멀티미디어 저작권 보호를 위한 디지털 워터마킹 기술의 현황

노철균* · 정연기** · 임성운* · 배상욱* · 구본호*

1. 서 론

워터마킹(watermarking) 기술이란 최근 각광받고 있는 저작권 보호에 관한 것으로서 영상 및 오디오와 같은 멀티미디어 데이터에 원 소유주 또는 저작자만이 아는 신호를 사람의 육안이나 귀로는 구별할 수 없게 삽입하고 이를 이용자에게 제공함으로써 불법복제에 대한 검출기능을 제공하는 기술을 말한다.

최근, 컴퓨터의 급속한 발달과 인터넷과 같은 컴퓨터 망의 확산으로 음성, 이미지, 비디오와 같은 멀티미디어 데이터들이 디지털화 되고 있다. 이런 디지털 데이터들은 기존 아날로그 데이터들과 비교하여 데이터의 저장과 편집이 매우 용이한 장점을 가진다. 하지만 데이터를 디지털화 함으로써 생기는 장점은 누구나 디지털 데이터의 내용을 쉽게 변형하고 복제할 수 있는 단점이 되기도 한다. 특히 디지털화 된 데이터는 원본과 복사본의 구분이 불가능하여 소유권 보호문제가 심각하게 대두되고 있는 실정이다.

실제로 네트워크에서 음악파일을 다운로드 받아 들을 수 있는 MP3 플레이어와 네트워크로부터 영상을 다운로드 받을 수 있는 영상 저장 디스플레이어 장치의 경우 불법 복제행위가 심각한 문제로 떠오르고 있다. 최근 인터넷 사용자들이 음악을 MP3 파일 형태로 다운로드받고 이를 MP3 플레이어에 집어넣어 들고 다니면서 듣기 때문에 음반회사에서는 CD와 테이프를 판매할 기회가 줄어들어 이러한 멀티미디어에 관한 불법 도용, 소유권 및 저작권을 보호하는 워터마킹 기술의 개발이 절실히 요구되고 있다.

디지털 멀티미디어 컨텐츠는 계속적인 복사나 유통에 의해서도 화질이나 음질이 저하되지 않을 뿐만 아니라, 저가의 대용량 저장 장치의 보급에 따라 이를 손쉽게 저장하고 복사하여 유통시킬 수 있으므로, 합법적인 구입자와 유통 경로의 파악을 통한 판매 활성화와 유료 서비스의 기반을 구축하기 위해서는 저작권 보호 기술의 개발 및 보급이 반드시 선행되어야 한다. IP 산업, 특히 고부가가치의 디지털 멀티미디어 컨텐츠를 기반으로 한 고급 IP 산업의 활성화를 위해서는 국가적인 차원에서 불법적인 복제 방지 및 저작권 보호와 관련된 기술 인프라를 제공할 필요가 있다.

현재 전세계적으로 활발히 연구되고 있는 워터마킹 기술은 비디오와 오디오 등의 멀티미디어 저작물에 지적 소유권자의 마크(mark)를 삽입하는 기술이다. 이 때 삽입되는 마크를 워터마크(watermark)라고 부르는데 이는 다음과 같은 특징을 가지고 있다. 첫째로 비디오나 오디오에 삽입된 워터마크는 눈이나 귀를 통해 인간이 인식할 수 없을 정도여야 한다. 한편, 저작권자가 누구인지를 알리기 위해서 눈에 잘 띄게 삽입하는 경우

*경일대학교 공과대학 제어계측공학과
**경일대학교 공과대학 컴퓨터공학과

도 있다. 그러나 대개의 경우 인식할 수 없도록 삽입한다. 여기서 주목해야 할 사항은 소비자에게 제공된 멀티미디어 컨텐츠는 워터마크의 삽입으로 인해 화질이나 음질 등의 서비스 품질이 저하되지 않도록 충분히 작아야 한다는 점이다. 둘째로 삽입된 워터마크가 고의적이든 그렇지 않든 그 컨텐츠에 변형을 가하더라도 쉽게 지워지지 않아야 한다. 이는 컨텐츠에 변형을 가했을 때, 쉽게 워터마크가 지워진다면 컨텐츠의 저작권자가 누구인지를 증명할 수 없으므로 저작권자의 권리를 보호할 수 없기 때문이다. 이러한 특징은 첫번째 특징과 서로 상충되는 관계에 있기 때문에 두 가지 조건을 모두 만족하는 워터마킹 기술의 개발이 활발히 전개되고 있다.

