CA 기반의 난수열을 이용한 동영상 암호화

윤재식* · 이소위* · 조성진* · 김석태*

*부경대학교

Video Encryption using Pseudo-random numbers based on CA

Jae-sik Yun* · Xiaowei Li* · Sung-jin Cho* · Seok-tae Kim*

*Pukyong National University

E-mail : yffyjs@gmail.com · lixiaowei@nate.com · sjcho@pknu.ac.kr · setakim@pknu.ac.kr

요 약

본 논문에서는 MLCA(Maximum length CA) 기반의 의사난수열(Pseudo-random numbers)을 이용하여 동영상을 암호화하는 방법을 제안한다. MLCA 기반의 난수열을 이용하여 기저영상을 생성한 후, 동영상의 모든 프레임과 기저영상 사이의 XOR 연산을 취함으로써 동영상을 암호화한다. 하나의 CA Rule 또는 두 개의 CA Rule을 이용하는 경우를 구분하여 영상을 암호화 하고 그 결과에 대해 평가한다.

ABSTRACT

In this paper, we propose a video encryption method using pseudo-random numbers based on MLCA(Maximal length Cellular Automata). Firstly, we generate a basis image which is composed with pseudo-random numbers, using MLCA. Futhermore, The original video is encrypted by computing XOR operation between the basis image and each frame of original video. The video encryption is conducted in accordance with one or two rules, and is evaluated.

키워드

CA(Cellular Automata), MLCA(Maximal length CA), 의사난수열(Pesudo-random numbers), Video encryption

Ⅰ. 서 론

정보통신기술 및 영상콘텐츠 산업의 발전으로 우리는 다양한 형태의 영상콘텐츠를 일상에서 쉽게 이용할 수 있게 되었다. 이와 더불어 영상콘텐츠의 보호 및 소유권자의 권리 보호를 위한 디지털 워터마킹, 암호화 기술 등의 개발이 활발하게 이루어지고 있다. 하지만 사용자들의 저작권에 대한 의식 부족으로 여전히 영상콘텐츠에 대한 불법복제가 이루어지고 있으며 이는 영상콘텐츠 산업의 발전을 저해하는 요소로 작용하고 있다[1].

기존에 CA(Cellular Automata) 및 CAT(CA Transform)를 이용하여 영상을 암호화하는 방법들이 제안되었다[2][3]. 기존의 CA 기반 암호화 방법에서 히스토그램, PSNR, 키 공간 등의 암호화 평가를 통해 CA 기반 영상 암호화 방법의 유효성이 입증되었다.

영상은 크게 정지영상과 동영상으로 분류할 수 있으며 영상콘텐츠에서 동영상의 활용이 점점 늘어나고 있다. 하지만 기존 CA 기반의 영상 암호화에서 동영상에 대한 암호화는 전혀 언급되지 않았다. 따라서 본 논문에서는 CA 기반의 의사난수열(Pseudo-random numbers)을 이용한 동영상 암호화 방법을 제안한다.

암호화 실험결과 웹캠으로 촬영된 1000 프레임의 동영상을 암호화하는데 대략 3~4초가 소요되었다. 또한 하나의 MLCA 규칙을 이용해서 암호화하는 방법에 비해 두 개의 MLCA 규칙을 이용하여 영상을 암호화하는 경우 더욱 향상된 암호화 결과를 얻을 수 있었다.

Ⅱ. 90/150 규칙의 3-이웃 NBCA 및 MLCA

CA는 이산적인 시간과 공간에 존재하는 셀들의 상태를 정의한다. CA의 전이규칙, 경계조건 등 CA의 정의에 의해서 이산적인 공간에 존재하는 셀들은 시간의 변화에 따라 새로운 값들로 상태가 전이된다. CA 원리를 이용하여 난수열을 생성하는 경우, 복잡한 수학적 연산을 피할 수 있으며 랜덤성이 강한 난수열을 생성할 수 있다[4].

난수열을 생성하기 위해 NBCA(Null Boundary CA) 경계 조건을 만족하고 90과 150 규칙만으로 이루어진 선형 3-이웃 CA 구조를 이용하였다. 그림 1은 3개의 셀로 이루어진 3-이웃 NBCA 구조의 상태전이를 나타낸다. 5개의 셀 중 가운데 3개의 셀에 관심이 있으며 90, 150 규칙에 따라 시간 t에서 t+1로 셀의 상태가 전이되는 것을 볼 수 있다.

