다수의 영상에 대한 스크램블 및 디스크램블 방법

Scramble and Descramble Scheme on Multiple Images

김승열*, 유영갑**
충북대학교 정보통신공학과*, 충북대학교 전기전자컴퓨터공학부**

Seung-Youl Kim(kimsy@hbt.chungbuk.ac.kr)*, Younggap You(ygyou@chungbuk.ac.kr)**

요약

본 논문에서는 다수의 비디오(video) 채널로부터 영상을 스크램블 및 디스크램블 하는 방법을 제안한다. 이 알고리즘은 다수의 영상 혼합과 이어 붙여진 영상의 화소 좌표의 뒤섞기를 이용한 암호화 방법이다. 조합된 프레임의 수직라인과 수평라인의 영상정보를 암호화 및 복호화 함으로서 암호화된 복합 영상을 얻는다. 이 알고리즘은 다수의 비디오 채널에서 모아진 다수의 영상을 하나의 영상으로 재구성하여 영상을 암호화함으로써 한 번에 다수의 영상 암호화하고 높은 보안성을 제공한다.

■ 중심어 : | 스크램블러 | 디스크램블러 |

Abstract

This paper presents a scheme which scrambles and descrambles images from multiple video channels. A combined image frame is formed by concatenating the incoming frames from channels in a two dimensional array. This algorithm employs an encryption scheme on row and column numbers of the combined image frame and thereby yields an encrypted combined image. The proposed algorithm is to encrypt multiple images at a time since it recomposes images from multiple video channels yielding one by composite image, and encrypts the composite image resulting in higher security.

■ keyword : | Scrambler | Descrambler |

Ⅰ. 서 론

최근 인터넷 및 통신 기술, 네트워크의 발달과 함께 이를 이용한 정보통신 기술이 빠르게 발달하고 있다[1]. 디지털 멀티미디어, 디지탈 TV, 화상 통신, 화상 회의 등 많은 정보통신 기술의 사용이 급격히 늘어나고 있다. 이러한 응용 기술들의 서비스가 다양화 되고 정보의 처리가 활성화됨에 따라 정보보호의 중요성이 지속적으로 증가하고 있다. 이렇게 개발된 멀티미디어 서비스 및 콘텐츠의 보호에 대한 지적 재산권의 요구가 증가하고 있다[2].

기밀 화상 회의, 인터넷을 통한 비디오 영상 판매 물등에 대하여 비인가자의 접근은 제한되어야 한다[3]. 화상 통신, 화상회의 또는 건물의 외부 및 내부 감시 등과

* 본 논문은 2006년도 교육인적자원부 지방연구중심대학 육성사업의 지원에 의하여 연구되었습니다.

접수번호 : #060220-001
접수일자 : 2006년 02월 20일
심사완료일 : 2006년 05월 15일
교신저자 : 유영갑, e-mail : ygyou@chungbuk.ac.kr

같이 다수의 카메라를 이용하며 기밀을 요구하는 정보 또한 비인가자로부터 보호되어야한다. 다수의 카메라가 설치된 내부 건물 및 외부 건물의 경우 관리자가 원격으로 다수의 카메라로부터 받은 모든 영상을 확인하고 감시 및 기록을 할 수 있도록 한다. 다수의 카메라로부터 얻어진 영상 정보가 암호화 되지 않으면 관리자 이외의 인가되지 않은 사용자에게 기밀정보가 누출되어 막대한 손실을 초래할 수 있다. 따라서 다수의 카메라로부터 얻어진 영상 데이터를 관리자 이외의 인가되지 않은 사용자로부터 보호하기 위한 영상 암호화 방법을 제안한다.

영상암호화 방법에는 스크램블 방법과 암호알고리즘을 이용하여 암호화하는 방법이 있다. 스크램블 방법은 영상의 화소의 계조 값은 변화시키지 않고 위치 정보를 변화시킴으로서 영상을 암호화 하는 방법이다. 기존의 피보나치 수[2]와 KTM(Knight Tour Matrix)[4]등을 이용한 영상 스크램블 방식은 하나의 비디오 채널로부터 입력되는 하나의 영상을 인가되지 않은 사용자로부터 보호한다. 다수의 영상물을 제공하는 환경에서는 보호 되어야 할 채널은 다수이다. 다수의 채널에서 입력되는 다수의 영상을 암호화 하는 방법이 필요하다.

