Ubiquitous 환경 하에서 고장 극복 암호 및 데이터 압축

Fault Tolerant Encryption and Data Compression under Ubiquitous Environment

유영갑*, 김한벼리*, 박경창*, 이상진*, 김승열*, 홍윤기**
충북대학교 정보통신 공학과*, 충북대학교 전자 공학과**

Younggap You(ygyou@cbnu.ac.kr)*, Hanbyeori Kim(hbkim@hbt.cbnu.ac.kr)*,
Kyungchang Park(kcpark@hbt.cbnu.ac.kr)*, Sangjin Lee(sjlee@hbt.cbnu.ac.kr)*,
Seungyoul Kim(kimsy@hbt.cbnu.ac.kr)*, Yoonki Hong(ykhong@dsd.cbnu.ac.kr)**

요약

본 논문은 암호화된 영상 데이터가 유비쿼터스 환경 하에서 무선 간섭에 의한 랜덤 오류를 가질 때 복호화 과정의 오류 산사태에 대한 해결책을 제시하였다. 영상 획득 장치는 영상 압축과 암호화 기능을 가지고서 데이터 트래픽 양을 줄이고 개인 정보를 보호하도록 구성한다. 블록 암호 알고리즘은 암호문의 단일 비트 오류가 여러 개의 픽셀 결함을 유발하는 산사태 효과를 겪을 수 있다. 새로운 고장 극복 방식은 오류의 산사태 효과를 다루는데 3 차원 데이터 셔플을 활용하여 에러 비트를 여러 프레임으로 분산시켜서 고립된 영상 결함으로 나타나도록 한다. 인접 화소 값에 대한 평균화 또는 다수결 회로는 에러정정을 위한 데이터 증가 없이 두드러져 보이는 화소 결함을 극복하도록 한다. 이 방식은 기존 Hamming code 방식보다 33% 적은 데이터 트래픽 부하를 가진다.

■ 중심어 : | 산사태 효과 | 고장 극복 | 이산 웨이블렛 변환 |

Abstract

This paper presents a solution to error avalanche of deciphering where radio noise brings random bit errors in encrypted image data under ubiquitous environment. The image capturing module is to be made comprising data compression and encryption features to reduce data traffic volume and to protect privacy. Block cipher algorithms may experience error avalanche: multiple pixel defects due to single bit error in an encrypted message. The new fault tolerant scheme addresses error avalanche effect exploiting a three-dimensional data shuffling process, which disperses error bits on many frames resulting in sparsely isolated errors. Averaging or majority voting with neighboring pixels can tolerate prominent pixel defects without increase in data volume due to error correction. This scheme has 33% lower data traffic load with respect to the conventional Hamming code based approach.

■ keyword : | Avalanche Effect | Fault Tolerance | Discrete Wavelet Transform |

I. 서 론

Mobile imaging systems proliferate as computer and communication network technology advances. Image data has been one of the major sources of heavy data traffic and requires efficient data

* This work was supported by the research grant of the Chungbuk National University in 2007.
접수번호 : #090713-002
접수일자 : 2009년 07월 13일
심사완료일 : 2009년 08월 04일
교신저자 : 유영갑, e-mail : ygyou@cbnu.ac.kr

compression to use bandwidth limited radio channels. Security issues are major problems to make data handling systems valuable by meeting public demands on the privacy and property protection. Efficient data compression and ciphering has become the core of the security measures to satisfy the requirements on security and data traffic under ubiquitous environment.

The discrete wavelet transform (DWT) has been one of valuable tools to compress data with two filter functions: high and low pass filters. The original image can be restored using the filtered image with an image quality control measure.

Two fundamental concepts of the cryptic algorithm, diffusion and confusion, make it extremely difficult to deduce the encryption key through analysis of the relationship among original and encrypted images. The diffusion and confusion may bring avalanche effect on the decrypted message when a transmitted encrypted message comprises erroneous bits.

