논문 2012-49CI-1-5

디지털 비디오 보호를 위한 카오스 사상 기반의 암호화 방법

(Encryption Method Based on Chaos Map for Protection of Digital Video)

윤 병 춘*, 김 덕 환**

(Byung-Choon Yun and Deok-Hwan Kim)

요 약

네트워크 환경과 유무선 통신 기술의 급속한 발달로 인해 비디오 콘텐츠의 배포가 손쉽게 이루어짐에 따라 비디오 콘텐츠에 대한 보안은 매우 중요시 되고 있다. 따라서 본 논문에서는 MPEG-2 비디오 인코딩 과정 내에 복수의 카오스 사상 기반의 디지털 비디오 암호화 방법을 제안한다. 제안방법은 카오스 사상인 텐트 사상(Tent map)을 기본블록으로 하는 해시체인으로부터 128-bit의 난수특성이 우수한 비밀 해시 키를 생성하고 이를 로지스틱 사상(Logistic Map)과 헤논 사상(Hénon map)에 적용하여 64개의 난수로 이루어진 8x8 난수블록을 생성한다. 제안한 방법은 8x8 난수 블록과 DCT 블록 내 영상정보에 대한 파급효과가 큰 저주파 계수들에 대해 선택적으로 XOR 암호화 연산을 수행함으로써 암호화 처리에 따른 오버헤드를 줄일 수 있으며, 복수의 카오스 사상을 결합한 구조를 사용하여 비교적 간단하면서 우수한 난수특성을 제공한다. 실험 결과를 통해 제안 방법은 암호화된 영상에 대해 PSNR이 12dB 이하로 좋은 시각적 암호화 성능을 나타냈으며, 압축 효율성 측면의 시간변화율과 압축변화율은 각각 2%와 0.4% 이내의 실시간성에 적용 가능한 성능을 나타냈다.

Abstract

Due to the rapid development of network environment and wireless communication technology, the distribution of digital video has made easily and the importance of the protection for digital video has been increased. This paper proposes the digital video encryption system based on multiple chaos maps for MPEG-2 video encoding process. The proposed method generates secret hash key of having 128-bit characteristics from hash chain using Tent map as a basic block and generates 8x8 lattice cipher by applying this hash key to Logistic map and Hénon map. The method can reduce the encryption overhead by doing selective XOR operations between 8x8 lattice cipher and some coefficient of low frequency in DCT block and it provides simple and randomness characteristic because it uses the architecture of combining chaos maps. Experimental results show that PSNR of the proposed method is less than or equal to 12 dB with respect to encrypted video, the time change ratio, compression ratio of the proposed method are 2%, 0.4%, respectively so that it provides good performance in visual security and can be applied in real time.

Keywords : MPEG-2, Video Encryption, Chaos Map

Ⅰ. 서 론

비디오 압축기술과 유무선 통신기술의 성장에 힘입어 비디오 콘텐츠들이 수많은 네트워크 경로로 손쉽게 배포됨으로써 많은 긍정적인 측면을 가져왔다. 하지만 이와 더불어 개방형 네트워크상에서 존재하는 저작권 침해와 서비스 이용자의 개인정보 침해 가능성에 대한 역기능 또한 존재한다. 비디오 콘텐츠의 응용에 있어서

* 학생회원, ** 정회원, 인하대학교 전자공학과
(Department of Electronics Engineering, Inha University)

※ 본 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2011-0004114)
※ 본 연구는 지식경제부와 한국산업기술진흥원의 전략기술 인력양성사업으로 수행된 결과임
※ 본 논문은 인하대학교 연구비 지원에 의하여 연구되었음
접수일자: 2011년5월6일, 수정완료일: 2012년1월3일

상업성뿐만 아니라 군사적 정보의 기밀성 유지나 CCTV와 같은 불특정 다수에 대한 사생활 침해문제 등이 고려될 때, 비디오 콘텐츠의 기밀성 유지를 위한 암호화는 유무선 네트워크를 통한 전송에 있어서 간과 할 수 없는 부분으로 인식되고 있다.

비디오 콘텐츠의 기밀성 유지를 위해서는 비디오 콘텐츠가 본래의 데이터를 추측할 수 없는 형태로 암호화 되어야 하고 인증된 사용자에게만 복호화의 권한이 주어져야한다. 이를 위한 직접적인 암호화 방법으로 제안된 naive algorithm (Agi and Gong, 1996)은 텍스트 데이터를 보호할 목적으로 사용되는 전통적 암호화 방법인 AES(Advance Encryption Standard, NIST, 2001)를 압축 비디오 스트림 전체에 적용하여 데이터를 암호화 하는 방법이다[2]. 하지만 통상적으로 영상데이터는 텍스트 데이터에 비해 매우 크기 때문에 AES 또는 DES (Data Encryption Standard, NIST, 1974) 와 같은 텍스트 암호화 알고리즘을 비디오 데이터에 직접적으로 적용할 경우 실시간 처리에 적합하지 못할 뿐만 아니라 암호화 처리 후의 비디오의 크기 오버헤드 측면에서 좋지 못한 성능을 나타낸다. 이러한 문제점들을 극복하고 동시에 비디오 콘텐츠를 효과적으로 보호하기 위해서 많은 암호화 기술들이 연구 되고 있다[1].

특히 최근에는 카오스 이론과 암호화의 밀접한 관련성으로 인해 카오스 사상(chaos map)에 기반 한 새로운 암호기술의 연구가 진행되고 있다. 카오스 사상은 초기 조건에 민감하게 반응 하여 난수 특성이 우수한 수열을 생성하기 때문에 일반 암호에서 요구하는 혼동(confusion)과 확산(diffusion) 특성과 깊은 관계를 가지고 있다[6].