제안된 영상 암호화 방법은 다수의 영상 채널에서 주어진 영상을 하나의 큰 영상으로 이어 붙인다. 이어 붙여진 하나의 큰 영상을 수직라인과 수평라인의 뒤섞기를 통하여 암호화하는 방법이다. 이 뒤섞기 순서는 난수표 등의 고속 알고리즘을 사용하려한다. 이 방식은 하드웨어의 부담이 적으면서도 높은 보안 특성을 달성할 수 있게 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 영상 암호화 기법에 대하여 기술하였다. Ⅲ장에서는 제안된 영상 암호화 방법을 이용한 스크램블 및 디스크램블 시뮬레이션을 나타내었고 Ⅳ장에서 결론을 내렸다.

II. 제안된 영상 암호화 기법

본 논문에서 제안하는 영상암호화 기법은 다수의 영상 정보를 이용하여 암호화하는 방법이다. 이 암호화 기법은 스크램블러와 디스크램블러로 구성되어진다. 스크램블러는 입력받은 영상 정보를 제3자가 알 수 없도록 암호화하는 블록이다. 디스크램블러는 암호화된 영상 정보를 인가된 사용자가 알 수 있도록 복호화하는 블록이다. 이 방식은 n개의 영상 정보를 입력받아 1개의 영상 정보로 재구성하고 이를 암호화하여 영상 정보를 보호하는 방식이다. 이 방식은 입력 받은 n개의 영상 정보를 모두 암호화하고 복호화함으로써 입력 받은 영상을 모두 보호할 수 있다.

1. 영상 스크램블러

스크램블러는 입력되는 영상 정보를 암호화하여 인가되지 않은 사용자로부터 도청을 방지하고 영상을 보호한다. 스크램블러의 구조는 [그림 1]과 같이 프레임 동기화 블록, 프레임 조합 블록 그리고 수직·수평라인 혼합 블록으로 구성되어 있다.

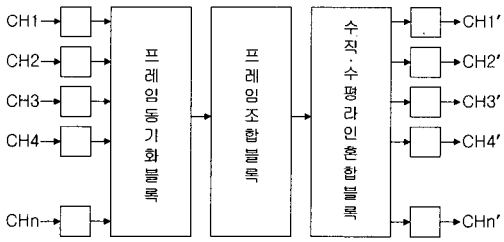

그림 1. 스크램블러 블록도

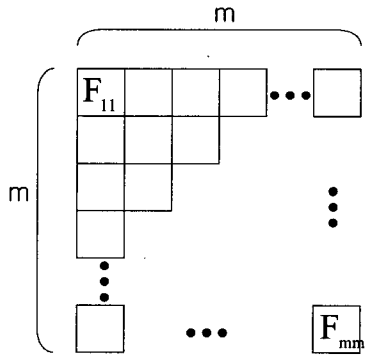

그림 2. m x m 프레임 조합 방법

[그림 1]에서 보듯이 스크램블러의 입력부분은 채널 CH_1에서 CHn까지 n개의 채널 입력을 갖는다. 프레임 동

기화 블록은 각각의 채널에서 입력된 영상의 프레임 동기를 맞춘다.

프레임 조합블록은 각각의 채널에서 입력된 영상의 프레임을 매트릭스 형태로 1개의 프레임으로 재구성하는 블록이다. 프레임 조합방식은 [그림 2]와 같이 구성된다.

[그림 2]에서 보듯이 입력된 각각의 프레임은 m x m 행렬의 형태로 배열된다. 그리고 배열된 형태는 프레임 조합 크기에 맞게 생성된 비 선형성이 우수한 S-BOX[5]에 따라 불규칙적으로 재배열되기 때문에 보다 높은 보안성을 보장할 수 있도록 한다.

수직·수평라인 혼합블록은 프레임 조합 블록에서 구성된 프레임을 수직라인과 수평라인의 라인과 라인을 혼합하여 암호화하는 블록이다. 프레임은 [그림 3]에서 보듯이 n개의 수직라인과 n개의 수평라인을 갖는다. 이렇게 배열된 n개의 수직라인과 n개의 수평라인을 재배열하여 암호화 한다.

