

암호화된 동영상 비식별화율의 정량적 분석 방법

김덕한^{1,2}, 김영갑^{3,†}

¹세종대학교 정보보호학과 석사과정

²세종대학교 지능형드론융합전공

³세종대학교 교수

lpsi4862@naver.com, alwaysgabi@sejong.ac.kr

Quantitative Analysis Method for Encrypted Video

Deok-Han Kim¹, Young-Gab Kim^{1,†}

¹Dept. of Computer and Information Security, and Convergence Engineering
for Intelligent Drone, Sejong University

요약

최근 다양한 동영상 미디어 콘텐츠가 늘어나면서 민감한 개인정보 유출의 위험성 또한 높아졌다. 이에 따라 다양한 동영상 비식별화 기법이 연구되었고, 그중에서 동영상 암호화 기술은 별도로 원본 동영상을 보관하지 않아도 복호화를 통해 원본 동영상을 얻을 수 있다는 장점 때문에 계속해서 연구가 진행되고 있다. 많은 동영상 암호화 연구에서는 암호화된 동영상의 비식별성을 입증하기 위해 기존의 이미지 암호화 연구에서 사용되던 평가 지표를 사용한다. 그러나 이러한 지표들은 암호화된 동영상의 비식별성을 입증하기에는 적합하지 않다. 따라서 본 논문에서는 암호화된 동영상이 전체 구간에서 비식별화되었는지 확인하는 방법을 제안한다. 본 논문에서는 기존의 지표들을 가중 합산하여 동영상의 모든 프레임에 대해 측정하고 이를 그래프로 표현하여 분석한다. 이 방법을 통해 암호화된 동영상에서 비식별화가 정상적으로 적용되지 않은 부분을 쉽게 파악할 수 있다.

1. 서론

최근 동영상은 미디어 콘텐츠의 주요 형태 중 하나로 부상하였으며, 우리는 일상생활에서 동영상 콘텐츠를 더 자주 접할 수 있게 되었다. 그러나 동영상 콘텐츠를 통해 민감한 개인정보가 저장 및 공유될 수 있으며, 민감 정보가 불법적으로 유출되거나 무단으로 공유되면 심각한 개인정보 침해 및 기업 데이터 유출 문제가 발생할 수 있다. 이에 따라 동영상을 통한 민감한 정보의 유출을 막기 위해 동영상에서 민감한 정보가 포함된 영역을 비식별화하기 위한 동영상 비식별화 기술이 연구되었다. [1]

동영상을 비식별화하기 위한 기법에는 모자이크(Pixelation), 블러링(Blurring), 암호화(Encryption) 기법 등이 있다. 동영상 암호화 기법은 다른 비식별화 기법과는 달리 원본 동영상을 별도로 보관하지 않아도 암호화된 동영상의 복호화를 통해 원본 동영상 정보를 얻을 수 있다는 장점 덕분에 계속하여 연구가 진행되고 있다. [2-4]

동영상 암호화 연구의 목표는 동영상을 시각적으로 변형하여 동영상에 존재하는 민감한 정보를 식별

하기 어렵게 하는 것이다. 기존의 동영상 암호화 연구에서는 동영상의 비식별화율을 측정하기 위하여 이미지 암호화 연구에서 사용되던 평가 지표를 사용하였다. 기존의 이미지 암호화 연구에서는 비식별화율을 측정하기 위해 PSNR(Peak Signal-to-Noise Ratio), SSIM(Structural Similarity Index Measure), CC(Correlation Coefficient), EDR(Edge Differential Ratio), NPCR(Number of Pixels Changing Ratio), UACI(Unified Average Change Intensity) 등의 평가 지표를 사용하였다. 동영상 암호화 연구에서는 동영상의 일부 프레임에 대해서 평가 지표를 측정하여 동영상의 비식별화율을 측정하였다. 그러나 동영상의 경우 전체 프레임 중 단 하나라도 비식별화 처리가 제대로 되지 않은 프레임이 존재하면 보안성을 유지할 수 없다. 따라서 암호화된 동영상에서 비식별화가 전체적으로 잘 되어 있는지 확인하는 방법이 필요하다.

본 논문에서는 암호화된 동영상에서 비식별화 처리가 정상적으로 적용되지 않은 부분이 존재하는지 쉽게 분석하기 위해 여러 평가 지표를 가중 합산하고, 그래프로 표현하여 분석하는 방법을 제안한다.

† 교신저자

2. 제안 방법

기존의 이미지 암호화 연구에서는 암호화가 잘 되었는지 측정하기 위해 PSNR, SSIM, CC, EDR, NPCR, UACI 등의 평가 지표를 측정하여 비교한다. 본 논문에서는 암호화된 동영상의 비식별화율을 측정하기 위해 동영상의 모든 프레임마다 SSIM, EDR 지표 2개를 가중 합산하여 측정한다.

