JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 11, pp. 97-104, November 2020
https://doi.org/10.9708/jksci.2020.25.11.097

Study to safely transmit encrypted images from various noises in space environment

Ki-Hwan Kim*, Hoon Jae Lee**

*Graduate Student, Graduate School of Computer Engineering, Dongseo University, Busan, Korea
**Professor, Dept. of Computer Engineering, Dongseo University, Busan, Korea

[Abstract]

In this paper, we propose a random number generator PP(PingPong256) and a shuffle technique to improve the problem that the encrypted image is damaged due to a lot of noise by the channel coding of wireless communication recommended in the special environment of space. The PP can constantly generate random numbers by entering an initial value of 512 bits. Random numbers can be encrypted through images and exclusive logical computations. Random numbers can be encrypted through images and exclusive logical computations. The shuffle technique randomly rearranges the image pixel positions while synchronizing the image pixel position and the random number array position and moving the random number arrangement in ascending order. Therefore, the use of PP and shuffle techniques in channel coding allows all pixels to be finely distributed and transmit high-quality images even in poor transmission environments.

▸ **Key words**: CCSDS, Channel coding, Gaussian noise, Synchronize error, Random number generator, Shuffle technique

[요 약]

본 논문에서는 우주라는 특수한 환경에서 권장하는 무선 통신의 채널 코딩으로 암호화된 이미지가 노이즈에 많은 영향으로 손상되는 문제를 개선하기 위해 난수발생기 PP(PingPong256)와 셔플 기법을 제안한다. PP는 512비트의 초기값을 입력받아 끊임없이 난수를 생성할 수 있다. 난수는 이미지와 배타적 논리연산을 통해 암호화가 가능하다. 셔플 기법은 이미지 픽셀위치와 난수 배열위치를 동기화하고 난수 배열을 오름차순으로 위치를 이동하면서 이미지 픽셀 위치를 무작위로 재배열한다. 따라서 채널 코딩에 PP와 셔플 기법을 사용하면 모든 픽셀이 미세하게 분산되어 열악한 전송 환경에도 높은 품질의 이미지를 전송할 수 있다.

▸ **주제어**: CCSDS, 채널 코딩, 가우시안 노이즈, 동기오류, 난수발생기, 셔플 기법

• First Author: Ki-Hwan Kim, Corresponding Author: Hoon Jae Lee
*Ki-Hwan Kim (ghksdl90@naver.com), Graduate School of Computer Engineering, Dongseo University
**Hoon Jae Lee (hjlee@dongseo.ac.kr), Dept. of Computer Engineering, Dongseo University
• Received: 2020. 09. 25, Revised: 2020. 10. 23, Accepted: 2020. 10. 23.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

우주 데이터 시스템 자문 위원회(Consultative Committee for Space Data Systems, CCSDS)는 1982년 설립되어 우주 공간 정보 상호 교환을 촉진할 목적으로 표준을 개발하는 국제 조직이다. CCSDS는 우주라는 특수한 환경에 맞춰 다양한 전송 기법과 TCP/IP 참조 모델에 적합한 계층화 모델들을 제시하고 있다. CCSDS 표준 모델들은 반드시 준수해야만 하는 구속력은 가지고 있지 않지만 각 계층별로 고유의 암호 프로토콜을 수행하여 통신 채널의 보안 요구사항을 만족하도록 권고한다[1,2].

CCSDS의 특이한 점은 채널 코딩이라는 기능으로 데이터 링크 계층에서 암호화 기능과 HDLC(High-level Data-Link Control)라는 프로토콜을 사용하는 것이다[3]. 데이터 링크 계층에 채널 코딩이 추가되면 보안성이 향상된다. 그러나 수신측에서 올바른 동기화를 유지할 수 없다면 문제가 발생한다. Barnwell의 논문[4]에 의하면 모듈레이터, 씨드 레이저, 앰프, 수신기, 디지털 전환기 등 다양한 데이터를 위성에서 176nW의 수신 광학 피크 전력으로 송신하여 대기권을 통해 지상의 기지국에서 수신 받은 데이터가 0.00257 비트 에러 비율(Bit Error Rate: BER)로 측정했다. 이는 실생활에서 사용되는 무선 네트워크 환경에 비추어볼 때 낮은 비율이지만 Barnwell 이외에도 많은 논문에서는 실시간 영상, 음성, 데이터 및 양자 통신 기술 데이터의 수요 증가 폭발적인 증가로 네트워크 포화상태를 우려하였다[5-9].

본 논문은 위성에서 이미지 데이터를 대상으로 송·수신 시 발생하는 대기권 노이즈와 네트워크 혼잡으로 프레임 동기코드 손상에 따른 문제점을 확인한다. 이후 발견된 문제를 해결하기 위한 이미지 픽셀 재배치 방법을 제안한다.

