ISSN(Print): 2287-5891

http://dx.doi.org/10.3745/KTCCS.2012.1.1.047

Digital Watermarking for Robustness of Low Bit Rate Video Contents on the Mobile

Jung-Hee Seo† · Hung-Bog Park††

ABSTRACT

Video contents in the mobile environment are processed with the low bit-rate relative to normal video contents due to the consideration of network traffic; hence, it is necessary to protect the copyright of the low bit-rate video contents. The algorithm for watermarking appropriate for the mobile environment should be developed because the performance of the mobile devices is much lower than that of personal computers. This paper suggested the invisible spread spectrum watermarking method to the low bit-rate video contents, considering the low performance of the mobile device in the M-Commerce environment; it also enables to track down illegal users of the video contents to protect the copyright. The robustness of the contents with watermark is expressed with the correlation of extraction algorithm from watermark removed or distorted contents. The results of our experiment showed that we could extract the innate frequencies of M-Sequence when we extracted M-Sequence after compressing the contents with watermark easily. Therefore, illegal users of the contents can be tracked down because watermark can be extracted from the low bit-rate video contents.

Keywords : M-Commerce, Video Content, Digital Watermark, Robustness

1. 서 론

새로운 소형의 포켓용 기기들의 등장은 기존과 다른 디지털 미디어의 소비 유형인 M-Commerce(모바일 전자상거래)의 특징을 가진다. 이런 소형 기기들은 메모리와 처리속도, 대역폭의 탁월한 처리 능력과 통신 기능을 갖춘 성능으로 모바일 장치를 이용한 디지털 미디어의 사용을 확산시키는 추세이다. 즉, MP3, 스트림 비디오, e-Book, 인터넷 검색, 지도의 인기 증가로 모바일 서비스의 사용이 활성화되고, 다양한 장치에서의 새로운 디지털 워터마킹에 대한 처리를 요구한다. 특히 모바일 분야에서 디지털 워터마크는 새로운 시도로의 연구가 요구되고 있다.

모바일 폰은 과거 음성 통화 위주로 서비스가 제공되었다. 그러나 오늘날 영화나 TV를 시청하거나 다양한 콘텐츠를 서비스하기 위해서 모바일 기기 자체의 성능이 미니 컴퓨터의 수준으로 사용되고 있다고는 할 수 있으나 기존의 컴퓨터와는 하드웨어적으로 많은 차이점을 가지고 있다. 이런 차이점은 컴퓨터에서 인터넷을 사용할 경우 대역폭이 초당 수 Mbyte인 반면 모바일 폰은 수 Kbyte의 대역폭을 가진다. 그리고 메모리와 처리 속도 또한 컴퓨터에 비해 낮다.

모바일 장치가 컴퓨터에 비해 많은 제약을 가지고 있음에도 불구하고 사용자들에게 컴퓨터에서 사용하는 것과 같은 어플리케이션을 제공하기 위해서는 모바일 폰에 알맞은 다양한 신호 처리 알고리즘이 개발되어야 한다. 그리고 다양한 디지털 콘텐츠는 컴퓨터 환경에서 모바일 환경으로의 서비스 유형이 변화하고 있으므로 디지털 워터마킹과 결합된 모바일 장치들의 사용을 확산할 수 있다.

기존의 연구는 인터넷에서 미디어 콘텐츠를 연구하는 모델인 콘텐츠 식별 기술(Contents Identification Technology)을 사용한 방법이 제안되었다. 콘텐츠 식별 기술은 콘텐츠-독립적인 기술과 콘텐츠-의존적 기술로 폭넓게 분류할 수 있다[1]. 콘텐츠-독립적인 기술은 디지털 워터마킹 기술을 포함하고 있으며 바코드와 같은 공개적인 기호 표시뿐만 아니라 메타 데이타, 태그 기술로 콘텐츠에 고유성을 부여한다. 콘텐츠-의존적 기술은 콘텐츠로부터 유도된 특징을 기반으로 콘텐츠를 식별하는 패턴 인식 기술과 같이 전자 개인정보(Digital Fingerprinting)에 포함된다.

논문 [2]는 낮은 비트율에서 비디오의 소유권 보호를 보장한다. 즉, 이전의 워터마킹 툴은 높은 비트율의 비디오를 위해서 설계되었고, 원영상과 공격된 영상을 통계적으로 기본적인 정보를 추측한다. 향상된 통계적 접근 방법으로 이 논문은 낮은 비트률의 비디오에서도 이런 가정이 옳다는 것을 신뢰할 수 있는 정보로 간주할 수 있도록 제공하고 있다.

논문 [3]은 퍼스널 컴퓨터과 비교하여 모바일 디바이스는 많은 제약이 따르므로 관심 영역의 트랜스코딩 기법을 이용한 모바일 프리젠테이션을 제안하고 있다.

논문 [4]는 FPGA 상에서 워터마크 삽입/추출 알고리즘을 구현함으로서 이런 알고리즘의 하드웨어와 시간 복잡도를 연구하고 있다.

스크린에 디스플레이한 비디오를 사용하는 모델은 모바일 디바이스의 카메라를 사용하여 비디오를 캡쳐하여 디스플리이된 비디오의 워터마크 추출을 기반으로 한다[1]. 비디오는 LCD 스크린에 디스플레이되거나 텔레비전, 영화 스크린, 또

† 종신회원 : 동명대학교 컴퓨터공학과 조교수
†† 정 회 원 : 부경대학교 컴퓨터공학과 교수
논문접수 : 2012년 1월 18일
수 정 일 : 1차 2012년 7월 13일, 2차 2012년 7월 26일
심사완료 : 2012년 8월 8일
* Corresponding Author : Hung-Bog Park(git@pknu.ac.kr)

다른 모바일 디바이스의 스크린 중 한 개일 수 있다. 추출된 워터마크는 비디오의 ID를 식별하고 사용자 경로를 알 수 있다.

