International Journal of Engineering & Technology, 7 (3.33) (2018) 285-289

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Influenced Encryption Key for AES based MF-TDMA in Mobile Communication

Won Ho Jeong[1], Sang-Lim Ju[2], Ju-Phil Cho[3], Kyung-Seok Kim[4]*

[12] *Department of Electrical and Electronic Engineering Chungbuk National University Cheongju, Chungbuk, Rep. KOREA*
[3] *Department of Radio Communication Engineering Kunsan National University Gunsan, Rep. KOREAr*
[4]* *Department of Electrical and Electronic Engineering Chungbuk National University Cheongju, Chungbuk, Rep. KOREA*
**Corresponding author E-mail:kseokkim@cbnu.ac.kr*

Abstract

In recent years, network security has become an important issue. Cryptography has been used for secure data and control access. In this paper, we analyze the effect of the key error according to plaintext size in the encrypted mobile communication. We have applied the Multi-Frequency Time-Division Multiple Access (MF-TDMA) based mobile communication environment and used the Advanced Encryption Standard (AES) algorithm. Simulator configured with the Convolutional Turbo Code (CTC) channel coder and Offset Quadrature Phase Shift Keying (OQPSK) modulation scheme and Additive White Gaussian Noise (AWGN) mobile channel. Depending on the length of the plaintext, we confirmed through the correlation of the bit error rate (BER) and the peak signal-to-noise ratio (PSNR). In addition, we analyze the correlation according to SNR in AES Counter (CTR) and Cipher-Block Chaining (CBC) mode and analyze the effect of encryption algorithm on communication. Finally, this study is used as data to analyze the performance of application of cryptographic service and various communication environments in the environment of MF-TDMA based mobile communication, and it is expected that it will be useful for performance analysis of image data restoration.

Keywords: *AES encrytion algorithm, CTC (Convolutional Turbo Code), Key error, Mobile channel, PSNR (Peak Signal-to-Noise Ratio)*

1. Introduction

The Advanced Encryption Standard (AES) has been lately accepted by NIST as the symmetric key standard for encryption and decryption of blocks of data and is widely accepted for error detecting and correction codes. However, in wireless networking security system, the need for lowering of power requirements has been on the rise and is often regarded as one of the prime requirements for the advancement of the industries of today[1]-[6].
Generally, sensor nodes are used for many wireless security purposes and accompanied by limited chip size and limited computing power. Despite this, the whole system can consist of different sensor modules, operating systems, microcontroller communication modules and many peripheral systems. These security issues force us to use more security systems for the prevention of impersonating, cloning identity related issues and various channel analyses. Therefore, it urgently necessary to find a balance between lowering the power needs along with the non-compromising security issues and its successful and efficient implementation.
The remainder of this paper is organized as follows. Section II introduces the general AES encryption and CTC encoder processing. Section III explains the analysis flow of key error effect on encryption and CTC encoder processing. The performance simulation results and corresponding analysis are presented in Section IV, and Section V provides concluding remarks and summarizes the paper.

2. General AES encryption and CTC encoder processing

There are many algorithms and methods involved with the encryption process. This section briefly discusses the encryption and decryption procedure based on the substitution method. The most important type of encryption is the symmetric key encryption. In the symmetric key encryption, the same key is used for both the encryption and decryption processes. Hence, the secrecy of the key is maintained and it is kept private. Symmetric algorithms have an advantage of not consuming too much computing power and working at high speed in encryption. A block cipher and a key are taken as inputs; the output block will be same in size in the symmetric key encryption. The symmetric key encryption takes place in two modes, either as the block ciphers or as the stream ciphers. In the block cipher mode, the whole data is divided into number of blocks and the key for encryption is provided based on block length the key is provided for encryption [7].
The main components of the CTC (Convolutional Turbo Code) encoder include an interlayer and two recursive systematic convolutional (RSC) encoders.
The conventional procedure is as follows.
The first four words are made from the cipher key (initial key). The key is an array of 16 bytes (k0 to k15). The first four bytes (k0 to k3) become w0, next four bytes (k4 to k7) become w1, and so on.

The rest of the words (w_i for i=4 to 43) are made as follows.