II. Relation works

1. CCSDS data link channel coding problem

CCSDS 데이터 링크 채널 코딩을 이해하기 위해서는 OSI(Open Systems Interconnection)를 알아야한다[10]. OSI는 네트워크에서 통신이 일어나는 과정을 7단계로 나눈 것으로 각 단계는 고유한 역할이 존재한다. 수신측은 OSI는 1단계부터 7단계까지 차례대로 연산이 진행된다. 1단계는 0과1의 전기신호로 표현되는 물리계층, 2단계가 데이터 링크로 프레임이라는 단위로 나뉘고, 주요 역활은 데이터 흐름 제어 및 오류 제어 기능이다. CCSDS의 데이터 링크 채널 암호화는 그림 1과 같이 송·수신측의 동기화에 문제가 발생 시 정상적인 데이터 교환이 불가능하다.

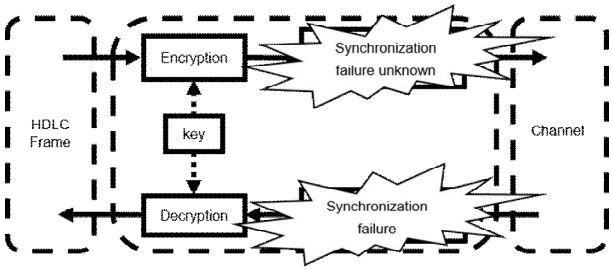


Fig. 1. CCSDS overall structure

따라서 CCSDS 채널 코딩은 AES(Advanced Encryption Standard) 암호 알고리즘과 HDLC 프로토콜을 사용한다[11]. 먼저 AES는 전 세계적으로 안전성이 검증된 암호 알고리즘이다. AES는 128비트 단위의 입력 데이터를 비밀키로 암호화하는 방법이다. 비밀키는 128,192,256비트 가운데 한 가지를 선택할 수 있고 송·수신측이 같은 비밀키를 사용하여 암호화 알고리즘은 문제가 없다. 하지만 AES의 특징 가운데 암호화된 데이터의 1비트라도 다르면 해독되는 결과는 무작위로 2비트 이상 변경되는 구조로 해독된 데이터에 영향을 준다.

다음으로 HDLC는 범용적으로 인터넷에서 사용되는 이더넷과는 약간 다른 규칙이다. 이더넷의 특징은 데이터를 표현할 수 있는 구역의 길이가 제한되어 있어 큰 데이터는 쪼개서 전송하지만 반면 HDLC는 길이 제한이 없다. 따라서 각 프레임마다 전송할 수 있는 길이가 제한된 이더넷을 사용하지 않고 길이 제한이 없는 HDLC를 사용하여 동기화 문제를 최소화한다. 그러나 대기권 상태와 인접한 위성간의 데이터 이용률 그리고 우주라는 특수한 환경은 예측할 수 없고 이는 문제를 유발시킨다.

결국 동기화 문제로 데이터 전체를 손해보는 경우와 성공적으로 수신 받은 데이터에 잡음이 추가된 경우 최대한 노이즈를 억압할 수 있는 방법이 필요하다.

2. Image comparison and verification method

원본이미지와 복호화 이미지를 비교하는 방법은 PSNR(Peak Signal to Noise Ratio)와 SSIM(Structural Similarity Index Map) 그리고 피어슨 상관계수 사용한다[12]. PSNR은 원본 영상과 비교영상이 얼마나 유사한지 평가할 때 사용되며, 수식 (1)과 같이 계산하여 값이 클수록 원본과 매우 가깝다고 해석한다. MAX_I는 하나의 픽셀이 표현할 수 있는 최댓값을 의미한다. 예를 들어 컬러 이미지는 빨강, 초록, 파랑 색상이 각각 8비트를 사용하여

수식 (2)로 계산한다. MSE(Mean Squared Error)는 $N \times M$ 크기의 이미지 a와 b를 대상으로 평균 픽셀 값을 차이를 나타내고 수식 (3)처럼 계산한다.

$$PSNR(N,M) = 10 \times \log_{10}(\frac{MAX_I^2}{MSE(N,M)}) \quad (1)$$

$$MAX_I^2 = 3 \times (2^8 - 1)^2 = 3*255^2 \quad (2)$$

$$MSE(a,b) = \frac{1}{NM}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(a_{xy} - b_{xy})^2 \quad (3)$$

SSIM은 인간이 영상을 평가하는 휘도(Luminance), 명암비(Contrast), 구조(Structure)의 값을 평가하여 계산하는 방법이다. 수식 (4)로 계산되며, 평가 결과는 0부터 1사이의 값을 가지며, 1에 가까울수록 좋은 품질로 평가된다. SSIM을 계산하기 위해서는 수식 (5)를 차례로 계산해야한다. μ_x와 μ_y는 신호 x와 y의 평균, σ_x와 σ_y는 신호 x와 y의 표준편차, σ_{xy}는 신호 x와 y의 공분산, c_1, c_2, c_3는 분모가 0이 되는 것을 방지하기 위해 사용하는 안정화 변수이다.

