동영상에서 스테가노그래피 적용에 관한 연구

이용배° 신동규 전문석
숭실대학교 대학원 컴퓨터학과
yb1003@hanmail.net°, nicesdg@empal.com, mjun@computing.ssu.ac.kr

A Study on the Application of Steganography for Moving Picture

YongBae Lee°, Donggyu Shin, MoonSeog Jun
Dept.of Computing in Soongsil Univ

요 약

인터넷의 사용이 나날이 증가됨으로써 많은 양의 데이터들이 서로 공유되어지고 있으며, 데이터의 양도 나날이 증가되고 있는 추세이다. 이렇게 많은 양의 데이터들이 공유되어짐에 따라 정보보호에 대해 인지를 해야만 한다. 최근 정보보호 시스템으로 전송 매체에 비밀 데이터를 직접 삽입하는 스테가노그래피 알고리즘에 대한 연구가 활발히 이루어지고 있다. 스테가노그래피는 데이터를 텍스트, 이미지, 오디오등 커버 데이터라 불리는 전송 매체에 숨겨 전송하는 방법으로 제 3자는 데이터가 숨겨져 있다는 사실 자체를 알지 못하도록 하는 것이다.

본 논문에서는 정지영상에 스테가노그래피 기법을 사용하던 기존 방식에서 좀 더 발전된 움직이는 영상에서 프레임에 데이터를 삽입하여 전송하는 방법을 제시한다. 동영상에 영향을 미치지 않는 선에서 정보를 삽입하여 제 3자는 이를 전혀 눈치채지 못하도록 한다.

1. 서 론

인터넷의 시대에 살고 있는 지금 우리는 무수히 많은 데이터들을 받기도 하고 보내기도 한다. 또한 정보 활용이 단순한 문자에서 이제는 정보전달 효과가 뛰어난 멀티미디어로의 정보 교환이 이루어지고 있다. 또한 많은 양의 데이터들이 서로 공유되어지고 있으며, 데이터의 양도 증가되고 있는 추세이다. 인터넷에서 개방되어 있는 데이터를 보호하고 전송 중에 정보의 안전과 신뢰, 보호 및 은닉에 대한 필요성이 요구되고 있다. 정보보호의 방법으로 전송매체에 비밀정보를 삽입하는 스테가노그래피 방법에 대한 연구가 활발히 이루어지고 있다.

스테가노그래피는 비밀 메시지를 이미지나, 오디오, 비디오 또는 텍스트 등 커버(cover)라 불리는 디지털 매체에 다른 비밀 디지털매체를 숨겨서 전송하는 방법으로 제 3자는 정보가 숨겨져 있다는 사실 자체를 알지 못하도록 하는 것이다.

스테가노그래피는 삽입 용량(capacity), 숨겨진 정보의 비인지성(imperceptibility), 그리고 제거공격에 대한 안전성 내지 강인성(robustness)등을 만족하여야 한다.

기존의 스테가노그래피 알고리즘들은 정적인 데이터인 JPEG(Joint Photographic Expert Group), GIF(Graphic Interchange Format) 등의 데이터 포맷에 의존적이다. 하지만 현재 인터넷의 흐름을 살펴보면 점점 더 많은 양의 데이터들을 주고 받는 것을 볼 수 있다. 거기에는 멀티미디어 즉 동영상에 관한 많은 데이터들의 사용량도 크게 증가하고 있다는 것을 알 수 있다.

본 논문에서는 정적인 이미지가 아닌 동영상에서 스테가노그래피 기법을 사용하여 비밀 메시지를 삽입하는 방법을 제안하고자 한다. 동영상 프레임에 LSB 삽입 알고리즘을 이용하여 비밀 메시지를 삽입하는 방법을 사용한다. 또한 전송할 때 비도를 높이기 위해 전송프레임 난수시퀀스 방식을 제안한다.

본 논문의 구성으로, 2장에서는 기존 스테가노그래피에 관한 은닉방식에 대해 언급하고, 3장에서는 논문에서 제안된 동영상에서 스테가노그래피 삽입 시스템의 전체 구상도와 삽입방법에 대해 알아보며, 4장에서는 향후 발전과정에 대해 언급하고 논문의 결론을 맺는다.

