Encryption and Compression Design of The COMS

Seok-Bae Seo, Durk-Jong Park, Chi-Ho Kang, In-Hoi Ku, and Sang-IL Ahn

Korea Aerospace Research Institute
P.O. Box 113, Yuseong, Daejeon, Korea
sbseo@kari.re.kr

ABSTRACT:
COMS (Communication, Ocean, and Meteorological Satellite) will be launch at end of year 2008. For speedy and security communication of COMS, KARI (Korea Aerospace Research Institute) decided encryption and compression design. Encryption design is based on DES (Data Encryption Standard), so that encryption key generation and management are important issues in COMS operation. And Compression is based on loss and lossless JPEG (Joint Photographic Export Group) standard. JPEG is one of generally using compression algorithm in image.

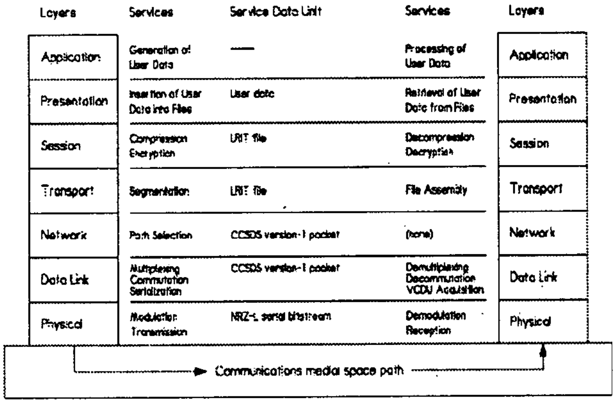
KEY WORDS: COMS, Image Compression, Data Encryption, DES, JPEG, CGMS, HRIT, LRIT

1. Introduction

In order to specify the CGMS (Coordination Group for Meteorological Satellites) LRIT/HRIT format ISO standard 7498 (OSI reference model) is used as a basis [CGMS 1999][ISO 1982]

LRIT/HRIT is mapped onto seven layers, conceptually similar to the OSI reference model. Figure 1 visualizes how the reference model is applied for LRIT/HRIT [JMA 2003a] [JMA 2003a]

There are seven layers specified for the communication process, with increasing level of abstraction, beginning with the physical layer at the bottom of the stack, ending up with the application layer at its top. Below the communication system there is the communications media, which is the space path from the uplink station towards the user station including the transponder functionality of the spacecraft. LRIT/HRIT files are the input for compression and encryption.



Layers	Services	Service Data Unit	Services	Layers
Application	Generation of User Data	——	Processing of User Data	Application
Presentation	Insertion of User Data into Files	User data	Retrieval of User Data from Files	Presentation
Session	Compression Encryption	LRIT file	Decompression Decryption	Session
Transport	Segmentation	LRIT file	File Assembly	Transport
Network	Path Selection	CCSDS version-1 packet	(none)	Network
Data Link	Multiplexing Commutation Serialization	CCSDS version-1 packet	Demultiplexing Decommutation VCDU Acquisition	Data Link
Physical	Modulation Transmission	NRZ-L serial bitstream	Demodulation Reception	Physical

Fig. 1 OSI reference model for CGMS LRIT/HRIT

The session layer describes how an LRIT/HRIT file (the session SDU) is send from the one system to the other system, without uncovering the transport mechanism. For LRIT/HRIT dissemination, there are two pairs of complementary services to be performed:

- Compression and decompression of data, if required
- Encryption and decryption of data, if required

In addition a mission specific data sequencing on 'LRIT/HRIT file level' could be applied as an alternative to the priority scheme used in the transport layer to cope with stringent data specific timeliness requirements.

From the session layer point of view, the underlying communication can be described as the transportation of an LRIT/HRIT file (prepared for shipping) from one transport layer to other transport layer.

2. COMS Compression Design

Compression is required to maximize the data available in the channel and encryption.

The ISO standard 10918 'Digital compression and coding of continuous-tone still images' known a Lossy/Lossless JPEG is chosen as the compression baseline for COMS compression. Compression type- lossy or lossless compression- is determined by schedule and kept stable on single COMS LRIT/HRIT file [ISO 1983].

COMS LRIT/HRIT files are composed by some kind of header and data that recommended by CGMS specifications. All of COMS LRIT/HRIT files must have primary header that is the first and mandatory header. Second header is Image structure header, that is not mandatory but all of image data have it. Compression flag is in Second positioned header of image data. The compression flag of the image structure header is set 0, 1, or 2. Compression flag = 0 notifies data are non-compressed, 1 is lossless compressed, and 2 is lossy compressed. Image structure header has bit per pixel information and Image size except for the compression flag. Table shows structures of image structure header of COMS LRIT/HRIT.

