

동영상 자막 정보를 위한 스태가노그래피 적용에 관한 연구

함준식*, 유황빈**

*광운대학교 컴퓨터학과

**광운대학교 컴퓨터학과

e-mail:hamjs@cs.kwangwoon.ac.kr

A Study on the Application of Steganography for Moving Picture Caption Information

Jun-Sick Ham*, Hwang-Bin Ryou**

*Dept of Computer Science, Kwang-woon University

**Dept of Computer Science, Kwang-woon University

요약

인터넷의 시대에 들어오게 되면서 현대는 무한한 정보바다의 물결에 휩쓸려가고 있으며 이러한 경향과 더불어 멀티미디어 데이터의 양도 급격히 늘어나고 있다. 인터넷의 가장 큰 특징이자 장점인 접근 가능성은 무제한으로 어떠한 정보 콘텐츠라도 이용 가능하게 한다. 그렇지만 접근 가능성은 누구나 쉽게 디지털 정보의 복제를 가능하게 함으로써 타인의 지적 재산권에 침해를 줄 수 있게 되었다. 이를 해결하기 위한 방법으로 워터마크 연구가 활발히 이루어지고 있다. 본 논문에서는 동영상 자막 정보인 SMI 파일을 동영상 내에 숨기는 방법을 이용하여 자막 정보 및 동영상 정보의 저작권 및 무결성 보호를 하고자 한다.

본 논문에서는 자막 정보를 분리, 암호화하여 동영상 내의 프레임에 삽입하는 방법을 제시한다. 동영상에 영향을 미치지 않는 각 프레임 내의 최하위 비트에 자막 정보를 삽입하여 다른 사람들이 동영상을 편집한 경우에는 자막 정보를 제공받지 못하도록 한다.

1. 서론

멀티미디어 데이터의 급속한 발전으로 인하여 인터넷을 통한 디지털 데이터를 쉽게 수집할 수 있으며, 수집된 디지털 데이터를 조작하는 강력한 도구들을 쉽게 구할 수 있다. 그러므로 이러한 도구들로 인한 피해를 줄이고자 멀티미디어 데이터의 저작권 보호를 위한 방법의 필요성이 대두되고 있다. 많은 콘텐츠를 제작하고 있으며, 인터넷으로 인한 정보의 양이 기하급수적으로 발전하고 있는 상황에서 모든 미디어에 대한 저작권을 보호하기 위해 특정 기관이 저작권을 관리한다는 것은 너무나 어려운 일이다[7].

본 논문에서는 데이터 보호 방법들을 이용하여 동영상 자막 정보로 사용되는 SMI 파일 및 동영상 파일에 대한 저작권 및 무결성 보호를 목표로 한다. SMI 파일은 ASCII 형식으로 일반 텍스트를 편집하는 툴에서 쉽게 읽혀지기 때문에 어느 누구나 쉽게

편집 가능하고 저작권은 보호 될 수 없게 된다. 이러한 저작권 침해와 불법 변조를 막기 위해 SMI 파일을 스태가노그래피(Steganography) 방법을 적용하여 보호하도록 한다. 또한 SMI 파일을 동영상 내부에 삽입할 때 암호 알고리즘을 사용하여 자막 정보가 임의의 사용자로부터 분리된다 해도 쉽게 인식하지 못하도록 한다. 이러한 자막 정보의 동영상 내 삽입은 자막 정보의 보호 외에 동영상에 대한 보호를 동시에 할 수 있다는 장점이 있다.

2. 스태가노그래피 기법

스태가노그래피는 메시지의 존재를 숨기는 비밀 통신의 방법 중에 하나로써 보이지 않는 잉크, 점 크기의 미소 사진, 문자 배열 순서, 디지털 서명, 은밀한 채널, 스프레드 스펙트럼 통신들이 있다[1, 2, 3].

스태가노그래피는 암호 알고리즘과는 달리 중요한 정보를 상대방에게 전송하기 위하여 정보와는 상관없는 다른 데이터의 내부에 보내고자하는 정보를 삽입하여 전송하는 것이다. 암호화는 비밀 통신이라는 사실이 알려지지만 스태가노그래피는 비밀 통신이라는 사실 자체도 숨겨 정보를 전송하는데 그 의미가 있다.