모바일 에이전트 워터마킹[5, 6]은 소프트웨어 워터마킹을 사용하여 에이전트의 코드에 워터마크를 내장한다. 여기서 소프트웨어 에이전트 워터마킹은 소유권을 보호하기 위해서가 아니라 완전한 실행을 보장하기 위해서 사용할 수 있고, 악의적인 호스트에 의해서 조작된 공격을 추적하기 위해서 사용된다.

본 논문은 M-Commerce 환경에서 모바일 장치의 낮은 성능을 고려하여 비트율이 낮은(low bit rate) 비디오 콘텐츠에 대한 비시각적인 대역 확산(Spread Spectrum) 워터마킹 기법을 제안하고, 동영상 콘텐츠의 불법적인 행위자들을 추적하고 소유권의 보호를 보장할 수 있다. 따라서 모바일 환경의 워터마킹은 워터마킹 처리에 따른 비용 증가와 추가적인 데이터 트래픽이 포함되므로 암호화와 복호화의 복잡도가 간단해야 한다. 디지털 콘텐츠의 공격에 대한 강인성은 워터마크를 제거하거나 손상된 콘텐츠에 대해 추출 알고리즘의 상관관계(Correlation)로 평가한다.

본 논문의 구성은 다음과 같다. 2절에서는 M-Commerce 어플리케이션에 대해 기술하고, 3장은 모바일 상에서 비트율이 낮은 비디오 콘텐츠의 워터마킹 알고리즘, 4장은 구현 결과 및 분석, 5장은 결론, 참고문헌 순으로 기술한다.

2. M-Commerce 어플리케이션

MP3, 오디오, 비디오와 같은 디지털 미디어는 온라인상에서 판매되고 있고 인기가 매우 높아 전자상거래와 M-Commerce 부분의 중요성이 증가되고 있다. M-Commerce의 중요한 요소는 비디오, 오디오, e-Book과 같은 무선 미디어의 다운로드와 스트리밍이다[7].

현재 인터넷을 이용한 전자상거래에서 모바일 기기를 이용한 M-Commerce의 사용이 증가되고 있는 추세이다. 기존의 연구에서 M-Commerce를 위해 제공되고 있는 인터넷 상품 정보를 효과적으로 모바일 폰에 제공할 수 있는 새로운 모델을 제시하였고[8], 인터넷 상에서 전자적인 미디어에 대한 소유권을 보호하기 위해서 수년 전부터 디지털 워터마크에 대한 연구가 진행되고 있다. 그러나 모바일 장치에서 전자적인 미디어에 대한 상거래의 확산은 예측되고 있고, 이런 모바일 네트워크 영역에서 디지털 워터마킹에 대한 새로운 기술이 요구되고 있다.

대표적인 예로, 재정적인 서비스 제공자는 모바일 폰을 사용하여 판매할 물건에 대한 중요한 정보를 전송하고 안전한 상거래를 실시한다. 은행 업종에서 두드러지게 더 많은 새로운 서비스를 위한 모바일 폰 은행 시스템이 요구되고 있다. 이런 종류의 어플리케이션의 주요 목적은 말하는 사람의 발음(Speech)을 인증한다. 발음 처리 기술을 통해 말하는 사람의 신분 증명은 사용자의 소리를 모방하여 속일 수 있으므로 말하는 사람을 인증하기에는 충분하지 않다. 따라서 디지털 워터마킹 기법은 이런 문제를 해결하기 위해서 사용할 수 있다. 디지털 워터마킹 기법은 사용자로부터 생성하거나 특정한 정보를 변형하여 생성된다.

모바일 폰뱅킹이나 금융 서비스 어플리케이션의 워터마크 내장과 추출은 실시간에서 이루어진다[7]. 모바일 장치는 이런 알고리즘의 구현을 위해서 타켓이 되고, 삽입/추출 알고리즘의 하드웨어적 복잡성이 큰 논점이 된다.

논문 [9]는 최근 새로운 포켓용 디바이스에서 오디오와 비디오와 같은 디지털 미디어를 변경하고 사용하는데 있어서 특별한 가치가 있다. 하지만 워터마킹은 비용이 많이 들고 포켓용 디바이스에서 에너지 소모가 추가된다. 이 논문은 다양한 워터마킹 알고리즘의 에너지 프로파일을 분석하고 에너지 소비에서 보안의 영향과 영상의 화질에 대해 연구하고 있다. 또한 워터마킹 삽입, 추출 알고리즘 부분과 프록시 서버로 어떤 작업을 이동하여 접근하는 것을 나타낸다. 실험 결과에서 프록시와 포켓용 디바이스 사이의 부분적인 워터마킹 작업의 실행을 보여준다.

논문 [5]는 조작된 공격을 추출하기 위해서 소프트웨어 워터마크 기법을 사용하고, 모바일 에이전트에서 마크를 내장하고 악의적인 호스트에 대응하는 방법을 설명한다.