$$SSIM(N,M) = L(N,M) \times C(N,M) \times S(N,M) \quad (4)$$

$$L(x,y) = \frac{2\mu_x\mu_y + c_1}{\mu_x^2\mu_y^2 + c_1}$$
$$C(x,y) = \frac{2\sigma_x\sigma_y + c_2}{\sigma_x^2\sigma_y^2 + c_2}$$
$$S(x,y) = \frac{2\sigma_{xy} + c_3}{\sigma_x\sigma_y + c_3} \quad (5)$$

- μ_x : x의 평균
- σ_x^2 : x의 분산
- σ_{xy} : x, y의 공분산
- c_1, c_2, c_3 : 안정화 변수

상관계수는 원본 이미지의 가로, 세로 및 대각선 방향을 포함하여 인접한 픽셀과 큰 상관관계가 있다. 좋은 암호화 체계는 인접한 픽셀의 상관관계를 효과적으로 줄여야한다. 상관관계 분석은 상관 계수를 사용하여 인접 픽셀 간의 상관관계를 분석하고 제안 된 방식을 추가로 확인한다. 상관계수는 [수식 6 - 수식 9]와 같이 각 x와 y축 픽셀의 평균을 픽셀과 비교하여 계산하는 방법이다. 이때, 상관계수는 -1에서 1까지의 범위를 가지며, -1에 가까울수록 부정, 0에 가까울수록 무관계, 1에 가까울수록 긍정으로 해석된다.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (6)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \quad (7)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (8)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (9)$$

III. Symptoms of link synchronization error rate

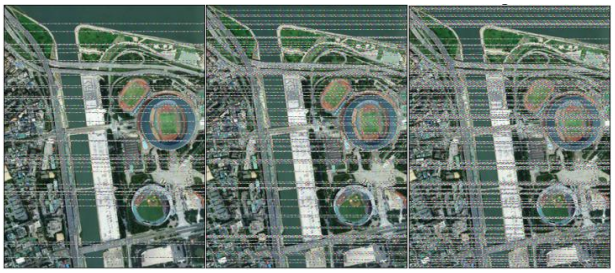
1. CCSDS channel coding experiments

실험환경은 링크 암호 프로토콜로 채널 간섭 및 대기권 영향에 따른 불안정한 채널 환경을 가정하고 이미지의 각 행을 HDLC 프레임을 사용했다. 대기권 잡음은 가우시안 노이즈로 구성하여 0.01에서 0.01까지 10배씩 증가한 경우에 대하여 실험하고 채널 포화에 따른 프레임 오류는 이미지의 각 행을 프레임 에러 단위(Frame error rate: FER)로 취급하여 10%에서 30%까지 10%씩 증가했다.

CCSDS 채널 코딩을 사용한 결과는 암호화와 동일하게 원본 이미지를 AES로 암호화하고 가우시안 노이즈에 따른 변화와 동기 오류에 따른 이미지 변화를 실험했다. 가우시안 노이즈 실험은 평균을 0으로 고정하고 분산을 0.1에서 0.3까지 0.1씩 변경했다. 동기 오류실험은 이미지 높이의 10%, 20%, 30%를 무작위로 선택하여 실험했다. 가우시안 노이즈 실험결과 그림 2처럼 분산이 커질수록 이미지 전체에 영향을 주었다. 동기 오류 실험결과 그림 3처럼 각 라인별로 나누어진 부분은 동기 오류로 이미지 손상이 크게 증가 했다.

(a) (b) (c)

Fig. 2. Apply gaussian noise of different variances to the AES image (a)0.1, (b)0.2, (c)0.3



(a) (b) (c)

Fig. 3. Applying the ratio of synchronization error for each AES image according to the height (a)10%, (b)20%, (c)30%

2. Random number generator and Shuffling technique

CCSDS 채널 코딩은 동기화를 유지하는 방법으로 AES 암호 알고리즘의 비밀키를 고정하는 것으로 동기화 문제를 최소화한다. 하지만 그림 2와 그림 3에서 손상에 영향을 주는 원인에는 AES 암호 알고리즘도 포함된다. AES는 128비트의 묶음 단위로 계산하여 암호문에 1비트의 변화가 발생하면 정상적으로 복원할 수 없다. 이 문제를 해결하기 위해서는 비트 단위의 암호 알고리즘을 사용하면 손상을 줄일 수 있다. 본 논문에서는 난수발생기와 사진의 픽셀 위치를 재배열하여 AES를 대체한다.

