제22회 한국정보처리학회 추계학술발표대회 논문집 제11권 제2호 (2004. 11)

클라이언트의 수집 정보 및 MPEG-4 객체를 이용한 정보 차단 방안

안원영*, 박정호**
*선문대학교 컴퓨터정보학과
**선문대학교 컴퓨터정보학과
e-mail:anwy@skcnc.co.kr

The methods intercepting injurious informations by using the information from clients and MPEG-4 object

Won-Young An*, Jung-Ho Park**
*Division of Computer and Information Science, SunMoon University
**Division of Computer and Information Science, SunMoon University

요 약

오늘날 멀티미디어 기술 발달과 더불어 멀티미디어의 활용 범위가 점차 넓어지고 있으며, 인터넷과 모바일 서비스를 이용하여 실시간으로 영상 및 정지영상을 재생할 수 있다. 그러나 이러한 멀티미디어 발달과 함께 유해정보 규제 방안이 사회적 문제로 대두되고 있다. 본 논문에서는 기존 방식과 다른 유해사이트 정보 수집의 한계성을 극복하는 방법으로 클라이언트에서 수집된 정보를 이용하여 유해 정보를 차단하는 알고리즘을 제안한다. 또한 MPEG-4 객체 기반을 이용한 방법으로써 영상을 객체 단위로 구분하고 부호화 정보를 이용하여 유해정보를 차단하는 알고리즘을 제안한다.

1. 서론

영상 데이터와 같은 방대한 정보를 효과적으로 저장하여 전송하는 압축기술 발달로 인터넷을 이용한 멀티미디어 컨텐츠의 활용 가치가 높아지고 있다. 멀티미디어 서비스를 받는 클라이언트의 다양한 단말기(데스크탑PC, PDA, 핸드폰)로 인해 각종 유해정보를 차단해야 하는 범위가 점차 넓어지고 있으며, 이로 인해 청소년 성장기에 있어서 사회적 문제로 발전될 가능성이 있다. 기존 유해정보 차단 방식은 유해사이트의 주소를 저장하여 클라이언트의 접속을 차단하는 방식이었다. 그러나 하루에도 수많은 사이트가 생성되고 소멸되는 시점에서 유해사이트의 주소를 알아내기에는 한계점이 있다. 또한 불특정 다수에게 보내지는 이메일 서비스의 유해정보를 차단하지 못하고 있다.

본 논문은 다음과 같이 정리할 수 있다. 첫째, 서버 환경에서의 유해정보 사이트의 주소를 수집하는 것이 아닌 클라이언트 환경에서의 포괄적 수집 방법을 제안한다. 둘째, 영상을 객체 단위로 구분하여 화소의 값을 비교하여 차단하는 방법이다[1].

본 논문의 구성은 2장에서는 클라이언트 수집정보의 활용 방안 기법에 대해 알아보고 3장은 MPEG-4 객체를 이용한 정보차단 방안과 실험 결과를 알아본다. 그리고 4장에서는 결론을 맺는다.

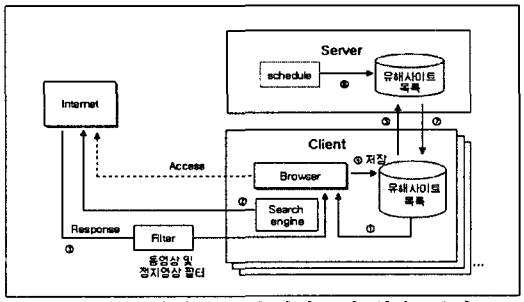
2. 클라이언트 수집정보의 활용 방안 기법

2.1 기존 방식의 서버 정보 활용

급속도로 확장되는 인터넷 유해사이트를 차단하기에는 여러 가지 어려움이 존재하기 때문에 다양한 차단방식이 제시되고 있다. 그 중 대표적인 방식은 서버 환경에서의 검색 엔진을 이용하여 불특정 사이트에 접속하여 유해정보를 검색하고 유해사이트의 주소를 수집하는 방식이다. 유해여부 판단시 서버측에 유해사이트 주소를 저장하고 이를 다시 주기적으로 클라이언트에게 정보를 제공한다. 유해사이트를 차단하기 위해서는 목록에 유해정보의 주소가 저장되어 있어야 한다. 그러나 새롭게 생성되는 유해사이트의 정보를 꾸준히 업데이트 하기에는 한계점이 있다.

