디지털 콘텐츠 보호를 위한 의사난수생성기 기반의 부분암호화 기법 연구

유성민*, 정광운*, 신진섭*, 김상우*, 정우탁*, 류재철*
*충남대학교 컴퓨터공학과
e-mail:mingoon@home.cnu.ac.kr

A Study on PRNG based Partial Encryption for Digital Contents Protection

SeongMin Yoo*, GwangUn Jung*, JinSeob Sin*, SangWoo Kim*,
WooTak Jung*, JaeCheol Ryou*
*Dept of Computer Engineering, Chungnam National University

요 약

디지털 콘텐츠가 대용량화됨에 따라, 부분암호화는 디지털 콘텐츠 보호를 위한 하나의 방안이 될 수 있다. 부분암호화 시에 고려해야할 사항 중 하나는 복호화를 위해 암호화된 부분의 정보를 별도로 관리해야하는 것이다. 부분암호화 정보의 관리가 제대로 이루어지지 않을 경우, 데이터가 완벽히 복호화되지 않거나, 보안위협에 노출될 수 있으며, 데이터 전체를 암호화하는 것보다 오히려 더 많은 비용이 발생할 수 있다. 본 논문에서는 이러한 부분암호화 정보를 안전하고, 효율적으로 관리할 수 있는 의사난수생성기와 진리표를 이용한 부분암호화 기법을 제안한다. 제안하는 방법은 복호화 시에 암호화된 부분의 식별을 위해 의사난수생성기 초기화 값과 진리표만 필요하기 때문에 부분암호화 정보를 관리하는데 용이한 장점이 있다.

1. 서론

2005년 이후, YouTube, Facebook 등이 유행하면서 사진, 동영상과 같은 디지털 콘텐츠들의 공유가 급증하고 있다. 이렇게 공유되는 디지털 콘텐츠 중에는 저작권 보호를 필요로 하는 콘텐츠들이 상당수 존재한다[1-3].

이에 따라 저작권 보호를 필요로 하는 디지털 콘텐츠의 무분별한 공유를 막기 위해, DRM(Digital Rights Management)과 같은 기술을 적용하기도 한다. 암호화는 이 DRM을 구성하는 핵심기술 중 하나이다[4,5].

최근에는 고성능의 디지털 카메라, 디지털 캠코더, 스마트 기기 등의 확산으로 디지털 콘텐츠의 품질이 향상되면서, 콘텐츠의 용량 또한 크게 증가하고 있다[6]. 이로 인해 콘텐츠의 암호화에 따른 속도저하가 예상되고 있다. 따라서 암호화의 성능향상을 위한 기술이 필요한 상황이다.

주어진 데이터의 일부분만을 암호화함으로써 암호화에 소요되는 시간을 줄이는 부분암호화는 이러한 요구사항을 해결할 수 있는 방안 중 하나이다[7-9]. 하지만 데이터 전체를 암호화하는 것과 다르게, 부분암호화 시에 추가적으로 고려해야할 사항 중의 하나는 복호화를 위해 암호화된 부분의 정보를 별도로 관리해야하는 것이다.

복호화 시에 암호화된 부분의 정보를 정확하게 알지 못할 경우에는 데이터를 완벽하게 복호화 하는 것이 불가능하며, 만약 이 정보가 외부로 공개될 경우에는 보안위협에 노출될 수 있다. 또한 관리해야할 정보가 커지면, 오히려 데이터 전체를 암호화하는 것보다 더 많은 비용이 발생할 수 있다.

본 논문에서는 이러한 부분암호화 정보를 안전하고, 효율적으로 관리할 수 있는 의사난수생성기(Pseudo Random Number Generator, PRNG)와 진리표를 이용한 부분암호화 기법을 제안한다. 제안하는 방법은 복호화 시에 암호화된 부분의 식별을 위해서, 의사난수생성기의 초기화에 사용되는 값과 진리표만을 필요로 하기 때문에 부분암호화 정보를 관리하는데 용이한 장점이 있다.

