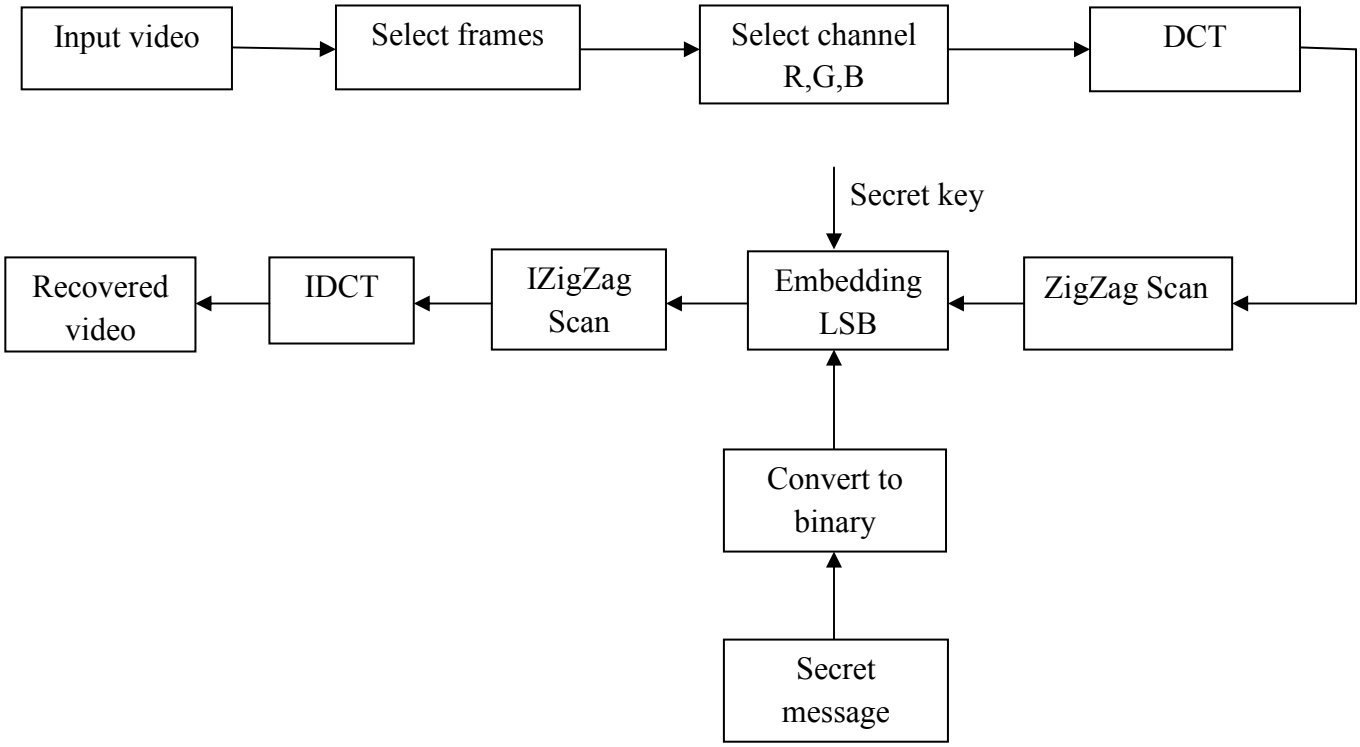


Figure (4): The proposed embedding algorithm.

7.

