MLCA와 비트 단위 연산을 이용한 컬러 영상의 암호화

윤재식* · 남태희** · 조성진* · 김석태*

*부경대학교 · **동주대학

Color Image Encryption using MLCA and Bit-oriented operation

Jae-sik Yun* · Tae-hee Nam** · Sung-jin Cho* · Seok-tae Kim*

*Pukyong National University · **Dongju College University

E-mail : yffyjs@gmail.com · thnam1@hanmail.net · sjcho@pknu.ac.kr · setakim@pknu.ac.kr

요 약

본 논문에서는 기존의 MLCA(Maximum length CA) 및 여원 MLCA를 이용한 영상 암호화의 문제점을 제시하고 이를 해결하기 위한 암호화 방법을 제안한다. 기존의 암호화 방법은 영상에서 인접한 픽셀간의 공간적 중복성(Spatial redundancy)으로 인해 암호화의 결과가 원 영상에 많은 영향을 받는 문제점이 있다. 본 방법에서는 MLCA 기반의 난수열을 생성하고, 이를 이용해 픽셀의 공간좌표를 암호화된 공간좌표로 변환한다. 이후 영상의 픽셀 값을 난수열과 XOR 연산을 취해 색상정보를 암호화한다. 이러한 방법은 원 영상의 픽셀 값뿐만 아니라 공간좌표를 암호화하기 때문에 픽셀의 공간적 중복성으로 인한 문제점을 해결할 수 있으며 암호화 수준을 향상시킨다. 히스토그램 분석, 키 공간 분석을 통해 본 암호화 방법의 유효성을 확인하였다.

ABSTRACT

This paper presents a problem of the existing encryption method using MLCA or complemented MLCA and propose a method to resolve this problem. With the existing encryption methods, the result of encryption is affected by the original image because of spatial redundancy of adjacent pixels. In this proposed method, we transform spatial coordinates of all pixels into encrypted coordinates. We also encrypt color values of the original image by operating XOR with pseudo-random numbers. This can solve the problem of existing methods and improve the levels of encryption by randomly encrypting pixel coordinates and pixel values of original image. The effectiveness of the proposed method is proved by conducting histogram, key space analysis.

키워드

CA(Cellular Automata), MLCA(Maximal length CA), 의사난수열(Pseudo-random numbers), 공간적 중복성(Spatial redundancy)

Ⅰ. 서 론

오늘날 정보통신 기술의 발달로 다양한 영상 컨텐츠를 인터넷을 통해 누구나 쉽게 이용할 수 있게 되었다. 그러나 영상 컨텐츠 이용자의 저작권에 대한 의식 부족으로 인해 영상 불법복제 문제는 날이 갈수로 심각해지고 있다[1].

영상은 최소 단위인 픽셀들로 이루어져 있으며 각각의 픽셀에 대한 색상, 명도, 채도 등의 속성을 픽셀의 값으로 가진다. 영상 암호화의 간단한 방법은 의사난수열(Pseudo-random numbers)을 생성하고 원 영상을 의사난수열과 같은 길이의 블록단위로 영상을 암호화하는 것이다. 이 같은 방법은 구현이 용이하고 암호화 속도가 빠르지만 암호화 수준은 의사난수열의 길이에 많은 부분을 의존하게 된다. 의사난수열의 길이가 짧으면 선형복잡도가 낮아져 암호화의 안전성이 떨어지며 픽셀간의 공간적 중복성이 암호화된 결과 영상에 유지되게 된다. 이는 암호 해독자에게 암호 해독에 필요한 단서를 제공하게 된다. 의사난수열의 최대 길이를 증가시킴으로써 이러한 문제를 해결할 수는 있지만 이는 하드웨어 구성, 암호화 속도

등의 제한이 따른다.

기존에 CA(Cellular Automata)의 분류 중 최대길이 CA(Maximal length CA, 이하 MLCA) 및 여원 MLCA 원리를 이용하여 의사난수열을 생성한 후, 이를 이용하여 영상을 암호화하는 방법이 제안되었다[2][3]. 이는 MLCA 기반의 난수열을 생성하여 영상의 픽셀 값을 암호화하는 방법이다. 이러한 암호화 방법은 lena, baboon, peppers와 같은 일반적인 실험 영상에서 비교적 높은 암호화 수준을 보인다. 하지만 원 영상이 인접한 픽셀간의 공간적인 중복성이 큰 영상일 경우 암호화 수준이 저하된다.

본 논문에서는 이러한 문제점을 해결하기 위해 색상을 표현하기 위한 픽셀의 값뿐만 아니라 픽셀의 공간좌표를 암호화하는 방법을 제안한다. 이는 픽셀간의 공간적 중복성으로 인한 기존 암호화 방법의 문제점을 해결하고 암호화 수준을 향상시킨다.

