What is a Smart Video?

J. J. Chae, J. W. Kim and J. U. Choi
MarkAny Inc. Jung-gu Ssanglim-dong Ssanglim-bldg, Seoul 100-400, Korea
E-mail: chaejj, jwkim, juchoi@markany.com

Abstract

인터넷의 발달과 더불어 멀티미디어에 대한 유통과 불법복제, 그리고 이에따른 저작권보호운동이 활발히 진행되고 있다. 이 논문에서는 이러한 multimedia 저작권 보호를 지원해주는 가장 일반적인 기법중에 하나인 watermarking 기법을 포괄적으로 포함하는 data hiding 기법의 일반적인 특징에 대해 논하고, 이 기법이 갖는 중요한 특성중에 하나인 embedding data 의 종류와 양를 활용하여 multimedia processing 에 적용하는 새로운 사례를 보여주며, 이를 토대로 스스로 생각할 수 있는 지능을 가진 intelligent smart video 의 개념에 대해 토의한다.

1 Introduction

오늘날 정보통신의 발달과 더불어 자유로운 정보유통은 인터넷의 폭팔적인 사용과 더불어 가장 중요한 이슈중에 하나로 되었다. 대부분의 user 들은 보다 간편하게 각종 multimedia 정보를 손쉽게 사용하려 할 것이고, 이로부터 멀티미디어 자원에 대한 건전한 유통보다는 효율적인 자료저장방법, 전달방식, 공유할 수 있는 방향으로 software utility 의 개발등 많은 노력이 이루어졌다.

그러나 multimedia 을 제공하는 contents provider 들은 반대로 이러한 불법적인 contents 유통에 대해 적당한 제재와 규칙의 제정을 요구하게 되었다. 정당한 절차와 비용을 지불한 후 필요로 하는 multimedia contents 을 제공받을 수 있도록 규제의 움직임이 가시화되었고, 국제적인 discussion working group 에서는 SDMI, CPTWG 등과 같은 정보제공 표준화작업을 진행하고 있다. 이러한 과정을 거쳐 대부분의 multimedia 정보들은 유료화될 것으로 예측되어 진다.

이와같은 움직임 속에서 Multimedia source 에 대한 불법 복제는 그 불법 사용자를 추적하고 또한 불법사용을 원천적으로 막으려는 각종 시도들로 이루어지며, 이를 위한 불법복제 및 사용금지에 관련된 기술개발이 눈부시게 이루어지고 있다. 이러한 저작권보호 및 불법방지기술로 가장 보편적으로 이용되는 방법은 현재까지는 digital watermarking 기술이 효율적인 방법으로 알려져 있다.

Watermarking 기술은 이미 많은 연구를 통하여 성과가 현저히 이루어졌다. 그러나 전자인증이나 저작권 보호를 위한 watermarking 기법을 포괄적으로 포함하고 있는 data hiding 기술은, 일정량 이상의 data 를 삽입하여 모든 삽입정보를 정보손실없이 추출하고 이를 보다 체계적으로 활용할 수 있도록 하는 기술로서, hiding 기법에 대한 연구가 그 중요성을 더욱 인정받고 있다.

그러나 watermarking 기법은 일반적으로 아주 적은 양의 정보를 삽입하거나 또는 pseudo-random noise 등과 같은 무가치정보를 삽입하는 방법이다. 반면에 data hiding 기법은 적은량의 data 를 삽입하는 watermarking 기법을 포함하고 이에 부가적으로 제공되는 기능에 추가하여, 특별한 목적을 갖는 data 의 삽입을 통하여 추출과 동시에 수신단에서 직접 그 정보를 활용하여 새로운 목적의 업무를 수행할 수 있게 된다. 새로운 목적의 업무는 그 원하는 응용프로그램에 따라 서로 달리 적용될 수 있는데 이 논문에서는 스스로 지능을 가지는 intelligent multimedia 에 대해서만 기술하고 있다.