먼저 난수발생기는 PP(PingPong256)을 사용했다. PP 구조는 255비트와 257비트의 크기를 가진 LFSR(Linear Feedback Shift Register)를 초기값으로 사용하는 난수발생기이다[13]. LFSR은 사용된 n비트 크기에 해당하는 고유값을 최대주기인 2^n-1만큼 반복할 수 있다. 그림 2와 같이 두 개의 LFSR은 각각 서로의 출력에 영향을 주는 가변 클럭 함수(f_a, f_b)와 연결되어 불규칙한 주기를 가진 결과(a_i, b_i)를 만들어 낸다. 두 개의 불규칙한 결과를 서로 다른 함수로 저장하는 메모리(c_i, d_i)를 계산한 결과(c_{i-1}, d_{i-1})와 배타적 논리합을 결과를 통해 예측할 수 없는 상태를 만든다.

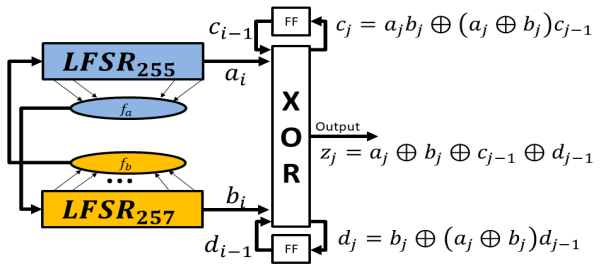


Fig. 4. PingPong256 Structure

다음으로 PP의 안전성은 1,000,000,000비트 길이의 난수를 생성하여 미국 NIST의 난수발생기를 검증 표준인 SP800-22로 검증하여 난수발생기의 안전성을 입증했다[14]. 이 구조는 입력하는 데이터와 단순히 배타적 논리합으로 데이터를 암호화하도록 구성하는 것으로 원본 데이터를 식별 할 수 없도록 한다. 그러나 암호화된 데이터의 비트 위치와 원본 데이터의 비트 위치가 같아 암호 알고리즘으로 바로 사용하기에는 문제가 있다.

따라서 입력 데이터를 비트 위치를 무작위로 재배열하는 셔플링 기법이 필요하다. 셔플링 기법을 사용하는 방법은 원본 이미지 픽셀 위치와 난수발생기를 통해 생성되는 난수의 순서를 동기화하고 난수발생기를 통해 32비트로 표현 가능한 정수를 무작위로 입력받아 순서를 오름차순으로 정렬한다. 이후 알고리즘 1처럼 입력된 이미지의 크기와 컬러 이미지인지 확인하여 입력 받은 이미지와 동일한 빈 배열을 생성한다. 이후 난수를 이미지의 가로길이로 나누어 몫과 나머지로 분류하여 몫은 y축, 나머지는 x축으로 설정하여 원본 이미지에서 x, y 축에 해당하는 픽셀 데이터를 빈 배열에 차례대로 저장한다. 이 과정을 이미지 크기만큼 반복하여 이미지 픽셀을 무작위로 재배열할 수 있고 반대로 복원할 수 있다.

Algorithm 1. Shuffle function

```
def shuffle(img, rand):
    height, width, channel = img.shape
    shuffle_img=np.zeros((height, width, channel),
dtype=np.uint8)
    count_x, count_y = 0, 0

    for i in range(len(rand)):
        y = math.floor(rand[:,0][i]/ width)
        x = rand[:,0][i] % width
        shuffle_img[count_y,count_x] = img[y,x]

        if (count_x+1) == width:
            count_y = count_y + 1
            count_x = 0
        else:
            count_x = count_x + 1

    return shuffle_img
```

셔플링 기법을 사용하여 그림 5처럼 이미지와 히스토그램을 그룹 (a), (b)로 나누어 표현했다. 그룹 (a)는 원본 이미지, (b)는 원본이미지를 셔플링 기법을 적용한 결과이다. 히스토그램이란 데이터의 최소 단위 값을 그룹별로 나누어 누적횟수를 표현하는 방법이다. 두 그룹의 히스토그램이 같은 것은 전체 픽셀의 값은 변화가 없이 위치가 교환되었음을 의미한다.

