情 報 保 護 學 會 誌
第20卷 第3號, 2010. 6

카오스 사상 기반 영상 암호 알고리즘 동향

남 길 현*, 고 승 철*, 박 춘 식**

요 약

오늘날 멀티미디어 응용의 인기는 매우 빠르게 확대되고 있는 추세이며, VoD 서비스 또는 화상 업무회의 등의 상업적 용도에서 영상의 암호화는 기본적인 요구사항으로 간주되고 있다. 본 논문에서는 영상통신의 필수요소인 데이터 압축과 암호화의 관계에 따라 암호 알고리즘을 분류하고, 알고리즘들의 성질과 응용 한계에 대한 조사 결과를 소개한다. 소개된 결과에 따르면, 영상 암호 알고리즘 각각은 고유의 강점과 취약점들이 있으며, 어떠한 알고리즘도 모든 조건들을 만족하지 않음을 알 수 있다. 이러한 조사 결과에 의해, 사용자들은 자신의 응용에 적합한 암호 알고리즘을 선택할 수 있다. 본 논문에서는 또한 다양한 기법들이 제안되고 있는 카오스 사상 기반 영상 암호 알고리즘 동향을 소개한다.

Ⅰ. 서 론

오늘날 정보통신 기술과 인터넷의 발전에 따라, IPTV, 디지털 CCTV 등 멀티미디어(multimedia) 데이터 기반 서비스가 출현하고 있으며, 최근에는 특히 스마트폰 기반 정보통신 서비스들이 선풍적인 인기를 얻고 있다.

그러나 이러한 서비스들은 국가 생산성 증진과 안전한 일상 환경 구축 및 다양한 볼거리 제공 등 긍정적인 측면과 더불어 디지털 콘텐츠의 저작권 침해와 서비스 이용자의 개인정보 침해 가능성 증대 등의 역기능에 관한 사회적 연구과제들을 도출하고 있다. 영상 데이터 의 대표적인 시스템인 CCTV의 설치 및 활용 증대로 인한 불특정다수의 초상권, 정보자기결정권, 사생활 침해 등 영상 감시에 대한 문제점은 이미 여러 문헌들에 많이 지적되고 있다[1]. 특히 디지털 CCTV에 의해 생성된 영상 정보는 국내 개인정보보호 지침에 의해 반드시 암호화하여 데이터베이스에 저장하도록 규정되어 있으나[2], 여러 가지 기술적 및 업체 사정으로 지침준수가 용이하지 않는 실정이다.

영상 데이터 암호 알고리즘은 이러한 역기능에 대처하는 가장 기본적인 도구로 인식된다. 암호화는 디지털 CCTV에 의해 생성된 영상정보들과 디지털 콘텐츠의 저작권을 보호하는 가장 효율적인 도구이다. 그러나 영상 데이터의 크기는 통상적으로 매우 거대하기 때문에, 필수적으로 데이터 처리 지연을 초래하고, 그 결과 실시간 처리가 곤란해지는 경우가 발생될 수 있다. 따라서 이러한 응용별로 적합한 암호 알고리즘을 개발 및 선택하는 일은 화상 데이터 보호의 첫 걸음이라고 할 수 있다.

국내에서도 이미 1990년대 중반부터 영상 암호화에 대한 연구들이 여러 학회들과 연구소 및 산업계에서 진행 되었으며, 최근에는 특히 타원곡선 암호 등 보안 수준이 높은 영상 데이터 암호방식에 대한 연구결과들이 발표되고 있다[3]. 그러나 영상 데이터 암호의 실시간 처리와 보안 수준과 관련하여 다양한 해결과제들이 남아있는 실정이다.

본 논문에서는 영상통신의 필수요소인 데이터 압축과 암호화의 관계에 따라 암호 알고리즘을 분류하고, 알고리즘들의 성질과 응용 한계에 대한 조사 결과를 소개한다. 이러한 조사 결과에 의해, 사용자들은 자신의 응용에 적합한 암호 알고리즘을 선택할 수 있다.