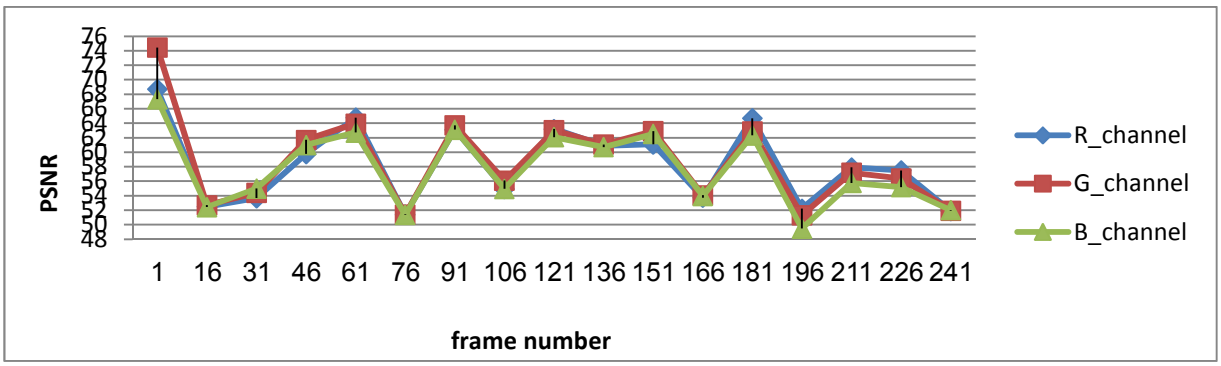


Figure (5): The relation between the frame number and the PSNR of the stego images for the first dataset.

Figure (6) shows the MSE values of the stego frames after data embedding when we select the red band, the green band and the blue band.

Figure (7) shows the correlation values of the stego frames after data embedding when we select the red band, the green band and the blue band. Figure (8) shows an example for selected frame used for embedding in the first dataset.

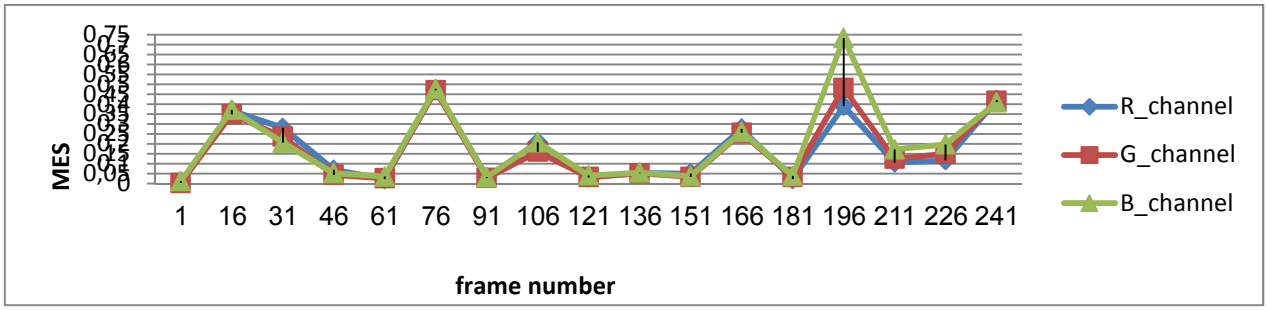


Figure (6): The relation between the frame number and the MSE of the stego images for the first dataset.

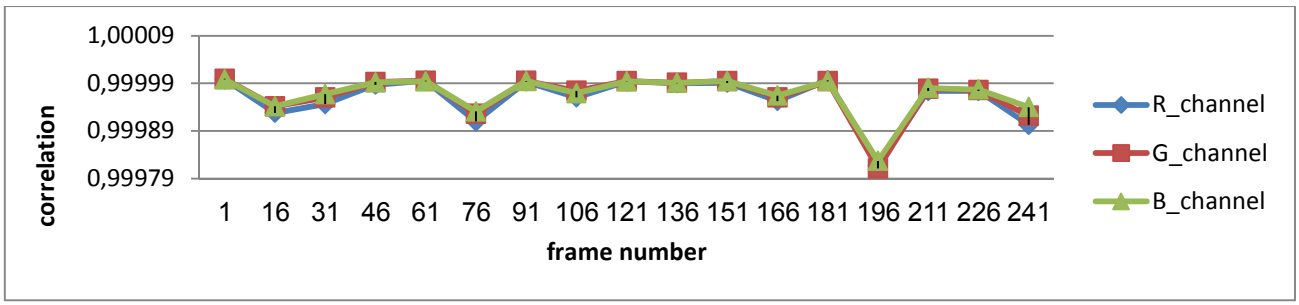
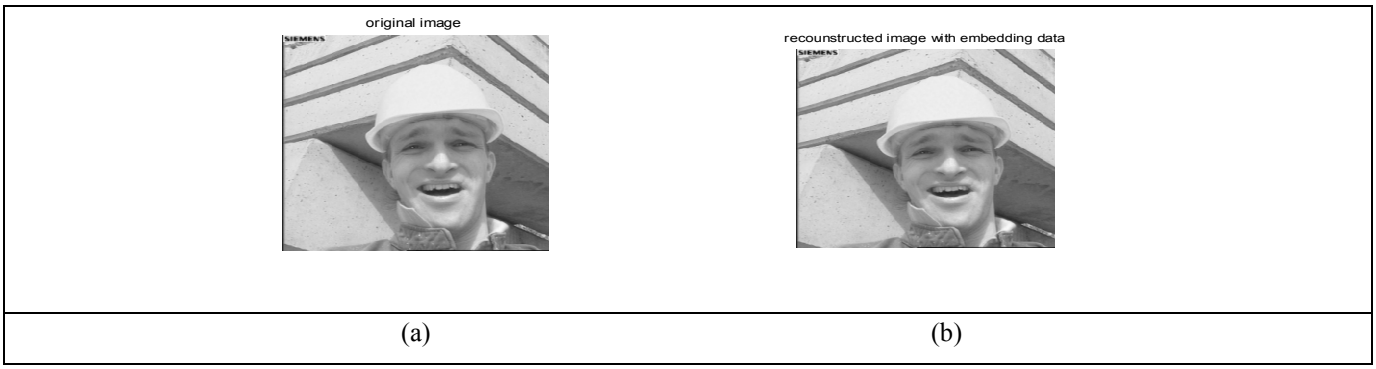


