공 학 석 사 학 위 논 문

미디어 콘텐츠 영상 복제 방지를 위한 SW 개발

2010년 5월

부경대학교 산업대학원

전산정보학과

박 봉 준

공 학 석 사 학 위 논 문

미디어 콘텐츠 영상 복제 방지를 위한 SW 개발

지도교수 김 창 수

이 논문을 공학석사 학위논문으로 제출함

2010년 5월

부경대학교 산업대학원

전산정보학과

박 봉 준

박봉준의 공학석사 학위논문을 인준함

2010년 8월 25일

주 심 이 경 현 (인)

위 원 김 종 남 (인)

위 원 김 창 수 (인)

목 차

표 목 차

그 림 목 차

The Software Development for Preventing Video Copy of Media Contents

Bong-Jun Park

Department of Computer and Information
Graduate School of Industry
Pukyong National University

Abstract

The popularization of the Internet has made to share data and exchange information easily, but because of the malicious web capabilities caused unauthorised copying of video content on the web and leaking to populace, these security incident occurs frequently nowadays. Moreover, a malicious user as a tool to the Web environment has been an incident such as unauthorized copying and spread out to the unauthorized person. For this reason, The content protection has become an important part of The company asset protection.

In this study is shown to prevent unauthorized copying methods about using both online and a bunch of media equipments for the use of digital content. Because digital

contents are very diverse, In this study is targeted video contents among a variety of digital content, movies, education (schools, institutes, companies) to restrain unauthorized copying of digital video contents, studying about preventing unauthorized copying for the following four kinds of environments. First, prevention of the copy program, Second, avoid the remote access program, Third, protection of copying content through the virtual machine, Finally, providing the way of copy prevention using external devices such as S-video jack. About presenting previous four kinds of techniques, this study presented implements module to be applied applicable in real life.

국문초록

인터넷이 대중화됨에 따라 손쉽게 자료를 공유하고 정보를 교환하게 되었지만, 악의적인 기능으로 웹상의 영상콘텐츠를 불법적으로 복제하여 유출하는 보안사고가 빈번히 발생하고 있다. 또한 기업이 구축한 고유의 콘텐츠 자산을 웹 환경을 이용해 악의적인 사용자가 무단 복제하여 유포하는 사고가 발생하고 있어 이에 대한 보호의 필요성이 대두되고 있다.

본 연구는 온라인과 다양한 미디어 장비를 활용한 디지털 콘텐츠의 활용에 대해 무단 복제를 방지할 수 있는 방법을 연구한다. 디지털 콘텐츠의 분류는 매우 다양하기 때문에 본 연구에서는 다양한 디지털 콘텐츠 중에서도 영화, 교육(학교, 학원, 기업) 분야의 영상 디지털 콘텐츠를 대상으로 한다. 이러한 디지털 영상 콘텐츠의 무단 복제방지를 위해 다음 4가지 환경에서 불법 복제를 예방하는 연구를 한다. 첫째는 복제프로그램 사용 방지이며, 둘째는 원격접속 프로그램 방지, 셋째는 가성머신을 통한 콘텐츠의 복제 방지, 마지막으로 S-Video 단자를 사용한 외부 기기에서의 복제 방지 기법을 제시하고 있다. 앞에서 제시한 4가지 기법에 대해 본 연구는 실생활에서 적용 가능한 모듈을 구현하여 현장에서 적용할 수 있도록 제시하고 있다.