카오스 사상을 기반으로 제안된 암호화 기법들은 둘 이상의 카오스 사상을 결합한 다중 카오스 기반의 암호화 알고리즘을 통해 이미지 또는 비디오를 암호화 한다. Lian은 CML(Coupled Map Lattice)을 기반으로 시공간 격자에 의해 생성되는 의사난수 수열을 영상 블록 안에서 선택된 매개변수에 대해 암호화 한다[7]. Gao 등은 지수승 함수와 탄젠트 함수를 결합하여 제안한 NCA(Nonlinear chaotic algorithm, 비선형 카오스 알고리즘) 로부터 생성된 카오스 수열을 이용하여 영상 데이터를 암호화 하였다[8]. 또한 Behnia 등은 카오스 사상을 혼합하여 생성된 사상을 기반으로 디지털 영상 암호기법을 제안하였고, 제안된 기법은 결합된 사상 등 고차원 카오스 시스템에 의해 매우 높은 안전성을 보장한다[3, 9]. Kwok 등은 스트림 암호 구조를 갖는 고속 카오스 기반 영상 암호 시스템을 제안하였다. 이 기법은 카오스 사상들을 폭포(cascade) 형태로 결합하여 의사난수 키스트림을 생성한다[3, 10].

본 논문에서는 MPEG-2 비디오 인코딩 과정 내에서 복수의 카오스 사상을 이용한 디지털 비디오 암호화 방법을 제안한다. 암호화에 사용되는 2^{128} 공간을 갖는 키 값은 텐트 사상(tent map)에 의해 빠르게 배포가 된다. 생성된 키 값을 기반으로 1, 2차원의 카오스 사상의 결합을 통해 난수특성이 우수한 난수블록을 생성한다. 난수블록은 DCT 이후의 영상 내 파급 효과가 큰 계수에 대해서만 선택적으로 암호화를 수행하여, 시각적인 보안을 유지하면서 암호화 처리에 따른 인코딩 오버헤드 측면에서 효과적으로 대응한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 카오스 사상의 특성과 1차원 카오스 사상인 로지스틱 사상과 2차원 카오스 사상인 헤논 사상에 대해 간략히 기술한다. Ⅲ장에서는 제안한 암호화 기법의 구조와 암호 키 생성 그리고 암/복호화 과정에 대해 기술한다. Ⅳ 장에서는 제안한 암호화 기법에 대한 암호화 보안성 및 성능평가를 기술하고 Ⅴ장에서 결론을 맺는다.

Ⅱ. 카오스 사상의 개요

카오스 사상의 혼동과 확산 특성은 빠른 처리와 높은 안전성을 요구하는 영상 암호화에 효과적인 방법으로 제시되고 있다. 본 장에서는 카오스 사상의 특성에 대해 간략하게 설명하고 본 논문에 적용된 로지스틱 사상과 헤논 사상의 랜덤특성에 대해 기술한다.

1. 카오스 사상의 특성

식 (1)과 같이 표현되는 차분 방정식을 반복하여 얻은 결과 값이 랜덤한 값을 가질 때 F 는 카오스 사상의 특성을 갖는다.

$$X_{n+1} = F(X_n), X_n \in [0,1] \quad (1)$$

카오스 사상은 일반적으로 다음과 같이 3가지 조건을 만족시켜야 카오스 특성을 가지고 있다고 한다[14].

- 파라미터에 대한 민감성 : 만일 카오스 사상의 모양을 결정하는 인자의 차이가 거의 없는 두 개의 카오스 사상을 생각할 때, 동일한 초기 값을

입력으로 하여 각각 반복하여 얻는 두 결과 값의 상관도는 거의 존재하지 않아야 한다.

- 초기조건에 대한 민감성 : 모든 카오스 사상은 초기 값(initial condition)에 매우 민감하게 반응한다. 초기 값이 아주 조금만 바뀌어도 그 결과에 따르는 시계열(time series)값은 크게 달라진다.
- 무작위성 : 거의 모든 가능한 초기 값을 입력으로 하여 카오스 사상을 반복해 얻는 결과 값들은 [0, 1) 구간에서 랜덤하게 발생해야 하며, 그들의 분포는 균일(uniform)해야 한다.

카오스 사상은 위에서 언급한 특성을 기반으로 많은 암호화 시스템에 다양한 방법에 의해서 결합되어 설계된다.

2. 로지스틱 사상(Logistic map)

식 (2)와 같이 정의할 수 있는 로지스틱 사상은 분기 파라미터 μ가 약 3.5695에서 4사이의 값을 가지면, 카오스 상태에 존재한다. 생성된 카오스 수열은 무한대에 가까운 주기성을 보이며, 수렴하지 않는 특성을 갖는다.

$$x_{n+1} = \mu x_n (1 - x_n) \tag{2}$$

초기치 x_0에서 매개변수 μ를 증가시켜가며 시계열의 정상상태의 x_n에 대해 나타내면 그림 1과 같은 그래프 형태를 얻을 수 있다. 매개변수 μ가 1과 3사이에서는 안정한 한 점의 상태를 가지지만 3이상의 구간에서 분기과정을 계속한다. 즉, μ가 증가함에 따라서 x_n과 $1-x_n$ 항이 수축과 팽창의 과정을 계속하면서 안정한 주기상태에서 분기과정을 반복하여 무한대의 주기성을 갖는 카오스 상태로 변화한다[13].

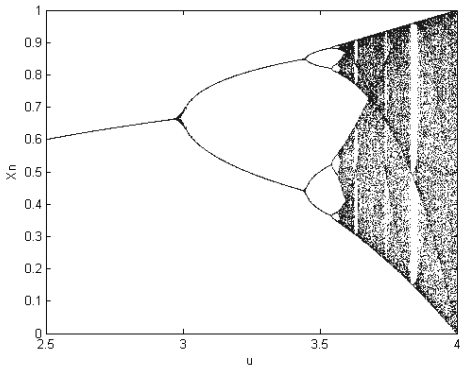

그림 1 로지스틱 사상의 분기 트리($2.5 \le \mu \le 4$)
Fig. 1. Bifurcation tree of the logistic map($2.5 \le \mu \le 4$).

