JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 8 : 1589~1596 Aug. 2017

워터마킹 기반의 암호동기신호 전송 및 검출

손영호[1] · 배건성[2*]

Watermarking-based cryptographic synchronization signal transmission and detection

Young-ho Son[1] · Keun-sung Bae[2*]

[1]Attached Institute of ETRI, Daejeon 34129, Korea
[2*]School of Electronics Engineering, Kyungpook National University, Daegu 41566, Korea

요 약

동기식 암호통신은 암호기와 복호기 간에 암호동기를 일치시키기 위하여 동기신호를 암호문에 부가하여 전송한다. 따라서 평문통신에 비하여 데이터 전송률이 낮아지고 전송 지연이 발생하게 되는데, 특히 무선채널과 같이 열악한 환경 등에서는 동기신호의 주기적인 전송이 요구되므로 동기신호 전송 방식은 암호통신의 품질을 좌우할 수 있다. 본 논문에서는 암호통신에서 전송 대역의 추가 없이 동기신호를 전송할 수 있는 새로운 형태의 동기신호 전송 기법과 이를 이용한 재동기 방식을 제안하였다. 제안한 방법에서는 동기신호를 전송 데이터 내에 워터마크 형태로 삽입하여 전송하고, 수신기에서 추출된 워터마크로부터 동기신호를 검출한다. 영상 데이터를 대상으로 한 모의실험을 통해 제안한 워터마킹 기반의 동기신호 전송 방법이 전송률 측면에서 효율적이며, 동기 검출을 안정적으로 지원할 수 있음을 확인하였다.

ABSTRACT

In synchronous secure communications, a synchronization signal is transmitted over the same channel where ciphertext is transmitted for cryptographic synchronization between an encryptor and a decryptor, so, it causes data rate lowering and transmission delay for plain communication. Especially, in poor environments such as wireless channels and so on, since secure communications require a periodic resynchronization protocol, synchronization signal transmission method can dominate its quality. In this paper, we proposed a new synchronization signal transmission method without additional bandwidth as well as resynchronization protocol based on it. We embeded a synchronization signal as a watermark in a transmission image and restored it from a detected watermark in the decryptor. Experimental results of image have demonstrated that the proposed synchronization signal transmission method using watermarking is efficient in transmission rate and can support reliable synchronization detection.

키워드 : 워터마킹, 동기신호, 재동기, 암호통신

Key word : Watermarking, Synchronization signal, Resynchronization, Secure communication

Received 17 April 2017, **Revised** 26 April 2017, **Accepted** 11 May 2017

* **Corresponding Author** Keun-sung Bae(E-mail:ksbae@ee.knu.ac.kr, Tel:+82-53-950-5527)
School of Electronics Engineering, Kyungpook National University, Daegu 41566, Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.8.1589 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

암호통신은 송신자가 암호 알고리즘과 암호키를 이용하여 데이터를 제 3자가 알아보기 어려운 형태로 암호화하여 보내고, 동일한 암호 알고리즘과 복호키를 가진 수신자만이 암호문을 해독할 수 있도록 하는 정보 전송 방식이다. 암호통신에서 전송 데이터의 암호화와 복호화는 암호 알고리즘과 키를 이용하여 이루어지는데, 암호 알고리즘은 암호화와 복호화에 동일한 키를 사용하는 비밀키 암호와 수학적으로 연계된 서로 다른 두 개의 키를 사용하는 공개키 암호로 구분된다. 일반적으로 전송 데이터 암호화에는 공개키 암호에 비하여 알고리즘이 간단하여 경량화와 고속 동작에 유리한 비밀키 암호가 사용된다[1].

비밀키 기반의 암호통신에서 수신된 암호문이 제대로 복원되기 위해서는 송신기와 수신기 간에 암호키와 복호키가 동일하여야 하며[1], 스트림 동기가 일치해야 한다[2,3]. 암호 시스템은 암호기에서 출력된 수열과 복호기에 입력되는 수열을 동기시키는 방법에 따라 동기식 암호 시스템과 자기동기식 암호 시스템으로 나누어진다[2,3]. 동기식 암호 시스템은 암호기의 출력이 평문이나 암호문과는 독립적으로 이루어지는 방식으로서 암호기에서 생성되는 암호문에 별도의 동기신호를 부가하여 전송하고, 복호기에서 이를 검출하는 방법으로 동기를 일치시키게 된다. 자기동기식 암호 시스템은 암호기에서 출력된 데이터 수열이 복호기로 입력되면 일정시간이 경과하면 자동으로 암호기와 복호기간에 동기가 일치되는 방식이다. 자기동기식 암호 시스템은 별도의 동기신호를 필요로 하지 않지만 전송 중 암호문에 오류가 발생하면 복호문에서 오류 전파 현상이 발생하기 때문에 비트 오류율(BER:Bit Error Rate)이 높은 채널에서는 대부분 동기식 암호 시스템을 사용한다[3].