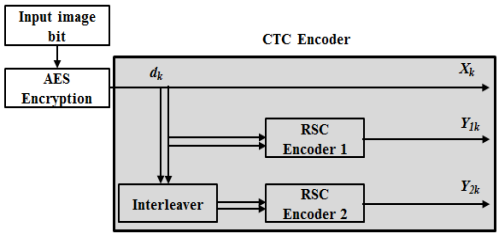


Fig. 1: Flow of the Normal Encryption Procedure

If (i mod 4) != 0, w_i=w_i-1 xor w_i-4.
If (i mod 4) = 0, w_i=t xor w_i-4. Here, *t* is a temporary word after applying SubByte transformation, rotating around w_i-1 and XORing the result with a round constant. Suppose the AES key is *k* and the RSC encoders are G1 and G2. Then the outputs of input bit d_k are [8][9]:

$$Y_{1k} = \sum_{i=0}^{k-1} G_{1i} d_{k-i} \qquad \text{mod1}, \tag{1}$$

$$Y_{2k} = \sum_{i=0}^{k-1} G_{2i} d_{k-i} \qquad \text{mod2}, \tag{2}$$

Fig. 1 is flow of the normal encryption procedure. In a Normal Log-Map decoding algorithm,

$$L(d_k) = \log\left[\frac{P(d_k = 1 \mid observation)}{P(d_k = 0 \mid observation)}\right] \tag{3}$$

Where $P(d_k = i \mid observation)$ i =0 or 1 is the posteriori probability if the source bit is d_k.

3. Analysis flow of key error effect on encryption and CTC encoder processing

3.1. Proposed encryption and CTC encoder processing and CTC encoder processing

To analyze the performance difference when changing as the plain-text, images with size of 12 Mbps were used as input data per 4 channels for the MF-TDMA based next-generation mobile communication channel. Fig. 2 shows a simulation flow of the MF-TDMA system in mobile channel. Encryption algorithms were applied to CTR and CBC modes of the most common AES algorithm. Encryption was performed while varying size of the plain-text in the encryption process. A channel coding scheme was used for the CTC channel coding scheme suitable for high speed mobile link. The OQPSK modulation scheme suitable for high-speed data transmission mobile was also used. Modulation of digital data was transferred to the MF-TDMA system in 4 channels. An AWGN channel was used as a reference channel by the mobile