2.2 본 논문의 제안 기법

본 논문에서 제안하는 기법은 서버 정보를 활용하는 방식과는 반대로, 검색엔진을 클라이언트 환경에 탑재하여 유해사이트 주소를 수집하고 클라이언트에서 수집된 정보를 서버에게 재전송하는 방식이다.



(그림 1) 클라이언트 수집정보의 활용 구성도

본 논문에서 제안하는 클라이언트 수집정보의 활용 방안 기법은 그림1을 이용하여 설명하기로 한다. 클라이언트는 브라우저(Browser)를 이용하여 인터넷에 접속을 시도할 때 먼저 로컬에 저장되어 있는 데이터베이스 목록에서 접속하려는 인터넷 주소가 존재하는지를 검색하게 된다. 데이터베이스 목록에 존재하는 유해사이트 주소는 클라이언트의 검색엔진에 의해 수집된 자료이며 각 클라이언트가 공유한 자료이다.

클라이언트가 접속하려는 인터넷 주소가 목록에 존재한다면 클라이언트 자체에서 해당 사이트 접속을 차단하게 된다. 그러므로 클라이언트가 접속하려는 사이트에 HTTP의 응답을 받을 수 없게 된다. 그러나 데이터베이스에 유해정보 목록이 존재하지 않는다면 클라이언트에 탑재된 검색엔진이 먼저 인터넷 주소에 접속한다. 검색엔진은 클라이언트가 접속하려는 인터넷 주소에 미리 접속하여 서비스 받을 페이지 및 링크페이지에 유해정보가 존재하는지를 판단한다. 이때 동영상 및 정지영상 데이터는 검색하지 않고 클라이언트가 서비스를 받을 때 필터기에 의해 검색된다.

클라이언트에 탑재된 검색엔진에 의해 유해정보로 판단되면 로컬 데이터베이스 목록에 유해사이트 주소를 저장하고 서버에 재전송한다. 이렇게 클라이언트가 유해사이트 주소를 수집함으로써 서버는 각 클라이언트가 보내온 유해사이트 목록을 병합하여 실시간으로 전송받아 저장한다. 서버에 저장된 유해사이트 목록은 일정한 스케줄에 의해 주기적으로 다시 여러 클라이언트에게 유해사이트 목록을 전송한다. 이때 서버와 클라이언트는 유해사이트 목록을 비교하여 서로 중복된 목록은 전송받지 않는다.

필터기는 클라이언트가 웹에 접속을 시도하여 서비스를 제공하는 서버측으로부터 정보를 받을 때 웹 페이지에서 실시간으로 동영상 및 정지영상에 대한 데이터가 존재하는지를 검색하고 유해정보 인지를 판단하여 해당 객체를 필터링 한다.

또한 학교 및 회사와 같이 지리적 위치가 한정되어 있는 경우에는 유해차단 서버를 구축하여 외부에서 들어오는 데이터와 내부에서 나가는 데이터의 유해여부를 검색할 수 있다. 유해차단 서버가 클라이언트와 같은 네트워크에 존재하기 때문에 클라이언트가 수집한 유해사이트 주소를 로컬에 저장하지 않고 곧바로 서버에 전송하여 저장하는 방식이다.

3. MPEG-4 객체를 이용한 정보 차단 방안

3.1 기존 유해정보의 차단 방안

서버에 탑재된 검색엔진은 유해정보 수집시 정상적인 사이트를 유해사이트 목록에 저장하는 오류를 범할 수 있으며, 특정 언어권을 제외하고는 유해사이트를 검색 하지 못하는 문제점이 있다. 또한 동영상 및 정지영상에 대한 음란의 범위를 세부적으로 판단하지 못하는 한계점을 가지고 있다.