A ubiquitous image transmission system is to be made include several distinct functions such as CMOS image sensor, memory, ultra wideband communication, DWT and AES blocks as shown in [Figure 1] The system can be built on multiple silicon die packaging.

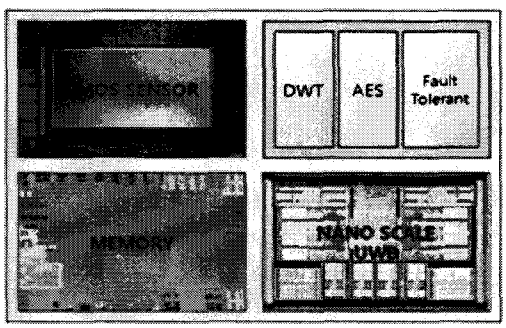


Figure 1. System on chip structure for ubiquitous image capturing and transmission

Some works have devoted to this error correction problem. Tae and Rhee proposed an application of the error correcting code in the stream cipher system aiming at the minimization of error propagation, error recovery and authentication[1]. Yang studied the application of the coding theory with wire-tap channels.[2] These results, however, did not address the avalanche effect of error spreading during the deciphering process. Another approach was to introduce fault tolerant circuits based on data shuffling and error correction codes[5]. This conventional error correction scheme brings substantial data traffic overhead due to additional bits for error correction.

This paper describes a robust model employing data compression for data traffic reduction and pixel defect recovery. It employs a data shuffling method to tolerate errors in encrypted messages due to noisy communication environment[5], The data shuffling and inverse shuffling sequences have revised to accommodate the filtering of prominent erroneous pixels. It opens a way to spread erroneous bits over many image frames so that the data filtering can easily correct them.

This paper is organized as follows. Chapter II introduces the new approach and explains the avalanche effect of errors. Chapter III shows operations of the new method. Finally Chapter VI concludes with evaluation.

II. 데이터 재배열과 오류 정정

Bit errors can be tolerated with data shuffling, filtering and averaging with neighboring pixels. The algorithm exploits inherent characteristics of continuous pixel data streams of a video clip.

1. Error Propagation

The AES algorithm complies with the two encryption principles, diffusion and confusion, proposed by C. Shannon[4]. Diffusion and confusion are to make it difficult to deduce the encryption keys by concealing the statistical relationship among originals and their corresponding encrypted messages. The detailed discussion in this paper is based on the AES algorithm, and applicable to other algorithms such as ARIA without modification, which is also a block cipher algorithm based on a substitution-permutation network[3].

Avalanche effect of erroneous bits is the consequences of the confusion and diffusion of block cipher algorithms. A single bit error in the encrypted messages may generate many erroneous bits in the text after decryption. One bit change in the original message may affect the half of the text bits after a ciphering process due to the high level of confusion and diffusion, which may be unrecoverable without a fault tolerant measure.

2. Compression and Encryption Scheme

The proposed method addresses the data recovery even though the decrypted message suffers severe damage due to the avalanche effect. The scheme is to spread the erroneous bits to multiple frames through a data shuffling process, and to place error bits at sparsely isolated locations.

The proposed scheme begins with compression of a plain image data as shown in [Figure 2] The DWT algorithm is used here followed by data shuffling. The AES algorithm will be used then to produce an encrypted text. The compressed, shuffled and encrypted messages are transmitted and may suffer some bit errors. The received data will be decrypted and shuffled inversely. Erroneous bits spread over a set of image frames resulting in sparsely isolated erroneous bits that can be repaired using averaging or majority voting of neighbor pixels. Then the decompression brings back the original image.