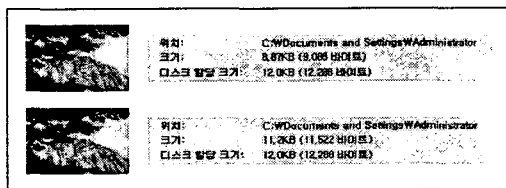
스태가노그래피는 다음과 같이 크게 네 가지의 요소로 이루어진다[3, 4, 5]. 중요한 비밀 정보를 삽입하기 위한 의미 있는 데이터로 cover-data, 비밀 정보를 삽입하기 위해 사용되는 키로 stegokey, cover-data에 은닉되어지는 비밀 정보로 secret-data, cover-data에 secret-data가 은닉되어 있는 결과 데이터로 stego-data가 있다.

이러한 스태가노그래피에서 사용되는 요소들은 다음과 같이 표현 가능하다.

$$\text{stego-dat} = \text{cover-data} + \text{secret-data} + \text{stego-key}$$

컴퓨터 스태가노그래피는 다음 두 가지의 방식이 있다. 첫째는 이미지 파일이나 사운드 파일을 데이터와 기능은 손실을 가하지 않고 겉모양만 바꾸는 방법이고 둘째는 이미지나 사운드 파일에 비밀 메시지를 포함하는 것이다. 이 경우 파일의 색깔이나 소리는 바뀌지만 그 변화가 너무 미미해 알아차리기 어렵다.

가장 널리 사용되는 것은 두 번째 방법으로 보통 윈도우즈용으로 제공되는 스태가노그래피 툴을 사용하는 것이다. (그림 1)은 같은 그림이지만 그 정보가 틀리다는 것을 알 수 있다.



(그림1) cover-data와 stego-data의 비교

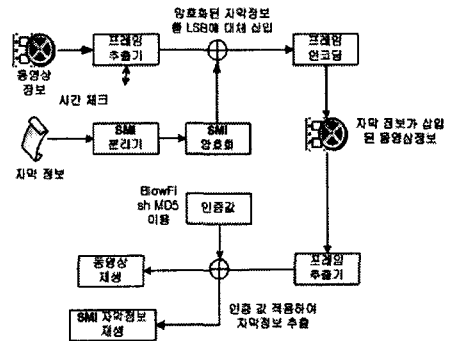
본 논문에서는 공간영역 삽입 방식으로 LSB에 삽입하는 방법을 이용하여 동영상 내에 ASCII 형태의 SMI 자막 정보를 삽입하고자 한다. 삽입되어지는 자막 정보는 자막 정보 그대로 삽입되어 지는 것

이 아니라 임의의 사용자로부터 추출되더라도 쉽게 알아 볼 수 없도록 Blowfish와 MD5[6] 로 암호화되어 저장된다.

3. 동영상 자막정보 삽입 시스템

3.1 전체 시스템 구조

(그림 2)는 본 시스템의 전체적인 구조이다.



(그림 2) 전체 시스템 구조

(그림 3)은 자막 정보 삽입 및 추출의 알고리즘을 보여준다.

```
writedata ()
{
    cntfile = readcntfile (cover-data);
    pinfile = readpinfile (secret-data);
    fco = readfco(stego-data);
    encrypt_data (pinfile, stego-key);
    embeddata (cntfile, pinfile);
    stgfile = createstgfile (cntfile, stgfilename);
    writecntfile (stgfile);
}

readdata ()
{
    stgfile = readcntfile (stgfilename);
    pinfile = crestepinfile (pinfilename);
    pinfile = extractdata (stgfile);
    decrypt_data (pinfile, stego-key);
    writepinfile (pinfile);
}
```