I. 서 론

컴퓨터 기능의 고도화와 인터넷이 활성화되면서 다양한 분야의 콘텐츠들이 제작되어 제공되고 있다. 이러한 콘텐츠의 다양한 개발은 최근 스마트폰의 열풍과 함께 사용자를 고려한 편리한 것에서부터 고도의 지식을 필요로 하는 유형까지 매우 다양하다. 본 연구에서는 모바일 환경과 인터넷 환경에서 모두 사용가능한 고가의 콘텐츠를 대상으로 복제를 예방할 수 있는 방법에 대해 연구한다. 불법복제는 우리나라의 대부분의 IT관련 회사들이 열악한 환경에서 어렵게 개발된 지적소유권을 무단 복제하는 것은 기업경쟁력은 물론 국가 경재력에서도 문제가 되기 때문에 영상 콘텐츠의 불법 복제를 방지하는 것은 매우 중요한 연구분야이다. 아래 [표 1]은 200개 기업체를 대상으로 디지털 콘텐츠 장르별로 불법 복제율의 현황을 나타낸 것으로 음악(47.3%), 영상(47.6%), 만화(46.4%) 콘텐츠의 불법 복제율은 상대적으로 게임 콘텐츠(35.8%)와 교육 콘텐츠(39.4%)에 비해 높은 불법 복제율을 나타내고 있다. 그러나 실제 해당 콘텐츠를 제작/판매하는 업체에서 추정한 장르별 불법 복제율은 음악(52.5%), 영상(46.0%), 만화(58.1%)는 매우 높은 수준으로 나타나고 있으며, 게임(39.1%) 및 교육(28.8%)은 상대적으로 낮은 수치를 보여주고 있다.

불법복제에 대한 위의 현상에 대해 디지털 콘텐츠 무단복제 방지를 위한 기존의 여러 정책 및 대응에 대해서는 실제 효과가 있다는 의견이 11.0%에 불과하여 실제로는 부정적인 시각이 매우 높은 상

태의 결과를 보여주고 있다[1].

[표 1] 불법 복제율의 현황

구분	음악 콘텐츠	영상 콘텐츠	게임 콘텐츠	교육 콘텐츠	만화 콘텐츠
불법 복제율(%)	47.3	47.6	35.8	39.4	46.4
업체 추정율(%)	52.5	46.0	39.1	28.8	58.1

디지털 콘텐츠의 불법저작물의 무단 사용은 첫째, 저작권자들의 권리가 침해됨에 따라 창작의 요인이 감소하게 되어 저작권의 보호를 통한 새로운 저작물의 창작과 문화의 발전이라는 '저작권법'의 목표를 훼손시키는 부작용이 발생한다. 둘째, 불법저작물은 관련 콘텐츠산업의 신규 투자를 위축시키는 등의 부작용을 야기된다. 셋째, 불법저작물의 확산은 다양한 사회적 문제를 야기할 수 있는데, 저작권에 대한 인식이 부족한 청소년들의 저작권 침해행위에 대한 일부 법무법인의 과도한 고소 대행이 대표적인 것으로 사회적으로 문제가 야기된바 있다[2]. 따라서 기존에 불법복제 방지를 위한 여러 가지 기술들이 제공되고는 있지만, 여러 분야에 있어 보다 많은 피해가 우려되는 상황에서 지속적인 불법복제 방지를 위한 솔루션 개발은 기반 연구는 물론 현장에서 사용가능한 불법복제 방지 모듈 개발이 반드시 필요하다.

본 연구에서는 기존의 디지털 콘텐츠 보호를 위한 복제 방지에 대한 기반 기술을 알아보고, 다양한 디지털 콘텐츠 중에서도 고가

의 교육용 콘텐츠에서 문제가 되고 있는 모니터 영상 불법 복제 방지에 대한 몇 가지 해결 방법을 연구한다.

II. 선행연구

1. 기존 콘텐츠 보호를 위한 복제방지 기술들

가. 워터마킹 기법

디지털 워터마킹은 저작권 정보를 디지털 콘텐츠 속에 삽입시켜 소유자의 저작권을 보호하는 것을 목적으로 하는 기술로 콘텐츠에 대한 소유권 등을 판별할 수 있는 기술이다. 디지털 워터마킹의 주요 응용분야는 저작권 보호, 데이터 모니터링, 데이터 인증 등이다[3]. 디지털 워터마킹은 이미 상용제품에 응용되고 있으며, 그 기술은 현재에 이르기까지 꾸준히 사용되고 발전되어 왔다.