3. 헤논 사상(Hénon map)

헤논 사상은 식 (3)과 같이 표현되는 2차원 카오스 사상이며, 파라미터 a와 b값은 카오스 신호를 발생하는 지배적인 값이다.

$$\begin{aligned} x_{n+1} &= y_n + 1 - a x_n^2 \\ y_{n+1} &= b x_n \end{aligned} \tag{3}$$

헤논 사상의 카오스 신호 특성은 그림 2에서 확인 할 수 있다. 파라미터 b를 0.3으로 고정한 상태에서 a의 변화 구간을 1.0부터 1.5까지 변화시켰을 때 발생 되는 x_n의 값을 볼 수 있다. 그림에서 보듯이 파라미터의 값에 따라 결과 값의 분포가 임의의 값으로 양분되면서 분포 하는 것을 확인 할 수 있으며, 이러한 분포는 카오스 신호로 암호화 된 신호 역시 임의의 값으로 분포되는 결과를 만들게 된다[15].

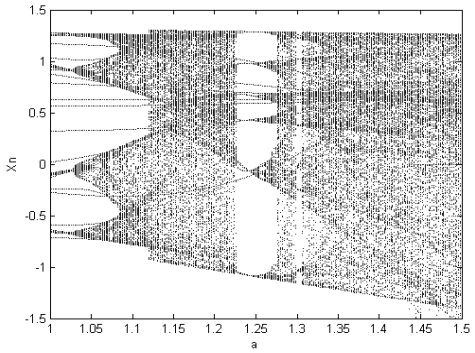

그림 2. 헤논 사상의 분기 트리($1 \le \mu \le 1.5$)
Fig. 2. Bifurcation tree of the Hénon map($1 \le \mu \le 1.5$).

Ⅲ. 카오스 사상을 이용한 비디오 암호화

본 장에서는 기존의 카오스 사상을 이용하여 다중 카오스 암호화 시스템을 제안하고, 각각의 단계에 적용되는 카오스 사상 기반의 암호화 방법에 대해 설명한다.

1. 제안하는 암호화 시스템의 구조

그림 3은 제안하는 암호화 방법의 전체구조를 나타낸다. 암호화는 MPEG-2 비디오 인코더의 DCT (Discrete Cosine Transform)이후에 생성된 8x8 DCT 블록 단위로 수행된다. 본격적인 암호화 과정에 앞서

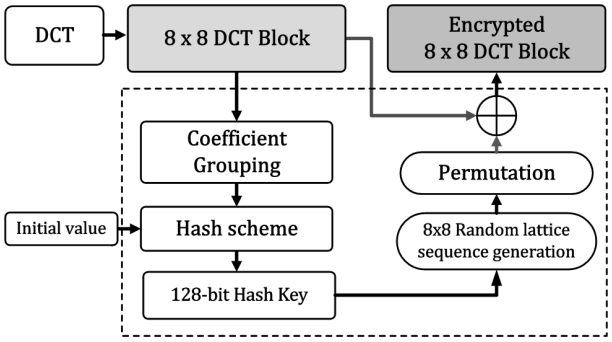

그림 3. 제안하는 다중 카오스 기반 비디오 암호화 구조

Fig. 3. Architecture of the proposed multiple chaos-based video encryption.

DCT 블록 내에서 DC계수와 이와 인접한 저주파 성분의 AC 계수들을 선택하여 그룹화 한다. 그룹화 된 계수들은 128-bit 해시 키를 생성하는 해시체인의 입력으로 사용된다. 생성된 해시 키는 로지스틱 사상의 초기값으로 사용되어 0에서 1 사이의 값을 갖는 64개의 난수로 구성된 8x8 난수블록을 생성하고, 난수블록의 랜덤 특성을 높이기 위해 헤논 사상을 이용하여 난수블록의 난수들에 대해 치환과정을 수행한다.

2. 암호화 과정

가. DCT 계수 선택과 계수 그룹화

계수의 그룹화 과정은 해시체인을 통해 128-bit 해시 키를 생성하기 위한 입력 데이터 결정 과정이다. DCT 이후 16-bit 정수형의 계수들은 그림 4와 같이 32-bit 크기의 4개의 그룹으로 묶여진다. 계수의 선택은 DCT 블록 내부에서 의미 있는 정보를 담고 있는 DC계수와 이와 인접한 7개의 AC계수가 선택 되어 진다[16].

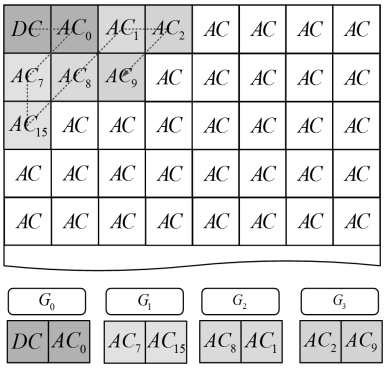

그림 4. 계수 선택 및 그룹화

Fig. 4. Coefficient selection and groupage.

나. 암호화 해시 키 생성

전 단계에서 생성된 계수들의 그룹을 입력 데이터로 하여 그림 5와 같이 제안한 해시체인을 통해 암호화에 사용되는 128-bit 해시 키를 생성한다. 각각의 해시블록은 1차원 카오스 사상인 텐트사상 $T(x)$로 구성된다.