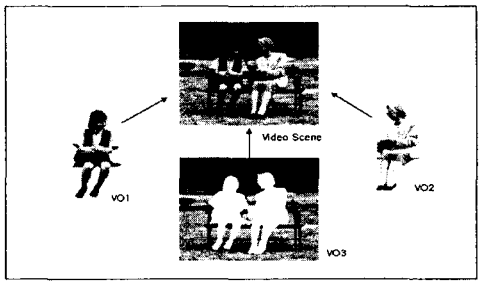
3.2 MPEG-4의 비디오 객체

본 논문에서는 MPEG-4의 부호화 방법 중 형상부호화 과정을 통해 사람형상의 객체를 얻어 유해정보의 범위를 측정하는 방법이다. 즉, 클라이언트가 동영상 및 정지영상의 서비스를 받기 전에 필터기에 의해 임의형상(Arbitrary Shape)의 객체를 얻어 영상의 화소 값을 비교하여 검색하는 방법이다.

MPEG-4는 압축, 객체기반의 대화형기능, 보편적 접속의 특징을 가지고 있으며, 영상의 화면내를 객체단위로 부호화 하고 표현함으로써 객체기반의 처리가 가능하다[2]. 영상을 객체표현이나 개체 조작, 비트열 편집, 확장성 등의 대화형 기능이 가능하다. 화면내는 매크로블록 단위로 처리하며, 4:2:0의 영상포맷을 가진 휘도신호(Y)와 색차신호(Cb ,Cr)의 6개 블록으로 구성된다.

영상 화면에서의 독립적인 여러 객체중 의미가 존재하는 하나의 객체를 VO(Video Object)라고 하며, 객체의 특정 시간에 해당하는 형상을 VOP(Video Object Plane)라 한다. MPEG-1과 MPEG-2는 프래임의 집합으로 구성되어 있다면, MPEG-4는 객체들의 집합이다. 또한 시각적인면에서는 사용자가 조작

하고 접근할 수 있도록 유동적인 비디오 객체를 정의하고 있다[3, 4].

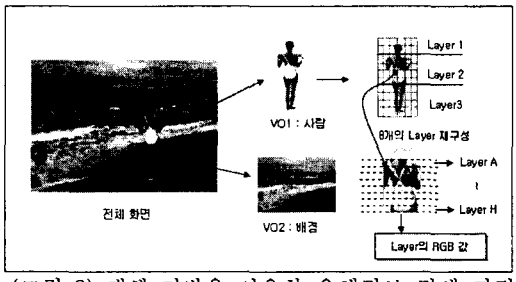


(그림 2) 비디오 객체의 구성

그림2의 비디오 화면은 각각 사람형상을 VO1과 VO2로 객체화 시켰고 나머지 배경화면은 VO3로 객체화 시켰다. 각 객체는 프레임에서 좀더 유동적으로 사용할 수가 있으며, 사람형상의 객체를 다른 프레임에 병합하거나 다른 배경객체로 변경할 수 있다. [5, 6].

3.3 MPEG-4 객체를 이용한 정보 차단 방안

본 논문에서는 MPEG-4 비디오 압축과정에서의 형상부호화를 이용하여 임의형상의 객체를 얻을 수 있는 방법에서 착안했다. MPEG-4 형상부호화는 16x16 화소의 매크로블록 단위로 이루어지고 화면내에 영상들을 여러 객체로 구분할 수 있다[7, 8]. 객체를 생성할 때 화소값의 부호화를 하게 되는데 임의형상을 갖는 영상 신호에서는 부호화 영역을 화면내의 좌표값을 설정하여 내부 영상 신호를 부호화 한다[9, 10].