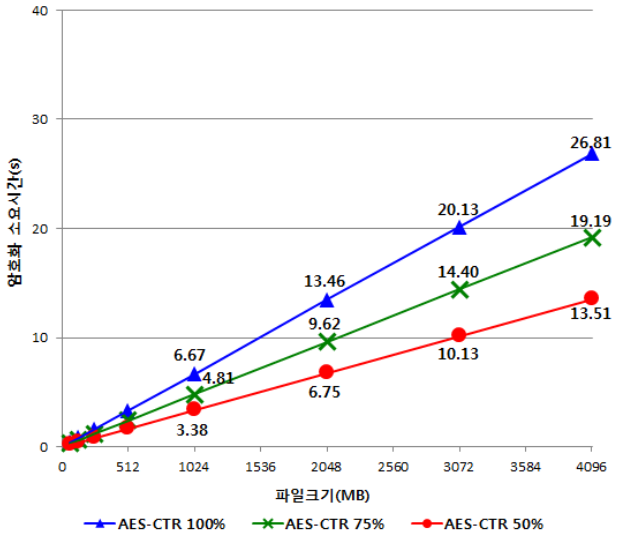
논문의 구성은 다음과 같다. 먼저 2장에서는 관련연구로 부분암호화에 대해 설명한다. 3장에서는 제안하는 의사난수생성기 기반의 부분암호화 기법을 설명한다. 4장에서는 제안한 기법의 효율성을 평가하고, 5장에서 결론을 맺는다.

2. 관련연구

디지털 콘텐츠의 품질향상을 위한 기술은 지속적으로 발전하고 있다. 사진 한 장의 해상도별 용량을 비교해보면 1980년대 주로 사용되던 VGA(320x240)의 용량이 230KB에 불과했지만, 최근 스마트폰에서 주로 사용되고 있는 WVGA(800x480) 급은 1MB, HD(1280x720) 급은 3MB에

이르며, 해상도가 7680x4320 달하는 UHD(Ultra HD) 급도 개발되어 있다. 음악파일도 1990년대에는 한 곡이 2.4~7.2MB 정도였지만, 최근에는 7.2~14.4MB까지 용량이 커졌다. 동영상 파일의 경우, 2000년대 초반 700MB에서 최근에는 4.7GB의 SD(Standard-Definition) 급과 15GB의 HD (High-Definition) 급 화질의 영상이 주로 사용되고 있고, 25~50GB까지 저장이 가능한 Blu-ray 디스크도 상용화가 시작된 상태이다.

이처럼 디지털 콘텐츠의 용량이 크게 증가하면서, 디지털 콘텐츠 보호를 위한 암호화의 성능향상이 요구되고 있다. 이러한 요구사항을 해결할 수 있는 방안 중 하나인 부분암호화는 데이터의 일부분만을 암호화함으로써 암호화에 소요되는 시간을 줄일 수 있다. (그림 1)은 64MB~4GB의 데이터를 AES 알고리즘 CTR 모드로 각각 전체 데이터의 100%, 75%, 50%를 부분암호화 했을 때 소요된 시간을 측정한 결과이다. 이를 통해 실제로 암호화를 하는 비율에 비례해 암호화 소요시간이 감소하는 것을 확인할 수 있다.



(그림 1) 부분암호화 비율에 따른 암호화 소요시간 비교

데이터를 부분암호 화할 때 고려해야할 사항 중 하나는 데이터의 어느 부분을, 얼마나, 어떻게 암호화할 것인가이다. 데이터를 특정한 비율만큼 랜덤하게 암호화하더라도 암호화하는 방식에 따라 결과가 달라진다. (그림 2)는 이러한 예를 보여준다. 위/아래 모두, 5.91MB의 동일한 사진 파일을 AES 알고리즘 CTR 모드로 75%의 부분암호화를 수행한 결과이지만, 암호화 블록 크기(위:100KB, 아래:4KB)에 따라 가시성에서 큰 차이를 보이게 된다.

하지만 디지털 콘텐츠 보호의 목적은 100% 기밀성 보장이 아닌, 저작자의 권리를 보호하기 위해 콘텐츠가 다른 목적으로 사용되지 못하도록 하는 것이기 때문에 두 그림

(그림 2) 부분암호화 방식에 따른 가시성 차이 비교

에 사용된 방식 모두 적합하다고 할 수 있다.