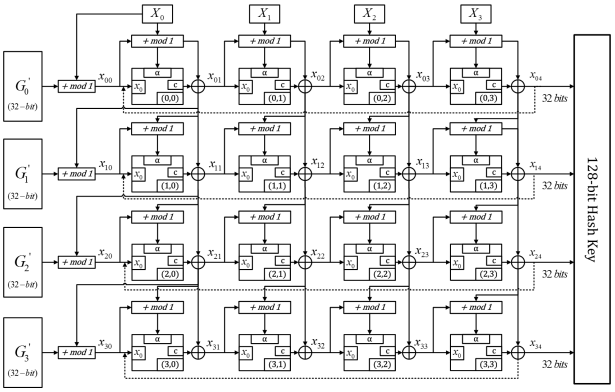

그림 5. 128-bit 해시 키 생성을 위한 제안하는 해시구조

Fig. 5. Structure of the proposed hash for 128-bit hash key generation.

(1) 텐트 사상 기반의 해시체인

해시체인 구조에 기본블록으로 사용되는 텐트 사상인 $T(x)$는 최근 암호 시스템에서 가장 단순하면서도 보편적으로 사용되는 카오스 사상이다. 이 사상은 오직 파라미터 α만을 갖으며, [0,1)의 구간을 정의역으로 취하고 같은 구간의 치역을 갖는다. 초기 파라미터 α를 갖는 텐트 사상은 식 (4)와 같이 정의 된다.

$$T_\alpha : x_{j+1} = \begin{cases} \dfrac{x_j}{\alpha}, & 0 \le x_j \le \alpha \\ \dfrac{1-x_j}{1-\alpha}, & \alpha < x_j \le 1 \end{cases} \tag{4}$$

계수그룹인 A와 B 그리고 C, D는 해시체인의 입력으로 사용되기 전 식 (5)와 (6)의 과정을 통해 [0,1) 범위의 값으로 정규화 된다. 이때 $X_i\,(i=0,1,2,3)$는 PRNG(Pseudo Random Number Generator)로부터 얻은 [0,1) 범위의 값을 초기 값으로 사용한다. X_0는 해시체인의 첫 번째 열에 대해서 매 행마다 갱신되어 각 행에 대한 정규화 과정에 사용된다[11].

$$G_i^{'} = (G_i + 0.8)/2^{32}, \quad i = 0,1,2,3 \tag{5}$$

$$x_{i0} \leftarrow (G_i^{'} + X_0^{(i+1),0}) \bmod 1,\ i = 0,1,2,3 \qquad (6)$$

(2) 텐트 사상의 반복

텐트사상을 기본으로 하는 해시체인의 블록들은 i번째의 행과 j번째의 열로 표현할 수 있다. 각각의 해시 블록은 $T_\alpha^{(i,j)}(x_0)$로 표현되며 전 단계의 블록인 $T_\alpha^{(i,j-1)}(x_0)$ 의 출력을 식 (4)의 초기 변수로 사용하고, 초기 파라미터 α는 식(7)과 (8)에 의해 각 블록에 대해 정의 된다.

$$\alpha = (x_{0j} + X_j) \bmod 1,\ i = 0,\ j = 0,1,2,3 \qquad (7)$$

$$\alpha = (x_{(i+1)j} + x_{i(j+1)}) \bmod 1, j = 0,1,2, j = 0,1,2,3 \qquad (8)$$

제안한 해시체인은 CBC(Cipher-Block Chaining)방식으로 반복 될 수 있다. 각각의 블록 행에 대한 최종 출력 $x_{i4}\,(i = 0,1,2,3)$는 반복과정이 수행 될 때 해시 블록 $T_\alpha^{(i,0)}(x_0)$의 입력으로 사용됨으로써 해시체인의 최종 출력 $x_{04}, x_{14}, x_{24}, x_{34}$ 는 갱신된다. 모든 블록에 대한 처리과정 후에 최종 출력 x_{04}, x_{14}, x_{24} 그리고 x_{34}는 식 (9)와 같이 32-bit로 추출 된다.

$$0.(b_0 b_1 b_2 b_3 b_4 \ldots b_{28} b_{29} b_{30} b_{31})_{(2)}, b_i \in \{0,1\} \qquad (9)$$

추출된 네 개의 32-bit 이진 수열은 h_0, h_1, h_2, h_3로 정의 할 수 있고, 128-bit 해시 키는 $h = (h_0, h_1, h_2, h_3)$와 같이 정의된다.

다. 난수블록 생성

본 단계는 해시체인에 의해 얻어진 128-bit 해시 키로부터 64개의 난수를 갖는 8x8 블록을 생성한다. 난수블록은 앞서 Ⅱ장에서 기술한 로지스틱 사상을 기반으로 생성되어지며, 로지스틱 사상은 생성된 해시 키 값을 초기 변수로 사용한다. 이를 위해 128-bit 해시 키는 식 (10)과 같이 [0,1) 범위의 실수 값을 갖는 8개의 보조키(sub-key)들로 나누어진다.

$$K_i = \frac{h_{16i} h_{16i+1} \cdots h_{16i+15}}{2^{16}},\ i = 0,1,\ldots,7 \qquad (10)$$

보조키 $K_i\,(i = 0,1,\ldots,7)$는 암호화에 사용되는 64개의 난수를 갖는 난수블록을 생성하는데 사용되며, 블록내의 난수 $R_i = r_{i0}, r_{i1}, \ldots, r_{i7}$는 식 (11)을 이용하여 생성된다.

$$\begin{cases} r_{ij} = f^{t_0+j}(K_i),\ i,j = 0,1,\ldots,7 \\ f(x) = \mu x(1-x) \end{cases} \qquad (11)$$

r_{ij} 는 로지스틱 사상 $f(x)$가 반복됨에 따라 [0,1) 구간의 랜덤한 수열이 생성되며 해당 블록의 위치에 그림 6과 같은 난수블록을 생성 한다.