SSIM[5]은 원본 동영상의 프레임과 암호화된 동영상의 프레임 간 밝기, 대비 및 구조적 유사성을 측정하기 위해 사용되며, 0에서 1 사이의 값을 가진다. SSIM은 0에 가까울수록 비식별화가 잘 되었음을 의미하며, 다음과 같은 공식을 통해 구할 수 있다.

$$SSIM = \frac{(2\mu_A\mu_B + C_1)(2\sigma_{AB} + C_2)}{(\mu_A^2 + \mu_B^2 + C_1)(\sigma_A^2 + \sigma_B^2 + C_2)} \quad (1)$$

μ_A 는 동영상 A 프레임 픽셀값의 평균, σ_A 는 동영상 A 프레임 픽셀값의 표준 편차, σ_{AB} 는 동영상 A, B 프레임 간의 공분산을 나타낸다.

EDR[6]은 원본 동영상과 암호화된 동영상에서 추출된 에지 이미지 사이의 차이를 측정하기 위해 사용하며, 0에서 1 사이의 값을 가진다. EDR은 라플라시안 에지 검출을 통해 구해진 에지 이미지 간의 비교를 통해 측정되며, 다음과 같은 공식을 두 에지 이미지 간에 적용하여 구할 수 있다.

$$EDR = \frac{\sum_{m,n=1}^N |G(m,n) - \bar{G}(m,n)|}{\sum_{m,n=1}^N |G(m,n) + \bar{G}(m,n)|} \quad (2)$$

$G(m,n)$ 과 $\bar{G}(m,n)$ 은 각각 원본 동영상과 암호화된 동영상 프레임에서 검출한 에지 이미지의 픽셀값이다.

암호화된 동영상 비식별화율은 SSIM, EDR 2가지 지표를 가중 합산하여 다음과 같이 계산된다.

$$\frac{k_1(1 - |SSIM|) + k_2EDR}{k_1 + k_2} \quad (3)$$

본 논문에서 k_1 , k_2 는 각각 1로 설정하였다. 본 논문에서 제안하는 동영상 비식별화율 지표는 1에 가까울수록 비식별화가 잘 되었음을 의미하며, 0에 가까울수록 원본 동영상과 차이가 없고, 비식별화가 잘 이루어지지 않았음을 의미한다.

동영상이 전체적으로 암호화가 잘 되었는지 확인하기 위해서는 동영상에 존재하는 모든 프레임에 대

해 잘 암호화가 되었는지 확인해야 할 필요성이 있다. 이를 쉽게 확인하기 위해 모든 프레임에 대해 비식별화율을 측정하고 이를 그래프로 나타낸다. 이를 통해 동영상 전체 구간에서 암호화가 되지 않거나 비식별화가 제대로 수행되지 않은 구간이 존재하는지 쉽게 확인할 수 있다.

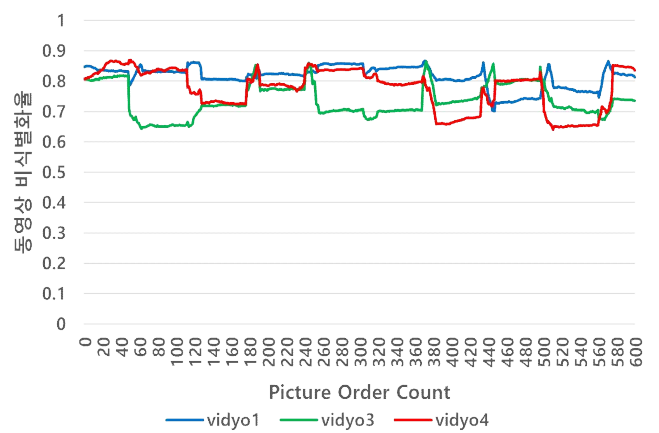
3. 실험 및 결과

3.1. 실험 방법

실험은 본 논문에서 제안한 동영상 비식별화율 분석 방법을 통해 비식별화된 구간 또는 그렇지 않은 구간을 쉽게 식별할 수 있는지 확인하기 위하여 수행되었다. 동영상 전체 구간을 암호화하였을 경우, 그리고 동영상 일부 구간을 암호화하지 않았을 경우, 본 논문에서 제안한 암호화된 동영상 비식별화율 측정 방법을 사용하여 분석하였다.