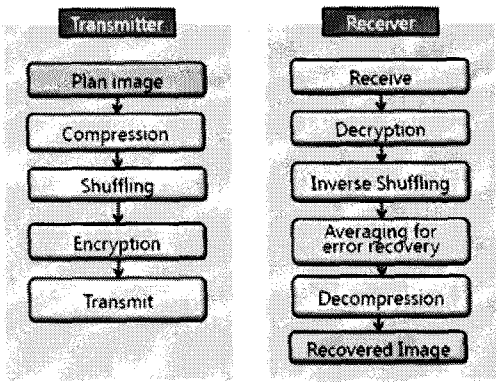
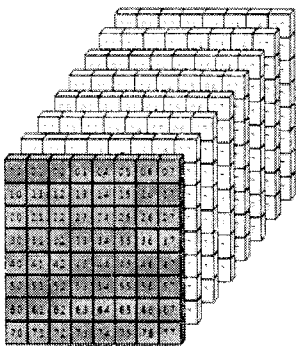


Figure 2. Block diagram of the new method

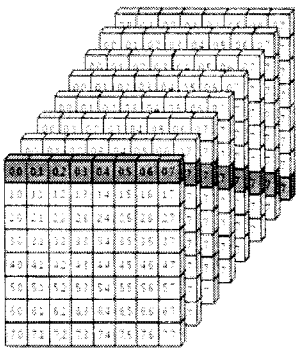
2.1 Data Shuffling

The conceptual shuffling process introduced here is as follows. The procedure starts with the original data frames shown in [Figure 3]a. Each row of the pixel data in a frame is sent to the subsequent frames in turn, yielding intermediate results shown in [Figure 3]b. Then diagonal shifting is performed on each frame as shown in [Figure 3]c. The final cubic structure comprising shuffled pixel data is illustrated in [Figure 3]d, which will be used for the subsequent encryption steps. The inverse shuffling of the receiver traces back the shuffling sequences in the reverse order.

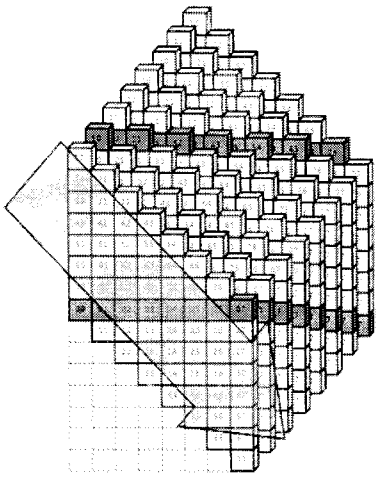
The shuffling process can be defined as follows. It is to spread adjacent bits to the locations with different row and column so that one row or column of data may not share the same row or the same column. A set of data bits forms a data matrix. Here k is the index in a data bit stream.



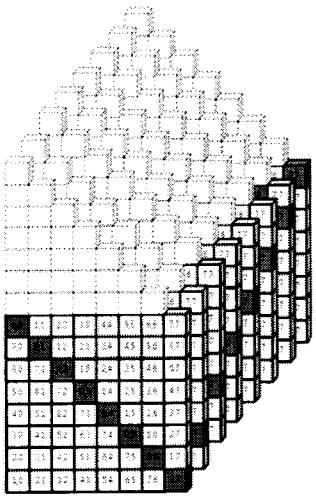
(a) Original image



(b) Row pixels shifted to subsequent frames



(c) Diagonally shifted data



(d) Shuffled image data

Figure 3. Three-dimensional shuffling process

The matrix D represents the original data. The matrix A represents the shuffled data matrix. D_{xy} (A_{ij}) represents the original (the shuffled) data value at the $x^{th}(i^{th})$ row and the $y^{th}(j^{th})$ column. p is the number of rows of the matrix D (A) and also the number of bits in a row. n is the odd number of shifts during the shuffling. The matrix D is obtained from the encrypted bit stream using equations (1) and (2).

$$x = [(k-y)/p] \bmod p \quad (1)$$

$$y = k \bmod p \quad (2)$$

The shuffling maps the x and y values onto the i and j values, respectively. Equations (3) and (4) define this mapping.

$$i = [(p-x) + (2n+1) \times y] \bmod p \quad (3)$$

$$j = y \quad (4)$$

The example shown in [Figure 3] assumes $n = 1$. The resultant shuffled data matrix shows that the adjacent data bits in a row or column place apart.

