암호화 속도 향상을 위한 디지털 콘텐츠의 특징 영역 암호화

조상일° 홍광진 정기철
숭실대학교 정보과학대학 미디어학과 HCI Lab.
i3011@chol.com°, {hongmsz, kcjung}@ssu.ac.kr

Encryption of Specific Area in Digital Contents for Improving Speed of Cipher

Sangil Cho° Kwangjin Hong Keechul Jung
HCI Lab., School of Media, College of Information Science, Soongsil Univ.

요 약

디지털 영상 콘텐츠는 쉽고 빠르게 복제와 전송이 가능하기 때문에 다수의 사용자가 동일한 콘텐츠를 공유하는 것이 가능하다. 이러한 디지털 콘텐츠의 특징은 많은 디지털 영상 콘텐츠 제작자의 창작 의욕을 저하시키고 콘텐츠 산업 발달을 저해하는 원인이 되고 있다. 따라서 최근 디지털 콘텐츠의 보호를 위한 다양한 연구가 활발하게 이루어지고 있다. 그러나 기존의 가산 암호 방식은 암호의 비도면에서 영상 암호화에 사용된 암호키를 추정할 수 있다는 단점이 있으며 난수 정보가 해독될 우려가 있다. 또한 주사선내 신호 절환 방식은 원영상의 히스토그램 정보를 그대로 담고 있어 암호화된 영상의 히스토그램 정보로 원영상의 종류를 추정할 수 있는 단점이 있고 블록간의 상관 관계를 계산하여 해독할 수 있다는 단점이 있다. 본 논문에서는 디지털 영상 콘텐츠의 특정 영역을 추출하고 이 영역에 대한 암호화를 함으로써, 새로운 암호 알고리즘의 개발 없이 기존의 알고리즘을 이용하여 암호화 속도를 개선하고 안전성을 향상시킬 수 있다.

1. 서 론

최근 컴퓨터의 성능 향상, 초고속 통신망의 보급, 인터넷 사용의 급증으로 인하여 대용량의 디지털 콘텐츠를 공유하는 것이 매우 쉬워졌다. 특히, 영상 콘텐츠의 비중이 높아짐에 따라 디지털 영상 콘텐츠 보호에 대한 관심이 고조되고 있다. 이런 디지털 영상 콘텐츠 보호 기술의 활용 분야로는 위성이나 유선 방송에서의 pay-TV 시스템, 기밀을 요하는 원격 회의나 영상 전화 시스템, 고부가 가치의 위성 사진의 전송, FAX를 이용한 기밀 서류의 전송, 멀티미디어 통신에서의 정보 보호 서비스 등을 들 수 있다[1,2,3].

그러나 영상 콘텐츠는 내재된 정보의 양이 방대하기 때문에 단순하게 기존의 암호 방식을 이용할 경우 암호화에 많은 계산 시간이 필요하다는 문제점이 발생한다. 실제로 MPEG-I 방식을 사용하는 비디오CD의 경우 1분의 영상을 저장하기 위해서 12Mbyte 정도의 공간이 필요하고, MPEG-II 방식을 사용하는 DVD의 경우 1분의 영상을 저장하기 위해서 40Mbyte의 공간이 필요하다[1]. 일반적으로 영화 한편의 상영 시간이 평균 2시간이라는 점을 감안하면 기존의 DES(Data Encryption Standard)나 RSA (Rivest Shamir Adleman) 방식으로 영상을 암호화하기 위해서는 엄청난 시간이 걸려 실용화가 어렵다[4].

이러한 부분을 해결하기 위해 특정 부분만을 이용하는 암호 방식에 대한 연구가 이루어지고 있으며, 윤정오 등이 제안한 쿼드트리를 이용한 구조부분 암호화 방식[5]과 Shioiri 등이 제안한 Shioiri-Kinoshita-Sakai(SKS) 방식[6]이 대표적인 예라 할 수 있다.