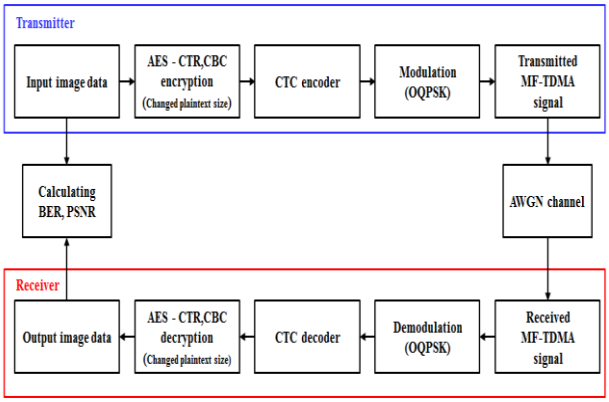


Fig. 2: MF-TDMA System

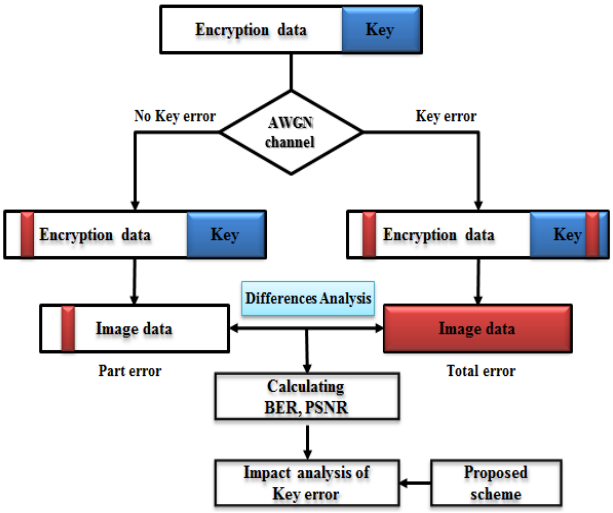


Fig. 3: Analysis Procedure of Encryption Key Error

Digital broadcast DVB-S2 [10]. BER and PSNR were computed to receive data through the transmitter and reverse process.
We used the round number of the 10 individual AES-128 (CTR, CBC) modes. The AES key expansion process of the general algorithm is as follows.
Pseudo code for AES key expansion: The key-expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates 4x (Nr+1) words. Nr is the number of rounds. The proposed procedure is as follows.
An added key is generated by an XOR operation to proceed with decoding of 16 bytes in the AES key.
An AES key is added across the entire plain-text when decoding a channel using error.

$$Y_{1k}^{*} = \sum_{i=0}^{k-1} G_{1i} (d_{k-i} \oplus k_{add}) \qquad \text{mod1}, \tag{4}$$

$$Y_{2k}^{*} = \sum_{i=0}^{k-1} G_{2i} (d_{k-i} \oplus k_{add}) \qquad \text{mod2}, \tag{5}$$

Where *A* key is added whenever the mobile communication is transmitted as the input image bits. AES decryption can be preceded if one of the key bits is found as an error bit. Fig. 3 shows the flow of the analysis procedure of encryption key error.

In the proposed Log-Map decoding algorithm,

$$L(d_k) = \log\left[\frac{P(d_k = 1 \mid d_k \oplus k_{add} = 1)}{P(d_k = 0 \mid d_k \oplus k_{add} = 0)}\right] \tag{6}$$

Where $P(d_k = i \mid d_k \oplus k_{add} = 1)$ is the joint probability of d_k under the condition of the received sequence $d_k \oplus k_{add} = 1$. Fig. 4 shows the flow of the proposed encryption procedure.

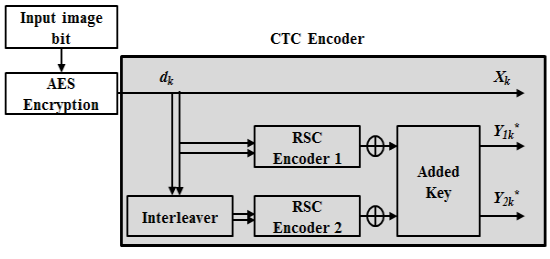


Fig. 4: Flow of the Proposed Encryption Procedure

3.2. Difference between encryption and normal images

By changing size of the encrypted packet through an AWGN channel coding scheme applied to CTC. The BER formulas used for analysis in each case are as follows:

$$P_{bit\ error} \cong \frac{1}{K} Q\left(\sqrt{2R\frac{E_b}{N_0}}\right) \tag{7}$$

Where K is input bit length, R is channel code rate, E_b is bit energy, and N_0 is noise power spectral density.
The difference in *BER* between the formulas was not applied to the encryption, as shown below:

$$BER_{dif} \cong \frac{N_{nor} - N_{ecy}}{K} Q\left(\sqrt{2R\frac{E_b}{N_0}}\right) \tag{8}$$

Where N_{nor} is the normal communication output code, N_{ecy} is the encrypted communication output code, K is input bit length, R is channel code rate, E_b is bit energy, and N_0 is noise power spectral density. When applied to a real image, quality of the image is represented by the *RMSE* formula below:

$$RMSE = \sqrt{\left[\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[f(x,y) - \hat{f}(x,y)]^2\right]} \tag{9}$$

Where *f(x,y)* is the position of pixel, *M and N* is image size. When applying to encryption, the pixel difference is shown as the number of pixel change rate (NPCR) as follows [1].

$$NPCR = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[f(x_{nor}, y_{nor}) - f(x_{ecy}, y_{ecy})]^2}{M \times N} \times 100 \tag{10}$$

PSNR is not applied when the formula that represents the difference between the cryptographic applications and this *NPCR* is as follows:

$$PSNR_{dif} = 10\log_{10}\left(\frac{peak - to - peak^2}{NPCR}\right), \quad \text{dB} \tag{11}$$

Where *peak-to-peak* is the maximum peak. BER_{dif} and $PSNR_{dif}$ values should correlate in the next section.