워터마킹은 멀티미디어 컨텐츠 내에 삽입하여 컨텐츠 소유권자의 권리를 보호하기 위한 기술의 하나이다. 그 응용 분야로서는 지적 소유권 보호, 데이터 인증, 소유권 확인 등이 있다. 워터마킹 기술의 연구는 데이터 라벨링(labelling)의 다양한 수단들을 개발하거나 좀 더 강인한 워터마킹 기술의 개발이 주요 목표이다. 여기서 강인한 워터마킹 기술이란 해적의 의도적인 공격이나 비의도적인 공격에 의해 제거될 수 없도록 워터마크를 삽입하는 것을 말한다. 여기서 공격이란 데이터의 압축, 필터링, thresholding, cropping 등을 모두 포함한다. 실제로 많은 연구들에서 이러한 특성을 만족하도록 하기 위하여 다양한 방식들이 제안되었고 많은 기술 개발이 이루어졌다. 그러나 워터마킹 기술이 어떠한 응용에 사용될 수 있는지에 대한 궁극적인 목표 분석이 거의 주어지지 않은 상태이다. 즉, 워터마킹 기술이 컨텐츠를 보호하기 위하여 언제, 어떻게 사용될 수 있는지, 합법성에 기초하여 워터마크를 이용한 컨텐츠 보호가 유효할 지에 대한 분석이 부족한 상태이다. 그러나 워터마킹 기술의 적용이 가능한 응용 분야에서 요구되는 사항들을 정리하는 것은 차후의 워터마킹 기술의 응용 분야의 개발에 중요하다.

2장에서는 워터마킹 기술의 몇 가지 응용 분야에 대해 살펴보고, 3장에서 워터마킹 기술의 요구사항을 분석한다. 그리고 4장에서 현존하는 워터마킹 기술의 한계 및 워터마킹 기술을 분류해보고, 5장에서 현재 워터마킹 방법으로 가장 널리 사용되는 spread spectrum을 이용한 워터마킹에 대해 설명한다. 마지막으로 6장에서 결론을 맺는다.

2. 응용분야

이 절에서 언급되는 응용 분야들은 주로 영상 또는 비디오 컨텐츠에 대한 것들이다[6].

2.1 Visible 워터마킹 기술을 이용한 영상 컨텐츠의 지적 소유권 보호

이 시나리오에서는 영상내에 소유권자의 visible 워터마크를 삽입하고 그 영상을 다른 목적에 사용하는 것을 금지하지 않는다. 여기서 visible 워터마킹이란 영상 내에 소유권자의 마크를 삽입하는데 있어서 그 마크가 눈에 쉽게 띄도록 하는 것이다. 예를 들어 영상에 자신의 이름을 크게 새겨놓거나 회사의 로고를 눈에 띄게 삽입하는 것을 생각할 수 있다. visible 워터마킹의 목적은 영상의 상업적인 사용이나 지적소유권을 쉽게 알리기 위함이다. 영상은 인터넷을 통해 쉽게 소비자에게 전달될 수 있고 이 때 visible 워터마크는 이 영상의 출처(source)가 어디인지를 쉽게 알릴 수 있다. 이 응용 사례에서 요구되는 특성은 워터마크가 눈에 잘 띄어야 하지만 눈에 거슬리지 않고, 제거하기 힘들어야 한다는 점이다.

2.2 인증을 위한 영상의 지적소유권[5]

방송사 기자가 뉴스 방송을 위해 디지털 카메라로 찍은 비디오가 있다고 생각해 보자. 이 비디오를 사용하기 전에 방송국은 이 비디오가 수정되거나 변조되지 않았는지 검증하기를 원한다. 이러한 검증을 위하여 invisible 워터마크가 카메라로 비디오를 찍을 당시에 자동적으로 삽입된다. 여기서 삽입된 워터마크는 이 비디오가 변조되지 않았음을 증명한다. 이러한 응용 사례에서 효과적으로 사용되기 위한 워터마킹 기술은 다음과 같은 특성을 가지고 있어야 한다. 첫째로 무감지성(invisibility)이다. 즉, 원영상에 워터마크를 삽입하였지만 눈으로 관찰되지 않아야 한다. 둘째로 해적의 워터마크가 삽입되기 힘들어야 한다. 셋째로 어디서 변형이 가해졌는지 알 수 있어야 한다.

2.3 무단 배포 방지

저작물을 구매한 소비자가 무료로 타인에게 저작물을 복사하여 제공할 수 있다. 이는 저작권자의 저작권료의 감소를 초래한다. 저작권자는 이를 방지하기 위해 저작물에 워터마크를 삽입한다. 저작권자 또는 그의 대리인은 저작물의 무료 배포를 방지하기 위하여 인터넷을 통해 공개된 저작물들에 대해 저작권자의 워터마크가 삽입되어 있는지를 확인하여 불법 사용 여부를 판단한다. 이러한 응용에 있어서 워터마크가 갖추어야 할 기능은 무감지성, 강인성(robustness), 워터마크의 빠른 검출 등이 있다.