카오스 사상(chaotic map)은 초기 조건에 민감하게 반응하며 난수 특성이 우수한 수열을 생성하기 때문에, 지난 25년간 다양한 암호 알고리즘의 기본 요소로 활용

이 논문은 한국과학기술정보연구원 ReSEAT 프로그램의 지원으로 작성되었습니다.
* 한국과학기술정보연구원 ReSEAT 프로그램 전문연구위원(khnammk@reseat.re.kr, goh5703@reseat.re.kr)
** 서울여자대학교 클라우드컴퓨팅연구센터 정보보호학과 (csp@swu.ac.kr)

되어 왔다. 카오스 사상 기반 암호 알고리즘은 복수의 사상들을 다양한 방법에 의해 결합하여 영상 또는 텍스트 데이터를 암호화한다. 본 논문에서는 카오스 사상 기반 다양한 영상 암호 알고리즘에 관한 최근 개발동향을 소개한다.

Ⅱ. 영상 암호 알고리즘의 분류

영상 압축과 암호화는 보안 기능을 제공하는 멀티미디어 시스템과 응용에서 서로 밀접하게 관련되는 영상처리 과정들이다. 본 장에서는 암호 기능이 적용되는 위치에 따라 암호 알고리즘들을 분류한 Liu와 Koenig의 분류 기법을 소개한다[4].

영상 암호 알고리즘들은 암호 기능이 적용되는 위치에 따라 압축과 암호 결합 알고리즘과 압축 독립적 암호 알고리즘으로 분류된다. 압축과 암호 결합 알고리즘은 암호화가 압축 알고리즘 내부에서 수행되는 알고리즘을 지칭하며, 압축 독립적 암호 알고리즘은 암호 기능이 압축과정 이전 또는 이후에 적용되는 알고리즘들을 의미한다.

2.1. 압축과 암호 결합 알고리즘

영상 압축 알고리즘은 변환과 양자화 및 엔트로피 코딩 등으로 구성된다. 이러한 압축 과정에서 암호 기능이 적용되는 위치에 따라, 압축과 암호 결합 알고리즘들은 변환 이후 암호화 알고리즘과 양자화 이후 암호화 알고리즘 및 엔트로피 코딩 내부에서 암호화가 적용되는 알고리즘으로 세분될 수 있다.

변환 이후 암호화 알고리즘의 대표적 예로서 Zeng-Lei의 주파수 영역 스크램블 알고리즘을 들 수 있다. 양자화 이후 알고리즘으로서는 Tang이 제안한 zigzag permutation 알고리즘과 Shi-Wang-Bhargava의 real-time video encryption algorithm(RVEA) 등이 있다.

엔트로피 코딩 내부 암호화 알고리즘으로, Wu-Kuo의 MTH(Multiple Huffman Table)과 Xie-Kuo의 REC/RPB(Randomized Entropy coding and Rotation in Partitioned Bit stream) 등을 들 수 있다.

2.2. 압축 독립적 암호 알고리즘

압축 독립적 암호 알고리즘들도 또한 암호화 적용 위치에 따라 암축 이전 암호화 알고리즘과 압축 이후 암호화 알고리즘으로 세분된다.

압축 이전에 암호화를 적용하면 압축 효율이 매우 낮아지는 단점이 존재한다. 따라서 압축 이전에 암호화를 적용하는 기법은 거의 사용되지 않는다. Pazarci-Dipcin 기법과 상관관계 유지 화상 암호화 알고리즘 등은 이러한 방식의 대표적 예이다.

압축 이후에 암호화를 적용하는 알고리즘으로는, Meyer-Gadegast이 제안한 SECMPEG(Secure MPEG)과 Qiao-Nahrstedt의 VEA(video encryption algorithm) 그리고 Liu-Koenig가 제안한 퍼즐(puzzle) 알고리즘 및 Wen 등의 format-compliant encryption framework 등을 들 수 있다.