영상/비디오에 대한 워터마킹 기술은 공간영역[4][5]에서 주파수영역으로 그 대상 데이터를 변화시키면서 발전하여 왔으며, 최근에는 주로 주파수영역 데이터에 워터마킹을 수행하는 기술들이 발표되고 있다. 주파수영역의 워터마킹기술은 DCT(Discrete Cosine Transform)[6], DFT(Discrete Fourier Transform)[7] 또는 DWT(Discret Wavelet Transform)[8] 등의 변환을 이용하며, 특히 DCT 기반의 워터마킹 기술은 JPEG[9], MPEG[10], H.26X[11]계열의 압축시스템에 적용할 수 있어 지속적으로 연구되고 있다.

지금까지 연구된 워터마킹 기술의 경우 부분적으로는 임의의 공격에 견딜 수 있으며, 지각적으로도 양호한 결과를 보인다고 발표

되고 있다. 그러나 디지털 워터마킹 기법으로 음성이나 영상 관련 분야에서 지적재산권의 딜레마 문제를 해결할 수 있을 것으로 예측하고 있으나 기존의 워터마킹 기법으로 불법복제나 다양한 컴퓨터 활용 측면에서 가상머신, 사진 복사, 가상 IP 등에 대한 불법복제를 완전한 해결방법을 제시하지는 못하고 있다. 이러한 관점에서 영상 콘텐츠의 불법복제 예방을 위한 연구는 매우 광범위하고 매력적인 연구 분야이다.

다음은 본 연구와 관련이 있는 워터마크의 역사와 워터마크(watermark)의 정의, 워터마크의 응용분야, 워터마크 기법이 갖추어야 할 요건을 알아본다.

1) 워터마크의 역사

워터마킹(watermarking)기법은 스테그라노그라피(steganography) 기법의 구체화된 형태이며 “감추어져 있다”는 뜻의 그리스어 말인 ″stegano″와 “통신하다”라는 뜻의 “graphos″가 결합된 단어이다. 최초의 워터마크 기록은 종이에 새겨진 워터마킹 기법으로 약 700년 전으로 거슬러 올라가게 된다. 13세기 말 무렵에 이탈리아의 Fabriano에서는 약 40여 개의 제지공장들이 난립하고 있었다. 이들 공장에서 생산되는 종이는 형태나 질, 그리고 가격에서 있어서도 천차만별이었다. 그리고 이들 공장에서 생산되는 종이들은 완제품이 아니라 중간단계의 제품이었고, 중간단계의 종이는 공예가들이 후처리를 하여 최종적인 종이를 판매하게 되었다. 따라서 공예가들

은 각자의 제품에 대한 출처, 형태 및 종이의 질에 대한 정보를 가지는 고유한 워터마크를 종이에 삽입하게 되었고, 이러한 워터마킹 기술은 유럽 전체로 급속히 전파되었다[12].

본격적인 디지털 워터마크의 개념은 1990년대 초에 정립되었고, 최근에 널리 사용되고 있는 워터마크라는 용어는 1993년도에 Tirkel이 “water mark″라는 용어를 사용한 것이 계기가 되었다[13]. 이때부터 워터마킹 기법은 많은 관심을 끌게 되었고, 관련 기술도 급속도로 발전하게 되었다. [표 2]는 KRPIA에서 2004년 이전부터 2008년 이후까지 발표된 워터마킹과 관련되어 발표된 논문의 편수를 나타내고 있다. 표에서 발표된 논문 편수가 매우 급격하게 증가하고 있음을 확인할 수 있다.