2.4 불법 배포자의 확인

저작권자는 무단 배포의 방지 뿐만 아니라 무단 배포자가 누구인지 알기를 원할 것이다. 이를 위해서 저작물을 판매할 때 누구에게 판매하는지에 대한 정보를 invisible 워터마크로 삽입한다. 불법 배포된 저작물이 적발되면 적발된 저작물에서 워터마크 검출을 통해 구매자의 정보를 알 수 있다. 이러한 정보를 이용하여 저작권자는 구매자의 불법 배포 사실을 증명할 수 있으므로 적절한 보상을 받을 수 있다. 이러한 응용의 가장 큰 특징은 저작물에 삽입되는 워터마크가 구매자에 따라 모두 다르다는 점이다. 이를 위해서는 굉장히 많은 수의 서로 다른 워터마크를 발생시킬 수 있어야 하고 불법 도용을 위해 가짜의 워터마크를 첨가하는 것이 불가능하도록 만들어야 한다.

3. 워터마킹 기술의 공통적인 요구사항

3.1 안정성(security)

워터마킹의 안정성이 워터마킹 알고리즘의 비밀에 의해 유지되어서는 않된다. 암호화 분야에서 공개키 기반의 암호화 기술이 효과적임이 잘 알려진 것처럼 워터마킹 기술에 있어서도 해적이, 삽입된 워터마크가 어떠한 알고리즘에 의해 삽입되었는지 모른다는 가정하에 워터마킹 알고리즘의 효율성을 논하는 것은 매우 위험한 일이다. 여기서 공개키 기반의 암호화 기술은 알고리즘을 공개하고 공개키와 비밀키로서 암호화와 복호화를 수행하는 방식이다. 알고리즘의 비밀에 기초한 방식이 위험함에도 불구하고 실제 상업 시장에서는 이러한 가정에 기반을 두고 있는 경우가 많다. 워터마킹 알고리즘의 비밀이 일단 알려지면 지금까지 그 알고리즘을 사용하여 제작된 저작물에 삽입된 모든 워터마크가 제거될 수 있고 또 다시 다른 알고리즘을 고안해야 한다는 문제점이 있다. 뿐만 아니라 알고리즘의 비밀을 유지하기 위하여 알고리즘 고안자들의 보안이 쉽지 않다는 문제점이 있다. 즉, 퇴직 등을 통해 경쟁사나 외부에 알려질

가능성이 높다.

3.2 무감지성(invisibility)

몇몇 응용에서는 visible 워터마크가 사용되지만 대부분의 응용에서는 invisible 워터마크가 사용된다. 그래서 현재 워터마킹 기술에 대한 연구는 대부분 워터마크를 보이지 않게 영상 속에 숨기는 방식들에 대한 것이다. 이것은 지적 소유권의 주장을 위해 워터마크를 삽입하면서도 서비스의 질을 떨어뜨리지 않게 하기 위함이다. 예를 들어, 워터마크가 음악에 삽입되었을 때 원래의 음악과 워터마킹된 음악 사이의 차이를 청취자가 구별할 수 없을 정도여야 하며, 영상 또는 비디오의 경우에도 마찬가지로 화질의 차이를 느낄 수 없어야 한다. 만약 음질이나 화질의 차이가 발생한다면 소비자로부터 그 제품은 외면당할 수 있기 때문이다. 워터마크의 무감지성은 해적의 공격으로부터 강인해야 한다는 워터마크의 조건과 상충되는 것이다. 예를 들어 워터마킹된 영상을 JPEG이나 MPEG과 같은 손실 부호화 방식으로 압축을 수행했을 경우 워터마크가 지워질 수 있다.

3.3 강인성(robustness)

디지털 형태의 음악, 영상, 비디오 등은 손실 부호화, 필터링, 크기 변환(resizing), 대비 강조(contrast enhancement), 클로핑(cropping), 회전(rotation) 등의 신호처리에 의해 쉽게 변형될 수 있다. 워터마킹 기술이 그 기능을 발휘하기 위해서는 워터마크가 위와 같은 신호처리 후에도 검출이 가능해야 한다. 신호처리에 강인한 워터마킹을 위해서는 워터마크가 신호의 중요한 부분에 삽입되어야 한다는 것이 일반적인 경향이다[4]. 해적의 공격은 원신호에 큰 변형을 주지 않고 워터마크만을 제거하려는 데 그 목적이 있다. 그래서 대개의 경우 저대역필터(low pass filter)를 사용하거나 압축과정을 수행 후 고주파 성분을 제거하는 방법으로 공격이 이루어질 것으로 예상된다. 따라서 신호의 중요 부분에 워터마크를 삽입함으로써 공격으로부터 제거되지 않도록 함이 타당하다.

