Video Steganography using LSB Scheme for Secure and Efficient Data Transmission

C. N. Sujatha, Y V Raghava Rao

Abstract— Digital communication provides more pros over analog communication like better quality, high fidelity, ease of editing, compression and so on. But with speedy growth of internet and advanced computer network, some issues are raised like data security, privacy, and multi-media authentication. Nowadays data is communicated through digital channel, where the fortification of data is main concern for any business association. This paper presents a easy way of securing text in multimedia. Digital steganography in an advanced way is planned to conceal the data which can't be detected easily. Steganography envelopes the message to such a degree that it is indistinguishable to viewer. This paper focused on increasing the concealed data security with video steganography. In this method confidential data is first inserted in host media and the resultant stego-media is again embedded into other host media of a video file and at last the confidential message is retrieved from the stego video. Proposed method provides a computation in terms minimum mean square error (MSE) and more peak signal to noise ratio (PSNR) measure between original host media and generated stego media of dual stenography. The proposed scheme elucidates the prominent imperceptibility of the stego video and the hiding capacity.

Keywords—Steganography, Cryptography, LSB, DWT, MSE, PSNR, SF

1. INTRODUCTION

In the dynamic growth of the network usage communication, one important factor is information security. Cryptography was meant for maintaining the secrecy of communication for security purpose. Many different cryptographic schemes have been evolved to encrypt and decrypt the message in order to keep the data secret [1], [2]. But woefully sometimes it is not adequate to keep the message content secret, it is also imperative to maintain the secrecy of existence of the message. Thus the need of steganography technique is arise to implement this. The art of invisible communication is nothing but Stegnography which is defined as "covered writing". This is accomplished through placing the information in another information. In image steganography, the message is implanted effectively in images [3], [4].

The features of human visual system and the redundant data of digital multi-media make it practicable to insert confidential data or messages. Unrevealed message can be communicated through various digital multi-media such as image, video and audio with steganographic technology. Different schemes used to insert information in digital carriers are well-known steganography methods. Steganography is the process of hiding data with an assurance of an unauthorized person not to identify the existence of information, where as in cryptography the hidden information is known to the public but it cannot be understand by unauthorized people except the authorized one [5]. The main objective of steganography is to make the viewers unable to detect the hidden messages compared to cryptography, where encrypted message will evoke the intuition and hence the hackers will always try to break this encrypted message. Steganography can be applied to different types of media including text, audio, image and video etc.

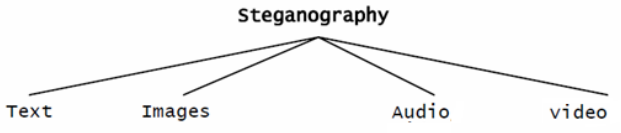

Fig. .1 Various Stegnographic media

Out of these media as shown in Fig. 1, text stenography is examined to be the more difficult due to the lack of redundancy in text compared to video, image or audio but has small memory occupation and simple communication. The method that could be used for text steganography is data compression. Data compression encodes information in one representation into another representation. Image steganography conceals the secret image in host multimedia [8]. Confidential text is embedded in color image instead of inserting in grayscale image, because color image provides more space to hide the secret information. Thus color image steganography became more popular than gray scale image steganogray as color image steganography will not cause any major color changes. Since few decades, various steganographic schemes were suggested for images, still Least Significant Bit (LSB) is the well known hiding method to insert the secret data directly in least significant bits of every pixel of an image [6], [7] and [9]. If video is chosen as media for hiding the secret information, then any of transform techniques such as Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) or Discrete Fourier Transform (DFT) are used for selecting embedding location [10], [11]. These steganographic schemes reduce the chance

Revised Version Manuscript Received on March 08, 2019.

C. N. Sujatha, Department of ECE, Sreenidhi institute of Science and Technology, Hyderabad, Telangana, India. (E-Mail: cnsujatha@sreenidhi.edu.in)

Y V Raghava Rao, Department of CSE, KL University, Vijayawada, Andhra Pradesh, India.(E-Mail: venkataraghav@kluniversity.in)

of infringement by intruders by making the hidden message imperceptible to them. To get more invisibility spatial domain schemes are combined with transform domain schemes to introduce hybrid steganographic system.