논문 [6]은 에이전트가 실행하는 동안에 수행되어진 조작된 공격을 추출하는 새로운 접근법을 소개한다. 이 접근법은 공격에 대해 책임을 져야할 악의적인 호스트를 추적한다. 소프트웨어 워터마크와 지문(Fingerprinting) 기법은 마크를 에이전트에 삽입하기 위해서 사용된다. 그리고 모바일 에이전트의 공격은 악의적인 호스트에 의해서 수행되기 때문에 모바일 에이전트의 실행은 고려되어야 한다. 지금까지는 모바일 에이전트의 보안성에 관한 해결에 많은 어려움이 있었다. 그러나 코드, 데이터, 또는 디지털 서명과 암호화 기법에 의해 다른 호스트로부터 온 결과의 순결성과 인증의 보장이 가능하다. 반면 에이전트가 실행하는 동안 악의적인 호스트에 의해서 수행되어진 공격을 추출하거나 방지하는 것은 어렵다.

논문 [7]은 DRM과 M-Commerce와의 관계, M-Commerce에 대한 비즈니스 모델이 미치는 영향을 설명하고 있다. 고정된 인터넷과 달리 모바일 단말기들은 사용자의 신원에 대해 더욱더 신뢰할 수 있는 정보를 제공한다. 따라서 개인화된 워터마킹의 유용성으로 인해서 데이터의 불법적인 복사는 개별적인 불법적인 행위로 추적할 수 있다.

3. 모바일 상에서 비트율이 낮은 비디오 콘텐츠의 워터마킹 알고리즘

컴퓨터의 성능과 비교하여 모바일 장치는 저성능과 추가적인 데이터 트래픽이 예상되므로 비트율이 낮은 비디오 콘텐츠에 대한 계산 복잡도가 낮은 워터마킹 알고리즘을 요구하고 있다.

비디오 콘텐츠는 사용자가 모바일 장치에 다운받기 전에 호스트에서 콘텐츠에 대한 워터마크를 내장하고 워터마크가

내장된 콘텐츠를 사용자의 모바일 장치로 전송한 후 디스플레이된다. 이때 워터마크 키는 비디오와 같은 미디어에 대해 고유성을 부여할 수 있다. 따라서 워터마크 키는 모바일 정보를 이용하여 콘텐츠를 구매하는 사용자의 정보를 인식할 수 있게 고유성을 부여하여 내장하고, 개인의 불법적인 행위에 대해 추적하고 불법적으로 콘텐츠를 변경한 행위를 찾을 수 있다.

기본적인 디지털 워터마크는 멀티미디어 데이터에 비시각적인 정보를 추가한다. 이것에 대한 기본적인 요구 사항은 다음과 같다.

(1) 무감지성(Imperceptibility) : 워터마크는 디지털 데이터의 화질에 지각할 수 있을 정도로 손상시키지 않는다.

(2) 보안성(Security) : 워터마크는 허가된 사람들에게만 접근 가능하게 해야 한다.

(3) 강인성(Robustness) : 워터마크는 워터마크 제거와 같은 심각한 조작을 포함한 다양한 조작을 한 후에도 멀티미디어 데이터에 존재해야 한다.

일반적으로 인터넷 상의 전자상거래 어플리케이션이 모바일 통신 시스템에서 항상 쉽게 적용되지는 않는다. 그리고 워터마크 관점에서 비트율이 낮은 콘텐츠는 보호되어야 한다.

기존의 퍼스널 컴퓨터와 마찬가지로 모바일 장치는 주문형 비디오, 텔레비전 시청, 온라인 게임 등과 같은 서비스를 지원하는데 아무런 제약이 따르지 않는다. 그러나 세계적인 모바일 네트워크의 평균 대역폭은 최대 7.2Mbps에서 최소 105kbps로 HSDPA, LET, WiMax로 네트워크를 교체하고 있어 평균 속도는 더욱 좋아질 전망이지만 일반 유선 인터넷의 평균 속도와 메모리, 처리 능력에 비교해서 여전히 부족하다. 또한 모바일과 일반 퍼스널 컴퓨터에서는 근본적인 하드웨어적인 차이점이 존재하므로 여기에 따른 어플리케이션 개발이 요구되고 있다. 그러므로 모바일 장치는 퍼스널 컴퓨터와 성능면에서 많은 차이점을 가지고 있지만 모바일 장치에서 디지털 미디어를 보호하기 위해서는 모바일 환경에 적합한 워터마킹 알고리즘을 개발해야 한다.

모바일 환경에서의 동영상 콘텐츠는 네트워크 트래픽과 같은 성능을 고려하여 일반 동영상에 비해 비트율이 낮은 비디오 영상을 처리하게 되고 이런 비트율 낮은 동영상에 대한 소유권 보호의 필요성이 요구된다.

워터마크 기법에서 강인성(Robustness)[2]은 악의적인 사용자가 내장된 워터마크를 제거할 경우나, 파일 포맷을 변경, 비디오 프레임율을 변경하는 것과 같이 일반적인 미디어의 공격이나 변형에서 내장된 워터마크를 추출할 수 있다. 이런 강인성은 모바일 환경의 낮은 비트율의 비디오와 같은 영상에서 더 많은 제약을 나타내고 있다.

대부분의 제안된 워터마킹 기법들은 대역 확산을 이용한 Pseudo-Noise 신호를 원신호에 내장하고 상관관계의 통계적인 분석을 통해서 워터마크를 추출한다.