지능을 가진 multimedia source 는 media 그 자신이 자기자신의 손실여부를 스스로 측정할 수 있으며, 그 측정된 결과로 판단하여 수신된 media 가 사용자에게 직접 제공하기에는 손실의 정도가 일정 한계를 벗어나는 경우, 손실없이 원래의 media 형태로 스스로 재복원(self-reconstructable)하여 사용자에게 제공해주는 intelligent 또는 smart media 라고 할 수 있다. 이 논문에서는 이러한 기능을 갖는 intelligent/smart video 에 대해 보다 구체적으로 소개하고 방송과 관련된 응용분야와 향 후 발전가능성에 대해 논의하고자 한다.

다음 장에서는 data hiding 기법에 대해서 간략하게 기술하고, data hiding 과 watermarking 과의 차이점을 살펴보며, 제 3 장에서는 실제 data hiding 에 적용되는 삽입기법들과 이를 video 에 적용하는 방법에 대해서 논하게 된다. 그리고 제 4 장에서는 이러한 삽입기법등을 토대로 intelligent 기능을 가진 smart video 를 고찰하며 토의와 함께 결론을 제 5 장에서 내린다.

2 Data Hiding Techniques

2.1 Data hiding 과 Watermarking

Digital watermarking 기법은 multimedia source 에 특정한 정보를 삽입하고, 비록 정보가 삽입된 multimedia 라 할지라도 원래의 media 와 비교하여 별도의 정보왜곡이 생기지 않는 상태로 유지하여, 삽입된 특정한 정보를 통하여 불법사용을 원천적으로 차단시켜주는 기법을 말한다. 즉 image (original host source)에 signature (embedding data) 정보를 삽입하게 되면, 인간의 눈에는 식별할 수 없는 시각적인 distortion 이 image 에 생기게 되지만, 인간의 능력으로 distortion 을 구별하기란 쉽지 않고, 우리가 원하는 정보를 그대로 다시 추출할 수 있어, 사용되어진 image(media)는 저작권보호를 위하여 특정정보를 삽입한 watermarked image 임을 알 수 있게 된다.

반면에 data hiding 기법은 digital watermarking 기법과 유사한 알고리즘을 갖고 있지만, 대신에 특정한 목적의 자료를 상대적으로 대단히 많이 삽입하고, 이를 수신단에서 추출하여 정보로서 직접 사용할 수 있도록 한다는 점에서 아주 큰 차이가 있다. 보통의 경우, watermarking 에서 사용되는 signature 는 1bit 단위의 binary image 라는가 또는 pseudo-random noise 와 같은 불특정 정보를 사용하지만, data hiding 기법에서 사용되는 signature 는 그 자체로 특정한 목적을 가질 수 있는 중요한 자료인 documents, image/audio, 또는 video 등을 사용하여 직접 multimedia source 에 삽입하는 방법을 사용한다. 이 방법은 넓은 범위에서는 watermarking 을 내포한다.

이렇게 삽입된 signature 정보를 수신단에서 활용하기 위해서는 원본없이 삽입된 정보를 추출할 수 있어야 한다. Digital watermarking 기법에서도 원본없이 삽입된 signature 정보를 추출하기란 쉽지 않은 일이지만, 대용량의 data 를 삽입하는 data hiding 기법에서는 원본없이 signature 을 추출하는 기법은 필수적이라 하겠다. 만약에 수신단에서 원래의 media source 를 필요로 한다면, 이는 별도의 transmission channel 이 필요하게 된다는 의미로 경쟁력없는 watermarking 기법이 된다.

2.2 Type of Embedding data

이미 앞에서 언급이 일부 된 바와 같이 data hiding 에서는 삽입되는 signature data 의 종류에 따라 매우 독특한 업무를 수행할 수 있다. Copyright protection 의 경우 직접 image 를 signature data 로 삽입하게 되면, 추출된 image 를 가시적으로 분석하여 즉시 변조여부 및 불법사용을 평가할 수 있다. 그래서 보통의 경우 logo image 등을 사용하여 저작권보호에 적극 이용된다.

뿐만 아니라, 특별한 control signal 을 삽입함으로써 수신단에서 그 control signal 을 그대로 목적된 system 에 적용함으로써, 아주 중요한 control 기능으로 활용할 수 있다. 방송의 경우, 특정 control signal 을 삽입함으로써, 지방방송국 또는 중계소를 무인으로 운영할 수도 있게 해줄 수 있다. 이러한 control signal 은 방송용 video 을 편집할 때에도 아주 유용하게 사용될 수 있다.