한편, 변위(translation), 크기변환, 회전, 클로핑 등의 기하학적 변환(geometric transformation)이 영상에 가해지는 경우, 워터마크의 강인성은 상당히 약한 편으로서 많은 보완이 필요하다. 워터마킹 기술이 영상, 오디오, 비디오와 같은 멀티미디어 저작물에 대한 지적 소유권 보호를 위해 성공적으로 적용되기 위해서는 강인성이 무엇보다 중요하다.

3.4 삽입될 수 있는 정보의 양

워터마킹 알고리즘들은 대개 수동적으로 정한 일정 양의 정보를 삽입하게 된다. 그러나 무감지성과 강인성 등의 특성을 만족하면서 자동적으로 삽입될 수 있는 정보의 양을 결정하는 알고리즘이 필요하다. 워터마크가 삽입된 영상이나 음악을 판매할 경우, 각 저작물에 저작물의 번호, 구매자에 대한 정보 등을 수록하기 위해서는 사용 가능한 워터마크의 수가 충분해야 하고 이를 서로 구별하기 위해서는 삽입되는 정보의 양이 충분히 클 수 있어야 한다.

3.5 낮은 오차 확률

워터마크의 검출 시, 신호의 왜곡이나 공격으로 인해 false-negative (워터마크가 있음에도 없다고 판정하는 경우)와 false-positive (워터마크가 없음에도 있다고 판정하는 경우)가 발생할 수 있다. 좀 더 믿을 만한 워터마킹을 위해서는 이러

한 false-negative와 false-positive의 오차확률이 충분히 작아야 한다. 일반적으로 지금까지 개발된 워터마킹 기술들은 이 확률이 상당히 작음을 보이고 있지만, 작은 오차 확률에도 불구하고 법적인 문제와 부딪혔을 경우의 해결책이 필요하다.

3.6 워터마크의 검출시 원신호의 사용

워터마킹 기법은 원신호를 사용하는지 여부에 따라 크게 두 부류로 나누어볼 수 있다. 우선 원신호를 사용하여 워터마크을 검출하는 부류이다. 이러한 접근 방식을 사용한 연구는[4,10,12,13] 등이 있다. 이 연구들에서는 신호처리나, 워터마킹을 제거하거나 검출할 수 없도록 데이터를 조작하는 경우들에 대해 강인한 기법들을 제안하고 있다. 그러나 이 방법은 실용적으로 적용하기 부적합하다. 왜냐하면 원신호가 유효하지 않은 경우가 존재할 수 있고, 신호처리 없이도 가짜 워터마크를 단순히 삽입함으로써 올바른 소유권자를 구별할 수 없도록 만들 수 있음이[3,14]에서 지적되었다. 또 다른 부류는 원신호를 사용하지 않고 워터마크를 검출하는 부류이다. 이 방식을 blind방식이라고 부른다[1]. 이 부류는 올바른 소유권을 증명할 수 있음을[3,14]에서 또한 지적하였다. 최근 보고된 blind 워터마킹 기법들로는[1,2,7,8,9,10,15] 등이 있지만 이 기법들은 보통의 영상처리에 의해 워터마크가 쉽게 제거 또는 파괴되는 단점을 가지고 있다. 그래서 좀 더 강인한 워터마킹 기법의 개발이 과제이다.

3.7 비밀 워터마킹 기법과 공개 워터마킹 기법

비밀 워터마킹(private watermarking) 기법은 권한이 주어진 사용자에 의해서만 워터마크의 검출이 가능한 반면, 공개 워터마킹(public watermarking) 기법은 누구나가 워터마크를 검출할 수 있다. 비밀 워터마킹 기법은 공개 워터마킹 기법에 비해 훨씬 안전성이 높다고 할 수 있다. 그러나 일단 워터마크의 코드가 알려지면 쉽게 워터마크가 제거되고 같은 워터마크 코드가 사용된 다른 저작물에 대해서도 피해가 파급되는 단점을 가지고 있다.

일반적으로, 상업용 제품들은 암호화 분야에서 공개를 기반으로 한 기법들이 널리 받아들여지고 있다. 그래서 워터마킹 기법도 공개를 기반으로 이루어져야 한다. 그러나 현재의 워터마킹 기법에 대한 연구는 비밀을 기반으로 한 기법에 좀 더 집중되어 있다.