본 논문은 매우 낮은 신호 대 잡음비에 대한 좋은 성능을 나타내는 대역 확산(Spread Spectrum) 기반의 워터마킹 기술을 사용한다. 따라서 모바일 전자상거래 환경의 비트율이 낮은 동영상에 대한 워터마킹 기법을 제안하기 위해서 웨이브릿 변환을 이용한 대역 확산 기법을 적용한다. Fig. 1은 본 논문에서 제안한 전체 시스템 구조를 나타내고 있다. 콘텐츠 서버는 콘텐츠를 요청한 모바일 사용자의 정보를 수집하고 사용자 고유의 키에 대한 M-Sequence를 생성한다. 이 M-Sequence를 워터마크 키로 사용하여 워터마크 처리를 수행한 후 사용자에게 비디오 콘텐츠를 전송한다. 또한 콘텐츠 서버는 인터넷 상에서의 워터마크가 내장된 콘텐츠를 수집하여 내장된 워터마크를 추출하고 고유한 M-Sequence에 대한 사용자의 불법적인 행위를 추적할 수 있다.

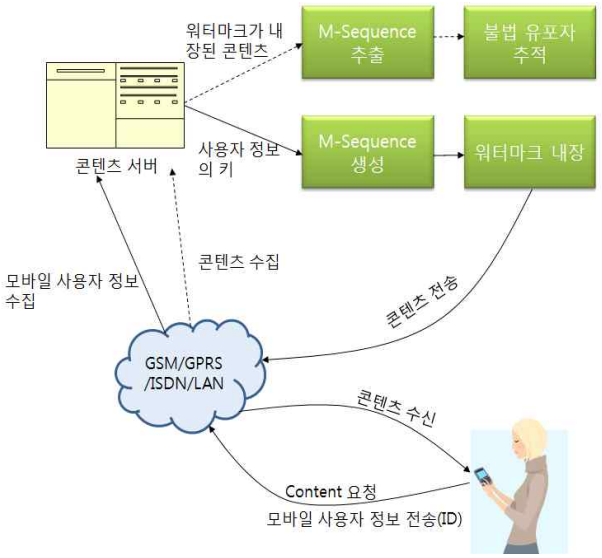


Fig. 1. Proposed System Structure

3.1 워터마크 생성

일반적으로 컴퓨터 기반의 인터넷 서비스와 달리 모바일 단말기는 사용자와 신원에 대한 정보를 아주 신뢰할 수 있고, 네트워크 공급자에 의해서 모바일 사용자의 단말기 시리얼 번호, 전화 번호, 신분 등을 확보할 수 있으므로 이런 정보들을 디지털 콘텐츠에 내장하고 M-Commerce에서 구매하게 함으로써 개개인의 불법적인 행위와 디지털 미디어의 불법적인 공격자들을 추적하기가 쉽다. 따라서 본 논문은 사용자의 개인 정보의 고유한 키를 이용하여 M-Sequence를 생성한 후 비디오 콘텐츠에 내장한다. 이런 사용자 정보는 {0, 1}로 구성된 Unipolar Sequence로 비디오 프레임에 내장할 마크인 M-Sequences를 생성한다. M-Sequences는 대역 확산(Spread Spectrum) 코드 분할 다중 접속(CDMA : Code Division Multiple Access)를 포함하는 통신 시스템으로 다양한 어플리케이션에 활용되고 있다. n-stage의 LFSR(Linear Feedback Shift Register)에 의해서 2^n-1개의 Pseudo-Random 이진 시퀀스(Binary Sequences)를 생성한다. M-Sequences는 이진 시퀀스의 최장 주기를 생성하고 자체 상관관계(Auto-Correlation)와 랜덤(Randomness) 속성을 가진다.

비디오 콘텐츠에 내장할 워터마크 키는 사용자의 고유한 값을 가지고 초기값은 다음과 같다. N개의 S_1, S_2, S_3, ...,

S_n를 초기값으로 지정하고, Linear Feedback Function을 $S_n = S_i \oplus S_{i+2}$ (i=1, 2, 3, ...)라고 하면, Fig. 2와 같이 입력과 출력을 생성한 M-Sequence의 초기 과정을 보여준다. 예를 들어, 초기값이 N 자리수이면 $N+2^N$개의 M-Sequence가 생성되고 여기에 반복적인 주기를 확인할 수 있다.

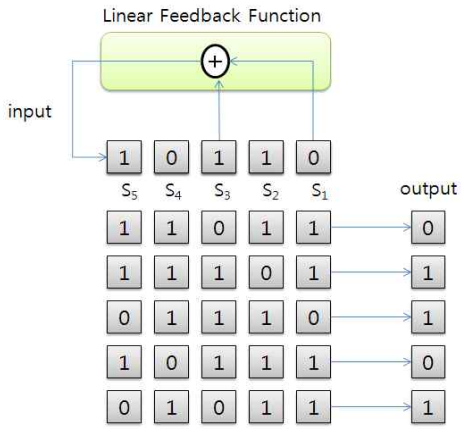


Fig. 2. LFSR(Linear Feedback Shift Register)

3.2 동영상 워터마크 삽입 및 추출

동영상은 휘도-색차 컬러 공간으로 표현되고, 워터마킹 처리에서 휘도 요소는 컬러 영상을 그레이 영상으로의 변형에도 워터마크의 요소 중 하나인 강인성을 보장한다. Fig. 3은 워터마크 내장 절차를 나타내고 있다.