쿼드트리를 이용한 구조부분 암호화 방식은 먼저 디지털 영상 콘텐츠를 압축하여 쿼드트리 구조와 쿼드트리 데이터라는 두 개의 압축열을 생성한다. 쿼드트리 구조는 동질 영역의 크기와 위치 정보들로 구성된 영상의 윤곽 정보들로써 구조 부분이 없이 데이터 부분만으로 영상을 복원하는 것은 매우 어렵다. 따라서 구조 부분에 대해서만 DES나 AES(Advanced Encryption Standard)등의 알고리즘을 이용하여 암호화하는 것으로 암호화 과정의 처리시간을 단축하는 것은 물론 압축열 전체에 대해 암호화하는 것과 유사한 효과를 얻을 수 있다. SKS 방식은 영상 콘텐츠를 DCT(Discrete Cosine Transform)를 이용하여 압축할 때, 정보의 대부분이 포함되어 있는 저주파 성분이 한쪽으로 집중된다는 점을 이용하여 암호화하는 방식으로써 DCT가 취해진 주파수 성분 정보 중에서 저주파 쪽 일부만을 암호화해도 IDCT(Inverse DCT)를 취하면 전체 영상에서 높은 암호 효과를 얻을 수 있다는 장점이 있다. 하지만, 쿼드트리를 이용한 방식은 압축과 암호가 결합된 구조이기 때문에, 압축 시간에 비해 암호화 시간이 훨씬 길어진다는 단점이 있고[7], SKS 방식은 암호화된 영상을 분석해보면 대략적으로 어떤 영상인지 파악할 수 있다는 단점이 있다.

본 논문에서 우리는 영상의 특징 영역으로 영상 내의 얼굴 영역을 사용하고, 기존 암호 알고리즘을 이용하여 특징 영역을 암호화함으로써, 영상에 대한 암호화 시간을 줄이는 방법을 제안한다. 제안된 방법은 암호화 시간의 단축 이외에 특징 영역의 좌표를 암호의 이중적 잠금 장치로 추가함으로써 암호강도가 향상된다는 장점을 가진다.

[1] 비디오CD는 352×240의 저해상도 화면을 초당 30프레임으로 저장하고, DVD는 720×480의 고해상도 화면을 초당 60프레임으로 저장한다.

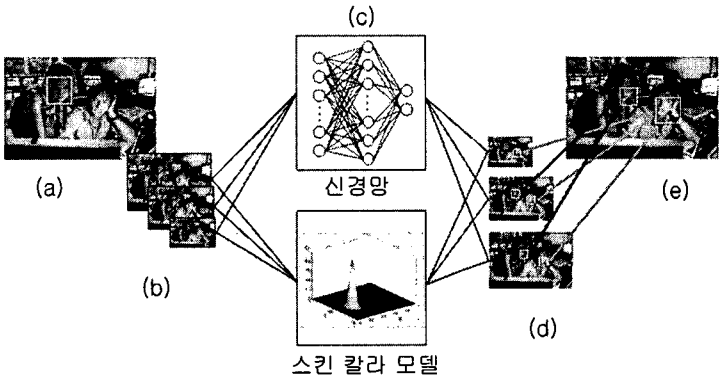

그림 1. 신경망과 스킨 칼라 모델을 이용한 얼굴 추출: (a) 입력 영상, (b) 입력 영상 크기 변환, (c) 얼굴 추출, (d) (b)에 대한 얼굴 추출 결과, (e) 최종 얼굴 추출 결과

2. DICS 시스템

Digital Image Contents Security(DICS) 시스템은 디지털 영상의 특징 부분을 추출하고 해당 영역을 암호화함으로써 디지털 영상을 보호하는 시스템으로 암호 알고리즘의 효율성과 암호화 속도를 향상시킨다. 제안된 시스템이 특징 부분으로 얼굴 영역을 사용하는 이유는, 영화나 드라마 등과 같은 디지털 영상 컨텐츠에서 등장 인물의 얼굴이 감정과 분위기를 전달하는 가장 중요한 부분이기 때문이다.