Figure (7): The relation between the frame number and the correlation of the stego images for the first dataset.



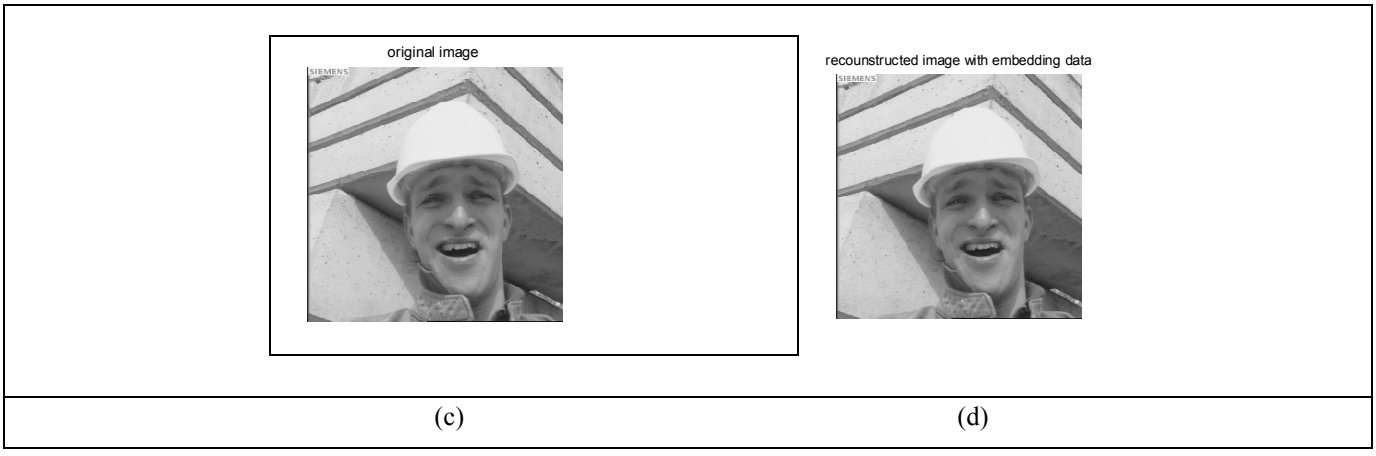


Figure (8): Illustrates frame from the first dataset, (a) shows the original frame (red channel), (b) shows the stego image (red channel), (c) shows the original frame (green channel), (d) shows the stego image (green channel).

For the second dataset we found that when we embed the secret message in red channel the average PSNR= **52.659554,** when we embed data in green channel the average PSNR= **53.02824902** and when we embed data in blue channel the average PSNR= **53.23792284**. Figure (9) shows the PSNR of the stego frames

.

