# 콘텐츠 딜리버리 네트워크에서 미디어 콘텐츠 제공을 위한 향상된 암호화 알고리즘 연구

박철우*, 김우빈**, 김기천*
건국대학교 컴퓨터공학과
e-mail:sporty82@konkuk.ac.kr
e-mail:tasikani@konkuk.ac.kr
e-mail:kckim@konkuk.ac.kr

# The Improved Encryption Algorithm to Delievry Media content for Contents Delivery Network.

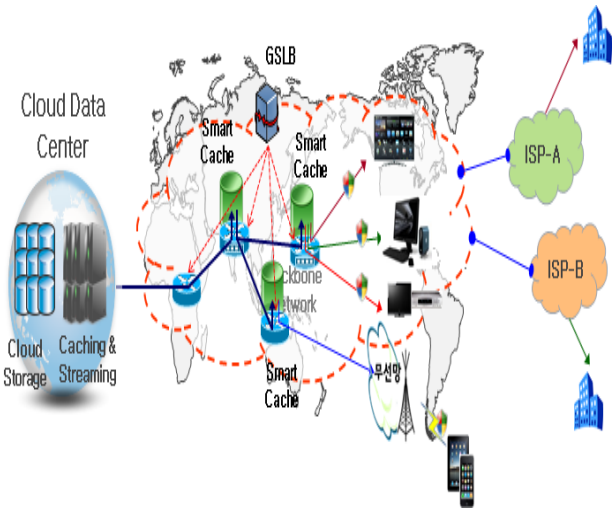
Chulwoo Park*, Woobin Kim**, Keecheon Kim*
*Dept of Computer Science, Konkuk University

요 약

CDN(Content Delivery Network)은 사용자의 콘텐츠 요청에 대해 캐쉬 서버의 부하를 줄이기 위해 사용자와 가장 인접한 캐쉬 서버를 통하여 사용자에게 보다 빠르게 콘텐츠를 제공 하도록 되어있다. 현재까지의 연구는 대용량 콘텐츠 스트리밍 서비스를 위한 속도적 측면만 고려하고 있으며 콘텐츠를 빠르게 제공하기 위하여 같은 콘텐츠를 여러 캐싱서버로 분산하여 보안성이 충분하지 못한 단점이 있다. 하지만 사용자에게 충분한 보안성을 갖춘 대용량 콘텐츠를 제공하려면 암호화 연산의 증가로 인하여, 속도적 측면이 감소하므로 CDN의 본연의 기능을 잃을 수 있다. 그러므로 본 논문에서는 해시기반 스크램블링을 이용한 암호화 기법의 보안의 취약성을 분석하고 이를 극복하기 위해 보안성을 향상시킨 RECOS(Robust Encryption for COntent Secure)기법을 제안한다. 제안 기법은 시뮬레이션에서 기존 기법과 제안 기법의 속도를 비교하였으며, 기존 기법의 취약성 분석을 통하여 제안 기법의 향상된 보안성을 보였다. 결과적으로 기존의 해시기반 암호화 기법과 비교하여 속도에 차이가 거의 없음에도 불구하고 향상된 보안성을 보였다.

## 1. 서론

오늘날 인터넷 정보통신 기술의 발달과 스마트폰과 같은 다양한 모바일 디바이스의 등장으로 인터넷 사용자가 기하급수적으로 증가하게 되었고, 디지털 콘텐츠 유통 시장이 활성화 되었다. 이러한 배경으로 사용자에게 동영상을 빠르게 전달하기 위한 CDN기술이 연구 되었다. CDN 서비스는 기존의 네트워크 구조 설비 등을 변경 없이 사용하면서 캐시 서버에 콘텐츠를 분산 저장 시키고 사용자의 요청에 따라 가까운 캐시 서버에서 콘텐츠를 제공하캐싱 기술을 이용한다. CDN기술은 (그림 1)과 같이 다수의 캐쉬 서버의 배치를 효율적으로 하는 것과 콘텐츠의 효율적인 저장 방식을 통하여 네트워크간의 트래픽을 효과적으로 감소시키며 서비스의 품질을 향상시키는 방법에 대한 연구를 하고 있다.[1] 하지만 광범위하게 분산 저장되어 있는 디지털 콘텐츠는 저작권 보호나 불법 복제 사생활보호와 같은 보안에 더 많은 취약성을 가지고 있고, 데이터를 분산 저장함으로 인하여 스니핑(Sniffing), ARP 스푸핑(Spoofing), 사전 공격측면과 같은 해킹 공격에 대한 보안성이 필요하게 되었다.[2] 스트리밍 디지털 영상 콘텐츠 전송은 블록암호화 알고리즘을 이용하여 암호화 하여 전송하였으나, 이것은 대용량 콘텐츠 전송에 있어 많은




