Design and Simulate Secure Video based Steganography Algorithm with Less Time Complexity

Student's Name	**N. M. Sandeep**	**RTES (FT-2014)**
Academic Supervisors	Subarna Chatterjee	
Industrial Supervisor(s)		

N. M. Sandeep
Sandeep4challa@gmail.com
Ph. No: 0 99865 96660

Keywords: 0

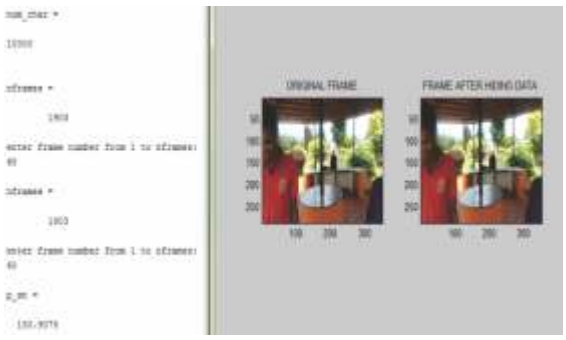
Abstract:

Steganography comes from a Greek word steganos which means covered or secret and graphy means writing or drawing. In this method the medium such as audio, text, image or video is used to hide the data without causing any variations in the medium. The increased utilization of digital communication leads to data piracy or modification. During the communication, data which is sent by the transmitter may be taken by the unauthorized person before reaching the receiver which leads to leakage of secured information.

Thus a technique called steganography is used to hide the secured information within an audio, text, image or video file. In this Dissertation, a video is taken and the data is hidden in the frames of the video that is the offline mode detection. The information which the Transmitter is sending should reach the Receiver without being stolen, removed or modified from the network. Security of the information is achieved by using Steganography.

The methods used in this system is encrypting the text using simple xor key and then hiding the encrypted text using simple LSB method in multiple frames in a video. The simulation is performed in the offline mode in the MATLAB video and the working of the system is tested. The developed system is able to encrypt, hide, extract and decrypt the data. The encrypt and hide is called encoding of data and the extract and decrypt is called decoding. In Hiding large amount of data in a single frame leads to more distortion in the frame. So here the multiple numbers of frames are used to hide the data. In this way the high PSNR is achieved.

PSNR and visual view of the frame after hiding 10000 characters in Video using existing methodology



PSNR and visual view of the frame after hiding 10000 characters in video using porposed methodology

Conclusion: Without sending the encryption key separately, the encryption key can also be hidden in the carrier file with data and then the key matching will be used to decrypt the extracted data. If the wrong key is given by the user then the user is not allowed to decrypt the data.