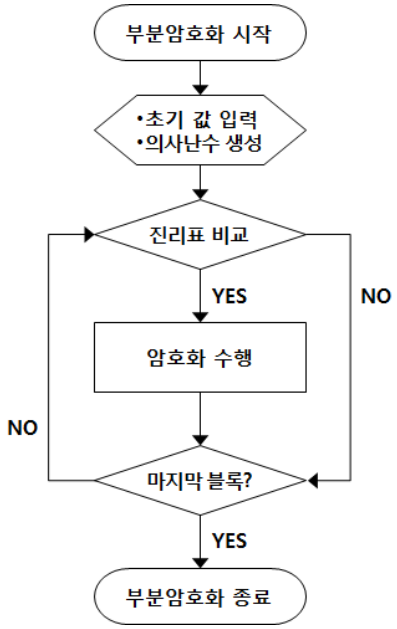
데이터의 부분암호화에 고려해야할 또 다른 사항은 복호화를 위해 암호화된 부분의 정보를 어떻게 관리하느냐이다. 부분암호화 정보의 관리가 제대로 이루어지지 않을 경우, 데이터가 완벽히 복호화되지 않거나, 보안위협에 노출될 수 있으며, 데이터 전체를 암호화하는 것보다 오히려 더 많은 비용이 발생할 수 있다. 다음 3장에서는 이러한 부분암호화 정보를 안전하고, 효율적으로 관리할 수 있는 의사난수생성기와 진리표를 이용한 부분암호화 기법을 제안한다.

3. 의사난수생성기 기반의 부분암호화 기법

의사난수생성기는 처음에 주어지는 초기 값을 이용하여, 이미 내부적으로 결정되어 있는 알고리즘에 의해 의사난수를 생성하게 된다[10, 11]. 따라서 초기 값을 알고 있으면, 동일한 의사난수를 생성할 수 있다. 이 장에서 제안하는 의사난수생성기 기반의 부분암호화 기법은 이러한 의사난수생성기의 특성을 이용한다.

3.1. 부분암호화 과정

(그림 1)의 순서도는 데이터를 부분암호화 하는 과정을 나타낸다. (1)먼저 부분암호화가 시작되면, 의사난수생성기에 초기 값을 입력해 의사난수열을 생성한다. (2)다음으로 미리 알려진 진리표와 현재 위치의 의사난수열을 비교한



(그림 3) 의사난수생성기 기반의 부분암호화 과정

다. (3)진리표 비교결과, 해당 블록이 암호화 대상이면 암호화를 수행하고, 암호화 대상이 아니면 그대로 통과한다. (4)다음 데이터 블록이 존재할 경우, (2)와 (3)의 과정을 반복하고, 남은 데이터 블록이 없을 경우, 부분암호화를 종료한다.

3.2. 복호화 과정

부분암호화 된 데이터의 복호화 과정은, 암호화 대신 복호화가 수행되는 것을 제외하면, 부분암호화 과정과 순서상으로 동일하다. (1)먼저 부분암호화에서 사용된 것과 동일한 초기 값을 의사난수생성기에 입력하면, 동일한 의사난수열이 생성된다. (2)다음으로 미리 알려진 진리표와 현재 위치의 의사난수열을 비교한다. (3)진리표 비교결과, 해당 블록이 복호화 대상이면 복호화를 수행하고, 복호화 대상이 아니면 그대로 통과한다. (4)다음 데이터 블록이 존재할 경우, (2)와 (3)의 과정을 반복하고, 남은 데이터 블록이 없을 경우, 복호화를 종료한다.

3.3. 진리표를 이용한 암호화 비율 설정

앞에서 설명한 의사난수생성기 기반의 부분암호화 기법은 데이터의 암호화 여부를 식별하는데, 의사난수열과 진리표를 비교한다. 의사난수열은 사용자만이 알고 있는 의사난수생성기의 초기 값에 의해 생성되며, 진리표는 미리 공개된 정보라고 가정한다. 데이터의 부분암호화 비율은 이 진리표에 의해 결정된다.

<표 1>은 진리표의 예를 보여준다. 표에서 보는 것처럼 데이터의 75%만큼 암호화를 할 경우, 현재 위치의 의사난수열이 {00}이면 암호화를 하지 않고, {01, 10, 11}이면 현재 데이터 블록을 암호화하게 된다. 암호화 비율의

<표 1> 진리표 예

난수 값	암호화 여부				
00	○	×	×	×	×
01	○	○	×	×	×
10	○	○	○	×	×
11	○	○	○	○	×
암호화비율	100%	75%	50%	25%	0%

단위는 비교하는 의사난수열 길이에 따라 식(1)과 같이 결정된다.

$$암호화비율단위 = \frac{100}{2^n}\% \quad (1)$$
$$where,\ n = 난수열길이$$

진리표는 암호화 및 복호화 여부를 결정하기 위해 꼭 필요한 정보이지만, 의사난수열 없이는 이것을 식별할 수 없기 때문에 기밀성을 요구하지는 않는다. 따라서 공개되어도 안전한 정보이다.