4. Performance analysis

4.1. Simulation conditions

We analyzed the differences in encryption and performed encryption to analyze the effects of the encryption key. MF-TDMA is a technology that has combines advantages of FDMA and TDMA.

Table 1: Simulation Parameters

Simulation parameters	Values
Input data	Video (H.264)
Encryption mode	AES-CTR, CBC
Channel code	CTC (Convolutional Turbo Code)
Modulation	OQPSK
Channel	AWGN
Frequency	8 GHz
MF-TDMA	Bandwidth: 48 MHz Frequency slot: 4 Super frame length: 400ms Time slot: 63
Encryption key	73 bytes

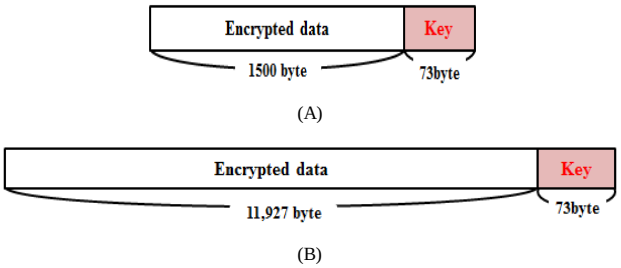


Fig. 5: Encrypted Packet Size (A) Case 1 (B) Case 2

Fig. 6: Input Video Frame

Table 2: Simulation Condition of Image

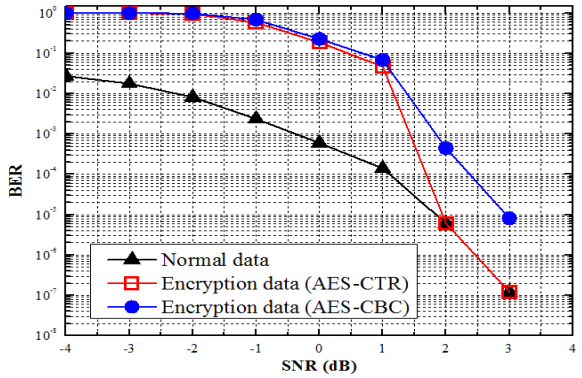
Parameters	Values
Codec	H.264
Bit transmission rate	743 kHz
Image file length	2 sec
Image file size	44,082 bytes
Image frame size	320 x 240

It is a technique used for dynamic and simultaneous operation, and is divided according to time and frequency of radio resources. It has an advantage of using limited resources more efficiently. The simulation parameters are summarized in Table 1.
Fig. 5 shows the MF-TDMA mobile channel based on plain size changed to analyze the effect of the encryption key. Plain and combined packet was the key that corresponds to an MF-TDMA time slot. Transfer rate of 12Mbps was applied by changing the number of time slots. The first plain-text data was configured as 1,500 bytes, followed by plain-text data of 11,927 bytes. This was intended to analyze the effect of changing plain-text size on key errors.
We constructed four channels and a time axis of 400 msec in accordance with the basic specifications of mobile communication. In this paper, we considered transfer rate of 12 Mbps. Since transfer rate of 12 Mbps can transmit 12 Mbit per second, 4.8 Mbit can be transferred in 400 msec.
Image parameters are as presented in Table 2 and photograph of input video frame is shown in Fig. 6. Image coding uses the H.264 image codec, which is the most common image codec available.
This codec has a very high data compression ratio. We performed a simulation using an image file that is about 2 seconds and 44 Kbytes. Also, image frame size is 320 pixels in length and 240 pixels in width. The AES algorithm was applied to the encryption algorithm of the MF-TMDA mobile communication system.

