Final Project Report

On

**A Novel Video Steganography Scheme using Network Coding**

**CS F401: Course Project**



**BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI (Rajasthan)**

**Hyderabad Campus**

**(Sept 2016)**

Sai Prathik S.B. 2013A7TS044H

Sagar Gupta 2014A7PS030H

Shiva Raj K 2013A7PS064H

A Novel Video Steganography Scheme using Network Coding

**Project Area:** Multimedia, Security

**Abstract:** Multimedia communication plays an important and ubiquitous role in today’s computing. In an age where cyber privacy has not yet been fully declared the right of every person on the net, the race to invent novel methods to keep one’s private data from prying eyes is always on. Steganography is one such broad topic that contains a class of such methods. Steganography is basically the art of concealing a file, message, image or video within another file, message, image or video. This project deals with coming up with a technique to use Videos as carrier message, hence Video Steganography. Over the course of the semester we have identified reasons why network coding can be used to provide inter-frame redundancy but cannot be used as an alternative to error correcting codes to provide intra-frame redundancy. We have also identified possible avenues of future experiments based on inter-frame redundancy and error correcting code performance comparison.

**Introduction**

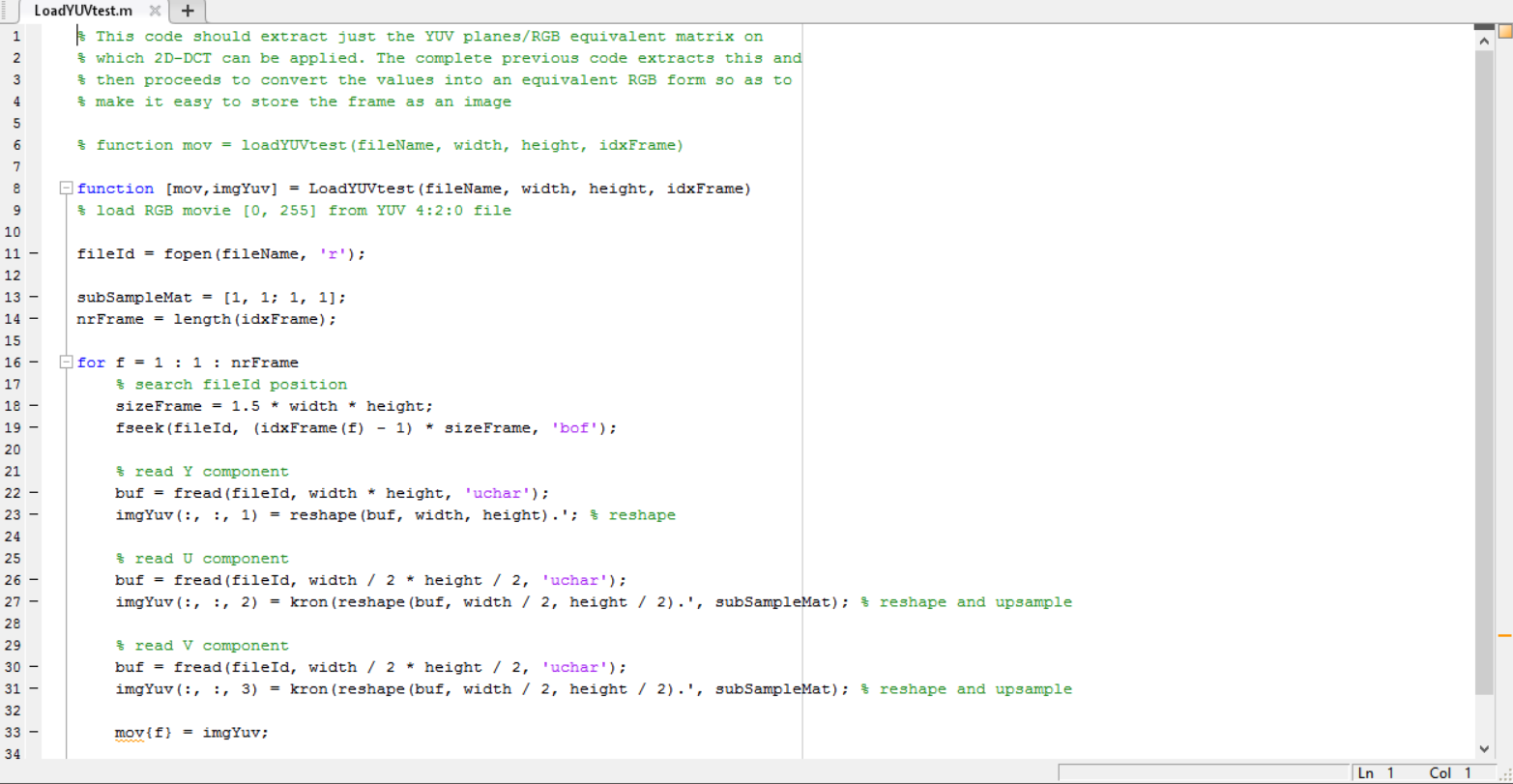
Scope and Objective

The sizes of videos make them an ideal carrier for data in steganography. The challenge lies in hiding the data without raising suspicion about the integrity of the video. The aim of steganography is to make sure any person who is not the intended receiver, is not alerted about the presence of data hidden within the carrier file, simply by possessing the file. To achieve the above, a novel method will be designed and tested over the course of this project, which would include but would not be limited to the following topics:

* DCT based Image Compression
* Network Coding

**Discrete Cosine Transform**

DCT based Image Compression has been around for a long time, Since videos are essentially a collection of multiple frames, embedding data in the compression stage of the frame keeps the data from being corrupted unlike spatial embedding before compression. It is also statistically harder to detect transform domain modification of images. The code basically reads in the YUV-CIF file and extracts the Y,U & V components as separate domains, giving us 3D an array with 3 2-D arrays. On each of the 2D arrays, the DCT operation can be applied, giving us the resulting transformed values.



**Network Coding**

Network Coding is a technique that was invented to improve a network’s throughput, efficiency and scalability. It also provides resilience to attacks and eavesdropping, the latter is of importance to us. How network coding works is, a linear combination of N is used to produce a new message. To keep the block size of the messages constant while applying the previous operations, a special set called a Galois Field with its own set of operations defined are used as the universe for the coefficients. The coefficients, along with the combination of messages are transmitted. Since this is essentially a system of linear equations with N variables. N such unique combined messages are required to be able to extract all the messages successfully. Assuming the block size to be 8 bits, effectively to transmit 1 byte of data, the overhead bytes (for coefficients) to be spent is