Ⅲ. 영상 암호 알고리즘 평가

3.1. 영상 암호 알고리즘 평가 요소

텍스트 통신과 대비되는 영상 통신의 특성으로서, 데이터 크기가 거대한 점과 실시간 처리가 요구되며, 표준화된 화상 코덱 기법 및 압축 포맷 사용 의무화 및 응용에 특화된 보안 요구조건이 존재하는 점 등을 들 수 있다.

영상 암호 알고리즘의 여러 평가 요소들은 이러한 화상통신의 특성에 기인한다. 본 논문에서는 암호화 효율, 보안수준, 영상 코덱 표준 준수, 압축효율, 구문 준수, 지각적 암호화 가능성 등을 주요 화상 암호 알고리즘 평가 요소로 고려한다.

문법 준수는 화상 스트림을 암호화한 결과가 화상 스트림의 압축에 관한 표준 문법을 준수하는 것을 의미한다. 오락 산업에서는 콘텐츠를 홍보할 목적으로 암호화된 콘텐츠의 일부를 고객에게 보여주는 기능이 필요하다. 이런 기능을 제공하는 암호 기법을 지각적 암호화라고 부른다.

3.2. 영상 암호 알고리즘 평가 결과

영상 암호 알고리즘들의 특성을 조사한 결과, 각 알고리즘들은 평가요소별로 서로 다른 장단점을 보이고 있으나, 압축과 암호 결합 알고리즘들은 영상 코덱 내부에서 암호화가 적용되는 특성 때문에, 화상 코덱 표준을 준수하지 않으나, 구문 표준은 준수하는 공통적인 특성

을 보이고 있다. 이와 반면에, 압축 독립적 암호 알고리즘들은 압축과 암호화가 별도로 적용되는 특성 때문에, 영상 코덱 표준을 준수하며, 압축 효율을 보존하는 공통적인 특성들을 보이고 있다.

압축과 암호 결합 알고리즘들은 원래의 코딩 과정을 단순히 변형하여 암호화를 처리한다. 따라서 암호화 처리에 소요되는 계산 부담이 극히 미미하며, 일반적으로 압축 독립적 암호 알고리즘들에 비해 암호화 효율이 매우 우수하다. 거의 대부분의 영상 데이터 암호 알고리즘들은 이미 알려진 공격방식에 의해 해독이 가능하며, 공격이 불가능한 것으로 알려진 알고리즘의 경우에도 전통적인 데이터 암호 알고리즘과는 비교할 수 없을 정도로 보안 수준이 매우 낮다. 따라서 영상 데이터 암호 알고리즘들은 주로 VoD(Video on Demand) 또는 일반 영상회의 등의 응용에서 채택되고 있으며, 군사 또는 외교 등의 응용분야에서는 거의 채택되지 않는 실정이다.

압축과 암호 결합 알고리즘들의 구현과정은 필수적으로 기존의 영상 코덱 시스템의 변형을 요구한다. 따라서 압축과 암호 결합 알고리즘은 하드웨어로 구현된 영상 코덱 시스템과는 통합이 불가능하며, 오직 소프트웨어로 구현된 시스템과의 통합만이 가능하다. 이와 반면에 압축과는 상관없이 암호 처리가 이루어지는 압축 독립적 암호 알고리즘들은 코덱 시스템과는 상관없이 구현될 수 있다.

영상 코덱에 암호 기능이 통합된 압축과 암호 결합 알고리즘들은 필연적으로 압축 효율의 심각한 저하를 초래한다. 이와 반면에 압축 독립적 암호 알고리즘은 일반적으로 기존 코덱의 압축 효율을 유지할 수 있다.

압축 독립적 암호 알고리즘은 일반적으로 기존 코덱의 압축 효율을 유지할 수 있다. 그러나 format-compliant encryption framework는 예외적으로 9% 정도의 효율 저하를 초래한다. 영상 스트림들의 구문은 압축 마지막 단계에서 포맷이 결정되기 때문에, 압축과 암호 결합 알고리즘들에 의해 암호화된 영상 스트림들은 본질적으로 표준 구문을 준수한다.