In this paper, text message is implanted in a color image with LSB scheme and it is further inserted in color video frames using transform domain method. This paper emphasizes the results of PSNR against each video frame. Results show the imperceptibility of this algorithm without any visual strangeness.

II. PROPOSED SCHEME

A. Data embedding scheme

Proposed method has two categories like image and video steganography. This method first embeds the secrete text message in a color image spatially using the following steps

- Read the color host image
- Isolate the R, G, B planes from host image
- Chose the text message
- Convert the text message into binary form of 8 bits
- Binary data is divided into two halves
- Lower 4 bits of binary data is inserted into R plane of host image
- Lower 4 bits of binary data is placed into G plane of host image
- Finally modified R and G planes are combined with B plane to get stego image
- PSNR is measured to prove the imperceptibility

The resultant stego image after inserting the binary form of text in color image is again implanted in video by following the subsequent steps

- Read the color video
- Segregate the video into frames
- Convert frame to YUV color model
- Transform the Y component into coefficient subbands (LL, LH, HL & HH) using DWT
- Horizontal, Vertical and Diagonal coefficient subbands (LH, HL & HH) are embedded with R, G, B bands of stego image at a selective scaling factor
- Inverse DWT is applied on modified subbands and LL band to obtain modified Y component
- Modified Y component is combined with UV component to form stego frame
- These steps are repeated for all frames in video
- Stego video is constructed from all implanted frames
- PSNR is computed to measure the imperceptibility video stream

B. Data retrieval scheme

From stego video, hidden color image is retrieved first and then the text message is retrieved from the stego color image by following the inverse steps of embedding process

- Read the stego color video
- Separate the frames from video
- Convert frame into YUV color space
- Use DWT on Y component to acquire frequency subbands
- R, G, B planes are withdrew from LH, HL and HH bands
- R, G, B planes are concatenated to form stego color image
- similarity factor is calculated between extracted stego image and inserted stego image
- Pixels in R and G planes are converted binary form
- Lower bits are taken from R and G planes
- Segregated bits are converted into decimal form and into character to obtain the inserted message at the receiver end

III. SIMULATION RESULTS

The proposed algorithm is executed using MATLAB simulation tool. Text message of 39 characters has taken as an input to insert into a color image. Using LSB scheme binary bits of text message are embedded into selected color bands of an image of size 64 x64. Host image and Stego image are displayed in Fig. 2 and Fig.3. The resultant stego image is again inserted into a color video of avi format which are shown in Fig. 4 and 5. Embedding in video has done at a scaling factor of on 0.01, which is selected on trial and error basis to compromise the quality and embedding capacity. Extracted stego image from embedded video is shown in Fig. 6. The algorithm is tested by placing different images of various formats in video without distorting the visual superiority of stego-image. To maintain the quality of video, Discrete wavelet transform is employed to embed the stego image in video. Results are observed by executing the algorithm while embedding various images in different videos of 20, 40, 120 frames.

Embedding text taken is:

"ThisisStegnographicTechniquetohidedata"