2. 관련연구

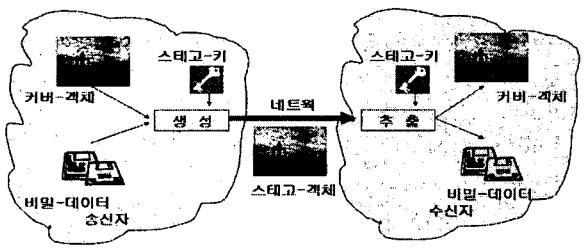
2.1 스테가노그래피 시스템

스테가노그래피는 보이지 않는 통신 기술을 뜻한다. 이것의 목적은 비밀메시지를 커버 객체에 삽입함으로써 통신의 실체에서 감추는 것이 목적이다.

스테가노그래피 시스템은 [그림2-1]과 같이 생성과정과 네트워크 및 추출 과정으로 구성되며 비밀 데이터를 전달하기 위하여 커버 객체로 불리는 원래 이미지에 삽입 알고리즘을 사용함으로써 변경되어 삽입 결과로 얻어진 이미지를 스테고 객체라 하고 스테고 객체의 안전성을 보장하기 위하여 사용된 키를 스테고 키라한다.

스테가노그래피의 기술은 공유하는 데이터의 특성에 따

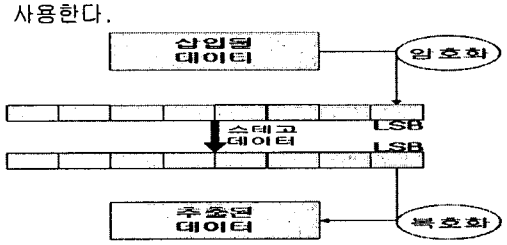
라 3가지로 나누는데, 송신자와 수신자가 서로 비밀 통신을 하기 위해 사전에 개인키를 공유하는 기술인 Private-Key 스테가노그래피 시스템과 비밀통신을 하기 위해서 공개된 상대방의 공개키를 이용하는 Public-key, 스테가노그래피 시스템 그리고 마지막으로 비밀 통신을 하기 위해 두 통신자가 사전에 어떤 정보도 공유할 필요가 없는 Pure스테가노그래피 시스템으로 나눌 수 있다.



[그림 2-1]스테가노 그래피 시스템 구성도

2.2 LSB 삽입 방식

[그림 2-2]은 LSB방식을 보여주고 있다. LSB방식은 가장 잘 알려진 이미지 스테가노그래피 기술이다. 이것은 그래픽 이미지 파일에 기밀정보를 집어넣는 가장 보편적인 은닉 방법이다. 본 논문에서는 동영상에 비밀데이터를 삽입하기 때문에 속도면에서 가장 빠른 LSB 삽입 방식을 사용한다.



[그림 2-2] LSB 스테가노그래피 삽입

24비트 이미지(각 픽셀의 RGB값)에서 LSB비트를 각 바이트에 적용할 때, 각 픽셀은 1이나 0으로 구성되어 있고, 3비트는 각 픽셀로 코드와 될 수 있다. LSB로 알려진 마지막 비트를 은닉정보의 비트 값으로 치환한다.

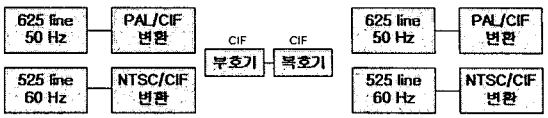
2.3 H.261 파일변환 포맷

본 논문에서 사용할 압축 변환 포맷인 H.261압축 포맷에 대해 알아본다.

H.261은 디지털 네트웍 서비스를 통합하기 위해 1990년에 ITu-T가 개발한 비디오 압축 표준이다. 데이터는 초당 64킬로비트 속도의 배수로 압축되는데, 이를 흔히 64P라고 하며 여기서 P 값은 ISDN 채널의 수에 따라 1~30사이에서 값이 변화된다. 이 H.261은 비디오폰과 화상회의 등을 지원하기 위해 개발된 것이다. 동영상을 사용한 본 논문에서도 실시간으로 전송을 구축하기 위해서 H.261포맷을 사용한다.