3.8 워터마크의 invertibility

Invertibility란 권한을 가진 사용자가 워터마킹된 데이터로부터 워터마크를 제거할 수 있음을 의미한다. 많은 응용에 있어서 데이터의 사용에 따라 워터마크를 통해 정보를 첨가하는 대신 기존의 정보를 삭제하고 새로운 정보를 삽입할 필요가 있다. 그 때, invertibility는 워터마킹 기법에서 필요한 요구 기능이 될 수 있다. 그러나 불행하게도 invertibility를 만족하는 워터마킹 기법이 공격으로부터 충분히 강인하도록 설계되는 것이 매우 어렵다. 그래서 암호화와 워터마킹이 함께 사용되는 방식에 대한 연구가 진행 중인 것으로 알려져 있다.

참고문헌[3]에서는 reverse engineering을 통해 소유권을 무력화시킬 가능성에 대해 분석하였고 성공적인 소유권 보호를 위해서는 워터마크가 invertibility가 없어야 한다는 결론을 내렸다.

3.9 신축성(scalability)

실제적인 응용에 있어서 워터마킹의 삽입과 검출의 계산량은 중요하다. 워터마크의 삽입 시간은

검출 시간에 비해 상대적으로 덜 중요하다. 삽입은 빠른 시간 내에 이루어질 필요가 없는 반면, 검출은 빠른 시간 내에 이루어질 필요가 있다. 예를 들어, 인터넷상에 공개된 저작물들 중, 저작권자 A의 워터마크가 삽입된 저작물을 찾고자 할 때, 빠른 검출은 중요하다. 그러나 검출에 있어서의 계산비용(computational cost) 감소는 강인성을 해칠 가능성이 높다. 급속한 컴퓨터의 발전은 계산비용의 급격한 감소를 가져옴에 따라 워터마크의 제거나 무력화를 더욱 더 용이하게 만든다. 그러므로 컴퓨터의 발전에 따라 워터마크의 검출 방식의 버전을 신축적으로 변화시킬 필요가 있다. 고의적인 워터마크의 제거나 무력화를 위해서는 현재 비싼 비용을 지불함에도 불구하고 다음 세대에 가서는 저렴한 비용으로 가능하다면 이 워터마킹 기술은 그 기능을 상실하게 된다. 따라서 컴퓨터의 발전에 따라 워터마킹 기법이 신축적으로 변할 수 있도록 설계되어야 한다.

4. 현존하는 워터마킹 기술의 한계 및 분류

4.1 현존하는 워터마킹 기술의 한계

현존하는 워터마킹 기술은 다음과 같은 많은 문제점을 가지고 있다. 따라서 이러한 현 워터마킹 기술의 문제점을 해결하기 위한 많은 노력들이 이루어지고 있다.

- 워터마크가 삽입될 데이터에 얼마나 많은 정보(bits)을 삽입할 수 있는 지를 아는 것이 힘들다. 비록 [11]에서 삽입될 수 있는 정보량에 대한 노력이 있었지만 실용적으로 사용하기에 다소 어려운 점이 있다. 영상에 대한 워터마킹 기법에서는 현재 수백 비트의 정보를 숨길 수 있는 것으로 알려져 있다.
- 지금까지 충분한 강인성을 지닌 blind 워터마킹 기법이 존재하지 않는다. 특히, 기하학적인 변환에 강인한 기법을 개발하는 것이 매우 어려운 것으로 인식되고 있다.
- 워터마킹 기법이 invertable하다는 점이다. 이것은 워터마크의 일부 또는 전체의 노출은 지적 소유권의 보호를 위협한다. 그래서 공개기반 워터마킹 기술의 개발이 요구된다.

4.2 워터마킹 기술의 분류

- 워터마킹 기술은 세가지 관점에서 다음처럼 분류해 볼 수 있다.
- Blind와 Non-blind 기법 : Blind 워터마킹 기법은 워터마크의 검출시 원영상을 사용하는 방식인 반면 non-blind 기법은 그렇지 않은 방식이다.
- Public과 Private 기법 : Public 워터마킹 기법은 누구든지 워터마크를 검출할 수 있도록 한 방식인 반면, private 기법은 권한을 가진 사람만이 워터마크의 검출을 허용하는 방식이다.
- Readable과 Detectable 기법 : Readable 워터마킹 기법은 워터마크의 검출을 통해 코드화된 정보를 얻을 수 방식인 반면, detectable 기법은 단순히 특정 저작권자의 워터마크의 존재 여부를 확인할 수 있는 방식이다.

5. Spread Spectrum을 이용한 워터마킹 기법[4]

과거의 워터마킹 기술이 알고리즘의 비공개에 주로 의존해 온 반면, Cox의 방식[4]은 알고리즘을 공개할 수 있다는 점에서 기술적으로 큰 변화를 가져온 계기가 되었다. 암호화 기술에서도 암호화 알고리즘의 공개를 기반으로 하는 방식이 안전성을 높이거나 관리하는데 훨씬 큰 장점이 있다. 그래서 워터마킹 기술에서 이 방식의 출현

은 의미가 크다고 할 수 있다. 이 방식의 특징은 다음과 같다.