동기식 암호 시스템은 채널의 품질, 통신모드 등에 따라서 동기신호를 암호통신 진입 단계에서 한번만 보내거나, 통신 중에 반복하여 보낼 수 있다. 그러나 기존의 동기신호 전송 방식[2,3]에서는 동기신호를 전송 데이터에 단순히 부가하여 전송함으로써 평문 통신에 비하여 데이터 전송률이 낮아지고, 통신 지연이 발생하는 문제점이 있으며[3], 통신 시스템에 따라서 동기신호의 반복적인 부가에 필요한 전송 대역 확보가 어려운 경우도 있다. 따라서 암호통신의 성능 향상을 위하여 동기신호의 신뢰성 있는 검출을 보장하면서, 전송 효율을 높일 수 있는 동기 신호 전송 방법에 대한 연구가 필요하다. 본 논문에서는 동기식 암호 시스템에서 동기신호 전송으로 인한 데이터 전송 효율 저하와 전송 지연 문제점을 해결할 수 있는 방안으로, 동기신호를 전송 데이터에 워터마킹 형태로 삽입하여 전송하는 기법과 이를 이용한 재동기 방식을 제안하였다. 정지영상을 대상으로 한 동기신호 전송 및 검출 모의실험을 통하여 워터마킹 기반의 제안한 방식이 동기식 암호 시스템의 전송률 측면에서 효율적이며, 동기 검출을 안정적으로 지원할 수 있음을 확인하였다.

본 논문의 구성은 다음과 같다. 2장에서는 먼저, 암호통신에서 일반적인 동기신호 전송 방법에 대하여 소개하고, 워터마킹 기반의 동기신호 전송 및 검출 방법에 대하여 설명한다. 3장에서는 정지영상 데이터를 대상으로 동기신호를 워터마킹하여 전송하고 검출하는 모의실험 결과를 제시하고, 4장에서 결론을 맺는다.

Ⅱ. 워터마킹 기반의 동기신호 전송

2.1. 암호 시스템에서 동기신호 전송 방법

그림 1은 일반적으로 암호통신에서 필요로 하는 동기신호(SYNC)의 전송 방법을 개념적으로 보인 것이다[2,3]. 그림 1의 (a)에서 제시한 초기동기 방식은 암호통신을 시작할 때 암호기와 복호기 간에 동기신호를 교환하여 암호동기를 일치시키는 방법으로, 사이클 슬립 현상[3,4] 등으로 인하여 동기 이탈 현상이 발생하면 스스로 동기를 회복할 수 없게 되어 해당 통신세션이 종료될 때까지 통신 불능상태가 된다. 따라서 시스템에서 해당 통신세션을 강제로 초기화하여야 하는 단점이 있다. 초기동기 방식은 재동기 기능의 부재로 채널 품질이 양호한 구간에서의 통신이나 짧은 시간 동안 이루어지는 통신에 제한적으로 적용할 수 있다[3]. 그림 1의 (b)에서 제시한 재동기 방식은 암호통신 진입 후에도 재동기를 위한 동기신호를 전송하는 방식으로, 단파채널과 같이 BER이 높은 무선 환경[5,6]에서 암호통신의 신뢰성을 향상시킬 수 있다. 그러나 주기적인 재동기 방식은 동기신호의 잦은 전송으로 전송 효율이 낮아지고 전송 지연이 발생하는 문제점 등으로 인하여 실제 적용에서는 어려움이 있다.