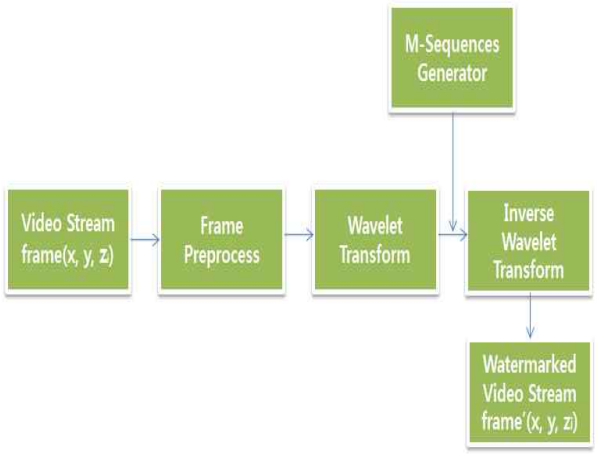


Fig. 3. Watermark Embedding

비디오 프레임은 YCbCr 컬러 공간으로 변형하고, Y인 휘도(Luminance) 요소에 워터마크를 삽입하기 위한 절차는 다음과 같다.

각 비디오 프레임을 프레임 전처리(Frame Preprocess) 과정을 통해서 YCbCr 컬러 공간으로 변형한 후 웨이브릿 변환(Wavelet Transform)을 수행한다. 여기서 frame(x, y, z_i)는 2차원 픽셀 (x, y) 좌표에서 z_i번째 프레임에 할당된 신호값을 나타낸다.

M-Sequence 생성기(Generator)는 길이 T의 워터마크 신호의 생성된 집합을 나타내고 웨이블릿 변환 영역에서 대역 확산을 통한 워터마크를 내장할 특정 주파수의 계수를 탐색한 후 Y-요소의 특정 주파수에 생성된 워터마크인 M-sequence를 내장한다.

워터마크가 내장된 Y-요소와 색차 신호(Cb, Cr)에 대해서 웨이브릿 역변환을 수행하고 주파수 영역에서 공간적인 영역으로 변환하면 워터마크가 내장된 비디오 프레임 (frame′(x, y, z_i))이 생성된다.

워터마크 추출 절차는 Fig. 4와 같다. W_x와 W_y 두 신호 사이의 상관계수를 구하여 두 신호에 대한 상관관계를 수학적인 통계치로 표현한다.

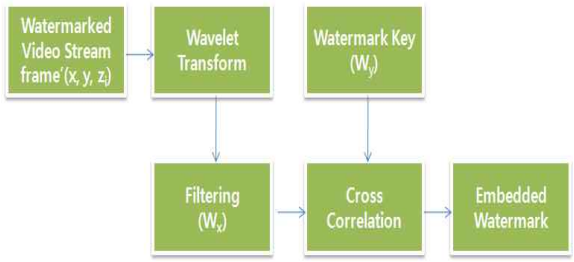
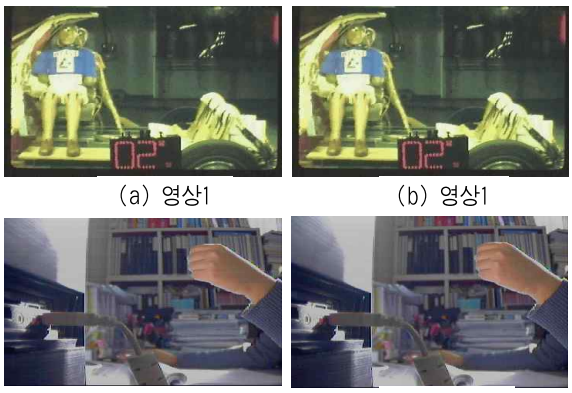


Fig. 4. Watermark Extraction

4. 구현 결과 및 분석

본 논문은 M-Commerce 환경에서 비트율이 낮은 비디오 콘텐츠에 대해 강인성과 비시각성을 만족할 수 있도록 다양한 실험을 통해 워터마크의 성능을 분석한다.

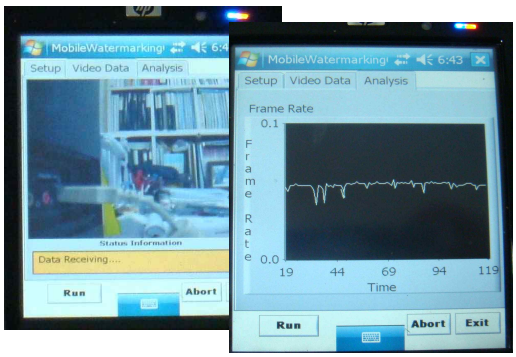
본 논문에서 사용한 실험 영상의 특징은 Table 1과 같이 프레임 크기는 360×268 픽셀로 초당 30~24 프레임율을 가진다. 그리고 각각의 실험 영상은 300~1000 사이의 프레임을 가진다. 워터마크 내장은 비디오 신호를 웨이브릿으로 변환한 후 주파수 대역 LL 영역에 M-Sequence을 내장했을 경우 비시각성에 아주 민감하여 LH와 HL 대역에 삽입하였다. 그리고 각각의 실험 영상에서 300 프레임에 대해 워터마크를 추출하였다.



(a) 영상1 (b) 영상1

(c) 영상4 (d) 영상4

Fig. 5. Watermark Embedding for Frame of the Original Image



(a) (b)

Fig. 6. Receiving Screen of Watermarked Content on Mobile

Fig. 5와 같이 (a)와 (c)의 영상 프레임은 원영상을 나타내고, (b)와 (d)의 프레임은 워터마크가 내장된 영상을 나타낸다. 실험 결과와 같이 워터마크가 내장된 프레임(b, d)은 원영상(a, c)과 시각적으로 구별하지 못하므로 워터마크의 비시각성을 만족한다. Fig. 6은 콘텐츠 서버에서 워터마크 처리된 비디오 영상을 수신한 결과를 나타내고 (a)는 워터마크가 내장된 비디오 영상과 (b)는 모바일에서 영상을 수신 받은 프레임율을 그래프로 나타낸다.