기존 암호화 방법과 본 방법의 결과 비교를 통해 기존 암호화 방법의 문제점을 명확히 하고 히스토그램 분석, 키 공간 분석을 통해 본 암호화 방법의 유효성을 확인하였다.

Ⅱ. MLCA를 이용한 의사난수열

CA는 Von Neumann에 의하여 스스로 조직화되고 재생산할 수 있는 모델로 처음 소개되었다. CA 가운데 다음 상태를 결정하는 함수가 선형적인 CA는 LFSR(Linear Feedback Shift Register)의 대안으로 제안되며, 의사난수열 생성기, 암호, 신호분석 등 많은 분야에서 응용되었다. CA는 셀의 배열상태, 적용되는 규칙의 논리, 상태전이 그래프의 형태 등 여러 기준에 따라 분류된다[4][5].

CA를 이용해 의사난수열을 생성하면 하드웨어 구성이 간단하며 복잡한 수학적 계산을 피할 수 있다. 뿐만 아니라 CA는 초기조건에 민감하고 랜덤성이 우수하다. 본 논문에서는 CA의 이러한 장점 때문에 최대길이를 갖는 CA를 영상 암호화에 이용한다.

Ⅲ. 암호화 방법

기존의 영상 암호화 방법에서 픽셀간의 공간적인 중복성(Spatial redundancy)으로 인해 암호화의 수준이 저하되는 것은 원 영상 자체의 공간적 중복성과 의사난수열의 최대주기가 충분히 길지 못하기 때문이다. 물론 MLCA를 이용해 의사난수열의 최대 길이를 증가시킬 수는 있지만 이는 하드웨어 구성, 암호화 속도 등의 제한이 따른다. 이러한 문제점을 해결하기 위해서 원 영상의 픽셀 값뿐만 아니라 픽셀의 공간좌표를 암호화한다.

영상 암호화 방법 및 과정을 간략하게 표현하면 그림 1과 같다. 우선 원 영상을 픽셀 단위의 연속된 수열로 재배열한다(그림 1, ①). 의사난수열을 생성하기 위해서 Null boundary 경계조건을 만족하는 서로 다른 두 개의 MLCA 규칙을 이용하였다(그림 1, ②). MLCA의 규칙을 다르게 하여 최대주기를 갖는 두 개의 의사난수열을 얻을 수 있으며 이를 이용하여 원 영상의 공간좌표를 암호화한다(그림 1, ③). 마지막으로 규칙 2에 의해 생성되는 의사난수열을 이용하여 모든 픽셀의 색상 값을 암호화하고 영상 데이터로 재배열한다(그림 1, ④).

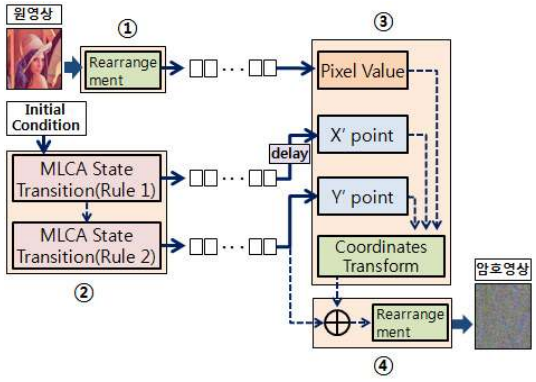

그림 1. 암호화 블록도

본 방법에서는 의사난수열을 생성하기 위해 Null Boundary 경계조건의 MLCA를 사용하였다. 식 (1), 식 (2)에서 $T1$와 $T2$는 서로 다른 규칙을 갖는 전이행렬(Transition matrix)이며 $S1_t$와 $S2_t$는 시간 t에서의 상태를 나타낸다. 다음상태 $S1_{t+1}$는 이전상태 $S1_t$와 전이행렬 $T1$에 의해 결정되며 $S2_{t+1}$의 초기상태를 결정한다. 또한 원 영상의 공간좌표 변환을 위해 x축(열 방향) 좌표를 결정한다. $S2_{t+1}$는 공간좌표 변환을 위한 y축(행 방향) 좌표를 결정한다.

$$S1_{t+1} = T1 \cdot S1_t \quad (1)$$

$$S2_{t+1} = T2 \cdot S2_t \quad (2)$$

Ⅳ. 암호화 결과

본 논문에서 암호화 실험을 위해 그림 2, 그림 5와 같은 255×255 크기의 24비트 RGB 영상을 사용하였다. 기존 픽셀의 색상 값을 암호화하는 방법과 본 방법인 픽셀의 색상 값과 공간좌표를 암호화한 방법의 결과를 그림 3, 4에 나타내었다. 두 암호화 방법 모두 히스토그램이 고르게 분포되는 것을 볼 수 있으며 이는 암호화된 영상의 명암 분포로부터 해독자가 원 영상의 명암 정보를 예측할 수 없도록 한다.