프레임의 수직라인과 수평라인의 재배열 방법은 수직·수평라인 혼합 블록의 크기에 맞게 생성된 S-BOX를 이용하여 키 값에 따라 수직라인의 라인 번호를 치환하고 수평라인의 라인 번호를 치환한다. 예를 들면 [그림 3]과 같이 본래의 수평라인 번호를 {1, 2, 3, 4,…,n}이라고 한다면 암호알고리즘을 사용하여 {3, 4, n, 1,…,2}와 같이 치환하고 수직라인도 같은 방법으로 치환한다. 이와 같이 치환하는 과정에서 주의할 점은 치환되는 라인의 번호가 중복이 되는 것은 허용하지 않는다. 그리고 주어진 라인 번호를 넘어서지 않는다. 반면 치환과정에서 중복이 되지 않고 주어진 라인번호를 넘지 않는 치환 알고리즘은 사용할 수 있다.

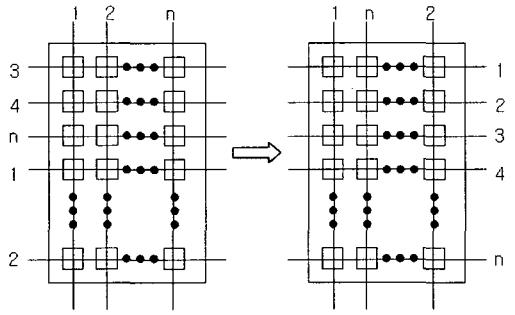

그림 3. 수직·수평라인 혼합 방법

2. 난수표 발생 방법

혼합을 위한 난수표는 비선형성이 우수한 S-BOX를 이용한다. S-BOX의 크기는 프레임 수와 수직·수평라인 수에 따라 결정된다. S-BOX의 크기는 갈로아체 n에 따라서 결정할 수 있다. 이와 같이 생성된 S-BOX의 값은 서로 중복되는 값이 없어야한다. 그리고 역 S-BOX가 존재해야한다. S-BOX는 스크램블에서 사용되고 역 S-BOX는 디스크램블에서 사용된다.

비선형성이 우수한 S-BOX의 생성 방법은 다음과 같다. 최소 다항식을 이용하여 갈로아체, $GF(2^n)$을 생성한다. 이후 생성된 $GF(2^n)$상에서 변환된 값을 아핀(Affine) 변환을 통하여 난수표 S-BOX를 생성한다. 아핀변환에 사용되는 행렬은 대칭행렬로 이루어진다. 또한 생성된 S-BOX의 값은 서로 중복된 값이 존재 하지 않고 역 S-BOX가 존재한다.

3. 영상 디스크램블러

디스크램블러는 인가되지 않은 사용자로부터 도청이 되지 않도록 스크램블된 영상 정보를 복호화하는 블록이다. 디스크램블러의 구조는 [그림 4]와 같이 프레임 동기화 블록, 수직·수평라인 복호 블록 그리고 프레임 조합 복호 블록으로 구성되어 있다.

[그림 4]에서 보듯이 프레임 동기화 블록은 스크램블러에서 송신된 영상신호의 프레임 동기를 맞추는 블록이다. 수직·수평 복호 블록은 수직·수평 혼합블록에서 사용된 S-BOX의 역 S-BOX를 이용하여 스크램블된 신호를 복호화한다. 프레임 조합 복호 블록은 프레임 조합 블록으로부터 매트릭스로 조합된 프레임의 순서를 스크램블된 프레임 조합순서와 같이 재배열고 본래의 영상을 송신하고 각각의 영상신호를 채널별로 수신한다.