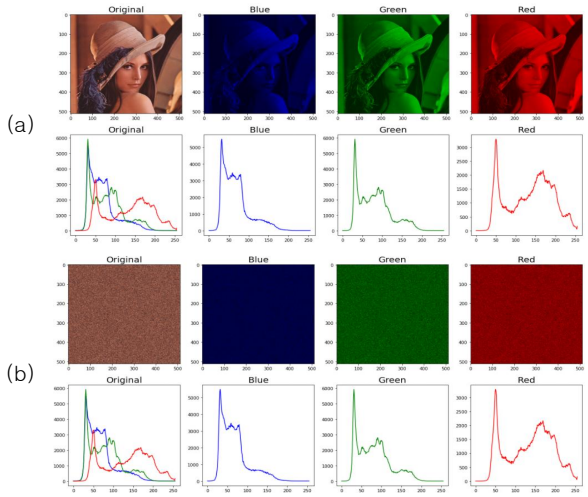


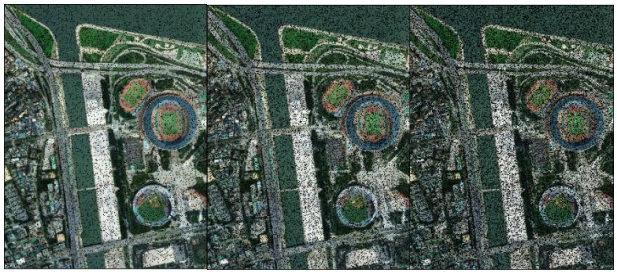
Fig. 5. Compare Original image to Shuffle image
(a) Original image, (b) Shuffle of Original image

3. Experimenting with image encryption

이전 CCSDS 실험과 동일하게 가우시안 노이즈와 동기 오류를 나누고 암호 알고리즘을 PP와 셔플링 기법을 적용했다. 가우시안 노이즈 실험결과 그림 6처럼 분산을 (a) 0.1부터 (c)0.3까지 변경하였으나 원본과 유사한 결과를 보였다. 그러나 동기 오류는 그림 7처럼 (a)10%부터 (c)30%까지 변경할 경우 노이즈가 확산되었다.

(a) (b) (c)

Fig. 6. Apply gaussian noise of different variances to the PP and Shuffle image (a)0.1, (b)0.2, (c)0.3



(a) (b) (c)

Fig. 7. Applying the ratio of synchronization error for each PP and Shuffle image according to height (a)10%, (b)20%, (c)30%

표 1은 그림 2와 그림 6을 PSNR과 SSIM 그리고 상관계수로 비교한 결과이다. 컬러 이미지를 대상으로 가우시안 노이즈를 비교하면 모두 PP가 상대적으로 AES에 비해 우수한 결과를 보인다. 추가적으로 원본을 흑백 이미지로 변경하여 채널에 따른 민감도를 줄여 실험해도 PP가 AES에 비해 좋은 결과를 보였다.

그러나 AES 동기 오류를 실험한 그림 3과 PP 동기 오류를 실험한 그림 7을 대상으로 PSNR과 SSIM 그리고 상관 계수를 비교한 표 2는 상대적으로 차이가 있다. 육안으로는 그림 7이 전반적으로 그림 3에 비해 좋은 품질을 가지고 있는 것으로 보인다. 하지만 컬러 이미지에서 PSNR과 SSIM은 AES가 PP가 거의 비슷하거나 약간 우수했지만 상관계수는 PP가 AES보다 약간 우수한 결과를 보였다. 흑백의 경우 AES가 PP보다 전체적으로 우수한 결과를 보였다. 이 문제는 노이즈에 따라 픽셀 데이터를 0으로 변경하여 수치 계산에서 AES가 PP보다 좋은 결과를 나타냈다.

Table 1. The result of applied only Gaussian noise

			PSNR	SSIM	CORR
Color	0.1	AES	28.7979	0.9568	0.9859
		PP	45.2461	0.9982	0.9997
	0.2	AES	17.0576	0.5567	0.8059
		PP	39.5520	0.9948	0.9988
	0.3	AES	13.1811	0.3010	0.5697
		PP	38.2899	0.9920	0.9984
Gray	0.1	AES	30.7474	0.9645	0.9904
		PP	49.0278	0.9984	0.9999
	0.2	AES	19.1343	0.6253	0.8625
		PP	42.8132	0.9954	0.9994
	0.3	AES	15.2387	0.3826	0.6634
		PP	40.7103	0.9926	0.999

Table 2. The result of applied both Gaussian noise and synchronization error

			PSNR	SSIM	CORR
Color	10%	AES	18.2863	0.7084	0.8532
		PP	16.8086	0.5299	0.8182
	20%	AES	14.6687	0.3941	0.6579
		PP	13.7259	0.3765	0.6847
	30%	AES	13.2676	0.3094	0.5759
		PP	11.9308	0.2927	0.5806
Gray	10%	AES	20.1360	0.7526	0.8934
		PP	16.6697	0.5113	0.8057
	20%	AES	16.4771	0.4617	0.7335
		PP	13.5876	0.3577	0.6681
	30%	AES	15.3051	0.3899	0.6675
		PP	11.7934	0.2761	0.5633

IV. Pixel rearrangement

1. Restore image redundancy

PP를 개선하는 첫 번째 방법은 사용된 방식을 같은 분산으로 중복 계산하고 픽셀 데이터를 비트 단위로 OR 연산하는 것이다. 가우시안 노이즈는 중복될 확률 낮아 중복된 횟수와 원본 이미지의 유사도가 높아질 수 있다.