(그림 1) 대용량 콘텐츠 전송을 위한 CDN 시스템

암·복호화 시간이 요구되어 속도적 측면에 취약하다. 이러한 속도적 측면을 향상 시킨 경량화 암호화 기법으로 스크램블링 암호화 기법이 있다. 본 논문에서는 스크램블링 암호화기법의 취약성 분석을 통하여 향상된 스크램블링 암호화 기법인 RECOS을 제안한다. 본 논문의 구성은 2장에서는 관련연구 및 기존의 스크램블링 기법의 취약성을

분석하고, 3장에서는 제안된 향상된 스크램블링 암호화기법에 대한 분석 및 보안성테스트를 하였고, 4장에서는 성능평가를 위한 시뮬레이션을 하였다, 5장에서는 결론 및 향후 연구방향을 제시한다.

## 2. 관련 연구

### 2.1 스크램블링

스크램블링 기술은 네트워크의 성능이 향상됨에 따라 대용량 미디어 콘텐츠를 안전하게 실시간으로 제공하기 위하여 나왔다. 스크램블링은 원래의 영상 데이터를 특정한 키에 의해 변형 또는 암호화하여 전송함으로, 특정한 키를 가진 수신자만이 정상적으로 영상을 복원할 수 있도록 하는 기술이다. 허가되지 않은 수신자는 수신된 영상을 복호화 하더라도, 원래의 영상이 아닌 스크램블링 과정을 거쳐 왜곡된 영상을 보게 됨으로써 정당한 수신자의 권리를 보호할 수 있다.[3]

### 2.2 암호화 알고리즘을 통한 스크램블링

SEED, ARIA 와 같은 암호화 알고리즘을 이용하여 영상을 암호화 하는 방식이다. 이 방식은 계산 량이 많아서 영상 전체를 압축할 경우 계산양이 매우 증가하게 된다. 따라서 프래임별 압축이나 영상의 중요도에 따라 선택적으로 암축하는 방법 등이 사용되고 있다.[4]

### 2.3 Gray Code

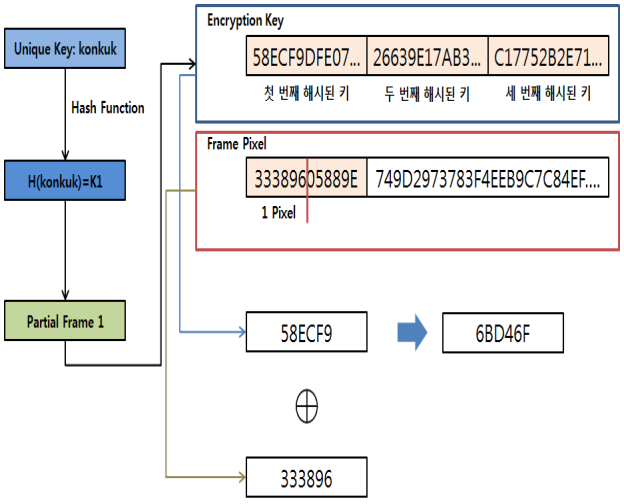
1947년 벨 연구소의 연구자인 Frank Gray에 의해 개발된 그레이 코드는 컴퓨터에 사용하도록 개발되었다. 연속되는 일련의 숫자비트를 하나의 비트만 변화하여 새로운 코드를 생성하며, 입력코드로 사용하면 오차가 적어지는 그레이 코드의 특징과 구조를 가지고 있다. 이러한 특징과 구조를 바탕으로 현재 이미지 필터링 [5], 암축 [6], 인식 [7], 스크램블링 [8], [9] 워터마킹 [10]등의 다양한 분야에서 사용되고 있다.