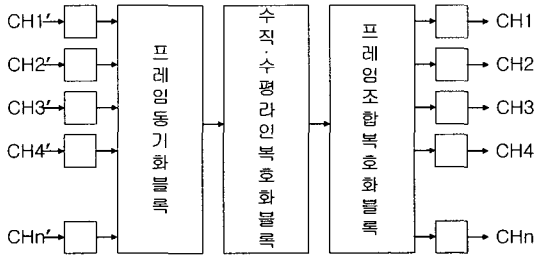

그림 4. 디스크램블 블록도

III. 시뮬레이션 결과

제안된 영상 암호화 기법을 사용한 스크램블 및 디스크램블 방법은 MatLab을 이용하여 시뮬레이션 하였다. 시뮬레이션 조건으로 보호하고자 하는 TV 방송 채널이 16개가 있다고 가정하였다. 스크램블러의 프레임 조합 블록은 [그림 5]와 같이 매트릭스 형태로 16개 채널의 16개 프레임이 배열되어 하나의 큰 프레임으로 구성된다. 구성된 하나의 큰 프레임은 [그림 5]와 같다. 각각의 프레임의 해상도는 64X64이고 하나의 큰 프레임의 해상도는 256X256이다. 제안된 방법을 사용하여 스크램블러를 통해 암호화된 영상은 [그림 6]과 같이 나타난다.

암호화된 영상은 비선형성이 우수한 S-BOX를 이용하여 스크램블 되었기 때문에 [그림 6]과 같이 서로간의 상관관계가 거의 없기 때문에 보안성이 높다. 또한 스크램블된 큰 프레임은 각각의 채널별로 각각의 프레임이 전송된다. 그리고 각각의 프레임은 서로 다른 프레임의 영상정보를 포함하고 있기 때문에 암호화된 각각의 영상정보를 통하여 본래의 영상을 추출하기가 어렵다. 암호화된 영상 [그림 6]은 디스크램블러를 통해 [그림 7]과 같이 영상이 복호화 됨을 볼 수 있다.

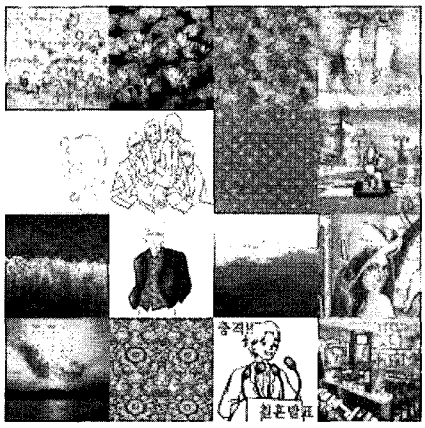

그림 5. 원본 영상

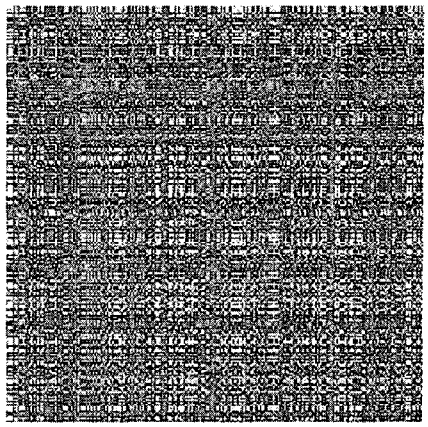

그림 6. 스크램블된 영상

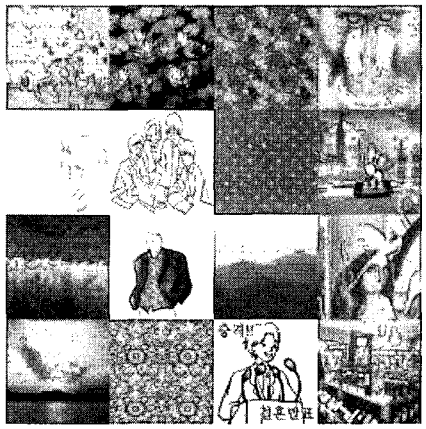

그림 7. 디스크램블된 영상

제안된 스크램블러를 사용한 영상의 암호화는 보안성이 뛰어남을 알 수 있다. 이 결과는 본 영상과 암호화된 영상의 히스토그램을 비교하여 분석한 것이다. [그림 8]은 [그림 5]의 16개의 각각의 프레임중 3행 4열에 위치한 64X64 레나의 영상 히스토그램이다. [그림 9]는 레나의 암호화된 영상의 히스토그램이다. 본 영상의 히스토그램의 명암이 한쪽으로 치우친 반면 암호화된 영상의 히스토그램의 명암은 차이가 크지 않다. 이 결과 두 영상의 히스토그램의 차이가 크다는 것은 암호화된 영상으로부터 본 영상을 복원하기가 어렵다는 것을 알 수 있다.