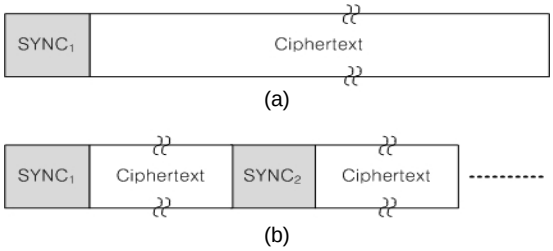

Fig. 1 Synchronization method in a secure communication

반면, 비주기적 재동기 방식은 동기 이탈이 검출되면 재동기를 수행함으로써 주기적 재동기 방식에서의 전송 효율 문제를 보완할 수 있으나, 해당 통신에서 사용하는 데이터 프레임이 갖는 특징을 이용한 동기 이탈 검출이 가능한 경우에만 적용할 수 있다는 단점이 있다[3].

일반적으로 동기신호는 신호 검출에 필요한 동기패턴(SP)과 알고리즘 등의 상태 동기에 필요한 동기 데이터(SKD)로 구성된다[2,3]. 그림 2는 기존 연구[2,3,7,8]에서 사용한 동기신호 구조로서, 동기 패턴과 동기 데이터를 연접한 형태의 동기신호 구조(그림 2 (a))와 최대길이 시퀀스(maximal length sequence)[9,10]로 동기 데이터를 마스킹한 형태의 동기신호 구조(그림 2 (b))를 비교하여 보인 것이다. 연접 형태의 동기신호는 상관특성 기반의 동기패턴 검출기로 동기신호를 검출하고[3], 마스킹 형태의 동기신호는 다수결 논리 복호기를 이용하여 동기신호를 검출한다[7,8]. 마스킹 형태의 동기신호는 동기신호 전 영역이 동기패턴과 동기 데이터로 활용되기 때문에 연접 형태의 동기신호에 비하여 잡음 환경에서 상대적으로 동기 검출에 장점이 있다[7,8].

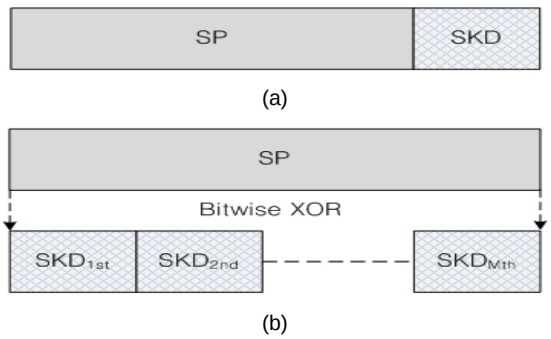

Fig. 2 Synchronization signal structures
(a) Concatenation structure (b) Masking structure

2.2. 워터마킹 기법을 이용한 동기신호 전송

디지털 워터마킹 기술은 디지털 콘텐츠의 저작권 보호를 목적으로 사람의 눈이나 귀를 통해 쉽게 감지하기 어렵게 디지털 문서, 이미지, 오디오, 비디오 등의 신호에 저작권 정보를 삽입하여 멀티미디어 저작물의 저작권 보호를 위해 제안되었다[11]. 디지털 워터마크란 디지털 데이터에 삽입된 후 검출되거나 추출될 수 있도록 원 신호에 추가된 신호를 의미한다. 그림 3은 정지영상에 워터마크를 삽입한 워터마킹 영상과 워터마킹 영상을 암호화한 영상을 예로 보인 것이다. 그림 3 (a)는 원 영상, (b)는 원 영상에 삽입하고자 하는 워터마킹 영상, (c)는 워터마크가 삽입된 영상이며, 마지막으로 (d)는 (c)를 암호화한 영상이다. 워터마크 삽입에 사용한 방법은 LSM(least significant modulation) 방식으로 영상 데이터를 표현하는 픽셀 값을 8비트 gray 스케일로 표현하고 워터마크 영상을 8비트 픽셀 값의 LSB(least significant bit) 위치에 직접 삽입한다[12,13].

기존 동기 방식에서 동기신호는 부가정보로 암호문에 연접되어 전송된다[2,3,7,8]. 초기동기 방식은 최초 암호문 앞에 동기신호를 연접하여 전송하고, 재동기 방식에서는 재동기가 이루어지는 시점의 암호문에 동기신호를 연접하여 전송하게 된다. 따라서 영상신호에 동기신호를 워터마크로 삽입하여 전송하는 방법에서도 동기 일치가 필요한 시점의 영상 데이터 앞부분에 동기신호가 워터마크로 삽입되어야 한다.