2.1 특징 부분 추출

본 논문은 디지털 영상의 여러 가지 특징 중 하나인 얼굴 영역을 추출하여 암호화에 이용한다. 우리는 보다 정확한 얼굴 영역 추출을 위해 텍스쳐를 입력값으로 하는 신경망과 가우시안 스킨 칼라 모델을 사용한다. 입력 영상에 대해 사용자가 얼굴 크기 기준으로 삼을 영역을 선택하면(그림 1(a)), 선택된 얼굴 영상 크기를 기준으로 전체 영상의 크기를 조정하고, 조정된 영상을 각각 30%씩 확대, 축소하여 얻어진 3개 영상을 사용하여 다수의 다양한 크기의 얼굴을 추출한다[2] (그림 1(b)). 이때, 신경망과 스킨 칼라 모델은 병렬적으로 수행되고, 각각 얻어진 결과에서 서로 겹쳐지는 영역을 얼굴 영역으로 결정한다(그림 1(c, d)). 마지막으로 3개의 서로 다른 크기의 영상에서 얻어진 얼굴 추출 결과를 이용하여 최종적인 얼굴 영역을 결정한다 (그림 1(e)).

2.2 암호화 및 복호화

암호화 모듈에서는 신경망과 스킨 칼라 모델을 이용하여 추출된 영역에 대한 좌측 상단(시작점)과 우측 하단(끝점) 두 개의 x, y 좌표값을 이용하여 영상 콘텐츠를 암호화하고, 좌표값을 워터마크 기법을 통해 영상에 숨긴다. 따라서 영상 콘텐츠에 대한 암호화 시간을 단축시켜줌과 동시에 이중적 암호화 구조를 통해 콘텐츠에 대한 암호 강도를 향상시킨다.

[2] 기준 영상을 정하고 각각 30%씩 확대, 축소한 영상을 사용하는 이유는 영상 내에서 의미를 가지지 못하는 너무 작거나 너무 큰 얼굴 영역을 찾지 않음으로써 얼굴 추출 시간을 줄이기 위함이다.

DICS 시스템은 암호화와 복호화 과정이 서로 다른 시스템이다. 암호화는 영상 콘텐츠의 특징 영역을 추출하고 추출된 영역에 대해 암호화하는 과정을 거치고, 복호화는 암호화된 콘텐츠에 삽입된 좌표값을 추출하여 해당 영역을 복호화하는 과정을 거친다 (그림 2).

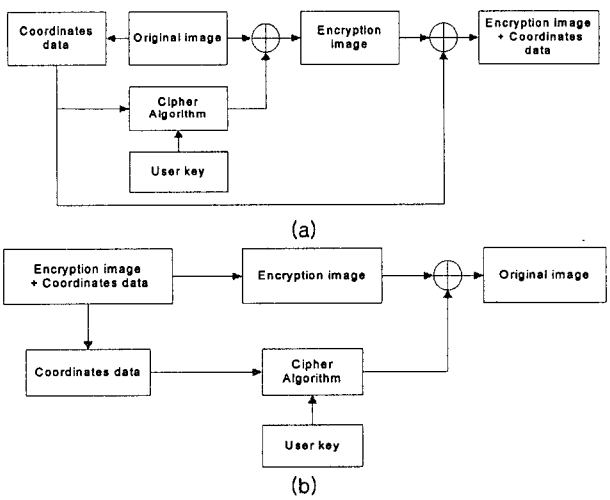

그림 2. DICS 시스템 구성도: (a) 암호화 과정, (b) 복호화 과정.