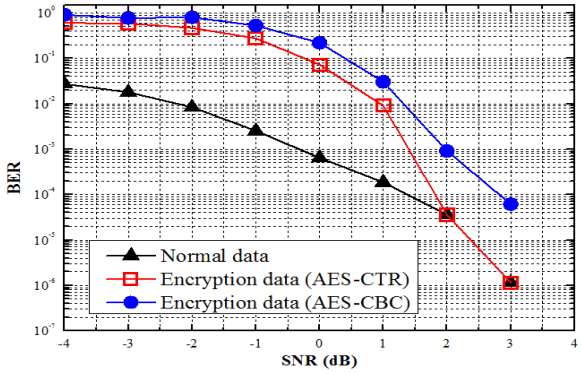
4.2. Impact analysis of key error

Excellent performance is shown by normal (unencrypted) data. Performance of AES-CTR encryption is lower than performance of normal data from −4 dB to 1 dB, because the key values are damaged. However, because the key values are all restored at 2dB, performance of AES-CTR encryption is similar to performance of normal data. In the AES-CBC encryption case, errors in the preceding stage influence the next stage. Because parallel processing is impossible while decoding, a shear password block is used and performance is severely reduced. Fig. 7 shows a case of applying specific BER to the AES-CTR, CBC mode. When applied to a real image, quality of the image is represented by the

RMSE in Fig. 8 according two cases. PSNR is not applied when the formula represents the difference between the cryptographic applications and this NPCR. Fig. 9 is PSNR for changed plain-text size and Fig. 10 shows average PSNR in each case.

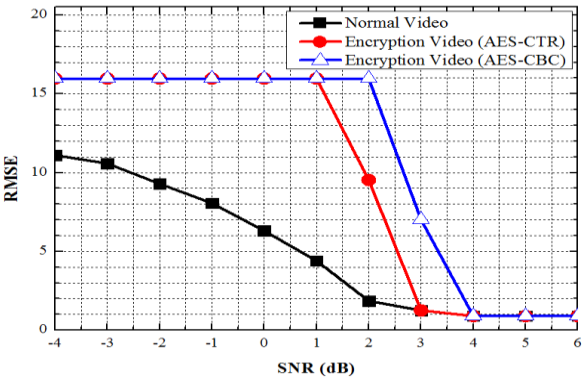


(A)

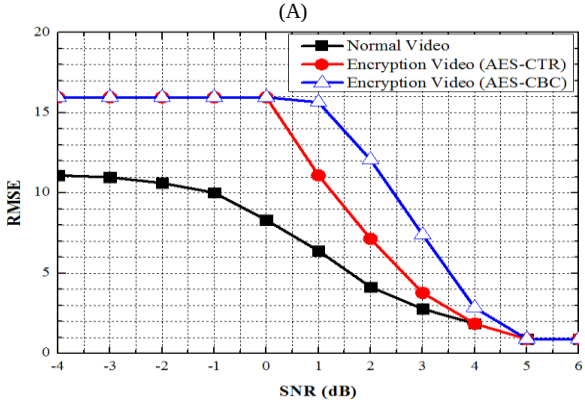


(B)

Fig. 7: BER for Changed Plain-text Size (A) Case 1 (B) Case 2

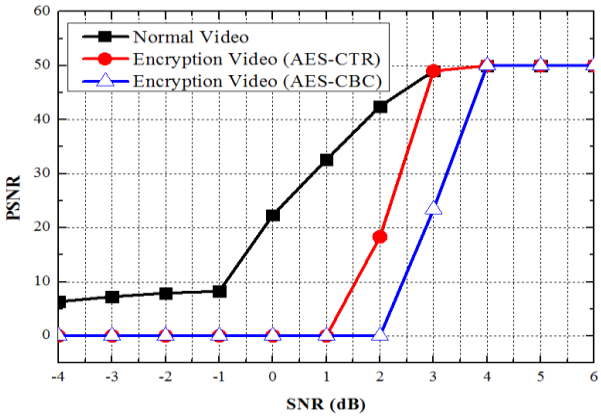


(A)

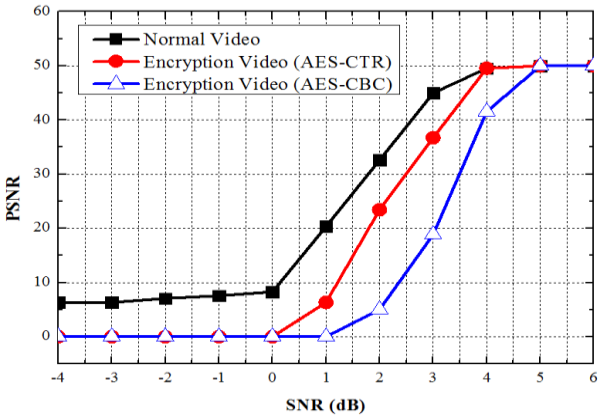


(B)