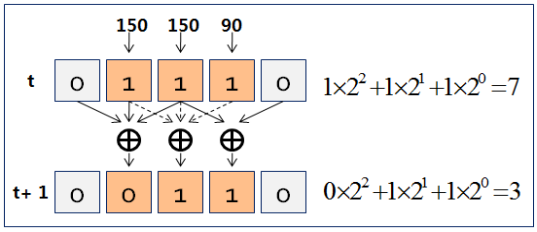

그림 1. 90/150 규칙의 3-이웃 NBCA

식 (1), (2)는 3-이웃 NBCA에서 90, 150 규칙의 상태전이를 수식으로 나타낸다. $x_i(t)$는 시간 t일 때 i번째 셀의 상태이다.

$$90\text{규칙} : x_i(t+1) = x_{i-1}(t) \oplus x_{i+1}(t) \quad (1)$$

$$150\text{규칙} : x_i(t+1) = x_{i-1}(t) \oplus x_i(t) \oplus x_{i+1}(t) \quad (2)$$

n개의 셀로 이루어져 있는 경우, 최대 2^n-1개의 상태를 가질 수 있으며 이러한 경우의 CA를 MLCA(Maximal length CA)라 한다.

Ⅲ. 기저영상 및 동영상 암호화

3.1 기저영상

동영상을 암호화하는데 필요한 난수열을 생성하기 위해 8셀로 이루어진 3-이웃 NBCA 구조를 이용하였다. 또한 8셀로 이루어진 CA에서 생성되는 난수열의 주기가 최대가 되는 MLCA를 이용하였다. 생성되는 난수열을 재배열해서 동영상과 동일한 가로 세로의 크기의 기저영상을 생성한다. 기저영상은 RGB 색상모델로 이루어진 정지영상이며 R, G, B 각 채널의 픽셀 값은 동일한 CA rule에 초기 값을 다르게 하여 생성한다.

8셀로 이루어진 NBCA에서 각 셀에 해당하는 규칙이 150,150,90,150,90,150,90,150인 MLCA를 이용하여 생성한 기저영상(Ⅰ)을 그림 2에 나타내었다. 또한 규칙이 150,150,90,150,90,150,90,150 와 150,90,150,90,90,90,150,90인 두 MLCA를 이용하여 생성한 기저영상(Ⅱ)을 그림 3에 나타내었다.

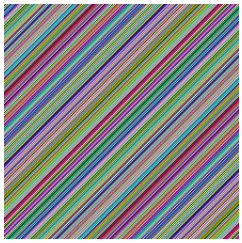

그림 2. 기저영상(Ⅰ)

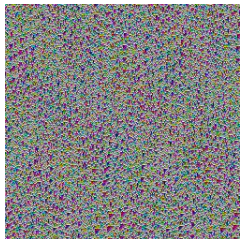

그림 3. 기저영상(Ⅱ)

그림 2와 그림 3을 통해서 기저영상은 하나의 MLCA 규칙을 사용하는 것 보다 두 개의 MLCA 규칙을 사용해서 생성하는 경우 더욱 무질서한 형태로 나타나는 것을 볼 수 있다.

3.2 동영상 암호화 방법

동영상을 암호화하기 위해서 우선 3.1절에서 설명한 기저영상을 생성한다. 이후 동영상 데이터를 프레임 단위의 정지영상으로 분리시킨 후, 기저영상과 각각의 정지영상에서 같은 공간좌표에 존재하는 모든 픽셀간의 XOR 연산을 취함으로써 정지영상을 암호화한다. 암호화된 정지영상을 다시 암호화된 순서데로 동영상 데이터로 병합시킨다. 동영상의 암호화 과정을 그림 4에 나타내었다.

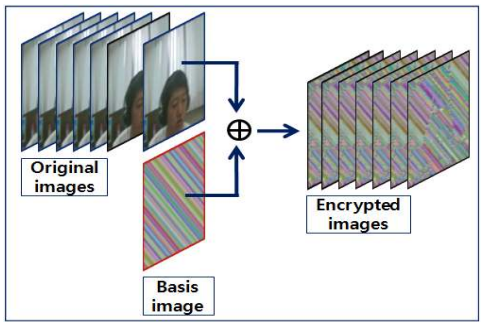

그림 4. 기저영상을 이용한 동영상 암호화

제안하는 동영상 암호화 방법에서 암호화의 기본단위가 한 프레임의 정지영상이다. 따라서 실시간으로 전송 및 재생되는 동영상 데이터를 패킷 또는 블록 단위로 암호화하는 경우, 송신자는 한 프레임의 영상을 암호화한 후 패킷 또는 블록 단위로 분할하여 전송하고 수신측에서는 수신된 패킷 또는 블록이 한 프레임으로 구성될 때 복호화한다.

본 논문에서의 암호화 실험은 실시간 동영상 전송 및 재생은 고려하지 않고 동영상 데이터 전체를 암호화한 후, 암호화한 동영상 파일을 전송

하는 경우에 대한 것이다.

암호화 실험에서는 웹캠으로 촬영된 크기가 255(H)×255(V)이고 1000 프레임으로 이루어진 동영상을 사용하였으며 1000 프레임의 동영상을 암호화하는데 대략 3~4초가 소요된다. 웹캠으로 촬영된 동영상과 기저영상(Ⅰ)을 이용하여 암호화한 동영상 화면을 그림 5에 나타내었다. 그림 6은 동일한 동영상을 기저영상(Ⅱ)를 이용하여 암호화한 결과를 나타낸다. 그림 5와 그림 6에서 암호화된 동영상을 살펴보면 두 개의 MLCA 규칙을 사용한 결과에 비해 하나의 규칙을 사용한 경우 동영상의 윤곽이 드러나는 것을 볼 수 있다.