또한 digital library 에 적용될 특정 정보들도 data base 을 검색할 때 아주 효율적으로 검색을 지원해두도록 도와주고 있으며, 이러한 기능들을 현재 MPEG-7 에서 적극 사용을 검토하고 있다. 예로서 Image/video retrieval, 또는 indexing 과 같은 분야에서 사용될 수 있다. 이외에도 이 논문에서 언급된 smart video 와 같은 분야에서도 좋은 응용분야가 된다. 이 내용은 제 4 장에서 자세하게 기술된다.

3 Application of Video data hiding

3.1 Video watermarking

대부분의 video 와 관련된 연구는 주로 불법 복제방지 및 저작권보호에 관심을 갖고 연구를 진행해 왔다. 그러나 몇몇의 연구들은 data hiding 의 관점에서 연구를 해왔지만, 삽입되는 정보량의 측면에서는 매우 적은 양의 data 이다.

Data hiding 의 기법을 사용하는 video watermarking 기법들 중에 대표적인 연구는 Swanson 의 연구기법으로 video 안에 MPEG 으로 압축된 형태의 또 다른 video 을 삽입하는 방법을 제안하였다[5][6]. 그들의 알고리즘에 의하면 8x8 블럭에 2bits 의 정보량을 삽입하게 된다. 그러나 이 연구에서의 가장 큰 단점은 수신단에서 에러가 발생된 경우로, 이때 watermarked video 로부터 추출하는 과정에 대한 소개가 자세히 되어 있지 않았다. 이 경우 삽입된 signature 정보는 복원이 불가능해진다 왜냐하면, 삽입된 정보의 형태가 MPEG 으로 압축을 한 data 이므로 error 에 대해 매우 민감해지게 된다.

보통의 video watermarking 연구들은 pseudo-random noise 을 signature data 로 사용하여 삽입을 한다. 이 경우 삽입되는 정보량은 host media data 에 대비해 0.5 – 1% 정도이다. 그러나 여기 소개되는 알고리즘은 최대 25% 정도의 정보량을 삽입할 수 있으며, 예로서 약 7%정도의 삽입 정보량을 보여준다[1][4].

[Figure 1]은 image 에 또 다른 image 을 삽입하는 algorithm 의 block diagram 을 보여준다[1]. 이 알고리즘은 기본적으로 image 을 근간으로 video watermarking 을 하는 것으로 각각의 video frame 를 하나의 image 화 하여 삽입할 수 있는 방법이다. 보다 세부적인 삽입방법은 참고논문을 참고하고, 여기에서는 단지 이러한 한 가지 방법이 있음을 보여준다.

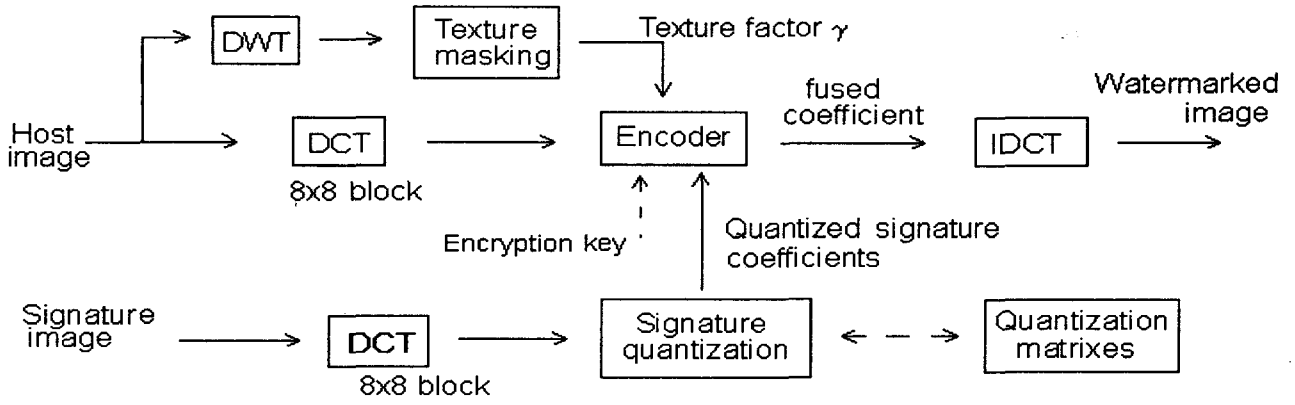


Figure 1 Data hiding 의 예: Image watermarking 기법중에서 삽입 알고리즘의 block diagram.