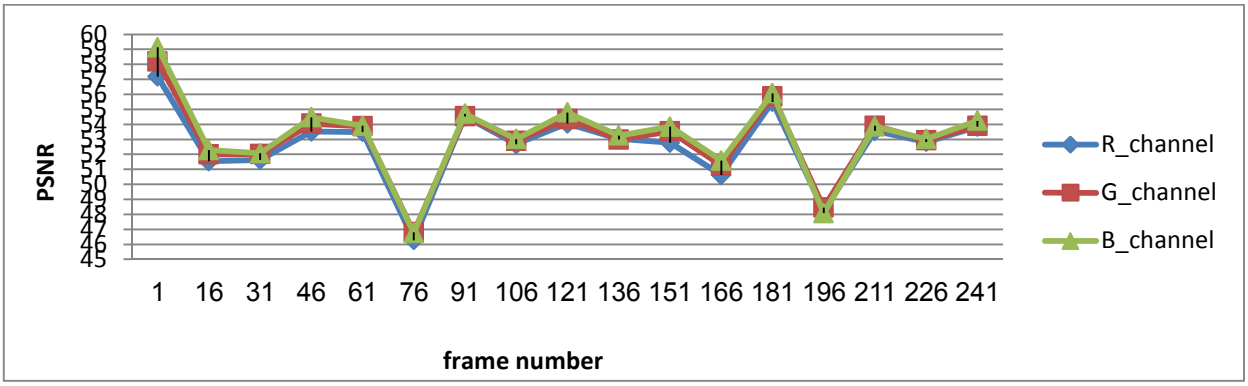


Figure (9): The relation between the frame number and the PSNR of the stego images for the second dataset.

Figure (10) shows the MSE values of the stego frames after data embedding when we select the red band, the green band and the blue band.

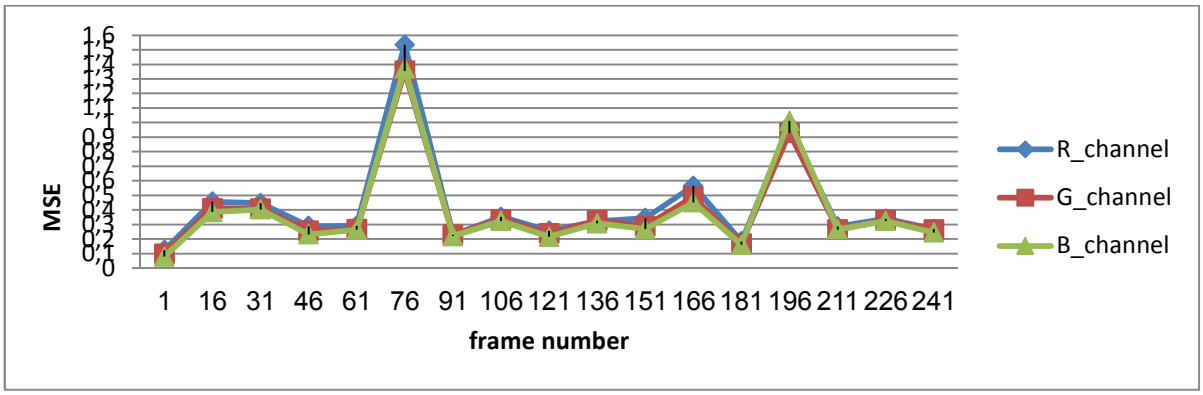


Figure (10): The relation between the frame number and the MSE of the stego images for the second dataset.

Figure (11) shows the correlation values of the stego frames after data embedding when we select the red band, the green band and the blue band. Figure (12) shows an example for selected frame used for embedding in second dataset.