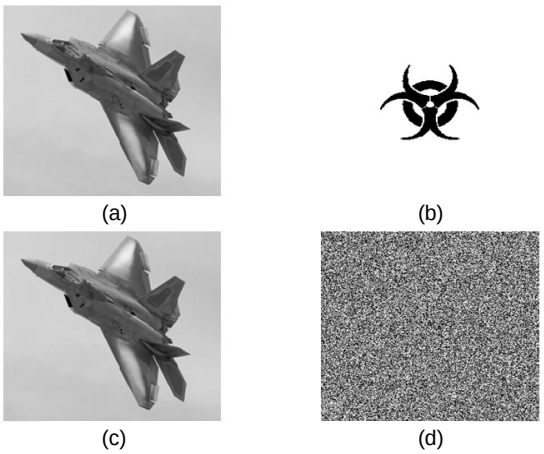

Fig. 3 Example of watermarked image encryption (a) Original image (b) Watermark (c) Watermarked image (d) Encrypted image

그림 4는 190비트 길이 동기신호를 LSM 워터마킹 기법을 이용하여 영상 단위로 삽입하여 전송할 때 동기신호를 삽입하는 과정을 개념적으로 보인 것이다. 송신기에서 생성한 동기신호를 영상 픽셀 내에 워터마크로 삽입하여 전송하고, 수신기에서 워터마크를 검출하여 동기신호를 검출함으로써 동기신호 전송을 위한 대역 추가없이 영상 단위로 암호 재동기를 이룰 수 있다.

그림 5는 헤더 없이 영상 데이터만 존재하는 raw 형식의 정지영상을 전송하는 암호 시스템에서 LSM 방식으로 동기신호를 전송 영상에 워터마크로 삽입하는 과정을 보인 것이다. 먼저 그림 5 (b)의 평문 데이터에서 워터마크로 대체될 영상 픽셀의 LSB를 제거한 후 암호화하여 (c)를 얻는다. 그리고 (d)와 같이 제거된 각 픽셀의 LSB 위치에 동기신호 (a)를 워터마크로 삽입한다. 그림 6은 190비트의 동기신호가 워터마크로 삽입되어 전송될 때 수신기에서 입력 스트림으로부터 동기신호를 검출하는 과정을 보인 것이다. 먼저 입력 스트림에서 영상파일의 시작점을 검출한 후 각 픽셀의 8번째 비트 값들을 추출하여 식 (1)과 같이 동기신호를 구성한다. 그러나 데이터 전송 중 비트가 삭제되거나 추가되는 사이클 슬립이 발생하는 경우에는 픽셀의 8번째 비트 값들이 그림 6에서 나타낸 위치에서 슬립이 발생한 비트 수만큼 당겨지거나 밀려서 입력될 수 있다. 예를 들어 1비트 삭제가 발생하면 190비트의 동기신호는 $[Bit_7 \| Bit_{15} \| \cdots \| Bit_{190*8-1}]$로 구성되며, 1비트 삽입이 발생한 경우는 $[Bit_9 \| Bit_{17} \| \cdots \| Bit_{190*8+1}]$로 구성된다. 그러나 동기신호가 삽입된 픽셀 구간에서 비트 슬립이 발생한 경우에는 해당 구간에서 동기 검출에 실패하게 된다.

$$SYNC = [Bit_8 \| Bit_{16} \| \cdots \| Bit_{190*8}] \quad (1)$$

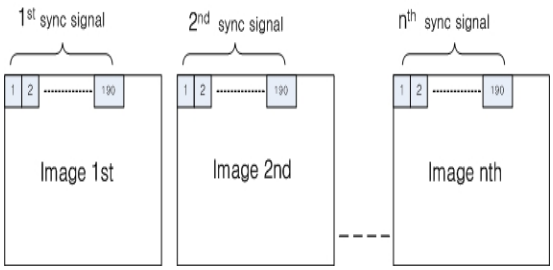

Fig. 4 Synchronization signal insertion in each image file

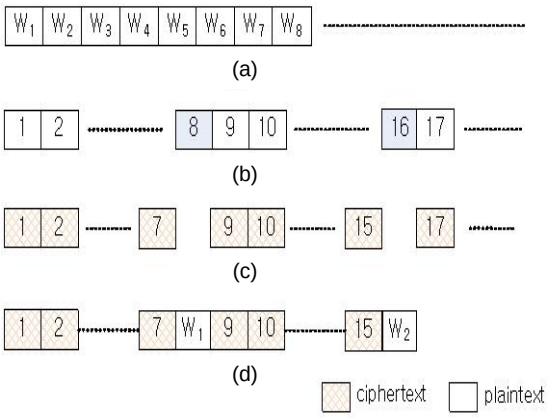

Fig. 5 Insertion procedure of a synchronization signal in a raw image file (a) Synchronization signal (b) Original image (c) Encrypted original image (d) Watermarked image