3.2 Embedding Video in Video

Video watermarking 에 대한 embedding 기법은 signature data 을 어떻게 video 에 삽입하느냐의 문제로, 가장 손쉬운 방법은 signature data 을 video frame 에 그대로 삽입하는 방법으로, image watermarking 기법을 그대로 video frame 에 확대한 방법이다. 그러나 이 방법은 MPEG codec 을 거치는 동안에 많은 정보손실이 발생하게 되고, 보다 robust 알고리즘으로 사용하기 위해서는 발생하는 error 을 복원해주는 과정이 추가적으로 필요하다.

또 다른 방법은 삽입하는 정보를 MPEG codec 내부에서 효율적으로 삽입하는 방법으로, 매우 다양한 삽입방법을 강구할 수 있다. 그러나 MPEG codec 자체가 매우 복잡해질 가능성이 커지며 실시간 처리를 위해서는 비싼 계산능력이 필요하게 된다. 그러나 매우 robust 한 알고리즘을 개발할 수 있는 여지는 더욱 커진다.

여기 실험에서 사용된 삽입기법은 [Figure 2]에 자세히 나타나는 바와 같이 video frame 을 근간으로 또 다른 video 을 직접 삽입하는 block diagram 을 나타낸다. 수신단에서는 원래 video 을 수신하고 나면 이로부터 새로운 video 을 획득할 수 있게 된다. 이와 더불어 signature data 로 특별한 control code 을 사용하게 되면, 추출된 code 을 이용하여 원하는 목적의 제어를 수신된 video 로부터 실행시킬 수 있다.

Video watermarking 에서 사용되는 attacking 기법은 보통 MPEG-2 codec 을 이용한 MPEG compression 이다. Compression 의 정도는 주어진 parameter 을 이용하여 압축정도의 변화를 주었고, 가능한 error 가 발생되지 않는 경우와 일부 error 가 생기더라도, 활용할 수 있는 정도의 compression 을 정하여 attacking 의 정도를 정할 수 있다. Watermarked data 는 NTSC 방식에서 주어진 기본적인 parameter 을 기준으로 이로부터 transmission bandwidth 을 변화하는 방향으로 실험하였다.

실험결과의 예는 [Figure 3]에 보여지고 있는데, 원래의 video 와 삽입에 사용된 signature image 가 (a)와 (b)에 보여주고 있다. 실험에 사용되었던 video 는 CIF format 으로 100kbps bandwidth 이하의 compression 율로 attacking 을 하였다. 그 결과로 추출된 host frame 과 삽입된 image 을 (c)와 (d)에 보여준다.

4 Smart Video

4.1 Intelligent multimedia

Data hiding 의 결과로 수신단에서 획득한 signature information 은 매우 유용하게 사용될 수 있다고 이미 설명하였다. 이러한 목적에서 video 에 또 다른 video 를 삽입한 후, 삽입된 video 를 추출하면 새로운 video 을 활용할 수 있음을 이미 설명하였다.

이러한 방법으로 새로운 video 가 수신단에서 추출되었을 때, 그 video 가 스스로 자신을 control 할 수 있다면, 이는 video 가 아주 간단하지만 어떤 지능을 가졌다고 말할 수 있다. 여기에서는 이러한 기능을 갖는 여러 종류의 multimedia 에 대해서 논하려고 한다.

일 예로써, 추출된 signature image 를 통하여 수신된 watermarked image 의 quality 를 측정할 수 있고, 또 측정된 값이 우리가 기대하는 일정 값 이하가 된다고 한다면, 수신된 watermarked image 가 그 image quality 를 자기 스스로 확인하여 원래의 image quality 로 복구해줄 수 있다. 물론 이것을 위해서는 먼저 image quality 를 정하는 quality measure 을 결정하여야 하며, 이러한 measure 을 사용하여 손쉽게 quality 를 구할 수 있어야 한다. 그래서 만약 이러한 quality measure 가 존재한다면, 간단한 data hiding 방법을 통하여 수신단에서 삽입된 image quality 정보를 추출하여 원래의 형태로 복원이 이루어질 것이다.