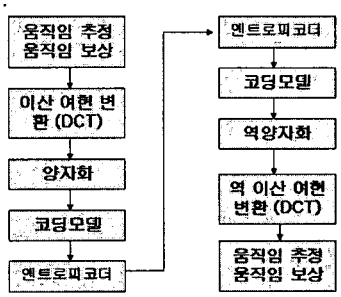
H.261은 효과적인 동영상 압축을 위하여 여러 가지 손실.무손실 압축 기법들을 결합하고 있다. 영상 전화와 TV에서 주로 사용이 되는데 이들 두 시스템은 직접적으로 형식이 호환성을 갖지 못한다.

두 시스템간의 변환을 위해 CIF(Common Intermediate Format)라는 공통 양식을 만들어 코덱의 영상 입출력 포맷으로 사용한다.



[그림 2-3] CIF(Common Intermediate Format)

H.261의 압축정보 흐름은 [그림 2-4]와 같다. 디코딩된 영상은 이산여현변환 DCT(Discrete Cosion Transform)을 통하여 압축되고 양자화를 통화여 디지털 샘플링 된다. 이때 여러 가지 코딩모델이 엔트로피와 결부하여 수행되고 전송되어진다. 전송된후는 역양자화와 영 이산 여현 변환을 수행하여 움직임 추정을 한다
여기서 삽입하는 부분은 양자화와 코딩모델 사이에서 삽입을 하고 추출은 코딩모델과 역 양자화 사이에서 이루어지게 된다.

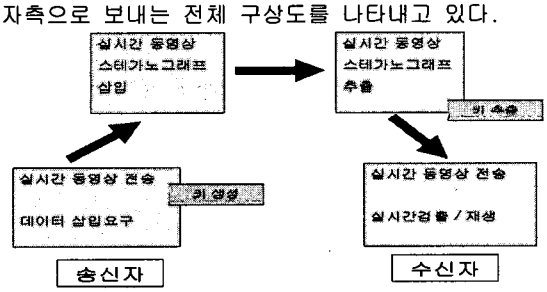


[그림 2-4] H.261 압축 정보 흐름

3. 동영상에서 스테가노그래피 삽입 시스템

3.1 전체시스템 구상도

동영상에서 스테가노그래피 전체 시스템 구상도를 보면 [그림 3-1]과 같이 송신자 측에서 동영상을 전송할 때 실시간으로 동영상내에 비밀 데이터를 삽입해서 수신자측으로 보내는 전체 구상도를 나타내고 있다.

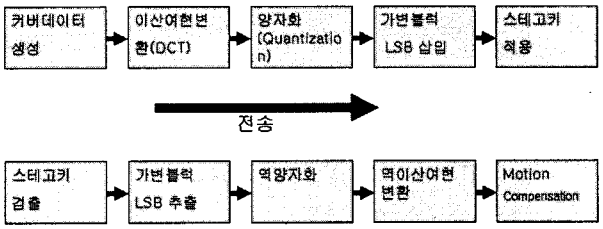


[그림 3-1]전체시스템 구상도

본 논문에서는 실시간 동영상 스테가노그래피 삽입과 추출하는데 있어서 보다 더 안전하고 빠르게 삽입하고 추출할 수 있도록 프레임 내에 LSB삽입 방법으로 비밀데이터를 삽입하는 방법을 제안한다.

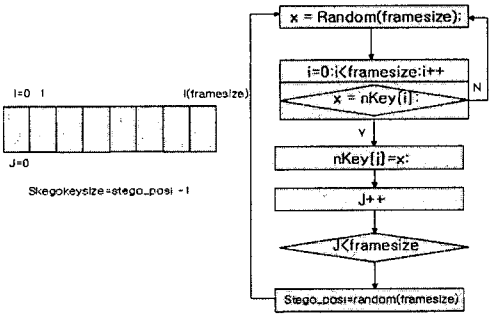
3.2 동영상에 스테가노그래피 삽입 방법

본 논문에서 제안한 프레임 저장 스테가노그래피 알고리즘 실행 흐름도는 [그림 3-2]와 같다.
1)움직임 추정(Motion Estimation)과 움직임보상(Compensation)을 통하여 이미지를 생성하여 압축을 하여 커버데이터를 생성한다 2)mpeg를 이산여현변환(DCT)를 통하여 압축한다 3)양자화(Quantization)를 통하여 디지털 샘플링을 수행한다. 4)프레임에 LSB삽입 방법을 이용하여 비밀 데이터를 삽입후 스테고키를 적용하여 전송을 하게 된다.