The error infected received data are subject to inverse shuffling to recover the original data. The

inverse shuffling is the reverse sequences of the shuffling operation. It is described in equations (5) and (6).

$$x = [(p-i)+(2n+1)\times j] \bmod p \quad (5)$$

$$y = j \quad (6)$$

Error may corrupt one row of the received data during transmission. One row of the matrix A may be erroneous. Only one bit error may be found in one row after reshuffling. Burst error bits in the decrypted image are spread out to other rows so that each row may have only one error bits.

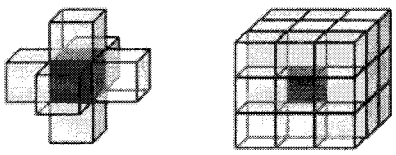
2.2 Image Recovery

Error bits in a pixel may or may not affect the image quality depending on the relative significance with respect to its neighboring pixels. The conspicuous defects in images should be alleviated to maintain the image quality level. The pixel data error can be fixed in various ways such as error correction based on a Hamming code[5] or filtering of abrupt pixel data changes. Each of luminance and chroma data of a frame can be treated as a black and white image. Discussion on black and white images can be extended over color images without loss of generality.

The low frequency in pixel data changes can be used for error correction purposes. Pixel data in the time axis does not change abruptly in most video data streams. Since the camera panning speed is much slower than human eye movement, most video images experience smoother pixel data variation than visual perception capability.

Erroneous bits spread over many frames resulting in sparsely isolated erroneous bits in a frame. If an erroneous bit of a pixel carries substantially different values, the pixel appears conspicuous. A filter such as a high pass DWT filter can identify isolated pixels with big differences from neighboring pixels. Filter coefficients can be selected to identify prominent pixels reflecting the ambient noise level.

The conspicuous pixel data can be fixed using averaging on analog values or majority voting only for an isolated defective pixel and its six surrounding pixels of three neighboring image frames. The seven-pixel neighborhood scheme includes front, back, upper, lower, left and right pixels as shown in [Figure 4]a : the erroneous pixel (shaded dark) at the center and six surrounding pixel. The twenty seven-pixel scheme comprises all the 26 pixels surrounding the erroneous pixel as shown in [Figure 4]b. This correction step can effectively compensate noise effect on the received and decrypted image due to pixel data errors. The resultant images go through the decompression stages to get the original data.



(a) 7-cell scheme (b) 27-cell scheme

Figure 4. Neighborhood schemes

The effect of most erroneous bits can be alleviated with the help of data values of neighboring pixels. The scheme can repair most sparsely located random pixel data corruption preventing serious image quality degradation.

III. 실 험

The error correction process has been demonstrated using computer simulation of the AES with a Hamming code for error correction. Shuffling and inverse shuffling can effectively spread out erroneous data to sparsely apart locations. [Figure 5] demonstrates the error correction process using a

simple memory map.

In the original text for demonstration, one row of data carries four bytes in this example. The AES can take 128 bits as an input. The data represented here are hexadecimal numbers. For the encrypted message error correcting codes such as Hamming codes are generated based on this encrypted bit patterns. Shuffling process yields the bit pattern as shown in the third item in [Figure 5]. This bit pattern will be transmitted.

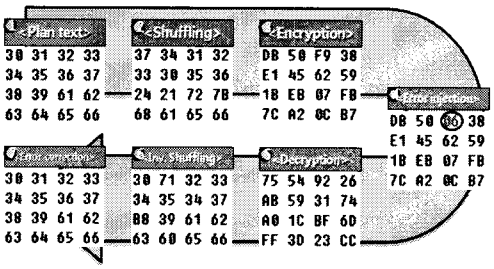


Figure 5. Data shuffle and error correction

The burst bit errors are illustrated as the circled value "06" in the 4th pattern which differs from the value "F9" in the 3rd pattern due to error. The received data goes through inverse shuffling so that adjacent bits in a row do not share the same row or column. The resultant bit pattern after the inverse shuffling is shown in the 5th data pattern in the figure.