DICS 시스템에서 암호화를 위해 먼저 그림 3(b)에서 보는 바와 같이 원본 이미지(그림3 (a))로부터 특징 부분을 추출한다. 특징 부분은 영상의 중요한 부분으로 영상 안의 얼굴, 신체 각 부분, 문자 등을 의미하고, 제안한 시스템은 얼굴 영역을 특징 부분으로 사용한다. 얼굴 영역 추출을 위해 2.1절에서와 같이 신경망을 이용하여 얼굴 부분을 학습시켜 얼굴 영역을 구하고, 스킨 칼라 모델을 적용하여 신경망 결과와 AND연산을 통해 좀 더 정확한 얼굴 영역을 추출한다. 추출된 얼굴 영역의 좌표값(시작점, 끝점)을 이용하여 원본 이미지의 특징 영역을 암호화한다(그림 3(c)). 또한 좌표값은 암호화된 영상에 워터마킹되어 복호화 과정에서 사용할 수 있도록 한다. 제안된 시스템은 특징 영역만을 암호화함으로써 좌표 영역을 알지 못 하는 경우 복호화가 힘들고, 전체 영상에 대해 암호화 방식과 비교하여 속도가 빠르다는 장점을 가진다. 암호화된 영상의 복호화

를 위해서 암호화된 영상에서 워터마킹된 좌표값을 추출하고, 암호화에 이용한 사용자 키와 함께 암호 알고리즘에 입력함으로써 복호화한다(그림 3(d)). 복호화 과정은 암호화 과정과 달리 특징 영역을 추출하는 과정을 거치지 않으므로 암호화 과정에 비해 시간이 적게 걸린다.

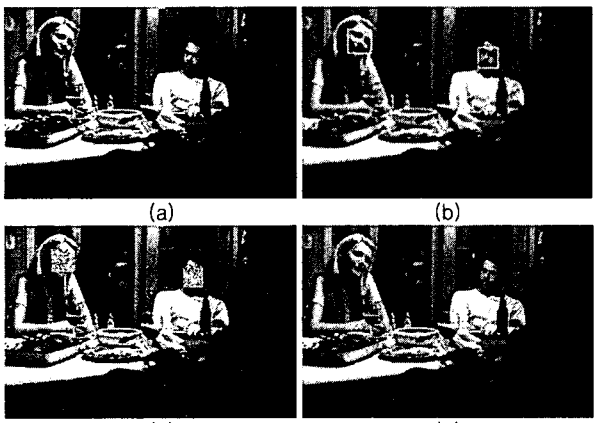

그림 3. DICS 시스템을 이용한 영상 보호: (a) 원영상, (b) 얼굴 영역 추출, (c) 추출 영역에 대한 암호화, (d) (c)에 대한 복호화.

4. 실험 결과 및 분석

실험을 통해 우리는 DICS 시스템의 안전성과 처리 속도 등에 대해 분석을 하였다. DICS 시스템은 특징 부분을 암호화함으로써 영상 전체에 대한 암호 효과를 주는 시스템으로 좌표값을 구하는 만큼 안전성이 증대되며, 좌표 영역만을 암호화함으로써 처리 속도가 향상되는 시스템이고, 영상의 블록화되는 좌표값(시작점, 끝점)을 구해야만 영상을 복원할 수 있다. 따라서 좌표값을 찾기 위해 식 1과 같이 영상의 안전성이 증가함을 알 수 있다. 식 1에서 P는 영상 크기 *image*에서 특징 블록 *n*개가 나타날 확률을 의미한다.

$$
\begin{aligned}
P(n \mid image) &= \frac{2n}{{}_{image}C_2} \\
&= \frac{2n \times 2 \times (image-2)!}{(image)!} = \frac{4n}{(image)(image-1)} \\
&= \frac{4}{(720\times480)(720\times480-1)} \quad (if, n=1) \\
&\approx \frac{1}{2^{35}}
\end{aligned} \tag{1}
$$

식 1에서 720×480 사이즈 영상에 1개의 특징 영역이 있다고 가정했을 때 좌표값(시작점, 끝점)을 찾을 수 있는 확률이 $1/2^{35}$로 낮아지고 이에 비례해서 알고리즘 비도가 향상됨을 알 수 있다. 또한 특징 부분의 개수가 증가할수록 암호 알고리즘 비도가 더욱 향상됨을 알 수 있다.