Fig. 7과 Fig. 8은 실험 영상1, 영상4에 대해 원영상에 워터마크가 내장된 영상(손상되지 않은 영상)에 M-Sequence 주기를 검출한 결과를 나타낸다. 각 그림의 X-축은 연속된 프레임에서 내장된 워터마크를 평가한 횟수를 나타내고, Y-축은 추출한 워터마크의 상관관계를 평가한 것으로 Y-축의 Detect 값이 1의 값을 나타내면 내장된 M-Sequence와 완전히 일치함을 나타낸다. 즉 내장된 워터마크의 주기를 추출함을 의미한다.

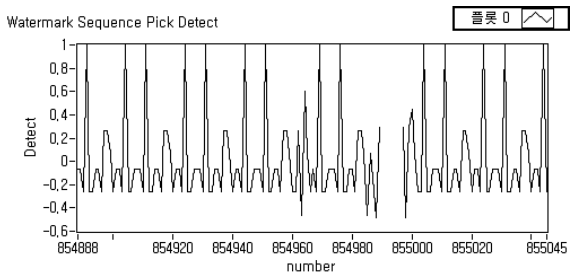


Fig. 7. Extract Watermark Sequence(영상1)

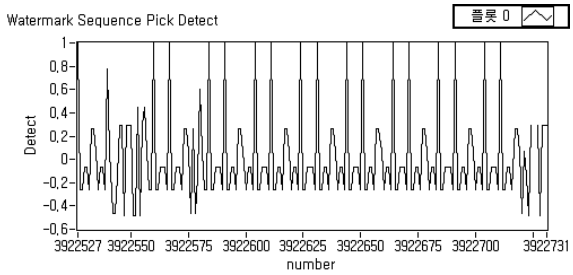


Fig. 8. Extract Watermark Sequence(영상4)

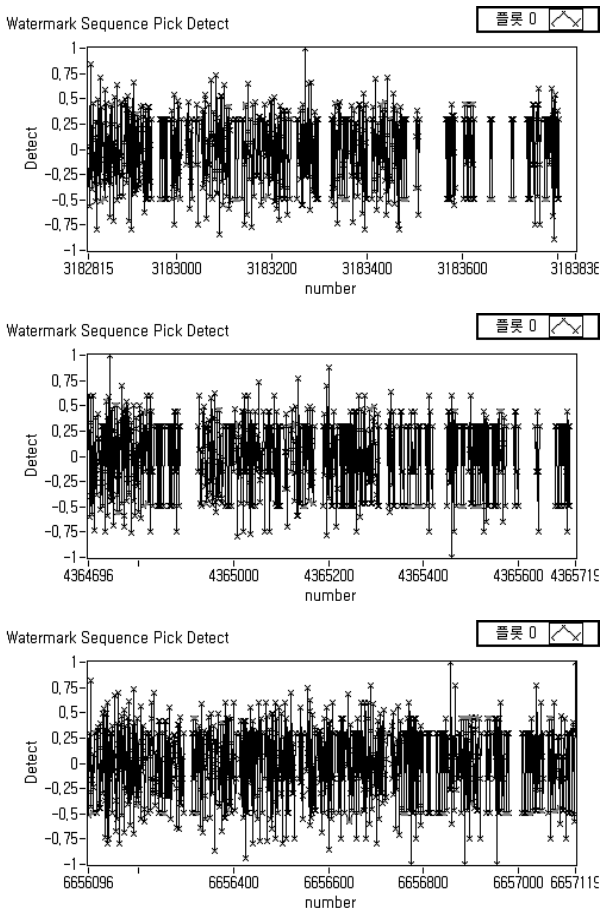


Fig. 9. Extract Watermark in the Compressed Frames

워터마크의 강인성에 대한 평가를 위해서 Fig. 9는 워터마크가 내장된 프레임에서 압축을 수행한 후 내장한 M-Sequence의 주기를 추출한 결과의 일부분을 나타내고 있다. Fig. 9의 X-축과 Y-축은 Fig. 7-Fig. 8과 같다. 여기서 프레임에 적용할 압축의 양으로 영상 화질(Image Quality)은 75%이다.

Fig. 10과 Fig. 11는 실험 영상1, 영상4에서의 워터마크가 내장된 영상에 대한 PSNR(Peak Signal to Noise Ratio)를 나타낸다. 각 영상의 평균 PSNR는 각각 57.62dB와 47.62dB로 평가되었다.

기존 연구의 PSNR 평가에 있어서 논문 [10]의 LSB-PSNR은 59.27dB~60.23dB, QIM-PSNR은 57.81dB~60.43dB로 평가되었다. 논문 [11]은 Case 1의 경우는 14~15dB까지 오류 없이 정보를 추출할 수 있었다. 이런 노이즈 시퀀스의 시각적인 품질이 매우 낮으므로 평균 BER에 대한 비교는 매우 낮은 PSNR 레벨에서 중요하지 않다. Case 2의 경우는 Foreman 영상에서 PSNR이 45dB 정도로 평가되었다.

이전의 워터마킹 툴은 매우 높은 비트율 비디오를 위해 설계되었고, DVD 보호와 같은 높은 비트율의 비디오는 다양한 종류의 수십 Mbps을 지원하지만 일반적으로 15Mbps이다.