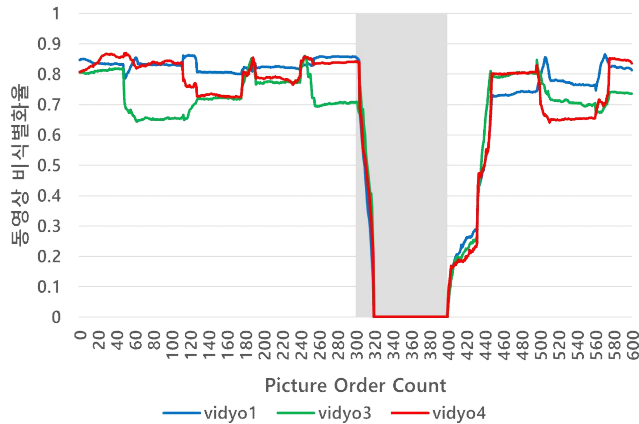
본 논문에서는 오픈소스 HEVC(High Efficiency Video Coding) 인코더인 kvazaar[7]를 사용하여 IPM(Intra Prediction Mode), MV(Motion Vector), MVs(MV sign), TC(Transform Coefficient), TCs(TC sing)와 같은 HEVC 동영상의 일부 구문요소만을 암호화[2]하였으며, 실험을 위한 데이터세트는 Xiph.org에서 제공하는 비디오 테스트 데이터세트인 Derf's Collection[8]에서 vidyo1, vidyo3, vidyo4 3가지 영상을 사용하였다.

3.2. 실험 결과



(그림 1) 전체 구간에서 암호화된 동영상 분석

그림 1은 전체 구간에서 암호화된 동영상을 본 논문에서 제안한 동영상 비식별화율 분석 방법을 사용하여 분석한 결과이다. 그래프를 통해 전체 구간에서 비식별화가 제대로 되었음을 확인할 수 있다.



(그림 2) 일부 구간에서 암호화된 동영상 분석

그림 2는 일부 구간이 암호화된 동영상을 분석한 것이다. 동영상은 300번째 프레임부터 400번째 프레임까지 암호화를 적용하지 않았으며, 이는 그래프의 회색 영역을 통해 표시되었다. 그래프를 통해 300번째 프레임부터 400번째 프레임까지 비식별화가 제대로 수행되지 않았음을 확인할 수 있다.



(그림 3) 일부 구간에서 암호화된 동영상에서 추출한 비식별화된 프레임과 비식별화되지 않은 프레임 예시

그림 3은 일부 구간에서만 암호화된 동영상에서, 암호화된 구간의 프레임과 암호화가 되지 않은 구간의 프레임을 보여준다. 동영상 비식별화율이 0으로 측정되는 구간의 프레임은 비식별화가 제대로 되지 않았음을 보여준다.

4. 결론

본 논문에서는 암호화된 동영상에서 비식별화가 정상적으로 수행되지 않은 구간을 쉽게 분석하기 위해 SSIM, EDR 2가지 측정 지표를 가중 합산하여 동영상 비식별화율을 구하고, 암호화된 동영상 전체 구간에서 동영상 비식별화율을 측정하여 그래프로 표현하여 분석하는 방법을 제안하였다. 실험을 통해 본 논문에서 제안한 방법을 사용하여 암호화된 동영상의 비식별화율을 측정할 수 있고, 비식별화된 구

간과 비식별화가 되지 않은 구간을 쉽게 분석할 수 있음을 확인하였다.

ACKNOWLEDGMENT

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2019-0-00231, 공공 인프라 안전을 위한 인공지능 기반 영상보안 기술 및 시스템 개발)

참고문헌

- [1] José Ramón Padilla-López, Alexandros Andre Chaaraoui, and Francisco Flórez-Revuelta "Visual privacy protection methods: A survey," Expert Systems with Applications, Vol. 42, No. 9, pp. 4177-4195, 2015
- [2] Shahid, Zafar, and William Puech "Visual protection of HEVC video by selective encryption of CABAC binstrings," IEEE Transactions on Multimedia, Vol. 16, No. 1, pp. 24-36, 2013
- [3] Yu, Jin-Yong, and Young-Gab Kim "Coding Unit-Based Region of Interest Encryption in HEVC/H.265 Video," IEEE Access, Vol. 11, pp. 47967-47978, 2023
- [4] 김덕한, 김유준, 김영갑 "HEVC 코덱에서 효율적인 관심영역 암호화," 정보처리학회 춘계학술대회, 서울, 2023, pp. 142-144
- [5] Zhou Wang, Alan Conrad Bovik, Hamid Rahim Sheikh, and Eero P. Simoncelli "Image quality assessment: from error visibility to structural similarity," IEEE Transactions on Image Processing, Vol. 13, No. 4, pp. 600-612, 2004
- [6] Nidhi Taneja, Balasubramanian Raman, and Indra Gupta "Chaos based partial encryption of spiht compressed images," International Journal of Wavelets Multiresolution and Information Processing, Vol. 9, No. 2, pp. 317-331, 2011
- [7] M. Viitanen, A. Koivula, A. Lemmetti, A. Ylä-Outinen, J. Vanne, and T. D. Hämäläinen, "Kvazaar: Open-source HEVC/H.265 encoder," in Proc. 24th ACM Int. Conf. Multimedia, Amsterdam, Netherlands, 2016, pp. 1179 - 1182
- [8] C. Montgomery "Xiph.org Video Test Media (Derf 's Collection)," the Xiph Open Source Community, 1994, <https://media.xiph.org/video/derf>