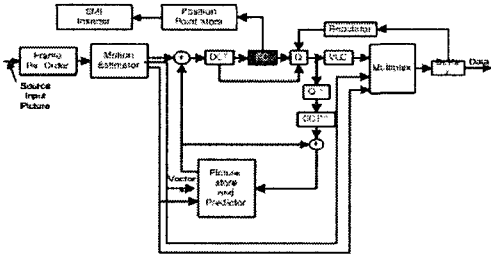
(그림 3) 자막 정보 삽입/추출 알고리즘

3.2 SMI 자막 정보 삽입 방법

3.2.1 동영상 자막 삽입 위치

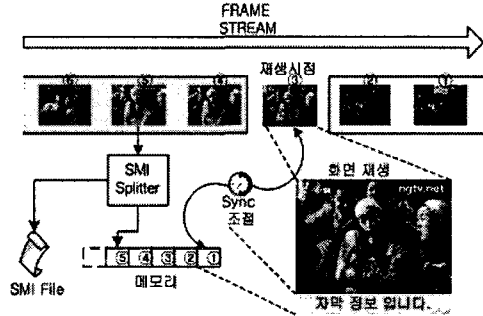
동영상 내에 자막 정보를 삽입하는 방법은 자막 정보를 여러 조각으로 나누어 동영상의 프레임 자체에 삽입하는 방법이다. 삽입되는 위치는 I 프레임에 삽입되어진다. 그러나 I 프레임은 부호화가 발생되기 때문에 자막 정보를 삽입 할 때에 이 문제를 해결해야 한다. 본 논문에서는 주파수 카운트 (frequency count)를 계산하여 자막 정보의 삽입 위

치를 결정할 수 있다. 주파수 카운트는 압축 시 삭제되는 고주파 영역을 계산하여 자막 정보를 삽입할 때 계산된 고주파 영역을 피하여 삽입하는 방법이다. (그림 4)는 Encoder에서의 주파수 카운트의 위치를 나타낸 것이다.



(그림 4) 주파수 Count를 위한 수정된 Encoder

자막 정보가 추출되어 메모리에 할당되었다면 동영상 재생시간과 동일시간에 자막 정보를 화면에 재생시켜 주기만 하면 된다. (그림 6)은 자막 정보의 재생을 나타낸 그림이다.



(그림 6) 자막 정보의 실시간 화면 재생

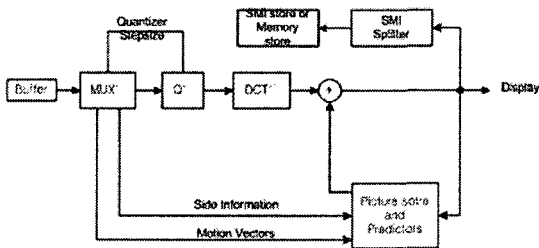
3.2.2 동영상 내 자막 삽입

동영상은 실시간으로 재생되어지기 때문에 자막 정보도 실시간으로 재생되어야 한다. 본 논문에서는 동영상과 자막 정보의 실시간 동기화를 위한 방법을 제안한다. 동영상은 수많은 프레임으로 구성되어 있고 그 프레임들은 순차적으로 재생하게 된다. 따라서 자막 정보를 해당 위치 프레임에 삽입하게 되면 디코딩 시 자막 정보를 추출하는 시간만큼 지연이 발생하게 되기 때문에 이전 프레임에 삽입하는 방식을 이용한다.

3.3 SMI 자막 정보 추출 및 재생 방법

3.3.1 SMI 자막 정보 추출

자막 정보의 추출은 MPEG Decoder에 SMI Splitter를 삽입함으로써 구현할 수 있다. (그림 5)는 SMI Splitter가 삽입된 Decoder를 나타낸 것이다.



(그림 5) 수정된 MPEG Decoder

4. 성능평가 및 분석

실시간 자막 처리를 위한 방법으로 자막 정보 삽입할 때 이전 프레임의 위치에 삽입함으로써 실시간으로 처리할 수 있다고 하였다. 하지만 이전 몇 프레임 뒤에 삽입되어질지는 연산시간의 총합시간이 계산되어야 한다. (표 1)은 시스템에 따른 연산 시간을 나타낸 것이다.

| 컴퓨터 사양 | I 프레임 추출 | SMI 추출 | 기타 | 총시간 |
|-------------------|--------------|--------------|-----------|-------|
| 펜티엄 Pro-200, 120M | 0.30 ~ 0.40초 | 0.22 ~ 0.40초 | 0.40 초 이상 | 1.4 초 |
| 펜티엄 II-233, 120M | 0.27 ~ 0.35초 | 0.22 ~ 0.32초 | 0.40 초 이상 | 1.3 초 |
| 펜티엄 III-700, 120M | 0.20 ~ 0.30초 | 0.20 ~ 0.30초 | 0.30 초 이상 | 1.1 초 |

(표 1) 시스템에 따른 연산 시간

본 논문에서는 펜티엄 III를 바탕으로 구현되었으며 자막 정보가 재생될 프레임의 이전 2 프레임 뒤에 삽입하였다. 2 프레임이라고 하면 시간상으로 1.2 초 정도의 시간을 나타내므로 연산시간 측정 결과로 나온 1.1 초의 시간을 충분히 보장할 수 있다.