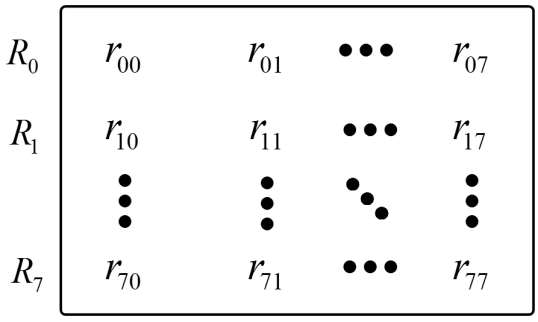

그림 6. 8x8 난수블록 생성
Fig. 6. 8x8 random-number block generation.

라. 난수블록의 계수 치환

본 단계에서는 Ⅱ장에서 기술한 헤논 사상을 이용하

표 1. 헤논 사상을 이용한 8x8 난수블록 치환
Table 1. 8x8 encryption lattice cipher permutation using Hénon map.

```
Input : K[8] (sub_key)
Output : Permutated r[8][8]

function Henon_map_Operation()
{
  for(int i = 0; i < 8; i++)
    for(int j = 0; j < 8; j++)
      r[i][j] = Logistic_map_Operation(K[i]);

  for(int x = 0; x < 8; x++)
    for(int y = 0; y < 8; y++){
      xn = abs(y + 1 - a* pow(x,2)) mod 8;
      yn = abs(b * x) mod 8;

      r[xn][yn] = r[x][y];
    }
}
```

여 난수 블록의 랜덤 특성을 높이기 위해 표 1과 같이 블록 내의 난수들의 위치에 대한 치환(permutation)과정을 수행한다.

라. 난수블록을 이용한 블록 암/복호화

생성된 난수블록은 본래의 DCT 블록과 각각의 위치에서 식 (12)와 같이 XOR 블록 암호화를 수행하고 암호화된 DCT 블록을 생성한다. 여기서 q 와 c는 각각 본래의 DCT 계수와 암호화된 DCT 계수를 의미한다.

$$c_{ij} = q_{ij} \oplus r_{ij},\ i,j = 0,1,\dots,7 \tag{12}$$

하지만 난수블록의 난수들은 [0,1) 범위의 실수 값을 갖고 있기 때문에 식 (13) 과 같이 16-bit의 정수형으로 정규화 되어 사용한다.

$$0.(b_0 b_1 b_2 \dots b_{13} b_{14} b_{15})_{(2)}, b_i \in \{0,1\} \tag{13}$$

복호화 과정은 암호화 과정과 대칭적으로 수행되어지며 식 (14)와 같다.

$$q_{ij} = c_{ij} \oplus r_{ij},\ i,j = 0,1,\dots,7 \tag{14}$$

Ⅳ. 성능 평가

본 장에서는 Ⅲ장에서 기술한 제안기법의 암호화 성능 및 암호화에 따른 압축 효율성에 대해 분석한다. 제안한 기법은 웹사이트 www.MPEG-2.org 에 오픈 소스로 공개되어 있는 MPGE 인코더 소스인 mpeg2enc 내에 Visual C++ 2005를 이용하여 암호화 과정을 구현하였다. 또한 구현된 시스템을 위한 실험환경은 표 2와 같다.

실험에서는 CIF 포맷의 영상인 'coastguard', 'hallmonitor', 'football', 'stefan', 'mobile', 'foreman'을 사용하여 제안 기법의 암호화에 따른 시각적 암호화 성능과 암호화 효율성을 판단하는데 사용하였다.

표 2. 실험 환경
Table 2 Experimental Environment.

항목	시스템 사양
CPU	Intel core 2 (2.4Ghz)
메모리	DDR2 1G*2개
운영체제	Windows XP

가. 키 공간 분석

암호 키 공간은 암호화 기법에 있어서 전사공격(brute-force attack)에 대응할 만큼 충분한 크기를 가져야 한다. 본 제안 기법에서 해시체인으로부터 생성된 128-bit비밀 해시 키 h는 해시 값 h_0, h_1, h_2, h_3로 이루어져 있으며 암호화와 복호화를 위한 암호화 난수블록을 생성하는데 사용된다. 따라서 해시체인의 입력 데이터(G_0', G_1', G_2', G_3')와 초기 값(X_0, X_1, X_2, X_4)으로부터 생성되는 해시 키 공간은 $2^{128} \approx 3.4028 \times 10^{38}$의 충분히 큰 키 공간을 가지고 있다.

나. 암호화 알고리즘의 보안성

2^{128} 의 공간을 갖는 해시 키와 카오스 사상을 통해 생성된 난수 블록은 $2^{128} \approx 3.4028 \times 10^{38}$ 의 키 공간을 고려해야 하므로 암호문 공격(ciphertext-only attack) 에 대응할 만큼의 충분한 키 공간을 확보하고 있다. 또한 프레임 내 일부분의 암호화 된 DCT 블록과 본래의 DCT 정보를 알고 있더라도, DCT 블록 단위로 난수블록이 생성되는 본 방법에서는 해시체인에 의해 생성된 해시 키에 대한 정보와 그에 상응하는 난수블록을 모두 고려해줘야 한다. 마찬가지로 일부분의 본래 DCT 블록과 XOR를 취한 난수블록에 대한 정보를 알 수 있다고 하더라고, 프레임 내의 모든 인트라 블록에 적용된 난수블록과 해시 키 값을 추측하기란 힘들다. 때문에 알려진 평문공격(known-plaintext-attack)과 선택된 평문 공격(chosen-plaintext-attack)에 대응 가능하다.