### 2.4 기존 스크램블링기법의 취약성 분석

스크램블링 기법중 하나인 콘텐츠발급기관 암호화 기법(Content Obfuscation Encrytion System)은[11] (식 1-1)과 같이 유니크 키를 해시하여 512비트 암호화키를 생성한다.

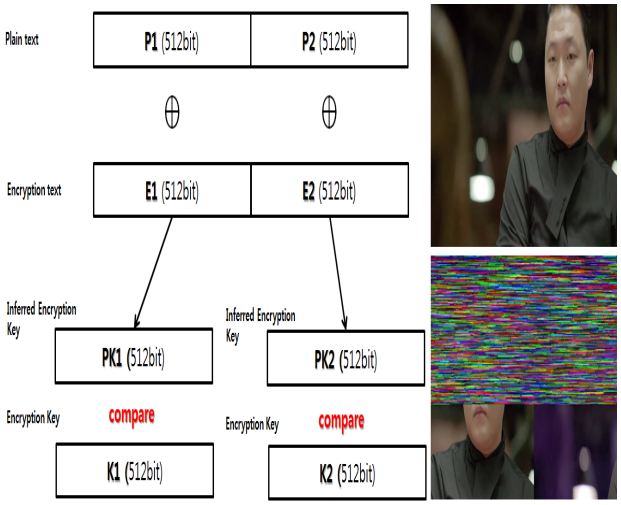
$$Encryption_{key} = SHA\text{-}512(Content_{Unique\_key}) \quad (식1\text{-}1)$$

이때 첫 번째 생성된 암호화키를 K1이라고 할 때, K1을 해시하여 두 번째 암호화키인 K2를 생성한다. 이 과정을 암호화할 영상의 크기만큼 암호화키(K1, K2... Kn)를 생성한 후 암호화 키와 원본영상을 (그림 2)와 같이 XOR 연산하여 스크램블링 기법을 통한 암호화 영상을 생성한다.




(그림 2) 암호화 과정

콘텐츠발급기관 암호화 기법은 암호화키가 영상의 크기만큼 생성되고 해시함수의 특성상 Kn+1로 Kn을 알아낼 수 없는 특성이 있기 때문에 안전해 보인다. 하지만 암호화영상과 원본 프래임의 일부가 노출되었을 때 이전영상은 알 수 없지만, 이후의 영상은 복호화가 가능하다는 것이 (그림 3)의 취약성 분석을 통한 암호화 키 유추를 통한 원본영상 복호화에 의한 보안 위협 시뮬레이션을 통하여 드러났고, 보안성에 심각한 영향을 미칠 수 있다는 것이 증명되었다.




(그림 3) 취약성 분석 및 보안 위협

## 3. 제안 기법

콘텐츠발급기관 암호화 기법은 디지털 영상 콘텐츠 전송에 있어서 빠른 전송 속도를 보이고 해시 함수를 통함 암호화키 생성으로 비록 암호화키가 노출되어도 이전 영상의 데이터를 복수할 수 없다. 하지만 일부 영상이 노출되었을 때 그 후의 영상이 복구되어질 수 있다는 문제점을 2장에서 설명하였다. 이를 보완하기 위하여 기존의 콘텐츠발급기관 암호화 기법과 속도차이가 거의 없음에도

불구하고 보안성이 향상된 RECOS기법을 제안한다.

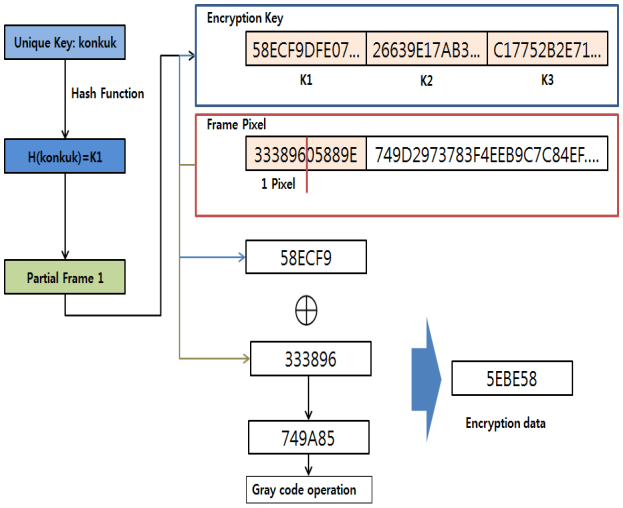



그림 4 제안된 RECOS기법

제안된 기법은 영상프레임 자체에 그레이코드 변환을 통한 연산을 추가하여 생성된 암호화키와 스크램블링 기법을 사용하여 (식 2-1)과 같이 콘텐츠를 암호화 한다.