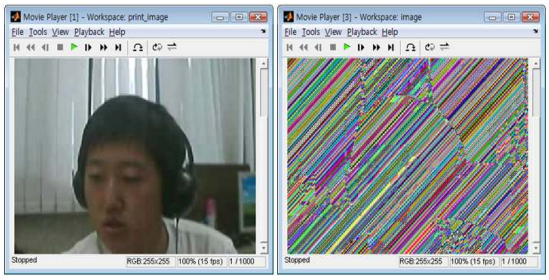

그림 5. 암호화 대상 및 기저영상(Ⅰ)을 이용한 암호화 결과 화면

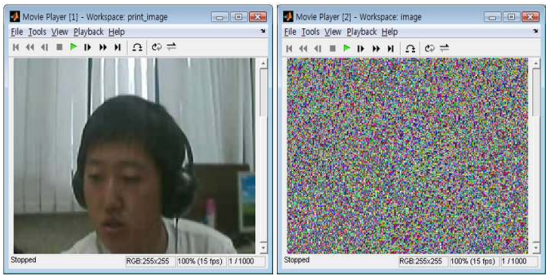

그림 6. 암호화 대상 및 기저영상(Ⅱ)을 이용한 암호화 결과 화면

그림 7은 그림 6에 나타낸 두 화면에 대한 히스토그램을 나타낸다. 암호화된 결과 영상의 히스토그램은 항상 균일한 히스토그램 분포를 가진다. 이는 해독자가 영상의 명암정보를 알 수 없도록 한다.

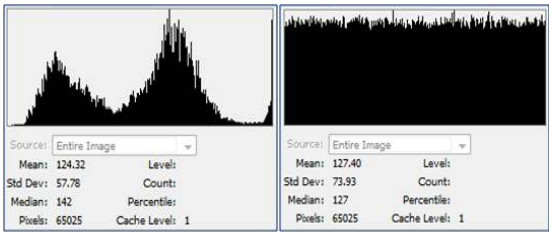

그림 7. 암호화 대상 및 암호화 결과 영상의 히스토그램

암호화에서 전사적 공격으로부터 안전하기 위해서는 충분한 키 공간을 가져야 한다. 본 논문에서는 8-셀, 2-상태, 3-이웃의 MLCA를 사용하였으며, CA 키 공간분석을 통해 $N_T^1 = 2^{2^3+8+2\times 8} = 2^{32}$에 해당하는 키를 가진다는 것을 알 수 있다[2]. 그림 2에 나타낸 기저영상(Ⅰ)은 하나의 MLCA 규칙을 사용하기 때문에 2^{32} 가지의 키를 가지며, 그림 3에 나타낸 기저영상(Ⅱ)의 경우 서로 다른 두 개의 MLCA 규칙을 이용하기 때문에 $2^{32+32} = 2^{64}$ 가지의 키를 가진다.

Ⅳ. 결론

본 논문에서는 영상콘텐츠의 불법복제를 방지하기 위해 CA 기반의 난수열을 이용하여 동영상을 암호화하는 방법을 제안하였다. 생성된 난수열로부터 기저영상을 생성한 후, 동영상의 모든 프레임과 XOR 연산을 취해서 동영상을 암호화한다. 하나의 MLCA 규칙을 이용하여 영상을 암호화한 경우와 서로 다른 두 개의 MLCA 규칙을 이용하여 암호화하는 경우의 암호화 결과를 CA 키 공간 분석을 통해 비교하였다. 서로 다른 두 개의 MLCA 규칙을 이용하는 경우 암호화 결과 및 수학적인 키 공간분석을 통해 하나의 MLCA 규칙을 이용하는 경우에 비해 높은 암호화 수준을 보인다.

참고문헌

[1] 이혜경, 김희완, "영상 컨텐츠 불법 복제에 관한 사용자 의식 수준", 한국콘텐츠학회논문지, Vol. 9, No. 11, pp. 212-224, Nov. 2009.

[2] 박영일, 조성진, 김석태, "MLCA와 CAT를 이용한 새로운 영상 암호화 방법", 한국해양정보통신학회논문지, Vol. 13, No. 10, Oct. 2009.

[3] 남태희, 김석태, 조성진, "IBCA에 기초한 여원 MLCA와 2D CAT를 이용한 영상 암호화", 전자공학회논문지, Vol. 46-SP, No. 4, pp. 34-41, Jul. 2009.

[4] 최언숙, 조성진, “최대길이를 갖는 셀룰라 오토마타의 생성”, 정보보호학회논문지, Vol. 14, No. 6, pp. 25-30, Dec. 2004.