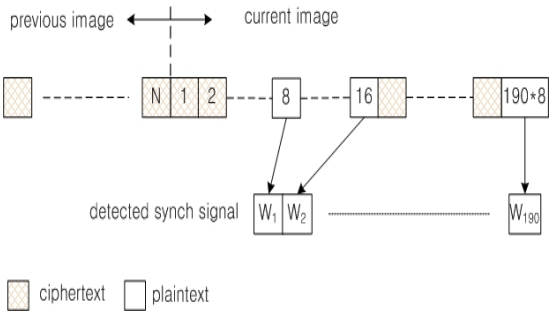

Fig. 6 Detection procedure of a synchronization signal in a watermarked image

앞에서 설명한 바와 같이 영상 데이터에 워터마킹 기법으로 암호동기신호를 삽입하여 전송하면 암호통신에서 동기신호 전송에 전송 대역을 추가하지 않고 송신기와 수신기 간에 영상 단위의 재동기가 가능하다. 그림 7은 워터마킹 기법을 이용한 영상파일 단위 재동기 방식의 개략적인 흐름도를 송신부와 수신부로 구분하여 보인 것이다. 송신부에서는 암호기로 입력되는 영상파일의 픽셀이 동기신호가 삽입되는 구간에 해당되고, 재동기 수행 조건이 충족되면 암호기의 상태를 갱신하고, 동기신호를 워터마크 형태로 삽입한다. 수신부에서는 입력되는 암호문 스트림이 동기신호가 워터마크로 삽입되어 있는 구간에 해당되면 워터마크가 존재하는 것으로 판단하여 워터마크를 검출한다.

이때 워터마크에서 동기신호가 추출되면 스트림 동기를 일치시키고, 추출된 동기 데이터로 복호기의 상태를 갱신하여 암호기와 알고리즘 동기를 이루게 된다. 수신부에서 입력 비트가 동기신호 삽입 구간에 해당하는지는 이전 영상파일의 시작점과 크기 값을 이용하여 판단할 수 있다. 예를 들어 raw 영상파일에 동기신호를 삽입하여 전송할 때, 이전 영상파일의 시작위치가 i번째 비트이면 다음 동기신호가 삽입된 구간은 식 (2)와 같이 정의할 수 있다. 식 (2)에서 size는 비트 단위의 영상파일의 크기를, L은 동기신호의 크기를 나타낸다.

LSM 알고리즘을 적용한 경우 수신부에서는 동기신호 구간에서 각 픽셀들의 LSB를 추출하여 동기신호를 구성한다. 식 (2)의 구간에서 검출된 동기신호는 식 (3)과 같이 구성된다.

$$SYNC_{region} = [Bit_{i+size} \sim Bit_{i+size+L\times 8-1}] \quad (2)$$

$$SYNC_{bit} = [Bit_{i+size+7-j} \| Bit_{i+size+15-j} \| \cdots \| Bit_{i+size+L\times 8-1-j}] \quad (3)$$

여기서 j는 비트 슬립이 발생할 때 삭제 또는 추가되는 비트 수를 의미한다.