- 이 방식에 있어서 워터마크란 백색잡음(white noise)를 의미하고 이 백색잡음은 슈도랜덤수(pseudo-random number)이다. 이 슈도랜덤수를 발생시키는 seed가 워터마크를 찾아내는 키(key) 역할을 한다. 여기서 암호화 기술에서의 키와 같은 의미라고 볼 수 있다.
- 워터마크의 검출시 원영상의 차를 이용한다. 원영상의 차를 이용한다는 점은 올바른 저작권자를 증명하는데 실패하는 문제점을 가지고 있다.
- 시각적으로 중요한 부분에 워터마크를 삽입함으로써 워터마크를 제거하려는 해적의 공격이 있을 경우 영상의 화질이 크게 저하되도록 설계되었다.
- 신호의 크기에 비례하여 워터마크의 크기를 신축적으로 변화시킴으로써 눈에 잘 띄지 않도록 하였다.

위의 특징들 중 원영상의 차를 이용한다는 점에서 이 방식의 약점이 존재하지만, 이 방식은 현재 연구되고 있는 대부분의 워터마킹 기술에서 수정되어 사용되고 있다. 그래서 이 방식을 잘 이해하는 것은 현재 연구되고 있는 워터마킹 기술을 이해하는데 큰 도움이 될 것이다.

5.1 워터마크의 발생

워터마크 $w(n)$는 다음 식과 같이 자기상관성이 임펄스 함수를 갖는 백색잡음이다.

$$R_w(\tau) \equiv E[w(n+\tau)w(n)] = \sigma_w^2\delta(\tau) \qquad (1)$$

이 잡음의 분포는 워터마크를 설계하는 사람이 정할 수 있다. 대개의 경우 균일 분포나 가우시안 분포가 사용된다. 실제 워터마크는 C 라이브러리의 rand 함수를 이용하여 주로 발생시킨다.

5.2 워터마크의 삽입

워터마크의 삽입에 있어서 고려하여야 할 사항을 앞 장에서도 언급하였듯이 가장 중요한 것은 무감지성과 강인성이다. 우선 무감지성의 특성을 만족하기 위하여 워터마크의 크기는 영상의 신호에 비해 상대적으로 굉장히 작도록 설정하여야 한다. 즉, σ_w^2가 작도록 정해줘야 한다. 또한 원영상의 주파수 성분 중, 크기가 큰 주파수 성분에 워터마크의 크기를 크게 삽입하고 크기가 작은 주파수 성분에는 워터마크의 크기를 작게 삽입한다. 즉,

$$w'(n) = \alpha \mid X(n) \mid w(n) \qquad (2)$$

여기서 는 상수이고 $X(n)$은 워터마크를 삽입하고자 하는 영상 신호의 n번째 주파수 성분이다. 식(1)과 식(2)에서 편의상 워터마크와 영상신호를 1차원적으로 표현하였다. 식(2)에서 얻어진 워터마크 $w'(n)$이 실제로 신호의 삽입된다. 여기서 $w'(n)$의 σ_w^2는 α와 $|X(n)|$에 의해 결정된다.

그리고 워터마크가 삽입되는 주파수 영역은 해적의 공격에 강하고 공격이 가해졌을 때 영상 신호의 화질을 크게 손상시킬 수 있는 영역이어야 한다. 주파수 영역은 크게 저주파 대역과 고주파 대역으로 나누어 볼 수 있다. 고주파 대역에 워터마크가 삽입될 경우 해적의 공격으로부터 쉽게 워터마크가 제거될 수 있다. 가장 손쉬운 방법으로는 저대역통과필터를 사용하는 것이다. 또는 압축 알고리즘을 통해서도 쉽게 손상될 수 있다. 반면, 저주파 대역에 워터마크를 삽입할 경우, 워터마크를 제거하기 위해서는 저주파 대역에 왜곡을 가해야 한다. 이는 영상 신호의 주파수 성분들이

저주파대역에 집중되어 있어 영상 화질에 큰 저하를 가져온다. 그래서 Cox는 영상을 2차원 DCT를 수행한 후 저주파 대역이고 주파수 성분의 크기가 큰 N개의 성분에 대해 식(3)처럼 워터마크를 삽입하였다.

$$X'(n) = X(n) + \alpha \mid X(n) \mid w(n) \tag{3}$$

여기서 $X'(n)$은 워터마크가 삽입된 주파수 영역에서의 원영상 신호이다.