[표 2] 디지털 워터마킹 기법과 관련된 논문 편수

연도	2004년 이전	2005년	2006년	2007년	2008년 이후
발표편수	177	15	23	34	62

2) 워터마크의 정의

디지털 워터마크는 디지털 데이터에 삽입된 후 검출되거나 추출될 수 있도록 원(source) 신호에 추가된 신호를 의미한다. 디지털 서명(signature)이라고 말하기도 하는 워터마크는 원신호의 매체에

가시성(visible) 또는 비가시성(invisible)의 신호를 추가함으로써 디지털 데이터에 삽입된 일종의 패턴으로써, 디지털 멀티미디어 저작물의 저작권 보호를 위해 제안되었다. 워터마크는 크게 2가지 형태의 기법이 있는데 가시성 워터마크와 비가시성 워터마크이다. 가시성 워터마크는 저작물의 소유를 가시적으로 명확히 나타나도록 표현하는 기법이며, 비가시성 워터마크는 원신호와 거의 구분할 수 없도록 저작물의 소유권을 은폐시키는 기법이다. 오늘날의 디지털 워터마킹 기법에 대한 연구는 대부분 비가시성 워터마크기법에 집중되고 있으며, MPEG(Moving Picture Experts Group), SDMI(Secure Digital Music Initiative) 등에서 표준화 기법을 규정하기 위한 연구가 진행되고 있다.

3) 워터마크의 응용

가) 가시성 워터마크를 이용한 콘텐츠의 지적소유권 보호

영상 데이터에 소유권자의 가시성 워터마크를 삽입하고 그 영상을 다른 목적에 사용하는 것을 금지하지 않는다. 여기서 가시성 워터마킹이란 영상 내에 소유권자의 마크를 눈에 띄기 쉽게 삽입하는 것이다. 예를 들어 영상에 자신의 이름을 크게 새기거나 회사의 로고를 눈에 띄게 삽입하는 것을 생각할 수 있다. 가시성 워터마크의 목적은 영상의 상업적인 사용이나 지적소유권을 쉽게 알리기 위함이다.

나) 인증을 위한 콘텐츠의 지적소유권 제어

방송사 기자가 뉴스 방송을 위해 디지털 카메라로 찍은 비디오가 있다고 생각해 보자. 이 비디오를 사용하기 전에 방송국은 이 비디오가 수정되었거나 변조되지 않았는지 검증하기를 원한다. 이러한 검증을 위하여 비가시성 워터마크가 카메라로 비디오를 찍을 당시에 자동적으로 삽입된다. 여기에 삽입된 워터마크는 이 비디오가 변조되지 않았음을 증명한다.

다) 무단 배포 방지

저작물을 구매한 소비자가 무료로 타인에게 저작물을 복사하여 제공할 수 있다. 이는 저작권자의 저작권료의 감소를 초래한다. 저작권자는 이를 방지하기 위하여 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.

라) 불법 배포자의 확인

저작권자는 무단 배포의 방지뿐만 아니라 무단 배포자가 누구인지 알기를 원할 것이다. 이를 위해서 저작물을 판매할 때 누구에게 판매하는지에 대한 정보를 비가시성 워터마크로 삽입한다. 불법 배포된 저작물이 적발되면 적발된 저작물에서 워터마크 검출을 통해 구매자의 정보를 알 수 있다. 이러한 정보는 저작권자는 구매자의 불법배포 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 한다.

4) 워터마킹 기법이 갖추어야 할 요건

가) 비지각성 (Imperceptibility)

몇몇 응용에서는 가시성 워터마크가 사용되지만 대부분의 응용에서는 비가시성 워터마크가 사용된다. 그래서 현재 워터마킹 기술에 대한 연구는 대부분 워터마크를 보이지 않게 또는 들리지 않게 영상이나 오디오 신호 속에 숨기는 방식들에 대한 것이다. 이것은 지적 소유권의 주장을 위해 워터마크를 삽입하면서도 서비스의 품질을 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.