압축 독립적 암호 알고리즘 경우, 암호화가 압축과정 이전에 처리되는 알고리즘에 의해 암호화된 데이터들은 표준 구문을 준수한다. 그러나 대부분의 압축 독립적 암호 알고리즘들은 압축 이후에 암호화를 처리하기 때문에, 암호화된 화상 데이터들은 표준 구문을 준수할 수 없다.

format-compliant encryption framework와 주파수 영역 스크램블 알고리즘은 지각적 암호화 기능을 제공하는 암호 알고리즘이다. 암호화된 데이터가 표준 구문을 준수하는 경우에만 지각적 암호가 가능하다. 따라서 지각적 암호 기능 관점에서는 일반적으로 압축과 암호 결합 알고리즘들이 압축 독립적 암호 알고리즘보다 유리하다.

Ⅳ. 카오스 사상 기반 영상 암호 알고리즘 동향

4.1. 그동안 제안된 카오스 사상 기반 암호들

카오스 사상(chaotic map)은 초기 조건에 민감하게 반응하며 난수 특성이 우수한 수열을 생성하기 때문에, 지난 25년간 다양한 암호 알고리즘의 기본 요소로 활용되어 왔다. 카오스 사상 기반 암호 알고리즘은 복수의 사상들을 다양한 방법에 의해 결합하여 영상 또는 텍스트 데이터를 암호화한다. 지금까지 카오스 사상, 카오스 로지스틱(Logistic) 사상 등 다양한 카오스 사상을 기반으로 여러 영상 암호 알고리즘들이 제안되었다.

Lian이 제안한 시공간 카오스 시스템 기반 영상 암호 알고리즘은 영상 블록에서 선택된 매개변수를 암호화하는 의사난수 수열을 시공간 격자(lattice)에 의해 생성한다[5]. Pareek 등이 제안한 카오스 로지스틱(Logistic) 사상 기반 영상 암호 알고리즘은 80 비트의 외부 비밀키와 카오스 로지스틱 사상 2개로 구성된다[6]. 로지스틱 사상의 초기 조건은 외부 비밀키에 의해 유도된다. Gao 등은 지수승 함수와 탄젠트 함수를 사용하는 NCA(nonlinear chaotic algorithm, 비선형 카오스 알고리즘)을 제안하였다[7]. 영상 데이터는 NCA 사상이 생성한 카오스 수열에 의해 암호화된다.

Behnia 등은 카오스 시스템들 혼합하여 생성된 사상 기반으로 디지털 영상 암호 기법을 제안하였다[8]. 제안된 기법은 결합된 사상 등 고차원 카오스 시스템에 의해 매우 높은 수준의 안전성을 보장한다. Kwak 등은 스트림 암호 구조를 갖는 고속 카오스 기반 영상 암호 시스템을 제안하였다[9]. 제안된 기법은 카오스 사상들을 폭포(cascade) 형태로 결합하여 의사난수 키 스트림을 생성한다.

이러한 영상 암호 알고리즘들은 기지 평문 공격 또는 선택 평문 공격에 안전하지 않거나 또는 암호화 처리에

많은 시간이 소요되어 실제 적용이 곤란해지는 단점들이 존재한다. 본 장에서는 최근 발표된 카오스 사상 기반 영상 암호 알고리즘들을 소개한다.

4.2. Amin 등이 제안한 카오스 블록 암호 알고리즘

Amin 등은 최근 암호 원시 연산(cryptographic primitive operation)과 비선형 변환함수 및 카오스 사상을 기반으로 설계된 CBCA(chaotic based cipher algorithm, 카오스 기반 암호 알고리즘)를 제안하였다[10]. 제안된 알고리즘은 카오스 텐트 사상을 기반으로 난수 특성이 우수한 세션 키를 생성한다. 텐트 사상 $T(x)$는 최근 암호 알고리즘에서 사용되는 가장 단순한 카오스 함수의 일종이다.

$$T(x)=\begin{cases} rx & x>0.5 \\ r(1-x) & x\le 0.5 \end{cases}$$

제안된 알고리즘은 순환회전(cyclic rotation)과 비트별 XOR 및 정수 연산을 사용하기 때문에 프로세스에 의해 효율적으로 구현할 수 있다. 알고리즘은 256 비트의 입출력에 의해 동작되며, 따라서 32개의 레지스터에 의해 구현될 수 있다. 제안된 알고리즘은 또한 CBCA-w/r/b 형태로 입출력 비트 길이와 라운드 수 및 비밀 키의 바이트 수가 가변될 수 있다.