352 × 240 동영상의 한 I 프레임에 삽입 될 수 있는 자막 정보는 15 KB 정도이다. 하지만 압축에 의한 손실에 대처하기 위해서는 3 KB 미만의 정보만 삽입 할 수 있다. 3 KB 정보는 일반 영화 자막

3.3.2 SMI 자막 정보 재생 방법

으로 50 라인 정도의 분량이기 때문에 자막정보를 삽입하기에는 충분한 공간임을 알 수 있다.

(그림 7)은 구현된 시스템에 대한 화면 인터페이스이다.



(그림 7) 구현된 시스템의 동영상 자막 재생

5. 결론

본 논문에서는 일반적으로 많이 사용되고 있고 동영상 정보에서 중요한 역할을 담당하는 SMI 자막 정보에 대한 저작권 보호 및 무결성을 보장하기 위하여 자막 정보의 동영상 내에 삽입하는 방법을 제안하였으며, 이렇게 삽입된 자막 정보는 동영상 자체에 대한 저작권 보호 및 무결성을 보장하는데 도움을 줄 수 있다. 또한 기존의 동영상 데이터에서 자막 정보를 이용하기 위해서는 SMI 파일을 동시에 동영상 파일과 같은 이름으로 가지고 있어야만 재생이 가능하였으나 본 논문에서는 자막 정보를 동영상 내 삽입함으로써 자막 정보를 파일로 별도로 가지고 있지 않아도 된다는 이점이 있다.

동영상 내 자막 삽입을 위해 제안한 알고리즘은 동영상 I 프레임의 이미지를 값으로 추출하여 LSB 영역에 자막 정보를 삽입하는 방법이었으며 또한 자막 정보 삽입 시 자막 정보의 화면내 부호화로 인한 손실을 막는 알고리즘을 제안하였다. 그리고 자막 재생은 Blowfish와 MD5를 이용하여 암호화하였다. 이는 동영상의 실시간 재생이라는 현실성을 고려한 방법이며, 시스템의 성능이 뒷받침된다면 LSB 영역에 삽입하는 방식이 아닌 주파수 영역에 삽입하는 방법을 이용하는 것이 자막 정보 보호에 더 강할 것이다.

향후 과제로는 동영상 삽입 방법에 사용되는 스테가노그래피의 방법을 공간 영역이 아닌 주파수 영역 삽입으로의 개선과 속도 향상, 동영상 실시간을

위한 자막 삽입 방법의 개선, MPEG 동영상 이외의 다양한 동영상 포맷에서도 쉽게 적용 가능하고 응용하기 쉽게 알고리즘을 수정해야 할 것이다.

참고문헌

- [1] E.Fanz, A.Jerichow, S.Moller, A.Pfzmann, I.Stierand, "Computer Based Steganography: How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best", *Proceedings of Information Hiding Workshop*, LNCS Vol.1174, pp. 7-21, Springer-verlag, 1996.
- [2] Eugene T. Lin, E. J. Delp, "A Review of Data Hiding in Digital Images," *Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference'99*, pp. 274-278, April 1999.
- [3] Neil F. Johnson and Sushil Jajodia, "Lecture Notes in Computer Science", *Workshop on Information Hiding Proceedings*, Portland, Oregon, USA, Vol. 1525, pp. 273-289, 15-17 April 1998.
- [4] 이진호, 김태운, "RSA 함수를 기반한 안전한 워터마킹 기법," *정보과학회논문지 : 컴퓨팅의 실제* 제 7권 제 3호, pp. 220-228, 2001. 6
- [5] Neil F. Johnson, Zoran Duric, Sushil Jajodia, *Information Hiding - Steganography and Watermarking - Attacks and Countermeasures*. Kluwer Academic Publishers, pp. 18-44, 2001.
- [6] 박창섭, *암호이론과 보안. 대영사*, pp. 164-167, 1999.
- [7] Ivy_research, "Data Hiding...", http://vega.icu.ac.kr/~ivy/ivy_research/watermarking.html