나) 강인성 (Robustness)

디지털 형태의 음악, 영상, 비디오 등은 손실 부호화, 필터링, 크기변환(resizing), 대비강화(contrast enhancement), 클로핑(cropping), 회전(rotation) 등의 신호처리에 의해 쉽게 변형될 수 있

다. 워터마킹 기술이 그 기능을 발휘하기 위해서는 그 워터마크가 위와 같은 신호처리 후에도 검출이 가능해야 한다. 신호처리에 강인한 워터마킹을 위해서는 워터마크가 신호의 중요한 부분에 삽입되어야 한다는 것이 일반적인 경향이다. 워터마크가 삽입된 데이터에 대한 공격(attack)은 원신호에 큰 변형을 주지 않고 워터마크만을 제거하려는 데 그 목적이 있다. 그래서 대개의 경우 저대역 필터(lowpass filter)를 사용하거나 압출과정을 수행 후 고주파 성분을 제거하는 방법으로 공격이 이루어질 것으로 예상된다. 따라서 신호의 중요부분에 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 편이기 때문에 많은 보완이 필요하다. 워터마킹 기술이 영상, 오디오, 비디오와 같은 멀티미디어 저작물에 대한 지적 소유권 보호를 위해 성공적으로 적용되기 위해서는 강인성이 무엇보다 중요하다.

다) 삽입될 수 있는 정보의 양

워터마킹 알고리즘들은 대개 수동적으로 정한 일정량의 정보를 삽입하게 된다. 그러나 자동적으로 비지각성과 강인성 등의 특성을 만족하면서 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 위

해서는 삽입되는 정보의 양이 충분히 클 수 있어야 한다.

나. DRM 기법

디지털 콘텐츠의 불법복제에 따른 문제를 해결하고, 저작권자의 권리를 보호하기 위해서 제안된 기술이 DRM(Digital Rights Management)이다. 이는 콘텐츠의 불법복제를 방지하고 지정된 사용자에게 허가된 범위 내에서 콘텐츠를 사용하게 하여 디지털 콘텐츠의 안전하고 투명한 유통을 가능하게 하는 기술이다. 현재 DRM 기술은 인터넷 방송, 모바일 기기, UCC 서비스, 문서보안 등 이미 다양한 분야에서 활용되고 있다. 다음은 DRM의 정의와 DRM시스템의 요구사항, DRM의 구조, 대표적인 DRM 시스템에 대해 설명하고자 한다.

1) DRM의 정의

DRM이란 디지털 콘텐츠의 불법 유통과 복제를 방지하고, 적법한 사용자만이 콘텐츠를 사용할 수 있도록 불법 콘텐츠 사용을 제한하고 정당한 사용자의 권리는 물론 저작권자의 권리와 이익을 보호하기 위한 불법 유통을 관리하기 위한 매우 중요한 보안관리 기능이다. DRM은 크게 두 가지의 형태로 구분할 수 있다. 하나는 콘텐츠를 정당한 권리를 가진 사용자에게만 안전하게 전송하고 허가된 사용범위 내에서 사용하게 제한하는 방법이다. 다른 하나는 불법으로 콘텐츠가 복제되어 유포됐을 때, 해당 콘텐츠의 저작권자가 누

구인지를 증명하고 어떤 경로를 통하여 불법 복제되고 유통되었는지를 추적하는 기능이다.

2) DRM 시스템의 요구사항

가) 지속적인 보호

DRM의 가장 기본적이며 중요한 기능은 지적 자산의 완벽한 보호이다. 배포된 콘텐츠 중 단 하나만이라도 보호되지 못한다면 그 피해는 심각하기 때문이다. 이를 위해 DRM은 허가되지 않은 사용자의 콘텐츠 접근을 차단해야 하며, 접근 권한을 가지고 있는 사용자라 할지라도 부여된 권한 내에서만 콘텐츠를 사용할 수 있도록 통제해야 한다. 또한 콘텐츠가 악의적인 사용자에 의해서 무단 변경되는 것을 막아야하며, 콘텐츠 배포과정에서의 무결성과 비밀성을 보장해야 한다. 콘텐츠를 관리하는 DRM 에이전트는 공격으로부터 강인성을 유지할 수 있어야 한다.