5.3 워터마크의 검출

워터마크의 검출은 워터마크가 삽입된 신호와 워터마크 사이의 상관성을 구함으로써 쉽게 이루어질 수 있다. 이는 워터마크가 자기 자신을 제외한 나머지 신호에 대해서는 상관성이 0인 것에 기인한다. 그림1는 워터마크의 검출을 도식적으로 나타낸 것이다. 예를 들어, 테스트하고자 하는 입력 신호를 $r(n)$이라고 하고 워터마킹된 영상 신호를 $X(n)+w(n)$이라고 하자. 이 때, 워터마킹된 신호가 일반적인 신호처리에 의해 왜곡이 일어난 경우, 입력 신호는 다음과 같이 쓸 수 있다.

$$r(n) = X(n)+w(n)+N(n) \tag{4}$$

여기서 $N(n)$는 왜곡 성분이다. 우선 입력 신호와 원영상 신호와의 차이를 구하고 이 차신호에 대해 워터마크와의 상관성을 구함으로써 상관 계수가 크면 워터마크가 검출된 것으로 결정하고 작을 경우 검출되지 않은 것으로 결정한다. 검출기의 출력은 다음과 같다.

$$\begin{aligned} O(n) &= \frac{1}{L}\sum_{n=0}^{L-1}[(X(n)+w(n)+N(n)) - X(n)]\cdot w(n) \\ &= \frac{1}{L}\sum_{n=0}^{L-1} w^2(n) + \frac{1}{L}\sum_{n=0}^{L-1} N(n)w(n) \end{aligned} \tag{5}$$

여기서 L은 워터마크의 길이이다. 윗 식의 두 번째 항에서 $N(n)$와 $w(n)$은 서로 상관성이 없으므로 상당히 작은 값을 가진다. 확률적으로 $E[\sum N(n)w(n)] = 0$ 이다. 그래서 워터마크의 길이가 충분히 길 경우, 즉, $L \to \infty$일 때, $\frac{1}{L}\sum N(n)w(n) \to 0$ 이다. 그래서 검출기는 워터마크가 존재하는지 그렇지 않은지를 검출한다. 검출 과정을 정리하면 다음과 같다.

1. 테스트하고자 하는 영상과 원영상을 DCT 변환한다.
2. 변환된 테스트 영상과 원영상의 차를 구한다.
3. 차영상과 워터마크 사이의 상관성 계수를 구한다. 이 상관성 계수로부터 워터마크의 존재 여부를 판단한다.

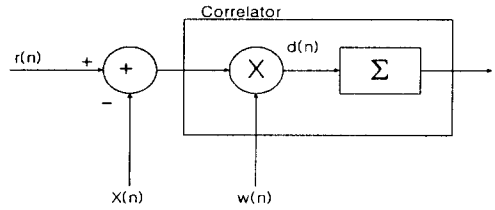


그림 1. 워터마크의 검출

6. 결 론

본 논문에서는 멀티미디어 저작물의 지적 소유권을 보호하기 위해 현재 활발히 연구가 진행중인 워터마킹 기술에 대해 살펴보았다. 해적으로부터의 공격에 강한 워터마킹 기술과 암호화 기술의 개발이 선행과제로서 중요하지만 인터넷이 구조적으로 보안상의 허점을 가지고 있으므로 이러한 기술들이 지적 소유권 보호를 완전히 해결해주지는 못한다. 이러한 소유권자의 권리를 보호하기 위해서는 기술 개발뿐만 아니라 제도적인 보완을 강화해야 할 것이다.

워터마킹 기술은 멀티미디어의 저작권 문제가 크게 대두되면서 많은 관심을 끌고 있다. 워터마

킹 기술은 키를 알지 못하면 컨텐트를 전혀 알 수 없는 암호화 기술과는 달리 키를 알지 못하더라도 그 컨텐트를 사용할 수 있으나 그 컨텐트의 조작이나 왜곡을 통해서도 삽입된 워터마크가 제거되지 않음으로써 저작권자가 언제든지 그 컨텐트에 대한 권리를 주장할 수 있다. 즉, 저작권자는 웹을 통해 자신의 권리 보호를 위해 자신의 컨텐트를 찾고 불법으로 사용되었을 경우 자신의 권리를 주장할 수 있다. 앞 장에서 살펴 보았듯이 워터마킹 기술에서 가장 중요한 요소는 무감지성과 강인성이다. 이 두 가지 요소는 서로 상충되는 관계에 있으므로 두 요소를 잘 만족하는 합의점을 찾아야 한다. 또한, 지금까지 연구된 기술은 해적의 공격에 상당히 약하므로 앞으로 많은 기술 발전이 있어야 현실적으로 멀티미디어 저작권 보호의 주요 역할을 할 수 있을 것으로 예상된다.