Amin 등은 제안된 알고리즘의 안전성을 전수공격 차단 능력과 생성된 수열의 통계적 특성 및 차분공격 차단 능력 측면에서 분석하였다. 제안된 알고리즘의 키 공간 크기는 2^{256} 이므로, 전수공격의 성공 가능성은 0에 근접 한다. 제안자들은 막대도표와 이웃하는 픽셀 사이의 상관관계 그리고 엔트로피 특성이 매우 우수하다고 주장한다.

Amin 등은 원래의 영상에서 발생된 약간의 변화가 암호화된 결과에 미치는 영향을 수치적으로 조사한 결과를 바탕으로 제안된 알고리즘이 차분공격에 안전하다고 주장한다.

〔표 1〕 CBCA-w/r/b 매개변수

매개변수	정의	값
w	비트의 워드 길이	16,32,64
r	라운드 수	0,1,2,...,255
b	비밀키의 바이트 수	0,1,2,...,255

4.3. Yang 등이 제안한 고속 암호 및 인증 체계

Yang 등은 최근 키를 사용하는 해시 함수를 기반으로 고속 영상 암호 및 인증 기법을 제안하였다[11]. 제안된 해시 함수는 1차원 텐트(tent) 함수인 블록 T_α 의 반복으로 구성된다.

$$T_\alpha : X_j=\begin{cases} \dfrac{x_{j-1}}{\alpha} & \text{if } 0\le x_{j-1}\le \alpha \\ \dfrac{1-x_{j-1}}{1-\alpha} & \text{if } \alpha< x_{j-1}\le 1 \end{cases}$$

키에 의해 동작되는 해시 함수는 평문 영상과 비밀 해키 키로부터 128 비트의 해시 값을 생성한다. 생성된 해시 값은 암호 및 복호화 과정에 필요한 키로서 이용되며, 비밀 해시 키는 복호화된 영상이 원본과 동일함을 인증하는 수단으로 사용된다. Yang 등은 모의실험 결과에 따라 제안된 해시 함수가 차분공격에 대해 안전하며 충돌회피 특성이 우수하다고 주장한다.

제안된 암호 및 인증체계는 치환(substitution)과 확산(diffusion) 및 키에 의해 동작되는 해시함수로 구성된다. 해시 함수에 의해 생성된 128 비트 해시 값은 치환과 확산 과정의 키 데이터로 입력된다. Yang 등은 제안된 알고리즘의 안전성을 전수공격 차단 능력과 키의 민감성 그리고 차분공격 차단 능력 및 생성된 수열의 통계적 특성 측면에서 분석하였다.

제안된 알고리즘의 키 공간 크기는 2^{128} 이므로, 전수공격에 안전하다. Yang 등은 모의실험에 의해 암호 결과가 비밀 값의 미세한 변화에도 매우 민감함을 보인다. Yang 등은 제안된 알고리즘의 차분공격 에 대한 안전성이 기존의 알고리즘들보다 NPCR(number of pixels change rate)과 UACI(unified average changing intensity) 측도 측면에서 우수하며, 평문과 암호 영상의 막대도표와 이웃하는 픽셀 사이의 상관관계를 조사하여, 제안된 알고리즘의 통계적 특성이 우수하다고 주장하고 있다.

V. 결론

본 논문에서는 영상 암호 알고리즘을 압축과 암호 결합 알고리즘과 압축 독립적 암호 알고리즘으로 분류하고, 영상 암호의 최근 동향을 소개하였다. 본 논문에서는 또한 영상 암호 알고리즘의 요구조건들을 소개하였

으며, 이러한 요구조건 관점 측면에서 암호 알고리즘들의 장단점들을 고찰하였다. 이러한 조사 결과에 따라, 사용자들은 자신의 응용에 적합한 암호 알고리즘을 선택할 수 있을 것으로 기대된다.