나) 사용 편리성

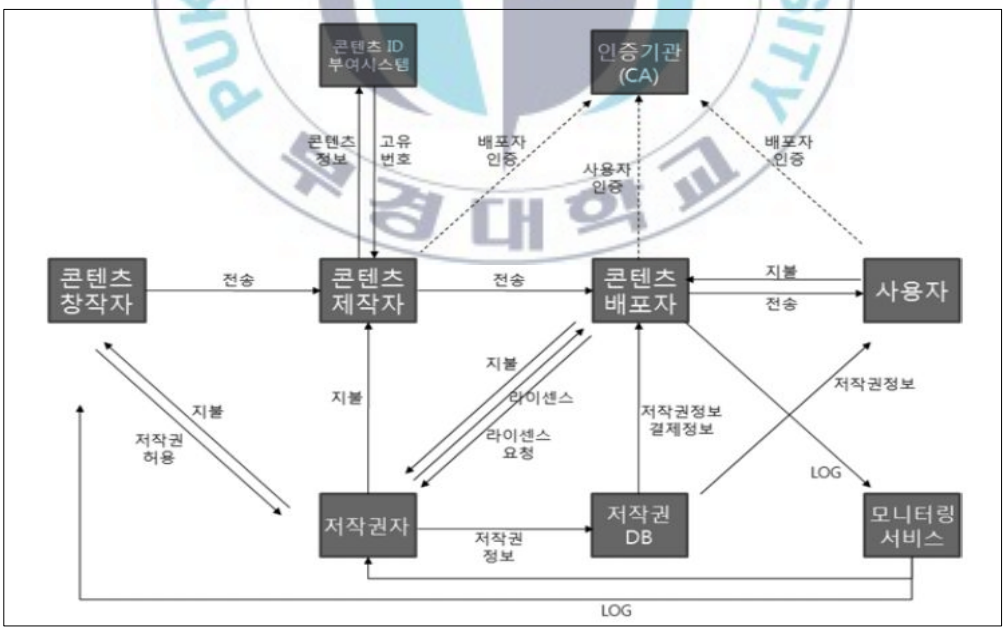
DRM은 콘텐츠의 저작권 보호를 위해 사용자에게 불편을 초래해서는 아니 된다. DRM의 보안성을 강화하다 보면 사용자의 편리성은 떨어질 수밖에 없다. 하지만 그렇다 할지라도 사용자가 디지털 콘텐츠를 쉽게 검색하고 얻을 수 있어야 하며, 허용된 권리 내에서는 자유롭게 콘텐츠를 사용하는 것을 보장해야 한다.

다) 유연성

DRM은 문서, 멀티미디어 콘텐츠, 웹 기반의 콘텐츠, 소프트웨어 그 밖의 디지털콘텐츠 등 여러 종류의 디지털 콘텐츠 형식이라도 지원할 수 있어야 한다. 또한, 여러 종류의 DRM간의 연동을 통해서 DRM 시스템의 상이함으로 인해 발생하는 사용자의 권리 제한 문제를 해결해야 한다.

3) DRM 구조

<그림 1> 은 디지털 콘텐츠 유통의 일반적인 유형을 나타낸다. 아래 그림은 디지털 콘텐츠의 일반적으로 유통 프로세스를 나타낸 것으로 어떤 부분에서는 생략된 형태가 고려될 수 있다.



<그림 1> 멀티미디어 콘텐츠 유통 모델

a. 패키징(packaging) - 패키징은 보호된 콘텐츠를 만들기 위해 디지털 콘텐츠를 암호화 하는 과정이다. 일반적으로 대칭키 암호화 시스템을 사용한다. 암호화된 디지털 콘텐츠는 추가적으로 저작권 정보, 미디어 정보를 포함하고 있는 메타데이터를 가지고 있다. 일반적으로 헤어 파일은 암호화 되지 않으며 여기에는 라이선스를 얻어 올 수 있는 URL정보가 포함된다.