이 논문에서 사용된 quality measure 는 signal 을 해석하는데 가장 일반적인 방법으로 널리 알려진 PSNR 을 사용하기로 한다. 어떤 media 에 대한 PSNR 은 원래

의 media와 비교할 대상의 media가 동시에 필요하고, 그 비교결과로서 media quality가 존재한다. 그러나, 수신단에서는 원래의 media 가 존재하지 않는 경우에는 PSNR을 계산할 수 없게 되므로 이를 측정하기 위한 값들이 필요해진다. 그래서 media 자신의 일부분 또는 quality measure 을 위한 중요한 요소들을 원래 host media에 삽입하게 된다. 물론 삽입되는 signature 정보는 원래 media보다 보통 적은 값을 갖지만, 가급적이면 원래 media을 모두 나타낼 수 있는 정보들로 구성이 되면 가장 좋다. 아직 이 부분은 추가적으로 연구가 필요한 실정이다.

이것은 중요한 data hiding 의 또 다른 문제로서, image의 경우 자기 자신을 표현할 수 있는 방법으로 위에서 설명한 삽입기법을 통하면 최대 25%의 정보량까지 삽입할 수 있으므로 25%범위 내에서 표현할 수 있어야 한다. 그렇지만 삽입된 25%의 정보량으로 원래 image quality을 결정하기란 쉬운 일이 아니다. Image의 가장 중요한 특징만을 골라 삽입함으로써 우리가 원하는 intelligence image의 기능을 조금이라도 구현하려고 한다. 다른 multimedia의 경우에도 마찬가지의 rule을 적용하여 스스로 반응하는 intelligent media을 생성할 수 있다.

4.2 Smart video

위에서 언급한 intelligent image의 경우, 최대 삽입할 수 있는 정보량은 25%밖에 되지 않는다. 이 경우 4개의 image에 분리하여 1개의 image 정보를 삽입할 수 있다면, 최소의 경우 4자의 image에서 1개의 image는 완벽하게 복원시킬 수 있게 될 것이다. 이런 가정이라면, 1개의 중요한 video frame (예로서, I picture)을 일정한 video frame들에 삽입할 수 있을 것이고, 전송상의 손실에 의해서 복원될 수 없게 되더라도 삽입된 frame은 추출된 후, 복원될 수 있을 것이다.

이것은 MPEG 에서 중요하게 여겨지는 stability 기능과도 연관관계가 된다. 즉 한 개의 중요한 I picture는 복원 과정에서 잘못된 error을 계속해서 뒤로 전달하게 되는 중대한 오류를 보여준다. 이 경우, I picture을 복원할 수 있다면, 복원과정에서 나타나는 잘못 전달되는 error는 나타나지 않게 된다.

이러한 기능을 가진 video는 video 스스로가 지능을 가진 것처럼 다시 원래의 video frame으로 복원할 수 있기 때문에 smart video 또는 intelligence video라는 개념으로 정의를 내린다. 이때 가장 중요한 것은 이미 앞에서도 언급한 바와 같이 어떤 내용을 삽입하는냐 하는 것이다. 이것을 수신단에서 그대로 추출하여 사용하기 때문에 quality measure 에 바로 사용 가능한 정보여야 한다. 이러한 방식을 사용하면, 손실이 잘 생기는 video frame을 중심으로 삽입하고, 복원시 그 손실을 보정해 주는 방법으로 video compression에 적용할 수 있게 된다.

5 Conclusions

지금까지 data hiding 기반 아래에서 추출되는 signature media를 이용하여 video 그 자신의 quality를 복원시킬 수 있는 방법과 이러한 현상에 대한 새로운 개념인 smart video에 대하여 기술하였다. 물론 이와 같은 현상을 실현하기 위해서는 아직도 더 많은 연구가 필요한 실정이다. 그래서 이 논문에서는 단지 새로운 개념을 정의하고 이에 대한 토의를 한번 시도해 보려는 노력을 했다.

앞에서도 잠깐 언급이 되었지만, 새로운 개념의 multimedia quality measure 의 탄생도 향 후 연구할 중요한 소재가 될 것이다. 이와 더불어 스스로 생각하고 행동할 수 있는 media의 탄생은 앞으로 더욱 지능적이고 끝없이 multimedia의 세상을 바꾸어 놓을 것으로 기대한다.