Fig. 8: RMSE for Changed Plain-text Size (A) Case 1 (B) Case 2

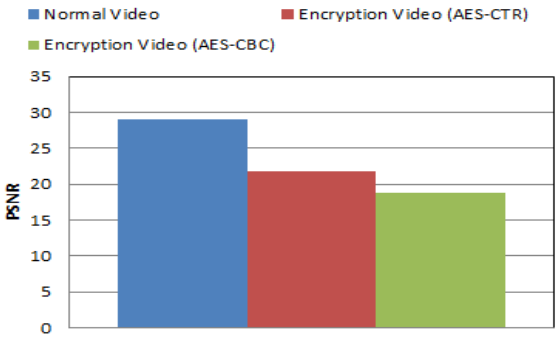


(A)

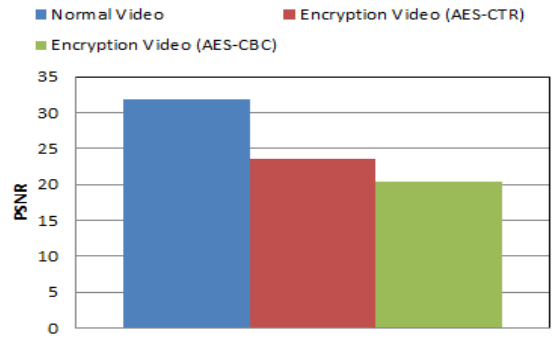


(B)

Fig. 9: PSNR for Changed Plain-text Size (A) Case 1 (B) Case 2



(A)



(B)

Fig. 10: Average of PSNR for Changed Plain-text Size (A) Case 1 (B) Case 2

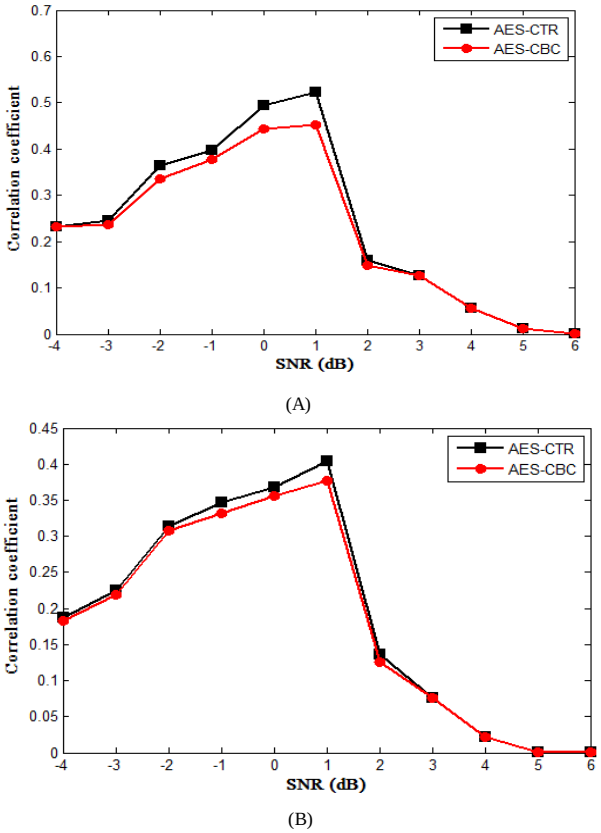


Fig. 11: BER vs PSNR Correlation Coefficient for Changed Plain-text Size (A) Case 1 (B) Case 2

The key impacts on mobile communication represent errors using the correlation of BER and PSNR. The cross-correlation coefficient between two different axes, BER on the x axis and PSNR on the y axis, is calculated as follows.