다. 초기 값 민감도 분석

제안된 기법의 초기 값에 대한 민감도를 평가하기 위해 해시체인의 초기 입력이 0.4829201895인 X_0의 값을 0.4829201896의 X_0'로 미세하게 변화하여 입력했을 때 발생되는 두 난수블록에 대한 상관계수를 구한

표 3. 초기 값 X_0 의 미세한 차이에 의해 생성된 두 난수블록간의 상관계수
Table 3. Correlation coefficient between encryption lattice by slight different of initial value X_0.

반복 횟수	1	2	3	4
$X_0 \rightarrow X_0'$	0.1178	0.0902	0.0754	0.0748

다. 또한 해시체인은 CBC 방식으로 반복될 수 있기 때문에 반복 횟수를 고려하였고 로지스틱 사상의 매개변수인 μ를 4로 고정 시킨 상태에서 상관계수를 구하였다. 결과는 표 3과 같다.

상관계수는 1에 가까울수록 두 변량 간에 연관성을 찾을 수 있으며 상관계수 r 이 $|r| \geq 0.65$ 일 때 두 변량 간의 상관관계에 대한 의미가 있다. 표 3에서 보듯이 초기 입력에 대해 미세한 차이를 두고 생성된 두 블록 내 난수들의 상관계수는 해시체인의 반복 횟수에 따라 0에 근접한 값을 보인다. 하지만 반복 횟수에 상관없이 두 변량간의 유의성을 찾아보기 힘든 수치를 나타내기 때문에 앞으로의 실험에서는 해시체인의 반복 과정은 생략한다.

라. 압축 효율성

압축 효율성은 암호화에 따른 압축 변화율과 시간 변화율을 포함하고 있으며, 본 실험에서는 제안 방법의 압축 효율성을 S. Lian 이 제안한 시공간 카오스 시스템 기반의 암호화 알고리즘[7]과 비교하였다. 시공간 카오스 시스템은 이차원으로 결합된 카오스 사상 기반으로 시공간적인 랜덤 특성을 나타내는 64개의 난수 수열을 시공간 격자에 의해 생성하고, 각각의 수열의 난수들은 DCT 블록의 선택된 계수들에 대해 암호화를 수행한다. 해시체인에 의해 배포된 해시 키를 기반으로 로지스틱 사상 및 헤논 사상을 이용하여 난수블록을 만드는 제안한 방법과 다르게 시공간 카오스 암호화 시스템은 초기 난수 격자의 시간적 반복을 통해 생성된 수열을 기반으로 블록 암호화를 수행한다. 표 4는 제안한 방법과 시공간 카오스 암호화 시스템의 압축효율성에 대한 비교 수치를 나타낸다. 표에서 알 수 있듯이 제안한 방법이 Lian의 방법에 비해 암호화에 따른 시간 변화율 측면에서 약 0.3% 높게 나타났지만, 압축 이후의 데이터 오버헤드 측면에서 0.2% 적게 나타나는 성능을 보였다. 이는 Lian의 방법은 128-bit 초기 키 값 생성 과정을 고려하지 않는 반면에 제안한 방법의 128-bit 해시 키 생성 과정은 많은 오버헤드를 차지하기 때문에 이러한 결과가 나타난 것으로 판단된다. 하지만 일반적으로 암호화에 의한 시간 변화율은 10% 미만일 때 인코딩 과정에 크게 영향을 미치지 않는 수치이고, 실시간 환경에 적용이 가능 하다[17~18]. 또한 표 5를 통해 암호화 과정에서 계수의 선택이 변화율에 많은 영향을 주는 것을 알 수 있었고, 실험 영상에 대한 계수의 선택적 암호화에 관계없이 평균적으로 2% 이내의 시간 변화율을 보였으며, 오직 DC 계수에 대해 암호화를 수행을 했을 경우 압축 효율성이 가장 좋게 나타났다.

추가로 L. Tang의 DCT 블록 계수들에 대한 단순치환방법[4]과 제안한 방법을 비교하였을 때, 제안한 방법이 인코딩 오버헤드 측면에서 낮은 성능을 보이지만, 압축률 측면에서 우수한 성능을 보인다. Tang의 방법의 경우 비교적 단순한 치환 과정을 사용하였기 때문에 제안한 방법에 비해서 인코딩 오버헤드 측면에서 좋은 성능을 보였다. 하지만 Tang의 단순치환 방법은 DCT 계수들의 지그재그 순서에 대한 영상코덱 부호화 구문을 고려하지 않기 때문에 제안한 방법과 비교했을 때 압축률 측면에서 매우 낮은 성능을 보였다. 또한 Tang의 방법은 암호학적 보안성 측면에서 알려진 평문공격(known-plaintext attack)에 취약함을 갖고 있다[19].

마. 시각적 암호화 평가

Liu, et. al[12]과 Meyer, et. al[21]의 주장에 의하면 일반적으로 DCT 이후의 많은 정보들은 저주파 쪽에 집중되기 때문에 DC와 이와 인접한 7개에서 9개의 AC 계수들에 대해서만 암호화를 수행해도 주어진 영상의 주요 정보들을 숨기기에 충분하다.

따라서 본 제안방법은 암호화에 따른 인코딩 시간의 오버헤드를 최소화하기 위해 인트라 블록(intra-block)의 DC 계수와 7개의 AC계수에 대해서만 선택적으로 암호화를 수행한다. 그림 7은 각각의 실험 영상에 대한 원본 영상과 암호화 되는 DCT 계수에 따른 암호화 후의 결과 영상을 보여준다. 오직 7개의 AC 계수들에 대해서 암호화가 수행될 경우, 영상의 전반적인 정보가 드러남에 따라 시각적 암호화 수준이 매우 떨어졌다. 반면에 DC 계수만을 암호화 했을 경우 영상의 전체 정보를 판단할 수 없었지만 영상 내 움직임 성분에 대해 취약함을 나타냈고, DC와 7개의 AC 계수에 대한 암호화는 DC 혹은 AC 만을 암호화 했을 경우의 단점을 보완하며 영상 내 밝기 정보 및 움직임에 대해 전혀 인지할 수 없을 정도의 수준을 나타냈다.

