Data Compression and Encryption Algorithms for Small Satellite Communications

Spectral Ocean Color Satellite (SPOC) - Undergraduate Student Instrument Project - NASA
Multi-view Onboard Computational Imager Satellite (MOCI Sat) – University Nanosat Program 9 – AFRL

Ethan Barnes, David L. Cotten, Small Satellite Research Laboratory, University of Georgia

Overview

CubeSat are powerful, small form-factor satellites that can perform complex and informative missions in low-earth orbit. Due to the nature of low-earth orbit, opportunities for communication between ground station and these satellites are limited in terms of both time and the amount of data that can be transferred. These constraints force satellite communications to utilize data compression. It is also essential that data is encrypted to prevent malicious individuals from accessing classified data. Both the compression and encryption algorithms chosen must be reasonable for the limited computational and electrical power on the satellite.

Computational Power Constraints

Both the SPOC and MOCI satellite missions will use the Clyde Space Onboard Computational Computer (OBC). This board will be the primary computer for these calculations. The OBC, however, does not have extensive computational power for calculating these complex algorithms. With only 8MB of RAM and 62.5 DMIPS (million instructions per second), comparable to a microprocessor [1]. This only allows for the most efficient algorithms that have a low computational footprint.

Electrical Power Constraints

Both the SPOC and MOCI satellite missions will be powered by onboard electrical power systems (EPS). Each mission will be using around a 40Whr battery as the primary source of power. The Clyde Space OBC will draw 1W or more of power during period of high computational load [1]. It has been concluded that the OBC will experience a “high computational load” when the compression and encryption algorithms are being executed. The entire satellite, however, must be powered via this battery and the OBC cannot drain the entire battery before being recharged via the spacecraft’s solar panels.

Finding the Optimal Data Compression Algorithm

The Small Satellite Research Laboratory has considered a fair number of algorithms and methods for data compression. The SPOC and MOCI satellites will be downlinking scientific data that will be used for research purposes at the University of Georgia. Due to the nature of scientific data, the compressed data may not suffer from any loss. The data compression algorithms that were chosen as candidates must utilize lossless compression. The following compression algorithms were chosen for research: **JPEG2000** - a wavelet based compression developed by the Joint Photographic Experts Committee Group in 2000, **FLIF** - Free Lossless Image Format that utilizes MANIAC based compression, **BZIP2** - a Burrows-Wheeler based compression developed by Julian Seward in 2000, **Sequitur** - a recursive based compression developed by Craig Nevill-Manning and Ian H. Witten in 1997, **SPIHT** - a state-of-the-art compression algorithm developed by SIlicon Imaging.

These algorithms were chosen as candidates for their popularity for modern data compression that utilizes lossless compression. Each algorithm was tested on a Raspberry Pi 2 Model B running Debian/Linux. The Raspberry Pi is a comparable board for computational power to the Clyde Space OBC. Each algorithm was tested against six images. Three of which were simulated test images that will be expected from the MOCI satellite mission (Figures A-C) and the remaining three were images from the Jet Propulsion Laboratory at the California Institute of Technology (Figures D-F), which are larger images that will be similar to what the SPOC mission will be downlinking [2].