그림 8은 가우시안 분산이 0.1, 동기 오류가 30%인 환경에서 (a)는1회부터 (d)는 4회까지 누적 연산한 결과이다. 표 3은 그림 8의 결과를 비교한 것으로 이미지가 누적 횟수가 증가할수록 원본이미지와 같아지는 것을 알 수 있다. 이를 통해 제안된 암호 방식과 픽셀 재배열을 사용하면 같은 이미지를 중복하는 것으로 대부분의 노이즈를 극복 할 수 있는 것으로 나타났다.

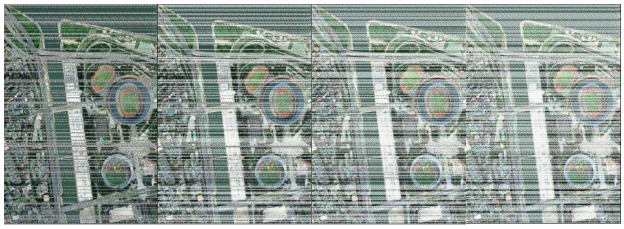
(a) (b) (c) (d)

Fig. 8. Image quality change between AES and image accumulation count in an environment where Gaussian variance is 0.1 and synchronization error is 30% of image height (a) 1time, (b) 2time, (c) 3time, (d) 4time

Table 3. Accumulate images with PP and shuffling techniques

Accumulation count		PSNR	SSIM	CORR
Color	1 time	11.9505	0.2889	0.5831
	2 time	16.8647	0.5334	0.8192
	3 time	24.0017	0.8404	0.9590
	4 time	Inf	1.0000	1.0000
Gray	1 time	11.8113	0.2720	0.5657
	2 time	16.7262	0.5145	0.8066
	3 time	23.8664	0.8315	0.9554
	4 time	Inf	1.0000	1.0000

그러나 AES는 동기 오류로 노이즈가 중첩될 확률이 높아 중첩을 사용하면 이미지 손상이 심해지게 된다. 그림 9는 AES에 분산이 0.1, 동기 오류가 30%인 환경에서 (a)는 1회부터 (d)는 4회까지 누적 연산한 결과이다. 이미지 중첩 횟수가 증가할수록 노이즈가 원본 이미지를 왜곡된 결과가 보인다. 표 4는 그림 9에 대한 결과이다. 표 3과 표 4를 비교하면, 누적 중복이 없는 경우 AES가 좋지만 누적 횟수가 증가할수록 PP에 비하여 상대적으로 품질이 떨어졌다. 특히 PP는 4회 누적된 경우 원본 이미지와 완전히 동일한 결과를 보였다. AES는 암호화된 데이터의 변화 따라서 복호화 결과에 블록 단위로 민감하게 반응하여 무작위하게 영향을 주는 노이즈에 따라서 원본 데이터를 상회하는 범위를 표현하기도 한다. 하지만 PP는 노이즈의 영향으로 원본 데이터가 0에 가까워지는 특성으로 원본 데이터를 상회하는 범위로 확산되지 않아 중첩될수록 원본에 가까운 결과를 나타낼 수 있다.



(a) (b) (c) (d)

Fig. 9. Image quality change between the cumulative number of images using PP and shuffling in an environment with a Gaussian variance of 0.1% and a sync error of 30% image height (a) 1time, (b) 2time, (c) 3time, (d) 4time

Table 4. Accumulate images with AES and shuffling techniques

Accumulation count		PSNR	SSIM	CORR
Color	1	13.5026	0.3769	0.6124
	2	10.6347	0.2626	0.5131
	3	9.2914	0.2160	0.4634
	4	8.6359	0.2003	0.4440
Gray	1	15.3905	0.4562	0.6987
	2	11.7969	0.3116	0.5777
	3	10.3394	0.2693	0.5375
	4	9.6436	0.2623	0.5316

2. Correction and restoration according to pixel average and initial value

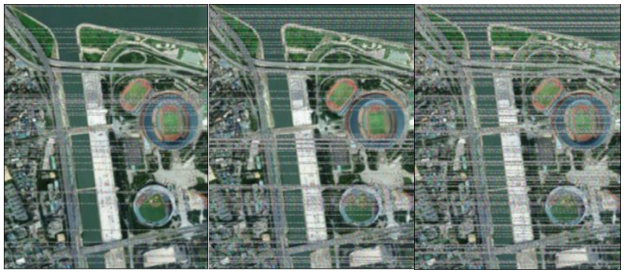
다른 이미지의 노이즈를 제거하는 방법은 가운데 주변 픽셀을 이용하여 보정하는 방법을 blurring 필터라고 한다[15]. blurring은 low-pass 필터를 이미지에 적용하여 고주파영역을 제거함으로써 노이즈를 제거하거나 경계선을 흐리게 할 수 있다. 기본적으로 3×3형태의 박스형 평균값 필터를 사용한다.

