Secure Communication through Data Hiding based on Video Steganography

Dr. R. Umadevi[1],
[1]Assistant Professor & Head,
Department of Computer Science and Application,
Vivekanandha College for Women, Unjanai, Namakkal,
Tamilnadu, India,
mail2deviuma@gmail.com

Abstract

In the rapid sharing system there are many kind of inputs like text, image, audio or video, but the user's needs are mainly focused on secure communication over the internet and intranet. We well thought-out for this kind of problem and this research are conceded for improving the security sharing. I proposed the system called Unified Mesh Steganography (UMS) technique. In this techniques some modern fashion used for implementation and the experimental evaluations are made using MATLAB. The technique attains some parameters like Embedding Capacity Level (ECL) and Transmission Ratio Level (TRL).

Index terms *– Secure Communication, Steganography, Transmission, Embedding capacity, Video.*

1. Introduction

The network has various methods for sending and receiving information from one place to another place and one network to another network. But it needs some basic deliberation like security with tolerable data transmission. Mainly, in our method focuses security and capacity of data while embedding data.

2. Literature Survey

In [1], the network based steganography has implemented. In [2] edge detection technique in addition to LSB substitution resulted in the improvement of stego object quality. Though LSB substitution is considered as the most popular method,

the range of embedding load in the cover image is partial broadly by pseudorandom number generator. In [3] an edge adaptive method is obtainable that useful the embedding portion on the basis of size of secret message and the cover image. The edge adaptive method though proved to be efficient, it did not considered the adjacent pixel values. In [4], the Secure Irreversible Rapid Fourier Transform used for secure communication and video files are taken for the experimental evaluation. But in this paper only concentrating the video files for achieve the better secret communication.. In [5], the hash polynomial function based steganography has been developed to tighten the multilayer security. In [6], the embedding capacity is determined by two factors, the embedding level and the peak points. In [7], The maximum number of pure embeddable pixels after excluding the bits that are used to embed the side information can be calculated

3. Proposed method

In this paper, the number of node connected for communication should be identified. The particular networking system may be connected to ready for communication. This implemented for small size of the network. Network has more security but using our proposed UMS method the result is better. The following algorithm is proposed for the method Unified Mess Steganography. Network steganography has some factors to be concealed for communication with fastness. By provide the secret key the system has achieves good results.

Algorithm:

Begin
Select the required nodes
Allocate the nodes i<=n
Connect the nodes
Choose the first node (default)
Embedding side:
For every transmission
Get original data
Select the pixel in selective frame
Make Embedding form with key
Extracting with key to destination node
End for
Extracting side:
For every transmission
Get covered data
Make extracting with key
Store the original data for processing
End for
End

Algorithm For Embed and Extract

The simple algorithm clearly explains the process of the UMS method. It is compared with High payload Steganography (HPS) and LSB matching revisited method, our method gradually achieves the better results.

4. Experimental results

A) Embedding Capacity Level (ECL)

The ECL factor calculated with size of the data (SD) and Time Taken for Embedding. ECL measured in terms of percentage (%).

$$ECL = \frac{SD}{TTE} * 100 \quad (1)$$

Table 1. Embedding Capacity Level (ECL)

Size of data (MB)	Embedding Capacity Level (%)		
	UMS	HPS	LSB -MR
1.0	2.8	2.0	1.9
1.5	2.7	2.2	2.4
2.0	3.0	2.6	2.2
2.5	3.2	3.0	2.6