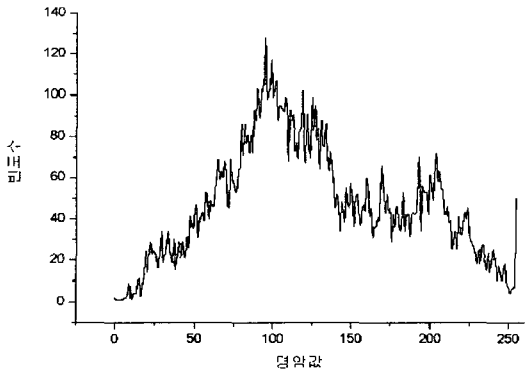

그림 8. 원본 레나 영상의 히스토그램

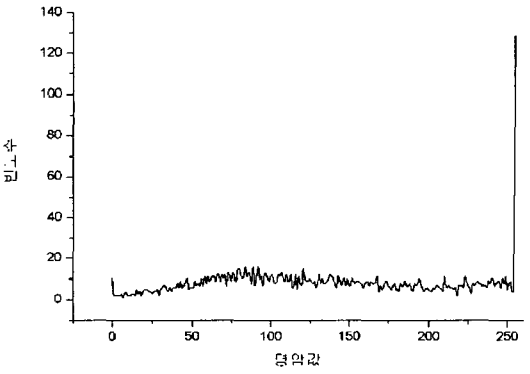

그림 9. 암호화된 레나 영상의 히스토그램

Ⅳ. 결 론

본 논문에서는 다수의 비디오 채널에서 주어진 모든 영상을 스크램블 및 디스크램블하는 방법을 제안하였다. 이 알고리즘은 다수의 비디오 채널에서 수집된 영상 정보를 이용하여 채널의 혼합과 영상의 혼합으로 본래의 영상을 보호한다. 영상의 혼합은 수집된 다수의 영상 정보인 프레임들을 하나의 프레임으로 조합하여 조합된 프레임의 수직라인과 수평라인을 각각 라인 대 라인으로 혼합한다. 제안된 알고리즘은 다수의 영상정보를 조합하여 암호화 하고 암호화된 영상정보를 복호화함으로써 사용된 모든 영상정보를 암호화 하고 모든 영상정보를 복호화하여 인가되지 않은 사용자로부터 영상정보를 보호한다. 또한 영상의 손실이 없으며 높은 보안성을 유지한다.

참 고 문 헌

[1] J. P. P. Dang and P. M. Chau, "Image encryption for secure internet multimedia applications," *IEEE Transactions on Consumer Electronics*, Vol.46, pp.395-403, Aug., 2000.

[2] J. Zou, R. K. Ward, and D. Qi, "A new digital image scrambling method based on Fibonacci numbers," *Proc. of the IEEE Inter Symposium on Circuits and Systems*, Vol.3, pp.III-965-968, May, 2004.

[3] W. Kanjanarin and T. Amornraksa, "Scrambling and key distribution scheme for digital television," *Proc. of the 9th IEEE International Conference on Networks*, pp.140-145, Oct., 2001.

[4] S. Bai and C. Cao, "A novel algorithm for scrambling the details of digital image," *Proc. of the 4th World Congress on Intelligent Control and Automation*, pp.1333-1336, Feb., 2002.

[5] National Institute of Standard and Technology(NIST), *Advanced Encryption Standard(AES)*, Federal Information Processing Standard Publication 197, 2001.

저 자 소 개

김 승 열(Seung-Youl Kim) 정회원

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

<관심분야> : 디지털 회로설계, Cryptography, 고속 인쇄 회로설계

유 영 갑(Younggap You) 정회원

- 1975년 8월 : 서강대학교 전자공학과(공학사)
- 1975년~1979년 : 국방과학연구소 연구원
- 1981년 8월 : Univ.of Michigan, Ann Arbor 전기전산학과(공학석사)
- 1986년 4월 : Univ.of Michigan, Ann Arbor 전기전산학과(공학박사)
- 1986년~1988년 : 금성반도체(주) 책임연구원
- 1993년~1994년 : 아리조나 대학교 객원교수
- 1998년~2000년 : 오레곤 주립대학교 교환교수
- 1988년~현재 : 충북대학교 정보통신공학과 교수

<관심분야> : VLSI 설계 및 Test, 고속 인쇄회로 설계, Cryptography