DICS 시스템의 장점인 블록화 영역의 암호화를 통해 처리 속도가 향상된다. DICS 시스템은 암호화와 복호화 시간이 다르기 때문에 아래 표 1, 2와 같이 암호화와 복호화 시간을 DES와 AES 알고리즘을 이용하여 측정하였다.

표 1. DICS 시스템의 암호화 속도

	DES	AES
전체영상의 암호	8162 ms	4800 ms
DICS 시스템	1005 ms	669 ms

표 2. DICS 시스템의 복호화 속도

	DES	AES
전체영상의 암호	8162 ms	4800 ms
DICS 시스템	646 ms	310 ms

암호화에는 얼굴 인식 및 좌표값 추출 시간이 추가되며, 복호화에는 좌표값을 이용한 복호화 시간만 걸리기 때문에 복호화 시간이 암호화 시간에 비해 빠르다는 것을 알 수 있다.

5. 결론

컴퓨터 기능의 향상과 모바일 기기의 보급으로 인해 디지털 컨텐츠에 대한 복제가 수월해짐에 따라, 디지털 영상 콘텐츠 정보 보호를 위해 빠르고 안전한 암호 알고리즘 및 방식이 제안되고 있다. 제안된 DICS 시스템은 디지털 영상 콘텐츠의 특징 영역에 대한 암호화를 통해 암호화 속도의 향상과 암호 알고리즘의 비도 향상(안전성)효과를 얻을 수 있는 시스템으로써, DVD나 HDTV 방송, 위성을 통한 영상 전송 등과 같은 디지털 영상 콘텐츠의 보호 분야에 적용하여 사용할 수 있을 것으로 기대된다. 또한 현재 시스템에서 암호화를 위한 얼굴 영역 추출 시간이 많이 걸리고, DES나 AES, RSA 와 같은 블록 암호 알고리즘을 사용함으로써 암호화 시간이 많이 걸린다는 단점은 영상 처리 알고리즘의 개선과 스트림 암호 알고리즘의 사용으로 해결할 수 있을 것이다.

6. 참고 문헌

[1] N. Katta, S. Nakamura, H. Murakami, H. Tanaka, "A New Approach to Digital Scrambling of Image Signals," 信學誌報, ISEC90-33, 1990.

[2] N. Shioiri, H. Kinoshita, Y. Sakai, "A Study on the Satelite Teleconferencing Protocol for Security," 信學技報, Vol. 90, No. 31, ISEC 90-34, 1990.

[3] H. Tominaga, Y. Ohtsubo, N. Komatsu, "On a Confidential Message Handling Facility for Facsimile Communications," 電子通信學論文誌, Vol. J65-B, No. 11, 1982.

[4] 前田章, 古村文伸, 白石高義, "デイゾタル 畫像に滴し たデータ暗號化の一方法," 電子通信學會論文誌, Vol. J69-B, No. 11, 1986.

[5] H. Kinoshita, N. Shioiri, Y. Sakai "Appropriate Image Data Encipherment Method for DCT Coding," Trans. of IEICE, Vol.J75-D-I, No.5, pp. 314-321, 1992.

[6] S. S. Maniccam, N. G. Bourbakis, "SCAN Based Lossless Image Compression and Encryption," IEEE Trans., Image Processing, Vol. 3, No. 5, pp. 490-499, Sept. 1999.

[7] 윤정오, 성우석, 황찬식, "실시간 처리를 위한 쿼드트리 기반 무손실 영상압축 및 암호화," 정보처리학회논문지C 제8-C권 제5호, pp. 525-534, 2001.