[그림 3-2]프레임 저장 스테가노그래피 알고리즘 실행 흐름도

스테고 데이터의 추출은 전송할 때 역으로 실행을 하면 된다.
그리고 전송할 때 비도를 높이기 위해 전송프레임 난수시퀀스 생성 방법을 이용하는데 [그림 3-3]에 전송프레임 난수시퀀스 생성 방법을 보여준다.



[그림 3-3] 전송프레임 난수시퀀스 생성 방법

이 전송프레임 난수시퀀스 방법은 모든 프레임에 스테고데이터를 삽입하는 것이 아니고 전송 프레임 난수시퀀스에 설정되어 있는 프레임에 스테고 데이터를 삽입하게 되는 방식이다. 여기에 따른 이점은 항상 같은 위치에 스테고 데이터를 삽입하지 않기 때문에 그만큼 위험 부담이 많이 떨어지게 된다.
전송프레임 난수시퀀스는 프레임사이즈에 의존적이다. 프레임은 초당 전송되기 때문에 각 초당 임의의 프레임을 정하여 스테고데이터를 삽입한다. 또한 연속적으로 스테고데이터를 전송하게 될 경우를 위하여 슈도 랜덤한 난수를 발생시킨다. 따라서 [그림 3-3]와 같이 nKey[] 배열 안에 이미 설정된 난수와 새로 생성된 난수를 연속적으로 비교하여 설정한다. 여기서, i는 설정된 배열의 내용을 확인하기 위한 변수이며, j는 nkey[] 배열을 인덱스하기 위한 변수이다.입력되는 프레임의 프레임 사이즈만큼 전송프레임 난수시퀀스를 설정하고 전송 프레임 난수시퀀스를 설정한 배열에 의존적으로 스테고데이터가 삽입될 프레임의 위치를 선택한다.

4 결론

인터넷으로 전송되고 있는 데이터의 양은 나날히 증가하고 있는 추세이다. 자신의 비밀 데이터를 제 3자 모르게 전달해야할 때 우리는 스테가노그래피 기법을 사용을 한다. 하지만 현재의 스테가노그래피 알고리즘은 정적인 데이터에 한정되어 있다. 본 논문에서는 정적인 데이터가 아닌 움직이는 영상에 비밀 데이터를 삽입하는 방법을 제안하였다. 정적인 영상에서 가장 크게 단점으로 나오는 것이 바로 비밀데이터의 삽입할 수 있는 데이터의 크기이다. 정지된 데이터이기 때문에 삽입할 수 있는 비밀데이터의 크기도 한계가 있기 마련이다. 물론 동영상에서도 크기는 한정되어져 있지만 정지 영상보다는 월등히 나은 데이터의 삽입 양을 보여준다. 그리고 제 3자가 정지영상보다 동영상에서 비밀 데이터를 빼낼수 있는 확률도 현저하게 떨어지게 된다.
향후 연구과제로는 단순 동영상에서만 삽입하고 추출하는 것이 아닌 비밀 데이터의 삽입과 추출을 실시간 환경에서 이루어 질 수 있도록 하고자 한다.
또한 동영상 데이터의 전송을 위한 스테가노그래피 알고리즘은 수행속도가 가장 중요하다. 이러한 속도 문제도 향후 많은 보완이 필요로 되어질 것이다.

5 참고문헌

[1] Johnson, N., Duric, Z., and Jajodia, S. : "Information hiding: Steganography and Watermarking-Attacks and Countermeasures," Kluwer Academic Publishers, (2001)
[2] 정우식, "안전한 스테가노그래픽 알고리즘 설계 및 분석," 박사학위논문 숭실대학교, (2003)
[3] 김현곤, 원동호, 정준원, 지적 재산권 보호를 위한 정보은닉 기술 및 표준화 연구, 한국전산원, (2000)
[4] ITU-T Recommendation H.261, Video Codec For Audiovisual Services at pX64kbt/s, March (1993)
[5] Anderson, R., Petitcolas, F. : "On the Limits of Steganography," IEEE Journal of Selected Areas in Communications (1998)
[6] F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the unseen," IEEE (1998)