Table 1. Image structure header of COMS LRIT/HRIT

Image Structure Record

Header_Type

::= unsigned integer (1byte), fixed value, set to 1

Header_Record_Length

::= unsigned integer (2bytes), fixed value, set to 9

NB unsigned integer (1byte) number of bits per pixel

NC unsigned integer (2bytes) number of columns

NL unsigned integer (2bytes) number of lines

Compression_Flag

::= unsigned integer (1byte), compression method

0 : no compression

1 : lossless compression

2 : lossy compressionHeader_Type

Detailed compression and decompression algorithm is omitted because of compression algorithm is based on the ISO standard 10918.

3. COMS Encryption Design

3.1 Encryption Principal

The encryption algorithm will only operate on the data fields of LRIT/HRIT files and leave all header records unmodified. The encryption principle is based on the substitution and transposition for the clear data.

If encryption is applied to the LRIT/HRIT data field, a key header (header type #7) will be part of the header records preceding the data field. The keys will be distributed separately via the file type #3 (encryption key message).

The encryption and decryption are based on a processing in accordance with the Electronic Code Book (ECB) mode of Data Encryption Standard (DES). This mode avoids error propagation in an error prone communication system [DoC 1993][Doc 1980]. Figure 2 shows the principle of encryption and decryption.

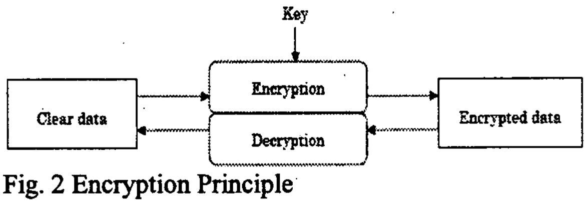


Fig. 2 Encryption Principle

3.2 DES

DES specifies a FIPS (Federal Information Processing Standards) approved cryptographic algorithm as required by FIPS 140-1. This publication provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

The algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64-bit key. Here, Blocks are composed of bits numbered from left to right, i.e., the left most bit of a block is bit one.

Deciphering must be accomplished by using the same key as for enciphering, but with the schedule of addressing the key bits altered so that the deciphering process is the reverse of the enciphering process. A block to be enciphered is subjected to IP (Initial Permutation), then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation IP-1. The key-dependent computation can be simply defined in terms of a function f, called the cipher function, and a function KS, called the key schedule. A description of the computation is given first, along with details as to how the algorithm is used for encipherment. Next, the use of the algorithm for decipherment is described. Finally, a definition of the cipher function f is given in terms of primitive functions which are called the selection functions Si and the permutation function P. Si, P and KS of the algorithm are contained in the reference document [DoC 1993].

The following notation is convenient: Given two blocks L and R of bits, LR denotes the block consisting of the bits of L followed by the bits of R. Since concatenation is associative, B1B2...B8, for example, denotes the block consisting of the bits of B1 followed by the bits of B2...followed by the bits of B8.

3.3 Record Type vs. File Type

A COMS LRIT/HRIT file consists of one or more header records and one data field. In the header records information describing the contents of the data field is provided. Some of header may occur several times with one file. The first header record (which is the only one being mandatory) must be of type 0 identifying it as the so called primary header record.

The global mandatory/optional use of headers is specified in the reference documents [CGMS 1999], [JMA 2003a], and [JMA 2003b]. Table 2 defines the COMS LRIT/HRIT mission specific use of header record types within certain LRIT/HRIT file types. 'KMA mandatory use' means that the identified header record will always be used in the COMS LRIT/HRIT dissemination. 'KMA optional use' means that only creation COMS LRIT/HRIT files contain such header record.

In Table2, we known that encryption key message has three mandatory headers. And that because of file type 0 and file type 2 have header record 7 (Encryption Key Header), image data file (type 0) and alpha-numeric text file (type 7) are can compress only.