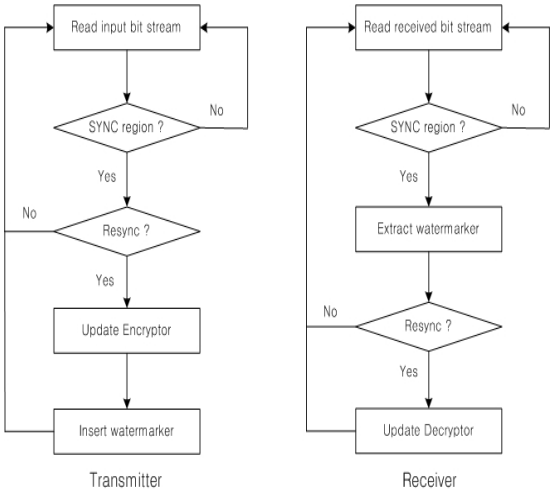

Fig. 7 Resynchronization method using watermarking

Ⅲ. 실험 및 검토

본 연구에서 제안한 동기신호 전송방식의 타당성과 동기 검출 성능을 분석하기 위하여 190비트 길이 동기신호를 256 x 256 크기의 raw 영상파일에 LSM 알고리즘을 이용하여 워터마크 형태로 삽입하여 랜덤 잡음이 부가된 채널로 전송하고 검출하는 모의실험을 수행하였다. 실험에서 사용한 동기신호는 그림 2에서 제시한 두 가지 방식으로 각각 구성하여 생성하였으며, 영상파일의 암호화에는 ARIA 암호[14]를 이용하였다.

그림 8은 42비트 동기 데이터에 BCH(63,45) 오류정정코드를 적용하고, 3회 반복하여 최대길이 시퀀스로 마스킹한 동기신호를 영상파일 시작 위치마다 워터마크로 삽입하고, 첫 번째 영상파일의 128 x 256 픽셀 위치에서 1비트 슬립을 발생시켰을 때, 수신기에서 동기신호를 검출하여 복호화 한 실험 결과를 보인 것이다. 비트 삭제가 발생한 위치부터 동기 이탈이 발생하여 수신기에서 영상 복호화에 실패하지만 두번째 영상에서는 동기신호를 바르게 검출하여 송신기와 재동기를 이룸으로써 암호화된 두번째 영상이 제대로 복원되는 것을 볼 수 있다. 그림 8 (b)의 Error 분포는 수신된 암호문에서 LSM 알고리즘으로 검출한 워터마크를 190비트 단위로 최대길이 시퀀스와 bitwise xor 연산을 한 후, 다수결 논리 복호기에 입력할 때, 실제 동기신호와 비트 단위로 불일치하는 오류 개수의 분포를 보인 것이다[8]. 동기신호와 일치하는 위치 1,520과 525,807에서 오류 개수가 '0'이고, 그외 구간에서는 30에서 60 사이의 분포를 보이는 것은 동기신호와 불일치하는 구간에서는 최대길이 시퀀스와의 bitwise xor 연산으로 다수결 논리 복호기의 입력 비트들이 랜덤하게 결정되기 때문이다. 그리고 두번째 영상에서 동기신호가 검출된 비트 위치 525,807는 식 (3)을 이용하여 계산한 동기신호의 최종 비트 위치 $Bit_{1+256\times 256\times 8+190\times 8-1-1}$ 와 일치하는 것을 볼 수 있다.

그림 9는 제안한 재동기 방식의 잡음 환경에서의 동기 검출 성능을 분석하기 위하여 동기신호가 워터마크 형태로 삽입된 암호화 영상을 랜덤 오류가 발생하는 채널로 전송하고, 수신기에서 동기신호를 검출하여 복호화한 영상을 보인 것이다. 동기신호는 그림 8에서와 같은 방법으로 구성하였다. 그림 9에서 보면 본 논문에서 제안한 워터마크 기반의 최대길이 시퀀스 동기신호 방

식에서는 전송채널의 BER이 0.1로 영상이 상당히 열화되는 수준의 열악한 잡음환경에서도 동기신호 검출이 가능하여 암호문을 해독할 수 있음을 볼 수 있다.

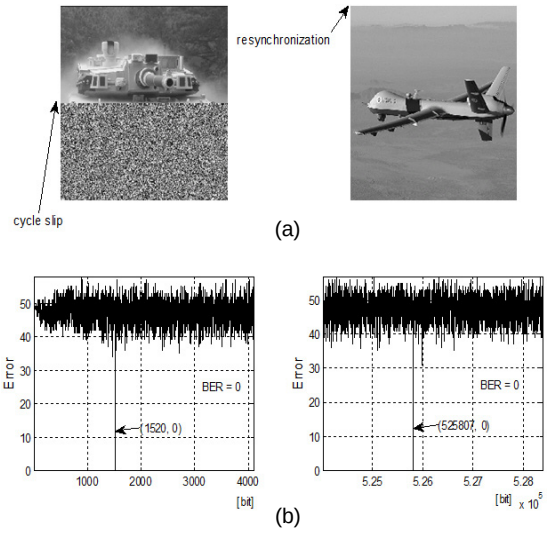

Fig. 8 Example of synchronization loss restoration by the proposed resynchronization method using watermarking (a) Decrypted image (b) Error distribution