b. 유통(distribution) - 패키징된 디지털 콘텐츠를 소비자에게 분배하는 과정이다. 콘텐츠는 비즈니스 모델에 따라 웹서버, 스트리밍 서버, 혹은 CD나 DVD 같은 매체를 통해서 사용자에게 전달된다.

c. 라이선스 발급 및 획득 - 라이선스 서버가 디지털 콘텐츠를 구매한 정당한 사용자에게 라이선스를 발급하는 과정이다. 이러한 과정은 사용자를 인증하는 것으로부터 시작된다. 라이선스에는 디지털 콘텐츠 사용 규칙과 콘텐츠 암호화키가 들어 있다.

d. 콘텐츠 사용 - 사용자가 자신이 가지고 있는 DRM에이전트를 이용해서 배포 받은 디지털 콘텐츠와 획득한 라이선스를 이용해서 디지털 콘텐츠를 사용하는 과정이다. 이때 사용자는 주어진 권한 내에서만 콘텐츠를 사용하도록 에이전트에 의해서 관리되어진다.

4) 대표적인 DRM 시스템

[표 3]에서와 같이 대표적인 DRM 시스템으로 Microsoft사의 WMDRM을 들 수 있다. 이는 Windows media 형식의 디지털 콘텐츠의 보호를 위한 DRM으로 콘텐츠 소유자, 라이선스 서버 그리고

사용자 PC에 설치된 플레이어 사이에 적용된다. WMDRM은 라이선스와 미디어가 각각 분리되어 배포되며, 라이선스의 조건 변경이 쉽고, 대여나 회원제 형태의 비즈니스 모델을 적용하거나, 미리보기의 제한 등의 세부 기능이 있어 유연한 DRM 시스템의 사용이 가능하다. mp3플레이어인 애플의 iPod에 사용되는 DRM인 Fair-Play는 iTunes라는 애플사의 음악다운로드 서비스와 iPod를 연결하는 DRM으로 다른 웹서비스나 다른 디바이스간의 연동을 허락하지 않는 성격을 가지고 있다.

[표 3] 대표적인 DRM 시스템

이름	사용	년도	특성
FaiaPlay	iTunes Library, iPod	2003	구매된 음악 파일은 AAC 형태로 인코딩되고 이러한 형식은 iTunes와 iPod에서만 사용 가능함
Janus WMA DRM	All laysForSure Devices	2004	janus는 휴대용 장치를 한 Windows Media DRM의 버전임
OMA DRM	550여개이상의 핸드폰	2004	Open Mobile Alliance에 의해서 개발된 DRM 시스템으로모바일 기기 상의 콘텐츠를 보호한다.
3-day-or-3-play	Microsoft Zune	2006	다른 Zune 장치에서 무선으로 받은 음악파일을 장치에서 오직 3번만 재생가능하며, 재생 여부와 관계없이 3일이 지나면 만료되는 방식.

IBM은 Cryptolope라는 암호화 패키징 제품을 이용한 디지털 뮤직 저작권 보호 기술인 EMMS(Electronic Media Management System)을 개발 하였으며 xCP(eXtensibile Content Portection)이라는 전략을 이용 좀 더 유연한 DRM시스템을 개발하고 있다. 또한

Adobe사는 acrobat을 이용 문서의 암호화와 전자서명, 접근권한 설정 등을 지원하고 있다[14].

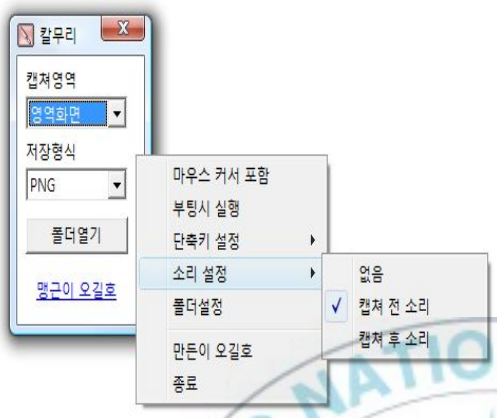
기존 DRM 기술의 문제점으로는 첫 번째 상호 호환성의 부재이다. 즉, 서로 다른 콘텐츠 제공자들은 각기 다른 DRM시스템을 사용하고 있다. 따라서 인식할 수 없는 DRM시스템으로 보호된 콘텐츠는 동작 할 수 없는 경우가 종종 발생할 수 있다. 두 번째로 새로운 시스템의 채택이 용이하지 않다는 점이다. 기존에 많은 DRM 시스템은 시간이 지나면 깨어질 가능성이 있으므로 새로운 시스템으로 쉽게 대치될 수 있는 유연성을 가지고 있어야 한다[15].