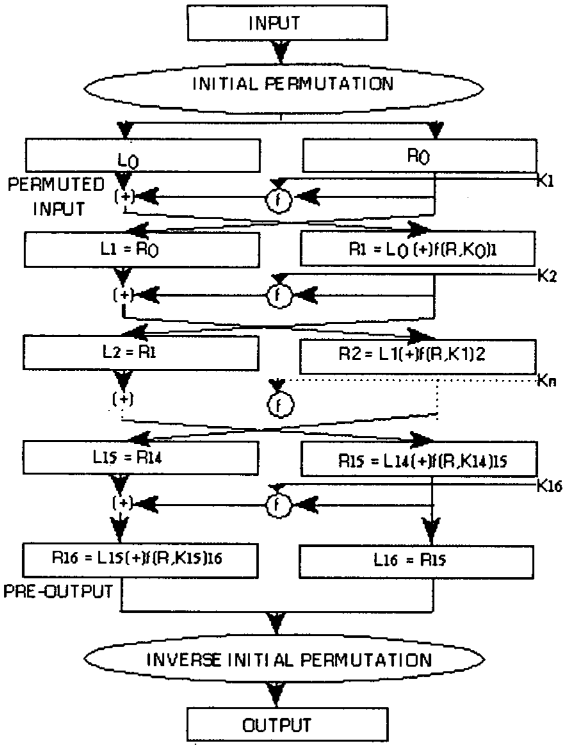


Fig. 3 Enciphering computation.

Table 2. Use of Header Records vs. File Type

file types	header record types									
	0	1	2	3	4	5	6	7	128	129
0: image data file	●	●	◎	◎	◎	◎		○	◎	
1: GTS message										
2: alpha-numeric text file	●				◎	◎		○		
3: encryption key message	●				◎	◎				◎
128 : NWP data	●				◎					
129 : Binary data	●				◎					

● as requested by CGMS ◎ KMA mandatory use ○ KMA optional use

0 primary header
1 image structure
2 image navigation
3 image data function
4 annotation

5 time stamp
6 ancillary text
7 key header
128 image segment identification
129 Encryption Key message header

3.4 Key Representation

The DES key consists of 64 bits, 56 of which are used as a decode/encode key and 8 of which are parity bits to detect errors in the key. The DES key numbering convention shown in Figure 4 conforms with the reference document [DoC 1993]. The 64 bits per a DES key are numbered from left to right. Bits (8, 16, 24,..., 64) are used for the parity checking of each 8-bit byte. The parity of the octet is odd.

DES Key	56 bit key + 8 bit parity K(1), K(2), K(3),... , K(64)

Fig. 4 DES Key decomposition

3.6 Encryption and Decryption Processes

Encryption key management is very important in encryption system. COMS applied MAC (Media access Control) address information of PC for generation and management of encryption key. The information of encryption key is in the Key Header of the Header Type #7 and in Encryption Key message header in File Type #29. These Keys have decryption solution, decryption key, for users having encrypted data.

First of all, user selects an encryption key bundle by 'File Type #129 Encryption Key Message Header', and next, selects a key of decryption key for decryption using selected key bundle number and system's MAC address. It is the point that main group for encryption distributes different bundle keys to every user. So bundle keys shuffled using user's MAC address, that every user has different key respectively. Fig. 5 shows an example of encryption key generation and distribution of COMS LRIT/HRIT.