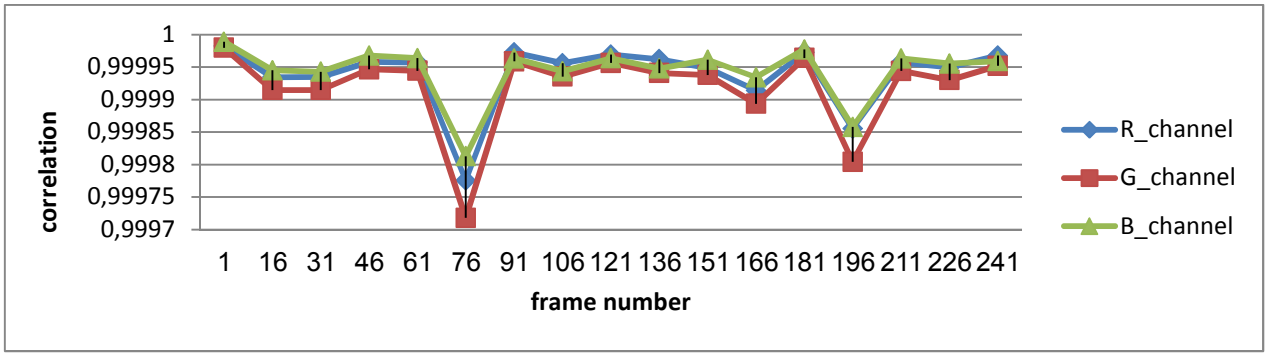


Figure (11): The relation between the frame number and the correlation of the stego images for the second dataset.

Comparing the results (PSNR) of the two datasets due to embedding in red, green and blue channel, we conclude that the quality of the stego images after data embedding depends on the nature of the dataset.

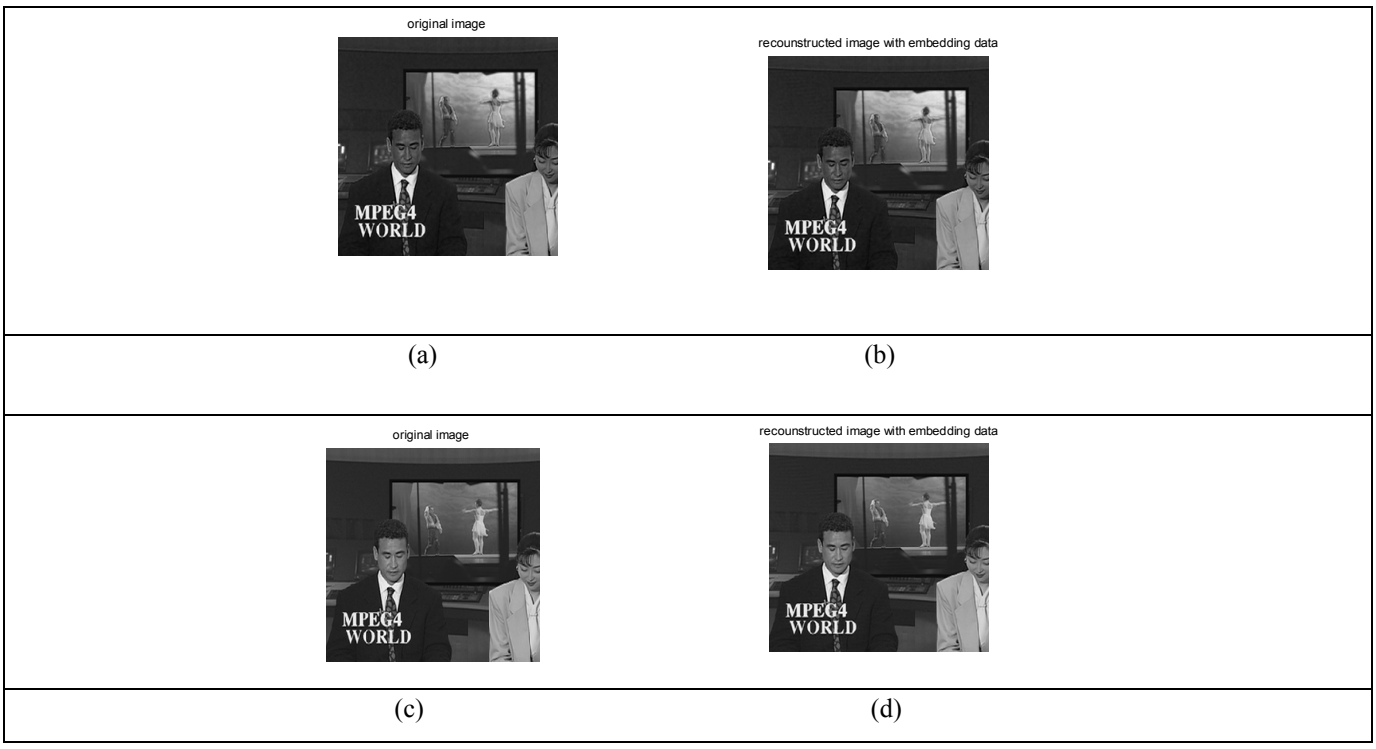


Figure (12): Illustrates a frame from the second dataset, (a) shows the original frame (blue channel), (b) shows the stego image (blue channel), (c)shows the original frame (green channel), (d) shows the stego image (green channel).