참 고 문 헌

[1] Barni et al., "DCT-domain system for robust image watermarking," Signal Processing.

[2] G. Braudaway, "Protecting publicly-available images with an invisible image watermark," Proceeding of ICIP'97, vol. 1, pp. 524-527, 1997.

[3] K. Ratakonda et al., "Digital image watermarking: issues in resolving rightful ownership," Proceedings of ICIP'98, pp. 414-418, 1998.

[4] I. Cox et al., "Secure spread spectrum watermarking for multimedia," IEEE Trans. On Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[5] G. L. Friedman, "The Trustworthy digital camera: restoring credibility to the photographic image," IEEE Trans. On Consumer Electronics, vol. 39, pp. 905-910, Nov. 1993.

[6] F. Mintzer et al., "Effective and ineffective digital watermarks," Proceedings of ICIP'97, vol. 3, pp. 9-12, 1997.

[7] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures," Proceedings of ICASSP'96, vol. 4, pp. 2168-2171, 1996.

[8] I. Pitas, "A method for signature casting on digital images," Proceedings of ICIP'96, vol. 3, pp. 215-218, 1996.

[9] A. Piva et al., "DCT-based watermark recovering without resorting to the uncorrupted original image," Proceedings of ICIP'97, vol. 1, pp. 520-523, 1997.

[10] J. J. O. Ruanaidh et al., "Phase watermarking of digital images," Proceedings of ICIP'96, vol. 3, pp. 239-242, 1996.

[11] S. D. Servetto et al., "Capacity issues in digital image watermarking," Proceedings of ICIP'98, pp. 445-449, 1998.

[12] M. D. Swanson et al., "Transparent robust image watermarking," Proceedings of ICIP'96, vol. 3, pp. 211-214, 1996.

[13] R. Wolfgang and E. J. Delp, "Watermark for digital images," Proceedings of ICIP'96, vol. 3, pp. 219-222, 1996.

[14] W. Zeng and B. Liu, "On resolving rightful ownerships of digital images by invisible watermarks," Proceedings of ICIP'97, vol. 1, pp. 552-555, 1997.

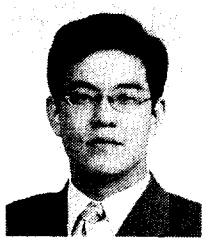
[15] J. Zhao and E. Koch, "Embedding robust labels into images for copyright protection," Proceedings of Intern. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, pp. 242-251, 1995.

노 철 균

• 1974년 서울대학교 전기공학과 (학사)
• 1983년 영남대학교 전기공학과 (석사)
• 1988년 영남대학교 전기공학과 (박사)
• 1980년~현재 경일대학교 제어계측공학과 교수
• 관심분야 : 회로 및 시스템, 바둑

정 연 기

- 1982년 2월 영남대학교 전자공학과 (학사)
- 1984년 2월 영남대학교대학원 전자공학과 (석사)
- 1996년 2월 영남대학교대학원 전자공학과 (박사)
- 1985년 3월~1990년 2월 가톨릭상지대학 전산정보처리과 조교수
- 1990년~현재 경일대학교 공과대학 컴퓨터공학과 부교수
- 1998년 1월~1998년 12월 호주 뉴캐슬대학교 전기 및 컴퓨터공학과 교환교수
- 관심분야 : 멀티미디어 통신, ATM/B-ISDN 기반의 초고속 정보 통신망, TMN/TINA 체계의 통신망 운용관리



배 상 욱

- 1985년 고려대학교 전기공학과 (학사)
- 1987년 단국대학교 전기공학과 (석사)
- 1994년 고려대학교 전기공학과 (박사)
- 1995년~현재 경일대학교 제어계측공학과 조교수
- 관심분야 : 지능제어, 패턴인식, 퍼지 및 신경망 이론 응용

임 성 운

- 1987년 경북대학교 전자공학과 (학사)
- 1991년 경북대학교 전자공학과 (석사)
- 1995년 경북대학교 전자공학과 (박사)
- 1995년~현재 경일대학교 제어계측공학과 조교수
- 관심분야 : 시스템 모델링 및 해석, 전동기제어, 전력변환

구 본 호

- 1980년 경북대학교 전자공학과 (학사)
- 1985년 경북대학교 전자공학과 (석사)
- 1991년 경북대학교 전자공학과 (박사)
- 1987년~1998년 한국전자통신연구원 선임연구원
- 1991년~현재 경일대학교 제어계측공학과 부교수
- 관심분야 : 컴퓨터제어, 전력전자, 센서공학, 전동기제어