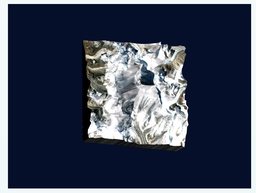

Figure A

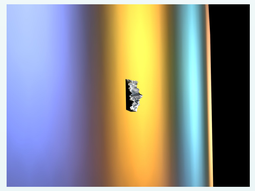

Figure B

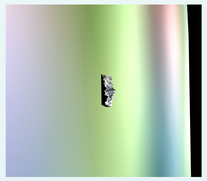

Figure C

Figure D

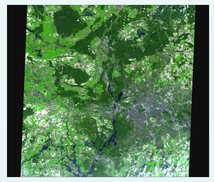

Figure E

Figure F

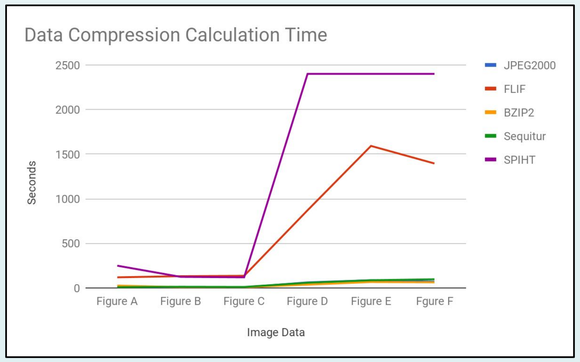

Figure G

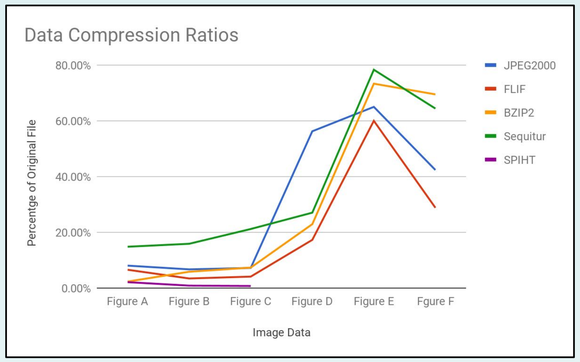

Figure H

Figure G concludes that JPEG2000 achieved one of the fastest calculation times while providing one of the best compression ratios as shown in Figure H. While the FLIF algorithm proved to have a better compression ratio, its calculation time far exceeded the maximum time that is viable for a small satellite. The BZIP2 algorithm also proved to have a faster calculation time, but did not have a superior compression ratio. Future iterations of this research will include the ICER compression algorithm developed by NASA for the Mars Rover Missions as a possible algorithm for SPOC and MOCI.

Finding the Optimal Encryption Algorithm

The data that SPOC and MOCI will downlink is considered to be classified data by NOAA and the U.S. Air Force. It is important that the data is encrypted in order to prevent malicious individuals from accessing data. The following encryption algorithms were considered for this research: Advanced Encryption Standard (AES), Triple DES, and Blowfish. It was determined that AES would be the optimal encryption algorithm for the SPOC and MOCI missions. The conclusion was made from AES’s popularity and low computational footprint. In addition, the AES-256 mode was chosen due to its full complexity and security. When choosing a mode for AES-256, the following modes were considered for this research:

1. Cipher Block Chaining (CBC)
2. Electronic Code Book (ECB)
3. Galois-Counter Mode (GCM)

The Electronic Code Book proved to be ineffective for the SPOC and MOCI missions. This is due to the nature of the algorithm in that it does not perform sufficiently for images with repeating features. While it is not anticipated that the data from SPOC or MOCI will have these identical, repeating features, however the possible security flaw is not an option for classified data. Galois-Counter mode proved to be ineffective for the SPOC and MOCI missions as well. While GCM is a fairly secure and popular mode for AES, if a bit flip occurs during data downlink, which is common for satellite communications, the entire data set is corrupted. Cipher Block Chaining has been chosen for the SPOC and MOCI satellite missions. This conclusion was found primarily from CBC’s ability to segregate data errors to single blocks of data. If any part of the encrypted data is corrupted, only the block of data that the corruption is contained in will be lost, instead of the entire data set being corrupted. The performance of AES-256 using CBC is illustrated in the chart below.

File	Encryption Time	Decryption Time	Original File Size	Encrypted File Size
image_1.jpg	0.08s	0.134s	100KB	100KB
small_2.jpg	0.382s	0.594s	701KB	701KB
med_1.jpg	0.68s	1.205s	1.5MB	1.5MB
med_2.bmp	4.183s	7.503	9.1MB	9.1Mb
large.tif	21.665s	39.816s	48MB	48MB
mesh.ply	3.411s	6.278s	7.4MB	7.4MB

The test data used includes two small images files of 100kb and 701kb in size, two medium images of 1.5mb and 9.1mb in size, one large image of 48mb in size and one .ply file (MOCI’s primary downlink data type).

References

[1] Clyde Space. “On Board Computer Interface Control Document” ICD-25-02555 RevE. 03 Jan. 2018.

[2] NASA/GSFC/METI/ERSDAC/JAROS, and U.S./Japan ASTER Science Team. Jet Propulsion Laboratory.

Center for Undergraduate Research Opportunities
UNIVERSITY OF GEORGIA

For more information about CubeSats, the Small Satellite Research Laboratory (SSRL), our missions, visit www.smallsat.uga.edu.