Plain_image ⊕ $Encryption_{key}$ = value_1

value_1 (Gray Code Converter) Encrypted_image (식2-1)

(식 2-1)은 원본영상을 Unique Key로부터 해시하여 생성한 암호화키로 XOR 연산을 한다음 그레이코드 변환(Gray Code Generation Algorithm)을 통하여 변환하여 암호화된 영상을 구한다.

## 4. 성능평가

### 4.1 취약성 극복

제안된 기법은 원본 영상의 일부가 노출되더라도 그레이코드 변환 기법을 추가하여 공격자가 암호화된 영상을 통한 암호화키 유추를 시도하더라도 암호화 키를 알 수 없기 때문에 안전하다. 또한 Unique Key가 노출 되었어도 영상 암호화 과정에 그레이코드 변환기법을 통하여 암호화 알고리즘과 변환기법의 두 연산을 알 수 없기 때문에 암호화 영상으로부터 원본 영상을 복호화 할 수 없다.

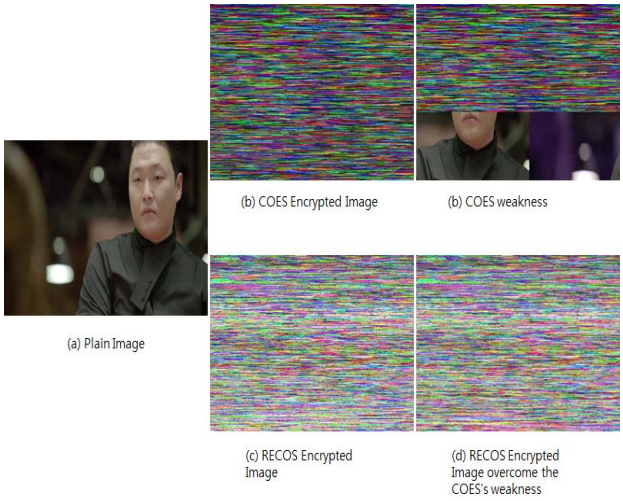
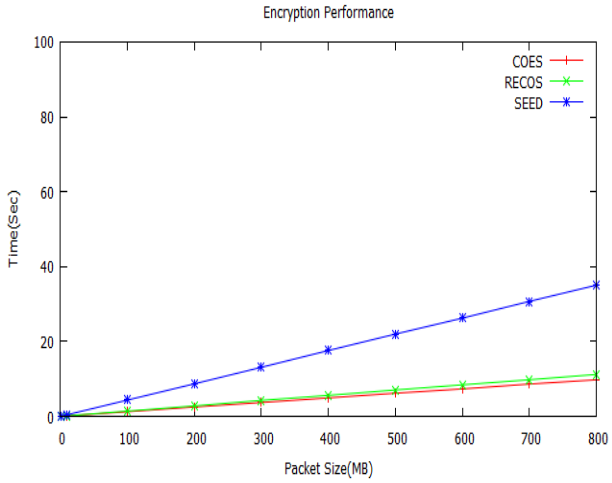



그림 5 COES와 RECOS의 성능 분석

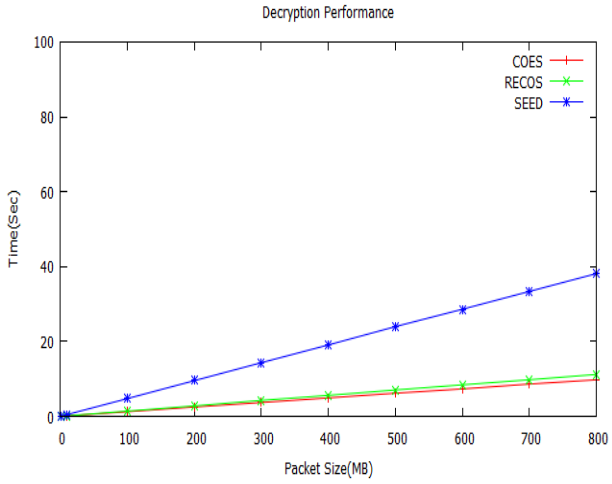
그림 5는 원본 영상을 기존 COES와 비교하여 제안된 RECOS기법의 보안 강도를 테스트하였을 때 기존 기법과 제안기법의 시뮬레이션 영상이다. 그림 4에서 보다시피 같은 해시값을 암호화 키로 사용하더라도 변환기법을 추가하였기 때문에 영상을 복호화 할 수 없다. 또한 암호화 기법과 변환기법을 둘 다 아는 것은 현실적으로 불가능하기 때문에 기존 취약성을 통한 암호화 키 유추에 대해 안전하다.