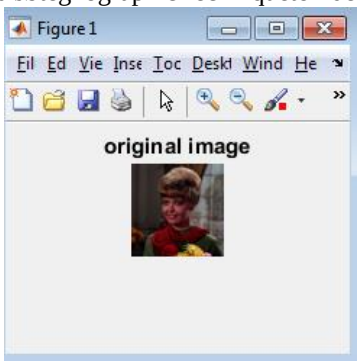

Fig. 2. Original color image

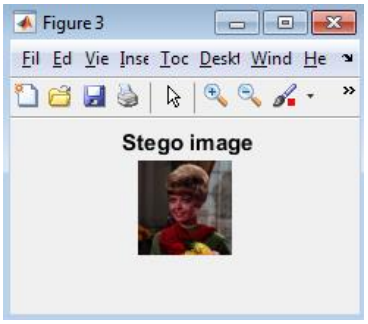

Fig. 3. Stego color image with text implantaion

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

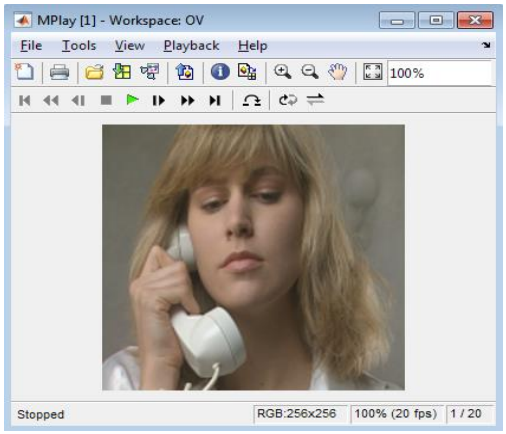

Fig. 4. Host color video

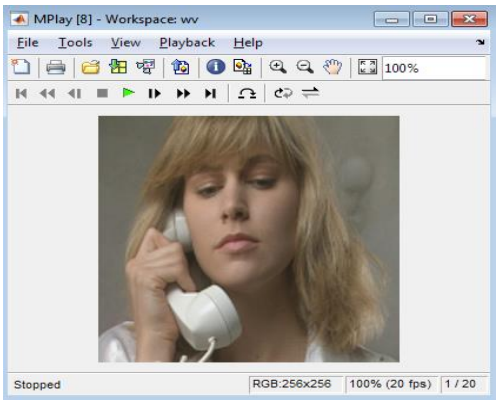

Fig. 5. Stego color video embedded with stego color image

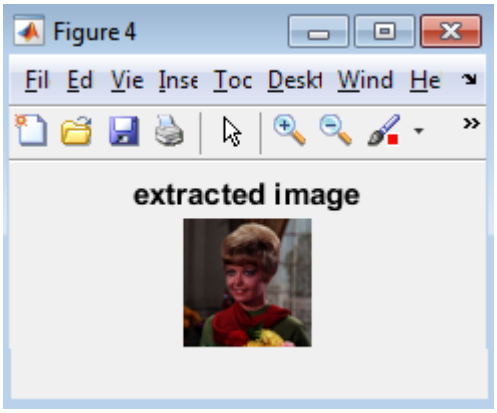

Fig. 6. Extracted image from color stego video

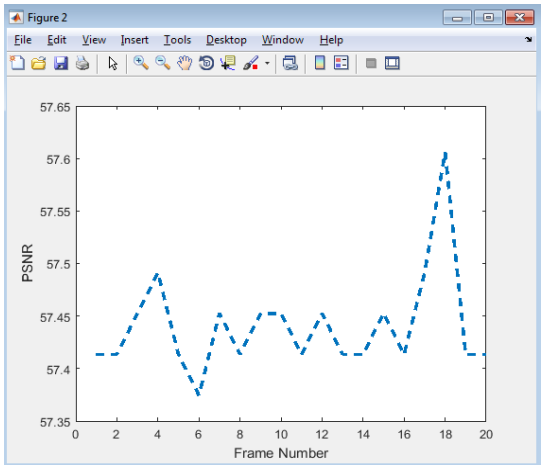

Fig. 7. Plot of PSNR against frames of video

. Similarity factor (SF) is computed to measure the correlation between inserted and extracted images. MSE and PSNR are calculated to estimate the invisibility of stego multimedia. The measured PSNR against each video frame is plotted as displayed in Fig. 7, which defines the impact of embedding in each frame. Based on the insertion of color information of stego image in each frame, PSNR value varies Table I evinces the MSE and PSNR values of stego image and SF values to relate the embedded and extracted stego color image. From the Table I, it has been detected that the algorithm performs well on Jpeg images compared to other formats and least effective for Bitmap images among other images. Similarity factors measured are almost unity that says retrieved image is very close to embedded image.