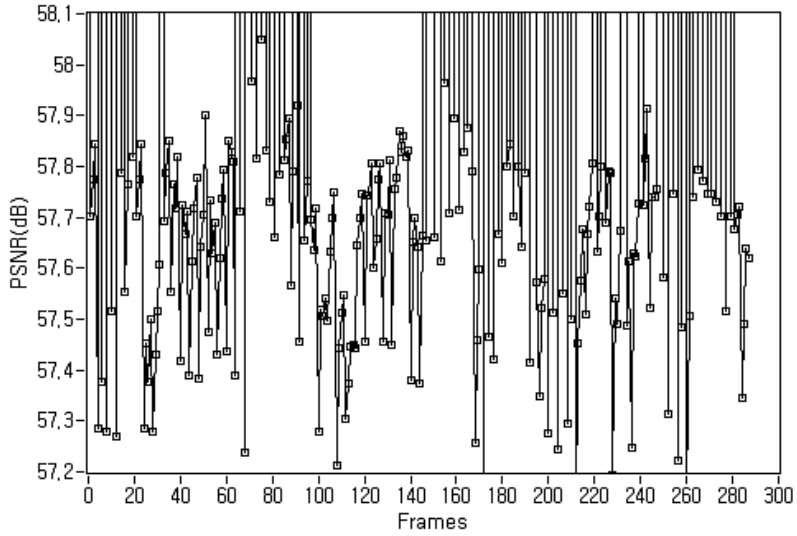


Fig. 10. PSNR of Original Frame and Watermarked Frame(experiments image-영상1)

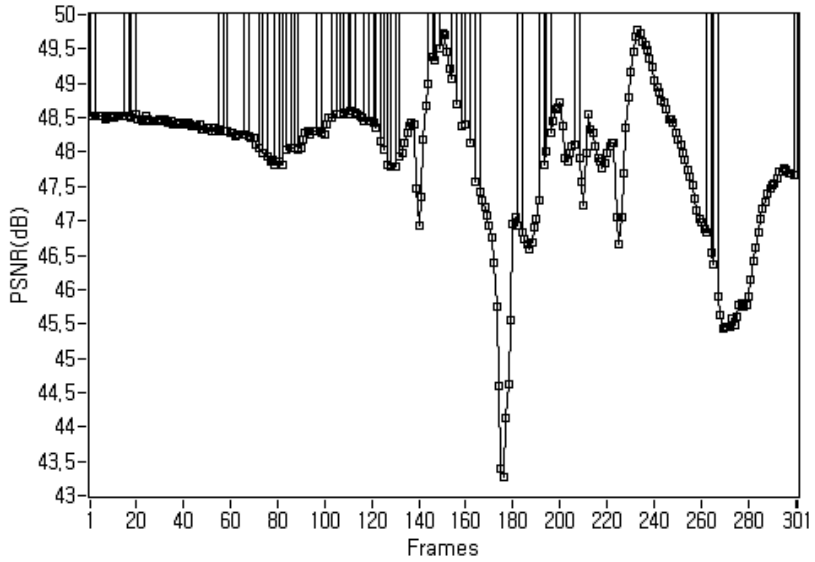


Fig. 11. PSNR of Original Frame and Watermarked Frame(experiments image-영상4)

Table 1. Comparative Analysis of Watermark Extraction of Compressed Frames and PSNR(Image Quality = 75%)

요소 \ 영상	영상1	영상2	영상3	영상4
용량	7,403KB	3,973KB	660MB	486MB
크기	360×268	360×268	360×268	360×268
재생 시간	10초	6초	1분 14초	43초
fps	25	25	24	30
kbps	5,646	5,134	74,096	92,620
워터마크 추출 횟수 (Correlation Value=1)	30	57	129	72
평균 PSNR	57.62	59.1	49.3	47.62

Table 1의 모든 영상은 영상 화질을 75%로 해서 압축한 후 300 프레임 사이에서 워터마크 추출 및 분석한 결과를 나타낸다. 영상1은 워터마크가 내장된 압축 프레임에서 M-Sequence의 주기인 워터마크를 추출(상관관계가 1인 경우)한 횟수는 30, 영상2는 57, 영상3은 129, 영상4는 72로 나타났다. 실험 결과에서와 같이 압축한 프레임의 비트율이 낮은 영상에서 워터마크를 추출할 수 있으므로 워터마크의 강인성을 보장할 수 있다.

5. 결 론

본 논문은 M-Commerce 환경에서 모바일 장치의 낮은 성능을 고려한 디지털 워터마킹 기법을 제안한다. 워터마크 키는 사용자의 고유한 키를 이용하여 {0, 1}로 구성된 Unipolar Sequence로 비디오 프레임에 내장할 마크인 M-Sequences를 생성하고, 워터마크를 콘텐츠에 내장한 후 사용자의 모바일 장치에 전송한다. 워터마크의 비시각성을 보장하기 위해서 M-Sequence는 Y-요소에 대한 주파수 영역의 LH와 HL 대역에 내장하였다. 콘텐츠에 고유한 사용자의 키를 내장함으로써 동영상 콘텐츠의 불법적인 행위자들을 추적하고 소유권의 보호를 보장할 수 있다.

모바일 환경의 워터마킹은 워터마킹 처리에 따른 비용 증가와 추가적인 데이터 트래픽이 포함되므로 암호화와 복호화의 복잡도가 간단해야 한다. 워터마크가 내장된 디지털 콘텐츠의 공격에 대한 강인성은 워터마크를 제거하거나 손상된 콘텐츠를 추출 알고리즘의 상관관계를 사용하여 평가한다. 본 실험은 워터마크의 강인성을 평가하기 위해서 워터마크가 내장된 영상을 압축한 후 M-Sequence의 주기를 추출한 결과 모든 영상에서 고유한 M-Sequence의 주기를 쉽게 검출할 수 있었다. 따라서 비트율이 낮은 콘텐츠에서도 워터마크의 추출을 보장하여 불법적인 사용자의 추적이 가능하다.