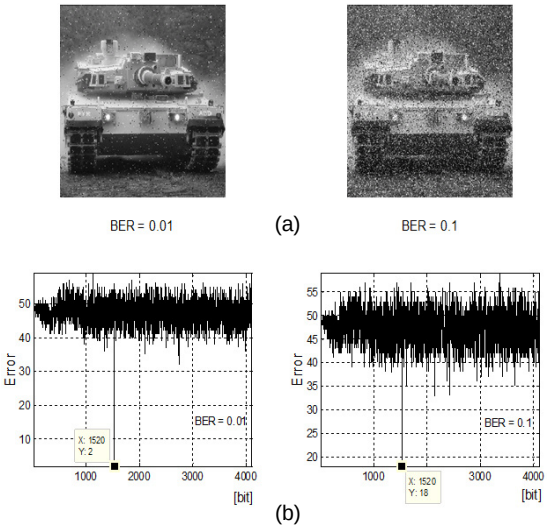

Fig. 9 Example of synchronization signal detection by the proposed resynchronization method using watermarking in random error environment (a) Decrypted image (b) Error distribution

그림 9 (b)의 Error 분포에서 그림 8 (b)와 달리 동기신호 구간에서 오류 개수가 각각 2, 18로 증가한 것은 채널의 전송품질 열화로 동기신호 구간에서 비트 오류가 증가하였기 때문이다. 그러나 다른 구간에서는 유사하게 나타나는 것을 볼 수 있다.

그림 10은 표 1에서와 같이 생성한 동기신호들을 raw 영상파일에 각각 워터마크 형태로 삽입한 후 랜덤 오류가 발생하는 채널로 전송하고 수신기에서 검출하는 모의실험에서, 채널의 BER에 따른 동기신호 생성 방법별 재동기 검출율을 비교하여 그래프로 보인 것이다. 실험 결과에서 BER이 높아질수록 최대길이 시퀀스 기반의 동기신호를 워터마크로 삽입하여 전송하는 동기 방식이 연접 형태의 동기신호를 사용하는 방식에 비하여 동기 검출 성능에서 상대적으로 우수함을 확인할 수 있다.

Table. 1 Synchronization signals used as watermark

Generation method	SYNC(190 bit)	
	SP(bit)	SKD(42 bit)
m-sequence based	190	BCH(63,45), 3 repetition
concatenation based	127	BCH(63,45)
	63	BCH(127,43)

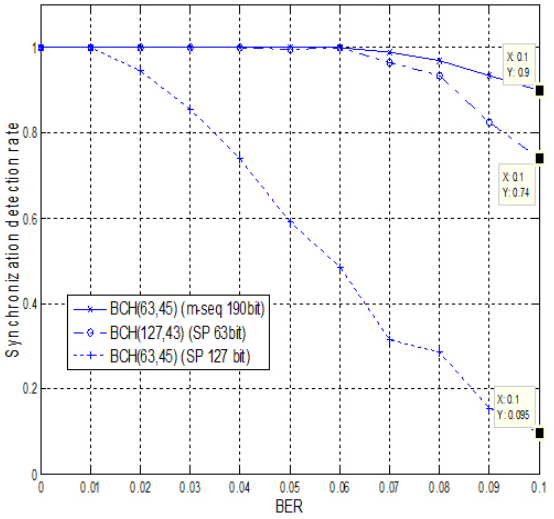

Fig. 10 Comparison of performance for synchronization signals in the proposed resynchronization method using watermarking

Ⅳ. 결 론

본 논문에서는 기존의 암호통신에서 열악한 채널환경에서는 동기신호의 잦은 전송으로 인한 데이터 전송 효율 저하와 전송 지연 문제를 해결할 수 있는 방안으로 동기신호를 전송 데이터에 LSM 방식의 워터마킹 형태로 삽입하여 전송하는 기법과 이를 이용한 재동기 방식을 제안하였다. 그리고 제안한 동기 방식을 정지영상의 암호화에 적용하여 다양한 BER을 갖는 채널에서의 전송 모의실험을 통해 암호 동기신호의 검출 성능을 분석하였다.