PSNR(Peak Signal-to-Noise Ratio)은 암호화 된 영상의 시각적 인식을 통한 암호화 평가 이외에 객관적인 영상의 품질을 나타내기 위한 측정방법으로 사용된다[7, 20]. 일반적으로 PSNR이 15dB 이하일 경우에 본래의 영상과의 상관도를 거의 갖고 있지 않으며, 그림 8을 통해 전체 실험 영상에 대해 12dB 이하의 수치를 나타냈

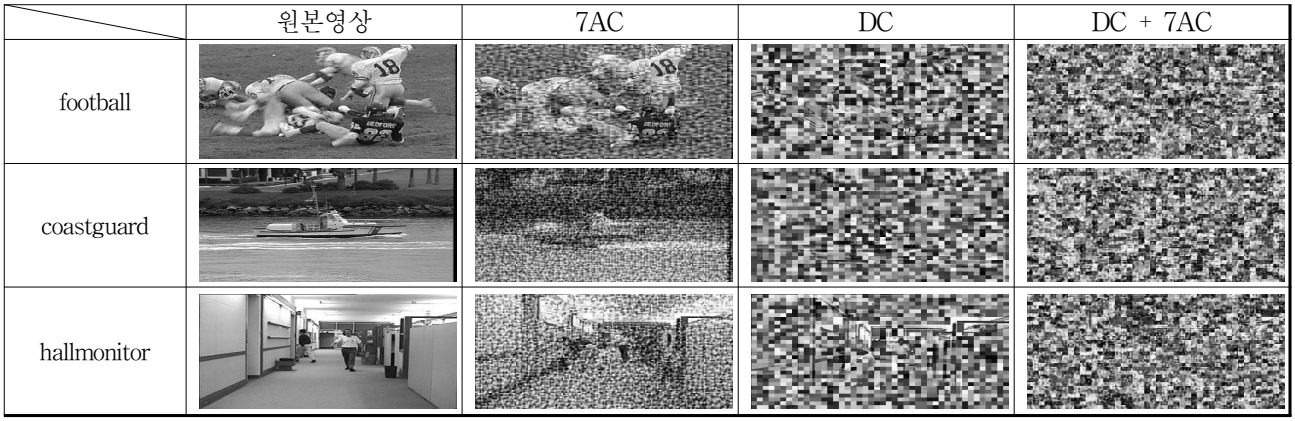

그림 7. 암호화 되는 계수의 경우에 따른 비디오 암호화
(a) 원본영상, (b) 7개의 AC 암호화, (c) DC 암호화, (d) DC+7AC 암호화
Fig. 7. Video encryption in different case, (a) original, (b) 7AC encryption, (c) DC encryption, (d) DC+7AC encryption.

표 4. 제안 방법과 S. Lian 의 알고리즘[7] 그리고 Lei Tang의 알고리즘[4]에 대한 암호화에 따른 압축효율성 비교
Table 4. Processing overhead of proposed method and other method on Three video sequences.

비디오(I:P:B)	해상도	제안 방법 DC+7AC		S. Lian의 방법[7] DC+ACsign		Lei Tang의 방법[4] 모든 계수	
		암호화/인코딩(%)	암호화/압축(%)	암호화/인코딩(%)	암호화/압축(%)	암호화/인코딩(%)	암호화/압축(%)
football(21:42:62)	352x288	1.83	0.35	1.52	0.53	0.65	17.77
coastguard(26:75:199)	352x288	1.92	0.29	1.58	0.52	0.54	12.05
hall monitor(76:75:149)	352x288	1.76	0.37	1.45	0.48	0.75	14.22

표 5. 암호화 적용 후의 인코딩 변화율과 데이터 크기 변화율
Table 5. The time ratio and compression ratio after applying encryption.

비디오(I:P:B)	해상도(프레임 수)	시간 비율(time ratio) 암호화/인코딩(%)		압축 비율(compression ratio) 암호화/압축(%)	
		DC	7 AC	DC	7 AC
football(21:42:62)	352x288(125)	0.45	1.24	0.02	0.07
coastguard(26:75:199)	352x288(300)	0.37	1.65	0.03	0.05
hall monitor(76:75:149)	352x288(300)	0.28	1.53	0.02	0.08

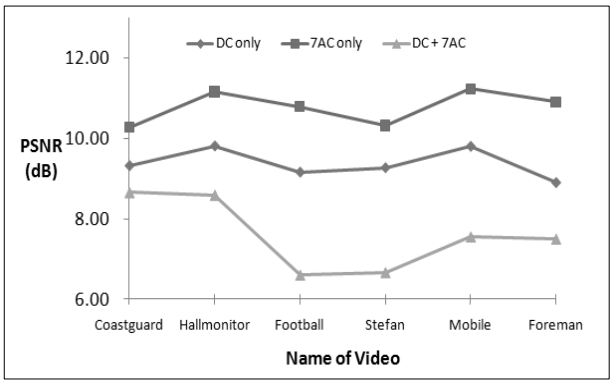

그림 8. 각각의 암호화 경우에 따른 PSNR 비교
Fig. 8. Comparison of the PSNR in different cases.

다. 앞선 압축 효율성 평가와 본 실험 결과로부터 오직 DC 계수만을 선택적으로 암호화를 하여도 최소의 오버헤드만을 발생시키면서 충분한 시각적 암호화 성능을 유지 할 수 있음을 알 수 있다.

V. 결 론

본 논문에서는 복수의 카오스 사상 기반의 비디오 암호화 방법을 제안하였다. 텐트 사상 기반의 해시체인으로부터 난수 특성이 우수한 키 값을 생성하고, 1, 2차원의 카오스 사상에 의해 생성된 난수블록을 인트라 블록

의 DCT 계수에 대해 선택적으로 암호화함으로써 영상에 대한 왜곡을 유도하였다.