참 고 문 헌

[1] Sierra Modro, Ravi K. Sharma, “Digital Watermarking Opportunities Enabled by Mobile Media Proliferation,” SPIE, Vol.7254, 2009.

[2] M. Mitrea, F. Preteux, S. Duta, M. Petrescu, “Wavelet based mobile video watermarking: spread spectrum vs. informed embedding,” SPIE, 2005.

[3] Jung-Hee Seo, Hung-Bog Park, “Mobile Presentation using Transcoding Method of region of Interest,” The Korea Information Processing Society(KIPS) Transactions : Part C, Vol.17-C, No.2, pp.197-204, April, 2010.

[4] Shilpa Arora, Sabu Emmanuel, “Real-Time Adaptive Speech Watermarking Scheme for Mobile Application,” ICICS-PCM 2003, 15-18, December, 2003.

[5] Oscar Espaza, Jose L. Muñoz, Miguel Soriano, Jordi Forné, “Secure brokerage mechanisms for mobile electronic commerce,” Computer Communications, Vol.29, No.12, pp.2308-2321, 2006.

[6] O. Esparza, M. Feenandez, M. Soriano, J. L. Muñoz, and J. Forné, “Mobile Agent Watermarking and Fingerprinting Tracing Malicious Hosts,” LNCS 2736, pp.927-936, 2003.

[7] Frank Hartung and Friedhelm Ramme, Ericsson Research, “Digital Right management and Watermarking of Multimedia Content for M-Commerce Applications,” IEEE Communications Magazine, November, 2000.

[8] Sangho, Ha, “Design and Implementation of a Mobile System for Exploiting the Internet Product Information Effectively,” The Korea Information Processing Society(KIPS) Transactions : Part D, Vol.12-D, No.3, pp.493-498, 2005.

[9] Arun Kejariwal, Sumit Gupta, Alexandru Nicolau, Nikil D. Dutt, Rajesh Gupta, “Energy Efficient Watermarking on Mobile Devices Using Proxy-Based Partitioning,” IEEE Transaction on Vary large Scale Integration System, Vol.14, No.6, pp.625-636, June, 2006.

[10] Dima Pröfrock, Henryk Richter, Mathias Schlauweg, Erika Müller, “H.264/AVC video authentication using skipped macroblocks for and erasable watermark,” Proc. of SPIE, Vol.5960, pp.1480-1489, 2005.

[11] Alper Koz, A. Aydin Alatan, “Oblivious Spatio-Temporal Watermarking of Digital Video by Exploiting the Human Visual System,” IEEE Transaction on Circuits and System for Video Technology, Vol.18, No.3, pp.326-337, 2008.

서 정 희

e-mail : jhseo@tu.ac.kr

1994년 신라대학교 자연과학대학 전자계산학과(이학사)

1997년 경성대학교 전산통계학과 (이학석사)

2006년 부경대학교 전자상거래시스템 전공(공학박사)

현 재 동명대학교 컴퓨터공학과 조교수

관심분야 : 멀티미디어 응용, 정보보호, 모바일 컴퓨팅

박 흥 복

e-mail : git@pknu.ac.kr

1982년 경북대학교 공과대학 컴퓨터공학과(공학사)

1984년 경북대학교 컴퓨터공학과 (공학석사)

1995년 인하대학교 전자계산학 전공 (이학박사)

현 재 부경대학교 컴퓨터공학과 교수

관심분야 : 모바일 컴퓨팅, 멀티미디어 응용, 원격 교육

모바일 상에서 비트율이 낮은 비디오 콘텐츠의 강인성을 위한 디지털 워터마킹

서 정 희[†] · 박 흥 복[††]

요 약

모바일 환경에서의 동영상 콘텐츠는 네트워크 트래픽과 같은 성능을 고려하여 일반 동영상에 비해 비트율이 낮은 비디오 영상을 처리하게 되고, 비트율이 낮은 동영상에 대한 소유권 보호의 필요성이 요구된다. 따라서 모바일 장치는 퍼스널 컴퓨터와 성능면에서 많은 차이점을 가지고 있으므로 모바일 장치에서 디지털 미디어를 보호하기 위해서는 모바일 환경에 적합한 워터마킹 처리 알고리즘을 개발해야 한다. 본 논문은 M-Commerce 환경에서 모바일 장치의 낮은 성능을 고려하여 비트율이 낮은 비디오 콘텐츠에 대한 비시각적인 대역 확산(Spread Spectrum) 워터마킹 기법을 제안하고, 동영상 콘텐츠의 불법적인 행위자들을 추적하여 소유권의 보호를 보장할 수 있다. 워터마크가 내장된 콘텐츠의 공격에 대한 강인성의 평가는 워터마크를 제거하거나 손상된 콘텐츠를 추출 알고리즘의 상관관계(Correlation)로 나타낸다. 실험 결과에 따르면 워터마크의 강인성을 평가하기 위해 워터마크가 내장된 영상을 압축한 후 M-Sequence의 주기를 추출한 결과 모든 영상에서 고유한 M-Sequence의 주기를 쉽게 검출할 수 있었다. 따라서 비트율이 낮은 콘텐츠에서도 워터마크 추출을 보장하여 불법적인 사용자의 추적이 가능할 것으로 예상된다.

키워드 : 모바일 전자상거래, 동영상 콘텐츠, 디지털 워터마크, 강인성