다음으로 컬러 이미지에 서로 다른 채널의 초기값을 다르게 계산하여 픽셀을 완전히 0으로 만드는 문제를 해결하면 PSNR과 SSIM이 증가할 수 있다. 이 부분은 알고리즘 1에서 채널별로 생성된 난수에 서로 다른 소수를 곱하여 이미지 범위를 초과하면 x=0,y=0의 위치로 되돌리는 것으로 계산하여 사용했다. blurring 평균 필터와 채널 초기값 보정을 사용한 결과 표 5와 같이 PP가 AES보다 높은 결과를 보였

다. 표 5에서 blurring을 적용한 AES는 그림 9 그리고 blurring을 적용한 PP와 셔플링 기법은 그림 10과 같다. 이미지를 육안으로 보면 AES는 흰색 선이 육안으로 보이고 PP는 검은 점이 거의 보이지 않아 상대적으로 PP의 이미지 품질이 좋아 보이지만 원본 이미지와 PSNR과 SSIM 그리고 상관계수의 차이는 거의 발생하지 않았다.

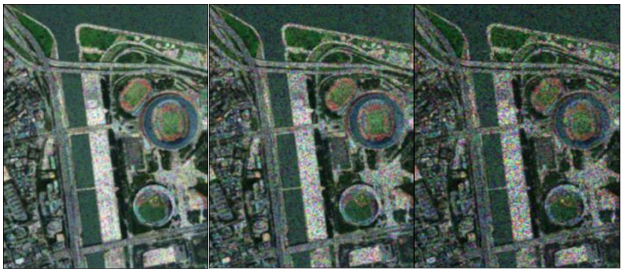
Table 5. The result of applied both Gaussian noise and synchronization error

			PSNR	SSIM	CORR
Color	10%	AES	21.0737	0.6564	0.9189
		PP	20.8219	0.6612	0.9296
	20%	AES	18.7897	0.5405	0.8658
		PP	17.8421	0.5641	0.8948
	30%	AES	17.1612	0.4593	0.8122
		PP	15.4603	0.4823	0.8545
Gray	10%	AES	21.5311	0.6705	0.9239
		PP	21.4469	0.7049	0.9424
	20%	AES	19.4132	0.5673	0.8806
		PP	18.3233	0.6197	0.9232
	30%	AES	17.8166	0.4946	0.8369
		PP	15.7734	0.5419	0.8999



(a) (b) (c)

Fig. 10. Applying the ratio of synchronization error for each AES image according to the height (a)10%, (b)20%, (c)30%



(a) (b) (c)

Fig. 11. Applying the ratio of synchronization error for each PP image according to the height (a)10%, (b)20%, (c)30%

V. Conclusions

CCSDS 표준 링크 암호를 SES Alarmed를 통해 위성과 지상 기지국에 대한 대기권 오류와 네트워크 트래픽 증가에 따른 프레임 동기 오류와 이미지의 상관도를 살펴보았다. 우주공간의 경우 환경에 따른 오차가 거의 없어 오류율이 낮으나 대기권과 지상의 기지국 수신 환경에 따라서 오류율이 극명하게 차이가 난다.

본 논문은 대기권과 수신환경으로 변화되는 환경에서 발생하는 노이즈와 위성 네트워크의 트래픽이 집중되는 경우를 가정하여 대표적인 암호 알고리즘인 AES를 이미지 암호화에 사용하여 가우시안 노이즈와 프레임 동기 코드 오류 제어를 실험했다. 또한 PP와 셔플링 기법을 제안하여 AES 이미지 암호화 결과에 가우시안 노이즈와 동기 오류를 추가하여 PP와 셔플링 기법에 대한 데이터 손상에 따른 차이를 연구했다. 실험을 통해 AES는 암호학적으로 안전하지만 노이즈에 영향을 받으면 원본 데이터 이상을 초과하는 데이터를 출력할 수 있어 인접한 모든 데이터를 올바르게 복원할 수 없었다.

본 논문에서는 이 문제를 해결하기 위해 이미지 크기와 동일한 난수 집합을 사용하여 배타적 논리합으로 연산하고 픽셀을 재배열하는 암호화 방법을 제안하고 AES와 비교 실험을 수행했다. 그 결과 신호충돌과 프레임 동기 코드 손상에 따른 이미지 데이터 손실에도 복원된 이미지에 많은 부분이 유지되는 것을 확인했다.

위성 네트워크는 민간, 군사 목적 등 다양한 분야에서 사용되고 있으며, 앞으로 더욱 많은 사용이 예상되는 분야이다. 본 논문의 실험을 통해 최악의 경우에 따른 이미지 데이터 송·수신 방법을 고려할 수 있을 것으로 기대한다.