(A) (B)

Fig. 12: Recovered Images (A) AES-CTR (B) AES-CBC

$$\rho(x,y)=\frac{\sum_{i=1}^{N}(x(i)-\bar{x})(y(i)-\bar{y})}{\sqrt{\sum_{i=1}^{N}(x(i)-\bar{x})^2\sum_{i=1}^{N}(y(i)-\bar{y})^2}} \quad (12)$$

Fig. 11 shows the correlation between BER and PSNR when the encryption process is not applied. If plain size is small, the key error suggests a result opposite to the simulation results. Because it is often the key value when key error occurs, the error occurs more often on the plain. Thus, when plain size is increased, the effect of key errors on mobile communication is reduced.

Fig. 12 shows images from decryption in AES-CTR and CBC modes. These images were decoded by the same 2 dB SNR. In CBC encryption mode, all bits in a decoding error of the decoded image are damaged, so we can see the effect in the next stage. In CBC mode, the effect of two key errors is smaller than CTR mode. Therefore, increasing size of the plain-text when it is passed through mobile communication is helpful in reducing the effect of key errors.

5. Conclusion

This paper analyzed the performance difference from changing size of the plain-text using images of 12 Mbps as input data in four channels of the MF-TDMA based next-generation mobile communication channel. The conventional encryption analysis system has an effect on the key and its error AES algorithm. The key value of decoded data passed through a separate mobile channel affects total error. First, when encrypted data are based on MF-TDMA mobile channel through the key value and if there is no error in the AES algorithm itself, the error originated by the firing key value affects the entire plain-text data. We used rounded number of the 10 individual AES-128 (CTR, CBC) modes. Increasing size of the plain-text when it is passed through mobile communication is helpful in reducing the effect of key errors. The results confirmed that CTR mode of key error analysis has greater effect. Based on image decoding, it was confirmed that CTR mode has desirable reconstruction ratio and that an error in the plain-text data does not affect subsequent errors.

Acknowledgement

1. This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (2017R1D1A1B03032420).
2. This work was partly supported by Convergence Technology Development Project, Small and Medium Business Administration [S2450063, Development of HMD AR system based on AR source embedded display and smart device camera].

References

[1] Andriyanova I, Soljanin E, "Optimized IR-HARQ Schemes Based on Punctured LDPC Codes Over the BEC", *IEEE Transactions on Information Theory*, Vol.58, No.10, (2012), pp.6433-6436.
[2] Tonde AR, Dhande AP, "Implementation of Advanced Encryption Standard (AES) Algorithm Based on FPGA", *International Journal of Current Engineering and Technology*, Vol.4, No.2, (2014), pp.1048-1050.
[3] Sumitra, "Comparative Analysis of AES and DES security Algorithms", *International Journal of Scientific and Research Publications*, Vol.3, No.1, (2013), pp.1-5.
[4] Bhalerao PV, Ghongade RD, Langote VB, "Hardware Implementation of Cryptosystem by AES Algorithm Using FPGA", *International Journal of Computer Science and Mobile Computing*, Vol.6, No.5, (2017), pp.84-89.
[5] Yan J, Chen F, "An Improved AES Key Expansion Algorithm. International Conference on Electrical", *Mechanical and Industrial Engineering (ICEMIE)*, (2016), pp.113-116.
[6] Shekhar S, Singh P, Jaiswal M, "An Enhanced AES Algorithm Based on Variable Sbox And 200 Bit Data Block", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol.4, No.4, (2016), pp.6470-6477.
[7] Ning L, Kanfeng L, Zhongliang D, "A Joint Encryption and Error Correction Method Used in Satellite Communications", *China Communications*, Vol.11, No.3, (2014), pp.70-79.
[8] Olteanu A, Xiao Y, Zhang Y, "Optimization Between AES Security and Performance for IEEE 802.15.3 WPAN", *IEEE Transactions on Wireless Communications*, Vol.8, No.12, (2009), pp.6030-6037.
[9] Haleem MA, Mathur C, Chandramouli R, Subbalakshmi KP, "Opportunistic Encryption: A Trade-off between Security and Throughput in Wireless Networks", *IEEE Transactions on Dependable and Secure Computing*, Vol.4, No.4, (2007), pp.313-324.
[10] Choi JH, "On Large Deviations of HARQ with Incremental Redundancy over Fading Channels", *IEEE Communications Letters*, Vol.16, No.6, (2012), pp.913-916.