본 논문에서 제안된 기법은 시각적인 보안 수준을 유지하면서 압축효율성에 최소한의 오버헤드만을 발생시키기 위함을 목적으로 하였다. 실험을 통해 얻어진 암호화 영상은 시각적 암호화에 매우 효과적인 특성을 보였지만 암호화 적용으로 인해 전체적인 인코딩 수행 속도와 데이터 크기에 있어서 오버헤드가 발생하였다.

전체적인 실험 결과를 토대로 제안 기법은 암호화 이후에 포맷의 변화 없이 우수한 암호화 특성을 유지하면서 압축 효율성에 작은 오버헤드만을 발생 시켰다. 이러한 특성을 통해 실시간성과 영상 콘텐츠에 대한 높은 보안을 요구하는 환경에서 효과적으로 응용 될 수 있을 것으로 기대된다.

참 고 문 헌

[1] Fuwen Liu, Harmut Koenig, “A survey of video encryption algorithms,” Computers & Security, vol. 29, no 1, pp. 3-15, 2010.

[2] I. Agi and L. Gong, “An Empirical Study of MPEG Video Transmissions,” Proceedings of the Internet Society Symposium on Network and Distributed System Security, pp. 137-144, Feb. 1996.

[3] 남길현, 고승철, “카오스 사상 기반 영상 암호 알고리즘 동향,” 정보보호학회지, 제20권 제3호, 43-56쪽, 2010년 6월

[4] L. Tang, “Methods for encrypting and decrypting MPEG video data efficiently,” in Proc. 4th ACM Int. Conference on Multimedia, pp. 219-230, 1996.

[5] B. Bhargava, C. Shi, and Y. Wang. “MPEG video encryption algorithms,” Multimedia Tools and Applications, pp. 57-79, 2004.

[6] 신재호, 이성우, “PLCM을 이용한 카오스 블록 암호화,” 전자공학회논문지 제43권 CI편, 제3호, 10-19쪽, 2006년 5월

[7] Lian Shiguo, “Efficient image or video encryption based on spatiotemporal chaos system,” Chaos Soliton Fract, 40 pp. 2509-2519, 2009.

[8] Gao Haojiang, Zhang Yisheng, Liang Shuyun, and Li Dequn, “A new chaotic algorithm for image encryption,” Chaos Soliton Fract 29 pp. 339-393, 2006.

[9] Behnia S, Akhshani A, Mahmodi H, and Akhavan A, “A novel algorithm for image encryption based on mixture of chaotic maps”, Chaos Soliton Fract 35, pp. 408-419, 2008.

[10] Kwok BS, Wallace K, and Tang S, “A fast image encryption system based on chaotic maps with finite precision representation,” Chaos Soliton Fract 32, pp. 1518-1529, 2007.

[11] Yang, H., Wong, K.W., Liao, X., Zhang, W., Wei, “A Fast image encryption and Authentication Scheme based on Chaotic maps,” Communications in Nolinear Science and Numerical Simulation,Vol 15, no. 11, pp. 3507-3517, 2010.

[12] Zheng Liu, Xue Li, and Zhaoyan Dong , Enhancing Security of Frequency Domain Video Encryption , In proc. of ACM Multimedia , pp. 304-307, 2004.

[13] Shiguo Lian, Jinsheng Sun, Zhiquan Wang, Yuewei Dai, “Fast Video Encryption Scheme Based-on Chaos“, 2004 8th International Conference on Control, Automation, Robotics and Vision (ICARCV), pp. 126-131, 2004.

[14] 이성우, 신재호, “다중 카오스 사상을 이용한 영상 암호시스템 설계,” 정보보호학회지, 제14권 제4호, 188-194쪽, 2004년 8월

[15] 임거수, “혼돈신호에 따른 암호화 정도 분석,” 한국정보기술학회지, 제7권 제6호, 167-171, 2009년 12월

[16] ISO. “ISO/IEC 13818-2:2000 - Information technology - Generic coding of moving pictures and associated audio information: Video”. ISO. Retrieved 31 October 2009.

[17] Lian Shiguo, Sun J, Wang Z., “A chaotic stream cipher and the usage in video protection,” Chaos Soliton Fract, vol.34, no.3, pp. 851-859, 2007.

[18] Lian Shiguo, Z. Liu, Z. Ren, and H. Wang, “Secure Advanced Video Coding Based on Selective Encryption Algorithms,” IEEE Trans. on Consumer Electronics, vol.52, no.2, pp.621-629, 2006.

[19] Lintian Qiao, Klara Nahrstedt, “Is MPEG encryption by using random list instead of zigzag order secure,” in Proc. IEEE Int. Symposium on Consumer Electronics(ISCE)'97, 1997, pp. 332-335

[20] S. Lian, Z. Liu, Z. Ren, and H. Wang, “Secure distribution scheme for compressed data streams,” in Proceedings of the IEEE Conference on Image Processing (ICIP ''06), April 2006.

[21] Meyer, J. and Gadegast, F., “Security Mechanism for Multimedia Data with the

example MPEG-1 video," Project Description of SECMPEG, Technical University of Berlin, Germany, May 1995.

저 자 소 개

윤 병 춘(학생회원)
2010년 수원대학교 전자공학과 학사 졸업.
2010년～현재 인하대학교 전자공학과 석사과정
<주관심분야 : 비디오 암호화, 시각정보처리, 임베디드 시스템>

김 덕 환(정회원)-교신저자
2003년 한국과학기술원 컴퓨터 공학 박사.
2006년～현재 인하대학교 전자공학부 교수
<주관심분야 : 시각정보처리, 스토리지 시스템, 임베디드 시스템>