카오스 사상(chaotic map)은 초기 조건에 민감하게 반응하며 난수 특성이 우수한 수열을 생성하기 때문에, 지난 25년간 다양한 암호 알고리즘의 기본 요소로 활용되어 왔다. 본 논문에서는 카오스 사상 기반 다양한 영상 암호 알고리즘에 관한 최근 개발동향을 소개하였다.

참고문헌

[1] 차건상, 신용태,"CCTV설치 증가에 따른 개인영상정보보호 주요 이슈,"정보과학회지, 제27권 제12호 통권 제247호, pp.25-33, 2009.12.

[2] http://www.kisa.or.kr/jsp/public/laws/laws2.jsp, "CCTV 개인영상정보보호 가이드라인", 한국인터넷진흥원, 1997

[3] http://cctvnews.co.kr/article/, "타원 곡선 암호화를 이용한 영상 저작권 보호 시스템 설계", CCTV News, 2010

[4] Fuwen Liu and Hartmut Koenig, "A survey of video encryption algorithms", COMPUTERS & SECURITY, 29, pp. 3-15, 2010.

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

[6] Pareek NK, Patidar V, and Sud KK., "Image encryption using chaotic logistic map", Image Vision Compu., 24, pp. 926-934, 2006.

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

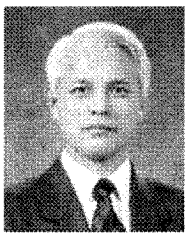
[8] Behnia S, Akhshani A, Mahmodi H, and Akhavan A, "A novel algorithm for image encryption based on mixture of chaotic maps", Chaos Soliton Fract 35, pp. 408 - 419. 2008.

[9] Kwok HS, Wallace K, and Tang S, "A fast image encryption system based on chaotic maps with finite precision representation", Chaos Soliton Fract 32, p. 1518 - 1529 2007.

[10] Mohamed Amin, Osama S. Faragallah, Ahmed A. Abd 띠-Latif, "A chaotic block cipher algorithm for image cryptosystems", Commun Nonlinear Sci Numer Simulat 15, p. 3484 - 3497, 2010.

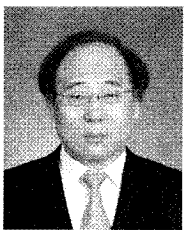
[11] Huaqian Yang, Kwok-Wo Wong, Xiaofeng Liao, Wei Zhang, Pengcheng Wei, "A fast image encryption and authentication scheme based on chaotic maps", Commun Nonlinear Sci Numer Simulat 15, p. 3507-3517, 2010.

〈著者紹介〉



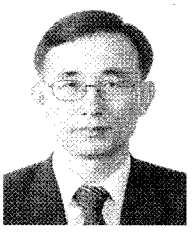
남 길 현 (Kil Hyun Nam)
정회원

1973년 2월: 서울대학교 토목공학과 졸업
1979년 8월: 미국 해군대학교 전산학과 석사
1985년 8월: 루이지아나 대학교 전산학과 박사
1985년 3월~2008년 2월: 국방대학원 교수
2010년2월~현재: 한국과학기술정보연구원 전문연구위원
<관심분야> 정보보호



고 승 철 (Sung Cheol Goh)
정회원

1981년2월: 연세대학교 수학과 졸업
1983년2월: 연세대학교 수학과 석사
1992년2월: 포항공대 수학과 박사
2004년6월~2008년 2월: 한국정보보호산업협회 상근 부회장
2009년 2월~현재: 한국과학기술정보연구원 전문연구위원
<관심분야> 정보보호



박 춘 식 (Choon Sik Park)
종신회원

1995년: 일본 동경공업대 공학박사
1982년-1999년: 한국전자통신연구원 책임연구원
2000년-2008년: 국가보안기술연구소책임연구원, 소장
2009년 3월~현재: 서울여자대학교 정보보호학과 교수
<관심분야> 개인정보보호기술, 클라우드컴퓨팅보안