(Number of coefficients per equation) \* (Number of equations) / (Number of messages) = N\*N/N = N

N bytes and one of our aims is to embed as much data as possible, we have chosen the coefficients using a pseudo-random stream of numbers in the Galois field, hence alleviating the need to send the coefficients sacrificing embedding capacity. One of the main issues with why Network Coding cannot be used to provide intra-frame redundancy is that the error correcting mechanisms in Network Coding are based on the structure of the network. For our case, the simulated network would be a simple one with one source and one sink. The most optimal solution in this case, even in network coding is to use error correcting codes.

The second challenge is that the embedding of the data occurs in the post quantization stage of compression, before application of Inverse-DCT. While applying DCT during extraction stage, the rounding off of the coefficients will cause the embedded values to vary by +-1. This will cause our coefficients to be modified, modifying the solution set, changing the embedded values. There is no fixed procedure to identify the correct solution set out of the possible many.

Implementation

Raw, unformatted videos in the YUV 4:2:0 format have been downloaded from online databases, which serve as standard in most video-steganography based research (<https://media.xiph.org/video/derf/>). Transform domain based embedding occurs at the frame level so individual frames are separated and the Y,U and V planes are extracted separately. The data to be embedded is first encoded using an error correcting scheme (BCH (7,4,1)) in this case. To implement the Network coding based encoding, code that implements GF(8) arithmetic has been built and the code extracting the embedded data is also done. In the current implementation, since the main aim of the project has proved to be unattainable, the code implements the logic behind the paper on which the project is based on.

Observations and Results

The embedding algorithm embeds data in the 3 least significant bits of AC coefficients. Embedding data without quantization and in a separate test after post quantization in the Y plane of the frame leads to an avg. PSNR value of 12-13 dB. The embedding capacity of the implemented algorithm conforms to the embedding capacity of the results in the research paper.

Code Repository:https://github.com/sgmonusg/Stegnography

Future Research

The immediate first issue to address is the difference in PSNR values in the Y plane from our experiments and the results reported in the paper. Once that is settled, two separate avenues of research arise from the original aim, the first of which is to provide inter-cover medium redundancy using network coding and the second is a comparison of various error correcting schemes used in the data protection (pre-embedding stage) and the comparison of the use of various degrees of error correcting measures.

References

* <http://www.igi-global.com/dictionary/multimedia-security/19609>
* <https://media.xiph.org/video/derf/>
* <https://en.wikipedia.org/wiki/Steganography>
* <https://en.wikipedia.org/wiki/Linear_network_coding>