Embedding capacity of the algorithm increases using color image as it provides space in three planes to insert the bits with no visual distortion. Due to the usage of DWT, lossless retrieval of data at the receiver is possible that was measured as SF. The proposed algorithm works well for all image formats except for GIF format.

TABLE I. MSE, PSNR and SF values for images of different formats

Format of an image	MSE	PSNR	SF
JPG	0.09	58.75	1.00
BMP	0.17	55.73	0.99
TIFF	0.11	57.65	1.00
PNG	0.13	55.77	0.99

Extracted text is:

"ThisisStegnographicTechniquetohidedata"

The extracted message from stego color image is same as inserted text message of size 39 characters. Though the stego image is embedded in transform coefficients of video frames using DWT, the algorithm proved its efficiency by retrieving the text message without any misconception. From the simulations, it is also seen that the higher values of scaling factor causes visual distortions in stego video that makes inefficient retrieval of hidden data. Thus the optimization of scaling factor is important at the time of data embedding.

IV. CONCLUSION

This paper presents a combination work of spatial and transform domain approaches for information security, like image and video steganography. However both the techniques are developed to provide security for hidden information. Therefore to improve the information security for the communication over the unsecured channel, an advanced technique is needed. Simulated results show that the average PSNR measured is all the time greater than 55 dB for different image formats. Thus the experimental results demonstrate that the proposed methodology is effective in achieving invisibility. The perceptual quality of the video is maintained and the difference between the cover data and stego-data can

be not be identified by the human visual system. Present work can be further extended by combining the concepts of spatial and different transform domain techniques to get hybrid steganography for additional improvement of protection to the secrete data.

REFERENCES

1. Sumeet Kaur, Savina Bansal, and R. K. Bansal., "Stengography and Classification of Image Stegnography Techniques". International Conference on Computing for Sustainable Global Development.978-93-80544-12-0/14, IEEE, 2014.
2. M. A. F. Al-Husainy, "A novel encryption method for image security", International Journal of Security and Its Applications, Vol. 6, No. 1, pp. 1-8, 2012.
3. R. Radhakrishnan, M. Kharrazi, and N. Memon, "Data masking: a new approach for steganography" Journal of VLSI Signal Processing, vol. 41, no. 3, pp. 293–303, 2005.
4. S. Jindal and N. Kaur, "Digital image steganography survey and analysis of current methods," International Journal of Computer Science and Information Technology & Security, vol. 6, 2016.
5. Z. Li, X. Chen, X. Pan, and X. Zeng, "Lossless data hiding scheme based on adjacent pixel difference," in Proceedings of the International Conference on Computer Engineering and Technology (ICCET '09), pp. 588–592, January 2009.
6. Anand J V and Dharaneetharan G D, "New approach in steganography by integrating different LSB algorithms and applying randomization concept to enhance security", Proceedings of the In: International Conference on Communication, Computing, pp. 474–476, 2011.
7. Fridrich J, Goljan M and Du R, "Detecting LSB steganography in colour and gray-scale images", IEEE Trans. Multimed, Vol. 8, no.4, pp. 22–28, 2001.
8. Li B, He J, Huang J and Shi Y Q, "A Survey on Image Steganography and Steganalysis", J. Inf. Hiding Multimed. Signal Process, Vol. 2, no.2, pp.142–172, 2011 .
9. Jain M and Lenka S K, "A review of digital image steganography using LSB and LSB array" Int. J. Appl. Eng. Res. Vol. 11, no.3, pp.1820–1824, 2016.
10. Ramadhan J. Mstafa and Khaled M. Elleithy., "A high payload video stenography algorithm in DWT domain based on BCH codes(15,11)", Wireless Telecommunication Symposium (WTS), 978-1-4799-6776-6/15, IEEE, 2015.
11. Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb "A secure covert communication model based on video stenography", 11331. 978-1-4244-2677-5 IEEE, 2008.