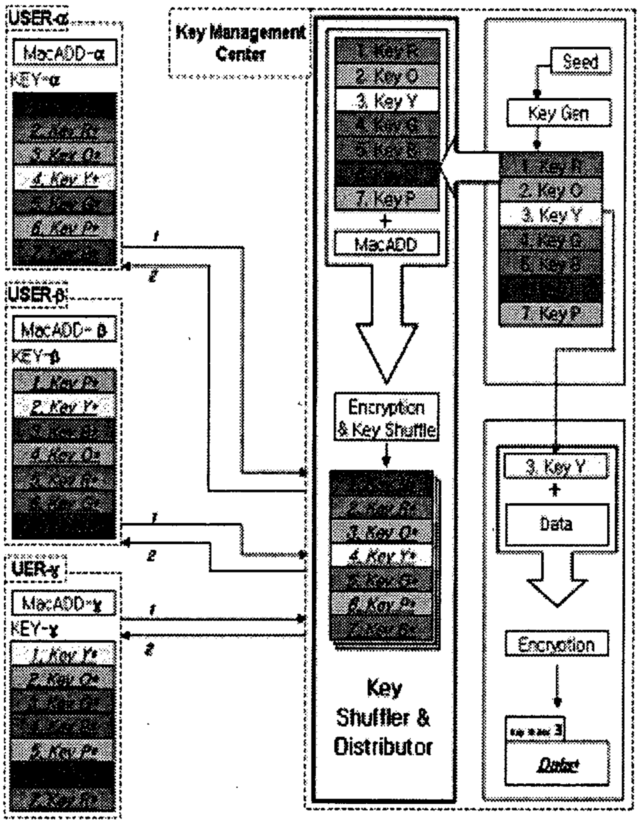


Fig. 5 An Example of Encryption Key Generation and Distribution

KMC (Key Management Center) requests MAC address of processing system to every user. For the first step, the center makes a lot of encryption keys. Second step, KMC makes an encryption key bundle using generated keys in first step. Third step, KMC shuffles key's order using each processing systems MAC address respectively. For the last step, Different shuffled keys' contents (not theirs order) are re-shuffled by each processing systems MAC address. For different encryption keys (bundles) generation, KMC should change seed value in a shuffle algorithm of encryption key management software. The seed value changing algorithm is included in the encryption key management software rightfully, so KMC administrator is not worry about that – needed just enter users MAC addresses.

If data are encrypted by Key 3 in Fig. 3, User-α should decrypt data using the Key no 4, User-β using Key no 2, and User-γ using 1. Each user has two bundles of key for decryption, and information of available decryption (encryption) key no. is in the Header Type #2 of COMS LRIT/HRIT Data.

Fig. 5 shows an example of decryption of COMS LRIT/HRIT. User α selects 4th key for decryption using User α's MAC address. So selected decryption key is encrypted also, that should decrypt the key using the MAC address one more time. As Use r-α, User-β and User-γ are should select and decrypt 2nd key and 1st key respectively.

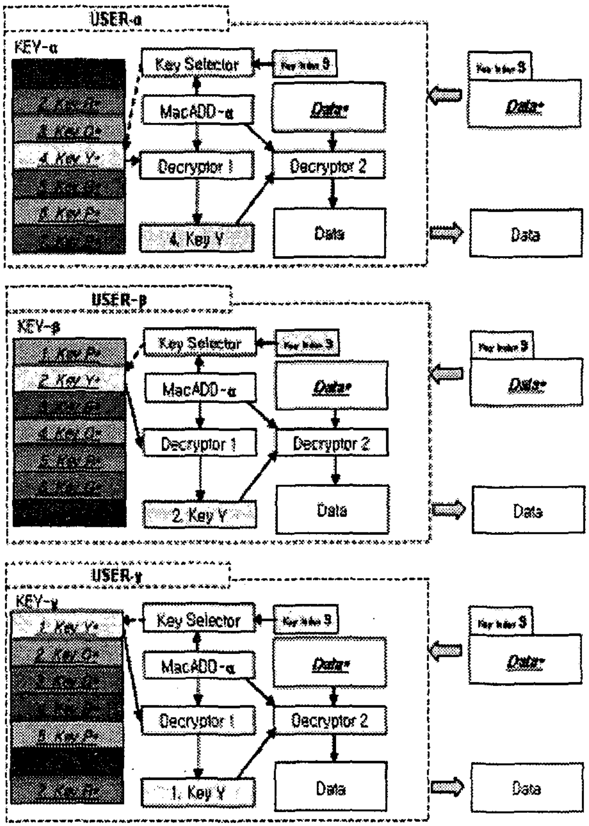


Fig. 5. An Example of Decryption

4. Conclusions

In this his paper we explain the compression and encryption method of COMS as the COMS LRIT/HRIT Specification. Compression of COMS is observed the ISO standard 10918 (lossy and lossless JPEG) and encryption is based on the DES algorithm. In the encryption algorithm of COMS, MAC address information is used for encryption key management and generation.

References

[CGMS 1999], 'LRIT/HRIT Global Specification', Rev 2.6.

[ISO 1982] 'Information Processing System - Open System Interconnection – Basic Reference Model', ISO standard 7498

[JMA 2003a], JMA LRIT Mission Specific Implementation -Issue 6

[JMA 2003b] JMA HRIT Mission Specific Implementation -Issue 1.2

[ISO 1983] 'Information Technology - Digital Compression and Coding of Continuous-tone Still Image - Requirements and Guidelines, Compliance Testing and Extensions', ISO standards 10918-1, 10918, DIS 10913-3

[DoC 1993] Data Encryption Standard (DES), Federal Information Processing Standard (FIPS) PUB 46-2, U.S. Dept. of Commerce, National Institute of Standards and Technology http://www.itl.nist.gov/fipspubs/fip46-2.htm

[DoC 1980] DES Modes of Operation, FIPS PUB 81, U.S. Dept. of Commerce, National Institute of Standards