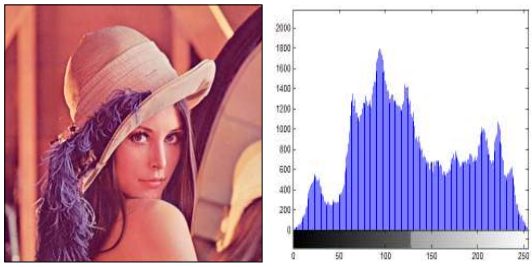

그림 2. 원 영상 및 히스토그램

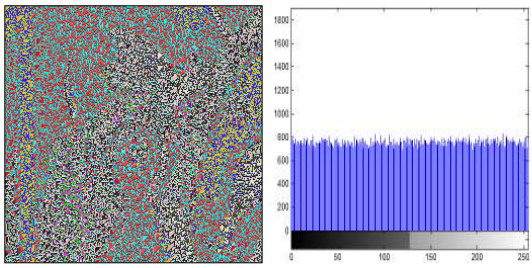

그림 3. 기존 암호화 방법 결과

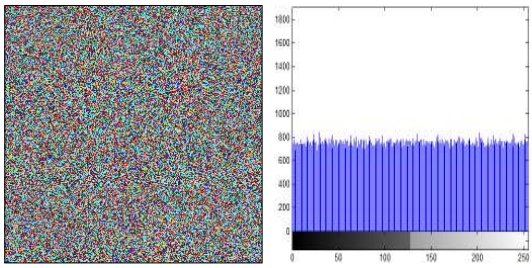

그림 4. 본 암호화 방법 결과

그림 2에 비해 원 영상의 공간적 중복성이 더 크게 나타나는 그림 5를 암호화하는 경우, 기존 방법을 이용하여 암호화한 결과 그림 6에서는 원 영상의 윤곽이 그대로 유지되는 것을 볼 수 있다. 이에 비해 본 암호화 방법의 결과인 그림 7에서는 원 영상을 전혀 예측할 수 없다. 이러한 결과로부터 공간좌표를 암호화함으로써 기존 암호화 방법의 문제점을 해결할 수 있다는 것을 알 수 있다.

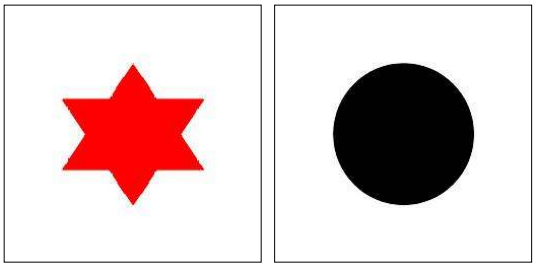

그림 5. 원 영상

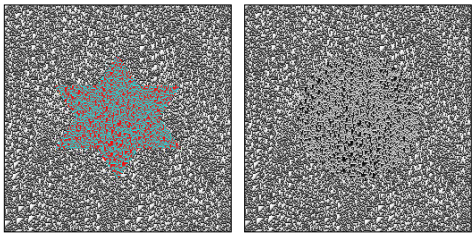

그림 6. 기존 암호화 방법 결과

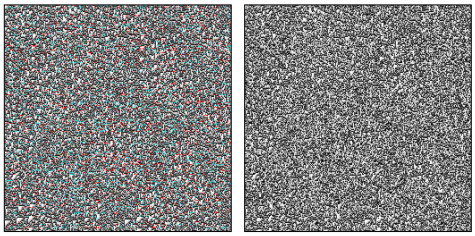

그림 7. 본 암호화 방법 결과

Ⅴ. 결 론

기존에 MLCA를 이용하여 영상을 암호화하는 경우 영상의 공간적 중복성으로 인해 암호화 수준이 저하되는 문제점이 있다. 본 논문에서는 이러한 문제점을 해결하기 위해 원 영상의 픽셀 값뿐만 아니라 공간좌표를 암호화하는 방법을 제안한다. 본 암호화 방법은 난수열을 생성하기 위해 CA의 원리를 이용하기 때문에 CA 키 공간 분석을 통해 2^{64}가지의 키를 가진다는 것을 알 수 있다. 실험 영상에 대해 기존 암호화 방법과 본 암호화 방법의 결과 분석을 통해 본 암호화 방법의 유효함을 확인하였다.

참고문헌

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

[2] 남태희, 김석태, 조성진, “90/150 NBCA 구조를 이용한 영상 암호화”, 한국해양정보통신학회종합학술대회, Vol. 13 No. 1 (2009. 춘계), pp. 152-155, 2009.

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

[4] Olu Lafe, " Cellular Automata Transforms: Theory and Application in Multimedia Compression, Encryption, and Modeling", Kluwer Academic Publishers, 2000.

[5] 최언숙, 조성진, "최대길이를 갖는 셀룰라 오토마타의 생성“, 한국정보보호학회, 情報保護學會論文誌 제14권 제6호, pp. 25-30, 2004.