For a video data stream, we introduce a more efficient image recovery method to suppress effects of random errors. The method described here does not introduce additional error correction bits. The error recovery is based on data filtering of partial functions of the discrete wavelet transform and averaging with ambient pixel values. Error correction based on Hamming codes is performed mainly for numeric data[5]. The error correcting code based system may bring additional data traffic to include error correcting code bits.

The demonstration of the scheme uses a video clip of scrolling a photo representing a camera panning upward. [Figure 6] shows the resultant video clip used as an experiment target. Multiple image frames are overlapped to form a three dimensional pixel array. The horizontal plane designated with the dotted rectangle represents the image frame along the time axis. [Figure 7]a is the time axis image frame of the video clip shown in [Figure 6]. This image goes through the DWT process and the resultant filtered images are shuffled, encrypted and transmitted.

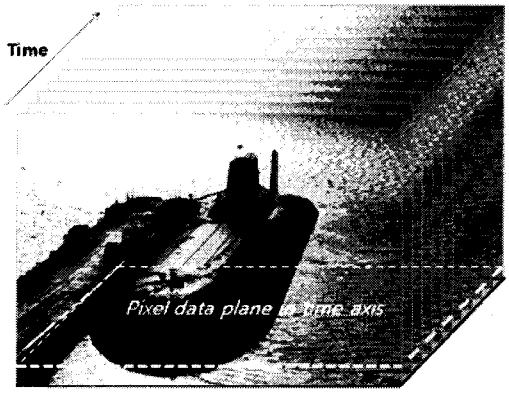
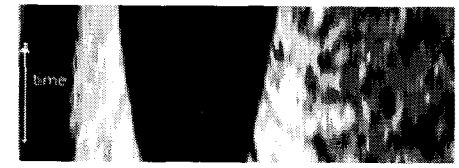


Figure 6. An upward panning video clip

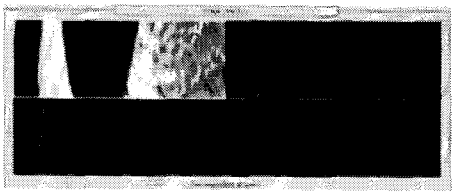
The received image may comprise erroneous bits. The subsequent decryption process will bring substantial bit errors due to avalanche effect. Shuffling spreads the error bits over the multiple frames in the video clip leaving sparsely isolated erroneous bits on each smooth frame. Most erroneous bits are recovered using the DWT filtering algorithm. [Figure 7]b shows the four images (LL, LH, HL, HH images) obtained through the 2D DWT filtering, which are subject to shuffling and encryption before transmission.

Noise in the communication channel may corrupt the encrypted image. We assume a single bit error in the received image, which will generate substantial

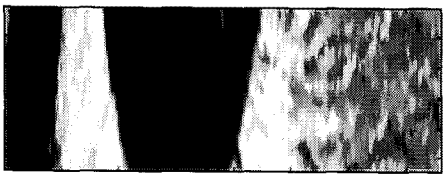
erroneous bits after decryption. The shuffling will spread the erroneous bits over many image frames resulting in sparsely isolated pixel defects. High pass DWT filtering will identify target pixels to be corrected. Averaging or majority voting with neighboring pixels data is to eliminate severe pixel defects such as isolated white(black) dots on a black (white) background.



(a) Time axis image



(b) DWT filtering image



(c) Recovered image

Figure 7. Image compression in the time axis

Data redundancy of 50% additional error correcting bits of the error correcting scheme[5] is not necessary in this case. The scheme does not introduce additional error correction bits, and reduces the channel traffic substantially. Preliminary estimation of the image quality shows that the resultant peak signal to noise ratio is around 63dB for 98% of energy retained.