### 4.1 암·복호화 속도 비교

제안된 기법과 기존 기법들의 속도 차이를 분석하여 위하여 시뮬레이션을 실행하였다. (그림 5),(그림 6)은 제안 기법과 국내표준 암호화 알고리즘인 SEED와 COES 스크램블링 기법의 속도를 비교하였다. 제안된 알고리즘은 영상자체에 변환기법을 통하여 기존의 스크램블링 암호화 기법과 속도의 차이는 거의 없음에도 불구하고 암호화 키를 통한 영상탈취에 대한 보안성을 향상시켰다.




(그림 6) 암호화 속도




(그림 7) 복호화 속도

## 5. 결론

제안된 RECOS 기법을 통하여 본 논문에서는 기존의 콘텐츠발급기관 암호화 기법의 취약성을 분석을 통하여 향상된 스크램블링 콘텐츠 보안 기법을 제안하였다. 기존의 콘텐츠발급기관 암호화 기법은 속도는 빠르지만 일부 영상의 노출로 인하여 이후 전송되는 콘텐츠에 대한 보안에 문제점이 발견되었다.

본 논문에서는 이전 기법의 보안 취약성을 영상 변환 기법을 통하여 극복하였고, 결과적으로 암·복호화 속도는 거의 같음에도 불구하고 원본 영상 탈취에 대한 암호화키의 보안성은 향상되었다. 향후 연구로는 다양한 모바일 디바이스를 대상으로 콘텐츠 전송에 있어서 자원 소모적 측면을 줄임으로 한정적 자원을 이용한 효율적인 콘텐츠 전송에 대한 연구를 진행할 것이다.

## Acknowledgement

"본 연구는 지식경제부와 한국산업기술평가관리원의 지원을 받아 수행된 연구임.[10041910, 가입자 구간 비디오 트래픽의 50% 절감이 가능한 글로벌 딜리버리 클라우드 플랫폼의 개발]."

## 참고문헌

[1] 곽은주, 조유희, 서영일, "CDN 기술 동향 및 Operator CDN 현황 분석", 전자 정보통신 학술대회, 2011

[2] 홍범석, 김태현, "CDN 서비스의 현황 및 이슈", 정보통신정책연구원, 2008.1

[3] 안진행, "H.264인트라 예측 모드를 이용한 디지털 비디오 스크램블링 방법", 전자공학회 논문지, 2005.]

[4] 김보승, 신용태, "스트리밍 영상을 위한 효율적 스크램블링 방법 연구", 한국정보과학회 학술대회, 2011.6 ]

[5] G. Ben-Artzi, H. Hel-Or, and Y. Hel-Or, "The gray-code filter kernels," IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007.

[6] H.-W. Tseng and C.-C. Chang, "Anti-pseudo-gray coding for VQ encoded images over noisy channels," IEEE Communications Letters, 2007.

[7] W.-S. Chen, K.-H. Chih, S.-W. Shih, and C.-M. Hsieh, "Personal identification technique based on human iris recognition with wavelet transform," in Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP '05). IEEE International Conference on, 2005,

[8] W. Ding, W. Yan, and D. Qi, "Digital image scrambling," Progress in Natural Science, 2000.

[9] J. Zou and R. K. Ward, "Introducing two new image scrambling methods," in Communications, Computers and signal Processing, 2003.

[10] I. Nasir, W. Ying, and J. Jianmin, "A new robust watermarking scheme for color image in spatial domain," in Signal-Image Technologies and Internet-Based System, 2007.

[11] 이 영구, "IPTV 환경에서 불법 사용 방지를 위한 콘텐츠 암호화 기법", 학위논문, 2010.12