References

[1] J. J. Chae and B. S. Manjunath, "Data Hiding in Video," *IEEE, Internation Conference of Image Processing '99*, Keio, Japan, October, 1999.

[2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Second edition, Springer-Verlag, New York, 1991.

[3] I. J. Cox, J. Killian, T. Leighton, and T. Shamoon, "A secure Robust watermark for Multimedia," *IEEE Trans. Image Processing*, Vol. 6. no. 12, pp. 1673-1687, December 1997.

[4] J. J. Chae and B. S. Manjunath, "A Technique for Image Data Hiding and Reconstruction without Host Image," *Proceeding of SPIE EI '99, Security and Watermarking of Multimedia Contents*, Vol. 3657, pp. 386-396, San Jose, California, January, 1999.

[5] M. D. Swanson, B. Zhu and A. H. Tewfik, "Data Hiding for Video-in-Video," *IEEE International Conference of Image Conference*, Vol. II, pp. 676-679, Santa Barbara, October, 1997.

[6] M. D. Swanson, B. Zhu and A. H. Tewfik, "Multiresolution Video Watermarking using Perceptual Models and Scene Segmentation," *IEEE International Conference of Image Conference*, Vol. II, pp. 558-561, Santa Barbara, October, 1997.

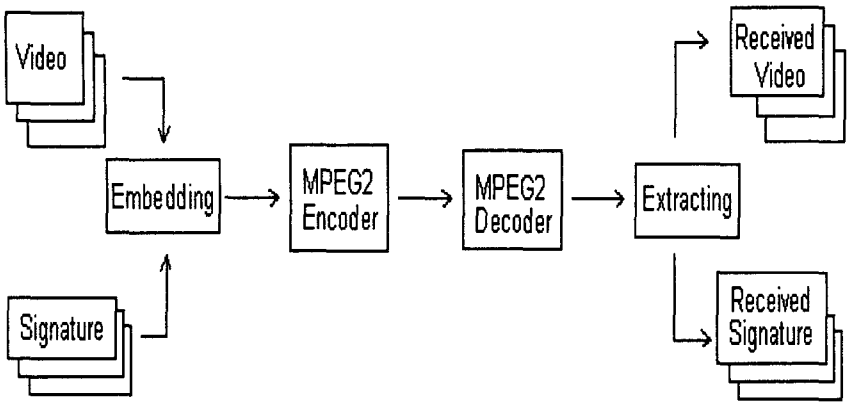
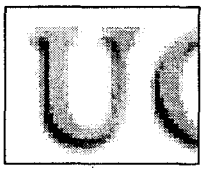
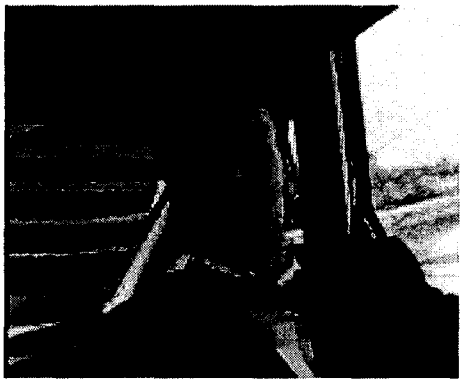


Figure 2 Video in Video data hiding: signature data 에 또 다른 video 을 삽입한 후, MPEG-2 attacking 의 결과로부터 삽입 video 을 추출해 내는 block diagram.

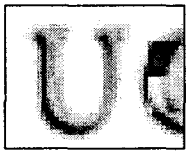
(a) Origianl video frame (B frame)



(b) Signature image



(c) Recovered host video frame



(d) Recovered signature image from (c)

Figure 3 Video data hiding 의 예: 원래의 cif format 의 host video frame(a)과 삽입될 signature image(b). 모든 video frame 에 반복적으로 삽입한 후 전체의 video frame 에서 추출하는 알고리즘으로 추출된 host video frame(c)와 추출된 signature image(d). 이때 사용된 MPEG-2 compression 에서는 100kbps 의 bandwidth 와 30 frame/second 으로 attacking 하였다.