4. 성능평가

본 논문의 목표는 부분암호화 정보를 안전하고, 효율적으로 관리할 수 있는 부분암호화 기법을 제안하는데 있다. 앞의 3장에서 설명한 의사난수생성기 기반의 부분암호화 기법은 부분암호화 및 복호화를 위해서 두 가지의 정보가 반드시 필요하다. 하나는 의사난수생성기 초기화를 위한 초기 값이고, 다른 하나는 암호화 비율을 결정하기 위한 진리표이다.

이 중에서 진리표는 암호화 및 복호화 여부를 결정하기 위해 반드시 필요한 정보이지만, 의사난수열 없이는 이것을 식별할 수 없기 때문에 기밀성을 요구하지는 않는다. 따라서 공개되어도 안전한 정보이다.

의사난수생성기에 사용되는 초기 값은 일반적으로 블록암호에 사용되는 암호키와 동일하거나, 작은 크기(128 ~ 256bit)를 갖는다[12]. 따라서 암호키가 다른 암호키 관리 체계에 의해 안전하게 관리된다는 가정 하에 의사난수생성기 초기 값을 암호키와 동일하게 사용하거나 암호키로부터 유도해서 사용하면, 초기 값의 보호를 위한 별도의 관리체계가 필요하지 않다.

5. 결론

본 논문에서는 부분암호화의 정보를 안전하고, 효율적으로 관리할 수 있는 의사난수생성기 기반의 부분암호화 기법을 제안했다. 제안하는 방법은 복호화 시에 암호화된 부분의 식별을 위해서, 의사난수생성기의 초기화에 사용되

는 값과 진리표만을 필요로 하기 때문에 부분암호화 정보를 관리하는데 용이한 장점이 있다. 특히 진리표는 공개되어도 안전한 정보이기 때문에 별도의 기밀성을 위한 관리가 필요 없으며, 의사난수생성기의 초기 값은 암호화에 사용되는 암호키로 함께 사용가능하기 때문에 별도의 관리체계를 필요로 하지 않는다.

본 논문에서는 데이터의 어느 부분을, 얼마나, 어떻게 암호화할 것인가에 대해서는 다루지 않았다. 데이터를 특정한 비율만큼 랜덤하게 암호화하더라도 암호화하는 방식에 따라 가시성이 달라지기 때문에 향후, 이 부분에 대한 연구를 추가적으로 진행할 계획이다.

본 연구는 지식경제부 및 한국산업기술평가관리원의 SW컴퓨팅산업원천기술개발사업(정보보안)의 일환으로 수행하였음. [10041579, 다양한 사용자 환경을 지원하기 위한 개인정보 대체기술 기반의 개인정보보호 솔루션 개발]

참고문헌

[1] Postigo, Hector. "Capturing fair use for the YouTube generation: The digital rights movement, the Electronic Frontier Foundation and the user-centered framing of fair use." Information, Communication & Society 11.7 (2008): 1008-1027.

[2] Pike, George H. "Google, YouTube, copyright, and privacy." Information Today 24.4 (2007): 15.

[3] Breen, Jason C. "YouTube or YouLose? Can YouTube Survive a Copyright Infringement Lawsuit." bepress Legal Series (2007): 1950.

[4] Subramanya, S. R., and Byung K. Yi. "Digital rights management." Potentials, IEEE 25.2 (2006): 31-34.

[5] Kundur, Deepa, and Kannan Karthik. "Video fingerprinting and encryption principles for digital rights management." Proceedings of the IEEE 92.6 (2004): 918-932.

[6] Wikipedia, http://en.wikipedia.org/wiki/Graphics_display_resolution

[7] Cheng, Howard, and Xiaobo Li. "Partial encryption of compressed images and videos." Signal Processing, IEEE Transactions on 48.8 (2000): 2439-2451.

[8] Candelore, Brant L., et al. "Elementary stream partial encryption." U.S. Patent No. 7,124,303. 17 Oct. 2006.

[9] Said, Amir. "Measuring the strength of partial encryption schemes." Image Processing, 2005. ICIP 2005. IEEE International Conference on. Vol. 2. IEEE, 2005.

[10] James, Frederick. "A review of pseudorandom number generators." Computer Physics Communications 60.3 (1990): 329-344.

[11] Rukhin, Andrew, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. BOOZ-ALLEN AND HAMILTON INC MCLEAN VA, 2001.

[12] NIST SP 800-90A, “Hash_DRBG, HMAC_DRBG, CTR_DRBG and Dual EC DRBG”.