(그림 3) 객체 기반을 이용한 유해정보 검색 과정

그림3은 객체 기반을 이용한 유해정보 검색 과정을 나타낸 것이다. 한화면내 임의형상을 VO1과 VO2로 객체화하고 사람형상(VO1)만을 이용하여 노출의 범위를 찾아 차단하는 방식이다. 사람형상의 객체에 대한 피부색 값을 얻기 위하여 VO1을 3개의 레이어(Layer)로 구분한다. 사람의 신체 일부중 레이어1은 머리에 해당되고 레이어2는 목 아래부터 허벅지 위까지이며, 레이어3은 허벅지 아래까지로 구분한다. 3개의 레이어로 구분하는 이유는 영상 화소의 픽셀값을 이용하기 때문이다. 즉 각각의 레이어 마다 사람의 피부를 표현하는 화소값의 범위가 다르다. 사람의 신체는 VO1의 각 레이어에 따라 피부색의 조금씩 차이가 있으나 검색에 있어서는 큰 영향은 미치지 않는다. 그러나 변환된 영상 및 흑백 영상일 경우에는 피부색 기준 범위를 벗어나므로 유해정보를 판단하지 못한다.

객체의 유해정보 판단은 화소 값을 기준으로 레이어2를 이용하여 음란의 범위를 측정한다. 음란의 범위가 어느정도인지를 파악하기 위해서는 레이어2를 세부적으로 8개의 레이어로 재구성하여 화소의 (피부색) 값을 읽는다. 8개의 레이어는 레이어A~레이어H로 표기하였다.

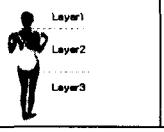
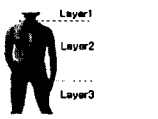
음란의 범위를 화소값을 이용하여 측정하기 위해서는 첫 번째로 객체에 피부색이 존재하는지를 검색하고 두 번째로는 어느 범위까지의 피부색을 검출할 것인지를 결정한다. 화소의 값은 왼쪽에서 오른쪽의 순서로 매크로블록 단위로 값을 읽어 2차원배열(X, Y)로 메모리에 저장한다. 황인종인 경우에 피부색을 RGB값으로 표현하면 R은 176~240이고 G는 126~235이고 B는 101~207까지의 범위로 피부색을 표현할 수 있다. 그러나 영상 촬영시 빛의 영향으로 화면내에 음영이 생성 될 수 있으므로 RGB의 화소 범위값이 유동적으로 넓어질 수 있다. 이에 대해 레이어2의 픽셀에 해당하는 RGB값을 읽어 전체 평균값을 구하여 ±50을 적용하면 RGB값의 범위를 작성할 수 있다. 평균 RGB값을 이용하여 레이어2의 피부색 화소값을 읽어 들인다.

음란의 범위는 객체의 레이어2의 화소값이 연속적이면서 특정 좌표(X, Y)에 특정 색상(사람의 가슴 및 음부의 색상값)이 검출되는지를 판단한다. 레이어2를 8개의 레이어로 재구성하는 이유는 특정 색상을 검색하기 위함이다. 그러나 사람형상의 객체가 전신이 모두 출력되는 경우와 상반신 또는 하반신으로 출력되는 경우가 있다. 이러한 상황에 따라 영상 촬영시에 객체의 형상이 앞, 뒤, 옆 등으로 위치가 변할 수 있기때문에 특정 좌표값의 위치도 유동적으로 다르게 적용하여 화소의 값을 비교한다. 이와 같은 방법으로 영상 및 정지영상에 대한 유해성 여부를 판단한다.

3.4 실험 결과

본 논문의 실험은 객체에 대한 피부색 분포도를 조사하기 위하여 별도의 프로그램을 이용하였다. 본 실험에 사용된 비디오 객체는 수영복을 입은 남·여의 정지영상을 이용하여 음란의 범위를 측정하였다. 표1에서 사용된 비디오 객체(①)과 비디오 객체(②)는 3.3절에서 설명한 방법과 같이 3개의 레이어(Layer1~Layer3)로 구분하고 다시 레이어2를 8개의 레이어(LayerA~LayerH)로 구분하여 음란의 범위를 측정하였다.