ACKNOWLEDGEMENT

This work was supported by Dongseo University, "Dongseo Cluster Project" Research Fund of 2020 (DSU-20200008).

REFERENCES

[1] Recommendation for Space Data System Standards, “TM SYNCHRONIZATION AND CHANNEL CODING,” The Consultative Committee for Space Data System, CCSDS 231.0-B-3, BLUE Book, Sep. 2017, *https://public.ccsds.org/Pubs/131x0b3e1.pdf*

[2] Report Concerning Space Data System Standards, “NEXT GENERATION UPLINK,” The Consultative Committee for Space Data System, CCSDS 230.2-G-1, GREEN Book, July.

2014, *https://public.ccsds.org/Pubs/230x2g1.pdf*

[3] Recommendation for Space Data System Standards, "TM SYNCHRONIZATION AND CHANNEL CODING," The Consultative Committee for Space Data System, CCSDS 131.0-B-2, BLUE Book, Aug. 2011, *https://public.ccsds.org/Pubs/131x0b2ec1s.pdf*

[4] N. Barnwell, "Free-Space Optical Links for Small Spacecraft Navigation," Timing and Communication, Ph.D. Thesis, University of Florida, Gainesville, FL, USA, 2018. DOI: 10.3390/aerospace6010002

[5] H. Li, Y. Huang, Q. Wang, D. He, Z. Peng, Q. Li, "Performance analysis of satellite-to-ground coherent optical communication system with aperture averaging." Applied Sciences, vol. 8, no. 12, 2496, 2018. DOI: 10.3390/app8122496

[6] T. Hanada, K. Fujisaki, and M. Tateiba. "Average bit error rate for satellite downlink communications in Ka-band under atmospheric turbulence given by Gaussian model," 2009 Asia Pacific Microwave Conference, IEEE, 2009. DOI: 10.1109/APMC.2009.5384382

[7] N. Alshaer, T. Ismail, H. Seleem, and M. E. Nasr, "Optimized Beam Size of Optical Ground-to-Satellite Link over Turbulence and Beam-Wandering," 2019 21st International Conference on Transparent Optical Networks, IEEE, 2019. DOI: 10.1109/ICTON.2019.8840526

[8] D. Vasylyev, W. Vogel, and F. Moll. "Satellite-mediated quantum atmospheric links," Physical Review A, vol. 99, no. 5, 053830, 2019. DOI: 10.1103/PhysRevA.99.053830

[9] X. Wang, and N. Guan. "A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA operation," Optics & Laser Technology, vol. 131, 106366, May. 2020. DOI: 10.1016/j.optlastec.2020.106366

[10] Deborah Russell, Debby Russell, G. T. Gangemi, Sr Gangemi, G. T. Gangemi, Sr. "*Computer Security Basics*," O'Reilly Media, Inc, 1991.

[11] GELENBE, Erol; LABETOULLE, Jacques; PUJOLLE, "Guy. Performance evaluation of the HDLC protocol," Computer Networks, 2(4-5), pp.409-415, Sep. 1978. DOI: 10.1016/0376-5075(78)90019-3

[12] HORE, Alain; ZIOU, Djemel. "Image quality metrics: PSNR vs. SSIM," 2010 20th international conference on pattern recognition. IEEE, pp. 2366-2369, 2010. DOI: 10.1109/ICPR.2010.579

[13] LOWY, Menahem. "Parallel implementation of linear feedback shift registers for low power applications," IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, Vol.43, No.6, pp.458-466, 1996. DOI: 10.1109/82.502318

[14] Bassham III, L. E., Rukhin, A. L., Soto, J., Nechvatal, J. R., Smid, M. E., Barker, E. B., ... & Heckert, N. A. (2010). "Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications," National Institute of Standards & Technology, 2010, *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf*

[15] Chen, T. J., Chuang, K. S., Chang, J. H., Shiao, Y. H., & Chuang, C. C. "A blurring index for medical images," Journal of digital imaging, Vol.19, No.2, pp.118-125, Jun 2006. DOI: 10.1007/s10278-005-8736-y

Authors

Ki-Hwan Kim received the B.S., M.S. degree in Computer Networking from Dongseo University, Republic of Korea in 2015.

Mr. Kim is now a Ph.D. student in the Computer Engineering department at Dongseo Graduate School in 2017. His current research interests are in Cryptography, Side-Channel Attack(SCA) and Artificial Intelligent(AI).

Hoon Jae Lee received the B.S., M.S. and Ph.D. degree in Electrical Engineering from Kyungpook national university in 1985, 1987 and 1998, respectively.

Dr. Lee had been engaged in the research on cryptography and network security at Agency for Defense Development from 1987 to 1998. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor. His current research interests are in security communication system, side-channel attack, USN & RFID security. He is a member of the Korea institute of Information security and cryptology, IEEE Computer Society, IEEE Information Theory Society and etc