실험 결과로, 제안한 동기 방식은 데이터 전송률 측면에서 효율적이며 사이클 슬립으로 인한 동기 이탈과 다양한 수준의 잡음환경에서도 안정적인 암호동기 검출을 지원할 수 있음을 확인하였다. 제안한 동기신호 전송 방식은 전송 데이터가 워터마킹이 가능한 암호 시스템에서의 응용이 가능하며, 특히, 전송 오류 등으로 데이터 복원에 실패하여도 재전송이 이루어지지 않는 통신 환경에서 암호통신의 생존성을 향상시킬 수 있을 것으로 기대된다. 그리고 기존에 연구된 다양한 워터마킹 기법에도 적용할 수 있을 것으로 생각된다.

REFERENCES

[1] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton, FL: CRC press, 1996.

[2] H. J. Lee, “Highly reliable synchronous stream cipher system for link encryption,” in *Proceedings of International Conference on Computational Science and Its Applications*, pp. 269-278, 2006.

[3] J. H. Yoon, “A non-periodic random sequence resynchronization method using the address data of LAPB and HDLC,” Ph. D. Dissertation, Kyungpook National University, Daegu, Korea, 1997.

[4] V. Smirnova and A. V. Proskurnikov. “Phase locking, oscillations and cycle slipping in synchronization systems,” in *Proceedings of European Control Conference*, pp. 873-878, 2016.

[5] P. Eliardsson, E. Axell, P. Stenumgaard, K. Wiklundh, B. Johansson, and B. Asp, “Military HF communications considering unintentional platform-generated electromagnetic interference,” in *Proceedings of International Conference on Military Communications and Information Systems*, pp. 1-6, 2015.

[6] R. J. Sutton, *Secure Communications: Applications and Management*, Chichester, U.K.: John Wiley & Sons, 2002.

[7] Y. H. Son, J. K. Hong, and K. S. Bae, “Authentication masking code against DoS of T-MAC protocol,” *Journal of Central South University*, vol. 20, no. 7, pp. 1889-1895, Jul. 2013.

[8] Y. H. Son and K. S. Bae, “Cryptographic synchronization signal generation method using maximal length sequence,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 21, no. 7, pp. 1401-1410, Jul. 2017.

[9] A. Ahmad, S. S. Al-Busaidi, M. J. Al-Musharafi, “On properties of PN sequences generated by LFSR - A generalized study and simulation modeling,” *Indian Journal of Science and Technology*, vol. 6, no. 10, pp. 5351-5358, Oct. 2013.

[10] N. S. Abinaya and P. Prakasam. “Performance analysis of maximum length LFSR and BBS method for cryptographic application,” in *Proceedings of International Conference on Electronics and Communication Systems*, pp. 1-5, 2014.

[11] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, Burlington, MA: Morgan Kaufmann, 2007.

[12] A. Z. Tirkel, G. A. Rankin, R. M. van Schyndel, W. J. Ho, and N. R. A. Mee, “Electronic Watermark,” in *Proceedings of International Conference on Digital Image Computing Techniques and Applications*, pp. 666-672, 1993.

[13] R. C. Gonzalez, R. E. Woods, and S. L. Eddins, *Digital Image Processing Using MATLAB*, 2nd ed(H. J. Yu, Trans.). Seoul, Korea: McGraw-Hill Korea, 2012.

[14] Korean Standards Association, KS X 1213-1, *128 bit block encryption algorithm ARIA-Part 1: General*, 2014.

손영호(Young-ho Son)

저자의 요청으로
사진 생략

1999년 2월: 경북대학교 전자공학과 석사
2017년 2월: 경북대학교 전자공학과 박사
2000년 ~ 현재: 한국전자통신연구원 부설연구소 책임연구원
※ 관심분야 : 음성신호처리, 디지털신호처리, 정보보호 등

배건성(Keun-sung Bae)

1977년 2월: 서울대학교 전자공학과 학사
1979년 2월: 한국과학기술원 전기 및 전자공학과 석사
1989년 5월: University of Florida 공학박사
1979년 ~ 현재: 경북대학교 전자공학부 교수
※ 관심분야 : 음성신호처리, 디지털신호처리, 적응필터링, 패턴인식, 소나/레이더신호처리 등