<표 1> 실험에 사용된 비디오 객체

	비디오 객체①	비디오 객체②
피부색	황인종	황인종
객체의 위치	뒷부분	앞부분
성별	여	남
노출 범위	일부분	대부분
정지영상		

비디오 객체(①)은 레이어2에서 48%의 사람 피부색이 검출되었고, 레이어2를 세분화한 8개의 레이어중 레이어A부터 레이어D사이에 대부분의 피부색이 검출되었기에 이는 음란의 수위가 높은 정보일 가능성이 있다. 하지만 레이어B와 레이어C에 특정 좌표값에 해당하는 화소의 값이 검출되지 않았기에 음란의 수위가 높다고 판단 될 수 없다. 여기서 특정 좌표값이란 사람 가슴부분에 해당하는 값을 말하며, RGB값의 범위는 짙은 살색부터 밤색까지의 영역으로 나타낸다. 또한 레이어E부터 레이어H사이의 영역은 모두 흰색값이 연속적으로 검출되었기에 하단부분에는 노출 정보가 없다고 판단된다.

비디오 객체(②)는 레이어2에서 70%의 사람 피부색이 검출되었다. 레이어A부터 레이어F까지 연속적이면서 전체가 피부색이 검출되었으며, 특정 좌표의 위치와 화소의 값이 검출이 되었다. 이는 음란의 범위가 높은 수위에 해당하며 사람의 가슴이 전체가 노출되었다고 판단되므로 유해정보이다. 그러나 본 실험은 화소의 값과 좌표의 위치만으로 남·여의 성을 구분하지 못하는 한계점이 있어 이에 대한 연구가 필요하다.

기존 유해차단 프로그램은 동영상 및 정지영상에 대해 음란의 범위를 세부적으로 판단할 수 없었으나 본 실험은 피부색의 분포도와 좌표값을 이용하여 노출 범위를 정확히 판단할 수 있었다.

4. 결론

본 논문에서 유해정보를 차단하는 방안으로 클라이언트 수집정보의 활용 방안 기법과 MPEG-4 객체를 이용한 정보 차단 방안을 제안했다. 본 논문의 실험 결과로 기존 인터넷 주소 기반의 차단 방식의 문제점을 보완할 수 있었으며, MPEG-4의 객체기반을 이용하여 화소의 값을 비교하고 유해성 여부를 판단하는 방법으로 확장성을 높였다. 서버에서 전송되는 동영상 및 정지영상의 데이터가 파일로 첨부되어 있는 경우와 불특정 다수에게 보내지는 스팸 메일에 포함되어 있는 경우에도 유해성 여부를 판단할 수 있다. 그러나 별도의 디코더 프로그램이 필요하며, 한 화면내의 영상을 객체화하기 전에 임의형상 객체를 찾아내는 검색 기술의 연구가 필요하다.

참고문헌

[1] 미키 스케이치 저(고성제, 김종옥 역) "MPEG-4의 세계", 브레인코리아, 1999.

[2] T. Ebrahimi and C. Horne, "MPEG-4 natural Video coding : An overview". Image Comm., Vol. 15. No. 4-5, pp. 365-385, Jan. 2000.

[3] 김재균, "영상통신시스템", 영지문화사, 2000.

[4] N.Brady, MPEG-4 standardized methods for the compression of arbitrarily shaped video object, IEEE Trans. Circuits Syst. Video Technol., pp. 1170-1189, 1999.

[5] Lain E.G. Richardson, "Video Codec Design", John Wiley & Sons, 2002.

[6] Lain E.G. Richardson, "H.264 and MPEG-4", John Wiley & Sons, 2003.

[7] 이호석, 김준기, "알기 쉬운 MPEG-2", 홍릉과학출판사, 2002.

[8] www.mpeg.org [MPEG resources]

[9] Hoang, Dzung Tien/Vitter, Jeffrey Scott "Efficient Algorithms for Mpeg Video Compression", John Wiley & Sons, 2002.

[10] Pereira, Fernando/Ebrahimi, Touradj, "MPEG-Book", Prentice Hall, 2002.