IV. 결 론

A novel fault tolerant algorithm is presented to alleviate error avalanche effect due to the erroneous bits in the cipher text. The new scheme employs the three-dimensional data shuffling operation to spread out erroneous bits to many image frames. The resultant data patterns make it easy to correct erroneous bits through filtering.

The fault tolerant method has been applied to the AES algorithm together with the DWT. This method can easily extend over other block cipher algorithms such as ARIA without any difficulty. The additional hardware requirements are minimal since it simply relocates the data on different locations. It does not involve any additional bits for error correction, and thereby does not bring any significant traffic load increase in ubiquitous environment. The scheme can be used for many applications requiring high security and reliability for some noisy mobile communication.

참 고 문 헌

[1] Y.-S. Tai and M.-Y. Rhee, "A study on the stream cipher system using error correcting codes," J. Korea Institute of Information Security and Cryptology, Vol.1, No.1, pp.66-78, 1991.

[2] K.-C. Yang, "An application of coding theory to cryptography," J. Korea Institute of Information Security and Cryptology, Vol.3, No.2, pp.36-42, 1993.

[3] J. Park, "Design and implementation of ARIA cryptic algorithm," J. KIEE, Vol.42-SD, No.4, pp.29-36, 2005(4).

[4] C. E. Shannon, "Communication theory of secrecy system," J. Bell System Tech., Vol.28, pp.656-715, 1949.

[5] Y. G. You, R. H. Park, Y. I. Ahn and H. B. R. Kim, "Fault tolerant cryptography circuit for data transmission errors," J. Korea Contents Assoc., Vol.8, No.10, pp.37-44, 2008(10).

[6] S. Y. Shin, H. S. Park, S. H. Choi, and W. H. Kwon., "Packet error rate analysis of ZigBee under WLAN and Bluetooth interferences," IEEE Trans. Wireless Comm., Vol.6, No.8, pp.2825-2830, 2007.

[7] L. Vreveglieri, I. Koren, and P. Maistri, "An operation-centered approach to fault detection in symmetric cryptography ciphers," IEEE Trans. Comput., Vol.56, No.5, pp.635-649, 2007.

[8] S. Mallat, *A Wavelet Tour of Signal Processing*, Academic Press, Inc, 1999.

저 자 소 개

유 영 갑(Younggap You) 정회원

- 1986년 4월 : Univ. of Michigan, Ann Arbor 전기전산학과(공학박사)
- 1988년 ~ 현재 : 충북대학교 정보통신공학과 교수

<관심분야> : VLSI 설계 및 Test, Cryptography

김 한 벼 리(Hanbyeori Kim) 준회원

- 2008년 2월 : 충북대학교 전자 공학과 (공학사)
- 2008년 3월 ~ 현재 : 충북대학교 정보통신 공학과 석사 과정

<관심분야> : Cryptography, Digital system design

박 경 창(Kyungchang Park) 준회원

- 2008년 2월 : 충북대학교 전자 공학과(공학사)
- 2008년 3월 ~ 현재 : 충북대학교 정보통신 공학과 석사 과정

<관심분야> : Cryptography, Digital system design

이 상 진(Sangjin Lee) 준회원

- 2008년 2월 : 충북대학교 화학 공학과(공학사)
- 2008년 3월 ~ 현재 : 충북대학교 정보통신 공학과 석사 과정

<관심분야> : Cryptography, Digital system design

김 승 열(Seungyoul Kim) 정회원

- 2002년 2월: 충북대학교 정보통신공학과(공학사)
- 2004년 8월: 충북대학교 정보통신공학과(공학석사)
- 2005년 3월 ~ 현재 : 충북대학교 정보통신 공학과 박사과정

<관심분야> : 디지털 회로설계, Cryptography, ASIC 설계

홍 윤 기(Yoonki Hong) 준회원

- 2009년 2월 : 충북대학교 전자 공학과 (공학사)
- 2009년 3월 ~ 현재 : 충북대학교 전자 공학과 석사 과정

<관심분야> : 디지털 IC 설계, DWT