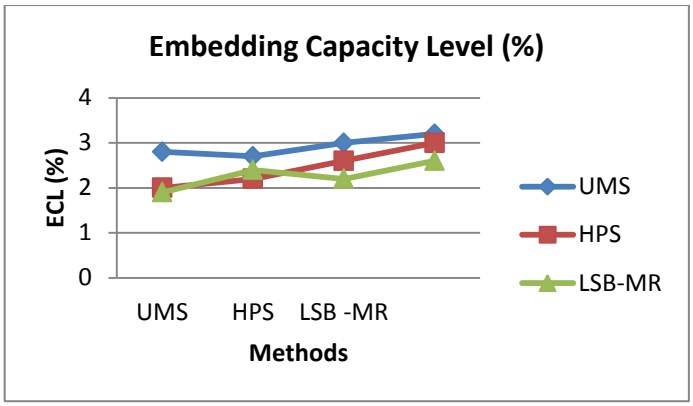

Figure 1. Data embedding capacity level

Figure 1 clearly illustrates the performance of capacity of embedding level with the data size of MB inside the video files using data hiding method is increasing.

B) Transmission Ratio Level (TRL)

After embedding process, the file can be transmitted to required node. This can be measured by time taken for transmission data size in MB and extraction time to be considered. The following formula is used to calculate the TRL in terms of milliseconds.

$$TRL = \forall TT / \sum \exists N \qquad (2)$$

Here TT for Transmission Time and N for Node, for all transmission time is taken for all the nodes.

Table 2. Transmission Ratio Level (TRL)

Size of data (MB)	Transmission Ratio Level (ms)		
	UMS	HPS	LSB -MR
1.0	20.5	36	35.4
1.5	24.3	30.5	40.5
2.0	28	44	51.2
2.5	33	49.5	53.5

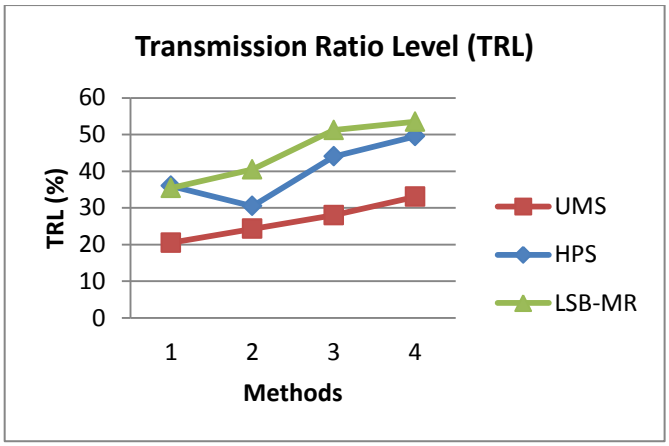

Figure.2.Data Transmission Level

5. Conclusion

This paper concluded with ECL and TRL values compared with previous work, our method shows the better results based on the network inference. The experimental results are done using MAT Lab simulator. In future the work carried out towards the increasing size of the data with similar factor to achieve speedy process.

6. Reference

[1]. Yu et al, "Digital Watermarking Based on Neural Networks for Color Images", Elsevier Signal Processing, 81 (2001), p.p. 663-671.

[2]. Wen-Jan Chen, Chin-Chen Chang, T. Hoang Ngan Le," High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications, Elsevier, Mar 2010.

[3]. Weiqi Luo, Fangjun Huang, Member, and Jiwu Huang," Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions On Information Forensics And Security, vol. 5, no. 2, June 2010.

[4] R.Umadevi, G.M.Nasira, "Secure Irreversible Rapid Fourier Transform For Secure Communication In Video Steganography, International Journal of Computational Intelligence and Informatics Vol. 5: No. 1, June 2015.

[5] R.Umadevi, G.M.Nasira, "Video Steganography Based on Hash Polynomial Function for Secure Communication", Indian Journal of Science and Technology, Vol.8 (23), September 2015.

[6] Zhe-Ming Lu, Shi-Ze Guo," Lossless Information Hiding in Images on the Spatial Domain" in Lossless Information Hiding in Images, 2017.

[7] Hiba Abdel-Nabi, Ali Al-Haj, "Frequency domain based data hiding for encrypted medical images" in Intelligent Data Security Solutions for e-Health Applications, 2020.