8. Conclusion

In this paper, we present a proposed Video Steganography using Least Significant Bit in Frequency Domain. It was applied to two datasets to study the effect of selecting red, green and blue band on the quality of stego images. From the results we found, the quality of the stego images after data embedding into red channel, green channel and blue channel depends on the nature of the dataset (the intensity values of pixels in the RGB frames).

References

1. Gunjan Chugh," Image Steganography Techniques: A Review Article",Acta Technica Corviniensis – Bulletin Of Engineering,Issn 2067-3809, 2013.
2. Suman Chakraborty And Prof. Samir Kumar Bandyopadhyay," Two Stages Data-Image Steganography Using DNA Sequence", International Journal Of Engineering Research And Development E-Issn : 2278-067x, P-Issn : 2278-800x, Volume 2, Issue 7, Pp. 69-72 69, August 2012.
3. Abhishek Mangudkar, Prachi Kshirsagar, Vidya Kawatikwar And Umesh Jadhav," Data Hiding Technique Using Steganography And Dynamic Video Generation**",** International Journal Of Scientific & Engineering Research, Volume 3, Issue 6, Issn 2229-5518, June 2012.
4. Shivani Khosla and Paramjeet Kaur," Secure Data Hiding Technique Using Video Steganography and Watermarking", International Journal of Computer Applications (0975 – 8887) Volume 95– No.20, June 2014.
5. Vanitha T , Anjalin D Souza , Rashmi B and Sweeta DSouza," A Review on Steganography – Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 5, October 2014.
6. G.R.Manjula and Ajit Danti," A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography In Spatial Domain", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015.
7. Zaidoon Kh. Al-Ani, A.A.Zaidan, B.B.Zaidan And Hamdan.O.Alanazi," Overview: Main Fundamentals For Steganography", Journal Of Computing, Volume 2, Issue 3,Issn 2151-9617, March 2010.
8. Jes´Us D´Iaz Vico," Steganography And Steganlaysis: Data Hiding In Vorbis Audio Streams", September 2010.
9. Jonathan Cummins, Patrick Diskin, Samuel Lau And Robert Parlett,"Steganography And Digital Watermarking",2004.
10. T. Morkel , J.H.P. Eloff And M.S. Olivier ," An Overview Of Image Steganography", In Proceedings Of The Fifth Annual Information Security South Africa Conference, June/July 2005.
11. Bret Dunbar," A Detailed Look At Steganographic Techniques And Their Use In An Open-Systems Environment", Sans Institute 2002.
12. M. Sitaram Prasad , S. Naganjaneyulu , Ch. Gopi Krishna And C. Nagaraju," A Novel Information Hiding Technique For Security By Using Image Steganography", Journal Of Theoretical And Applied Information Technology,2009**.**
13. Preeti Singh And Charu Pujara," Comparative Study Of Various Techniques Employ In Image Steganography", International Journal Of Engineering And Advanced Technology (Ijeat), Issn: 2249 – 8958, Volume-1, Issue-5,June 2012.
14. Samir K Bandyopadhyay, Debnath Bhattacharyy,Debashis Ganguly, Swarnendu Mukherjee And Poulami Das," A Tutorial Review On Steganography",2008.
15. A. Swathi and Dr. S.A.K Jilani," Video Steganography by LSB Substitution Using Different Polynomial Equations", International Journal Of Computational Engineering Research (ijceronline.com) ,Vol. 2 ,Issue. 5,2012.
16. Poonam V Bodhak and Baisa L Gunjal," Improved Protection In Video Steganography Using DCT & LSB", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.
17. Prof. Dr. P. R. Deshmukh and Bhagyashri Rahangdale," Hash Based Least Significant Bit Technique For Video Steganography", Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 4, Issue 1(Version 3), January 2014.
18. Dr.ManishShrivastava, Richa Ranjanand and SushmitaKumari," Video Steganography Using Pixel Intensity Value and LSB Technique", International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, Volume: 3, Issue: 2, February 2015.
19. Koumal Kaushik and Suman," An Innovative Approach for Video Steganography", I.J. Computer Network and Information Security, 2015.