2. SW을 이용한 복제 기법들

가. 복제프로그램을 이용한 복제 기법

모니터 영상 복제 프로그램은 컴퓨터의 화면과 사운드를 복제하여 동영상을 만드는 프로그램으로, <그림 2>의 칼무리, <그림 3>의 Camtasia와 같은 동영상 복제 프로그램이 있으며[16], The KMPlayer, 안카메라[17], Snaglt, 오픈캡쳐 등 수많은 동영상 복제 프로그램이 유포되고 있으며, 개인적으로 필요한 작업 때문에 사용하는 경우 외에 동영상을 복제하는데 불법적으로 이용되고 있다. 그리고 이러한 불법복제에 대해 개인 블로그, 카페, 개인 사이트 등에서 어떤 방법으로 사용할 수 있는지 등이 소개되고 있어 소프트

웨어 저작권자들의 경쟁력을 약화시키는 문제점을 가지고 있다.



<그림 2> 칼무리 캡쳐프로그램

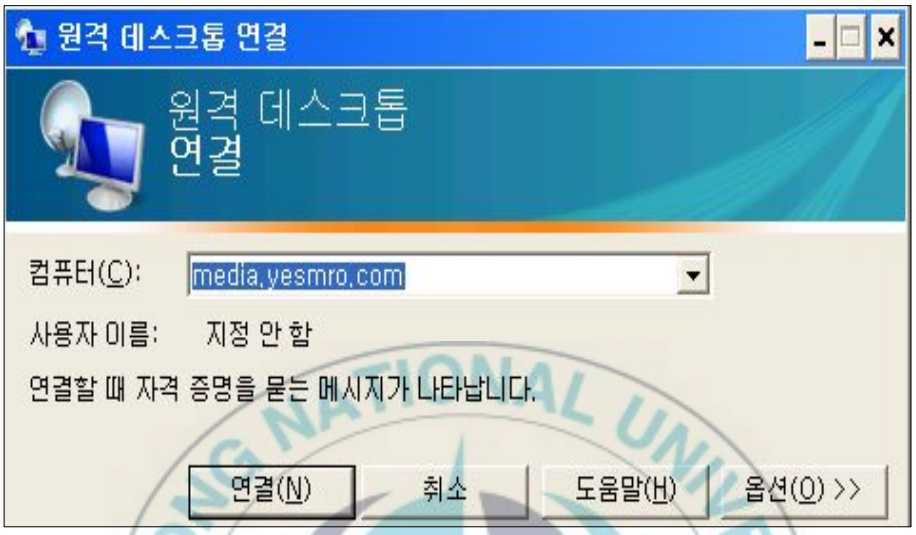
<그림 3> Camtasia 캡쳐프로그램

나. 원격접속 프로그램을 이용한 복제 기법

원격 데스크톱으로 다른 컴퓨터로 접속하여 동영상을 플레이하고 복제프로그램은 접속한 컴퓨터에서 실행하여 원격지 컴퓨터에서 실행되고 있는 동영상을 복제하는 방법이다.

<그림 4>에서와 같이 공개되어 있는 원격 데스크톱 프로그램을 다운받아서 로컬 컴퓨터에서 설치를 한다. 원격 데스크톱 프로그램을 실행하여 원격지 컴퓨터 화면을 보려면 우선 원격지 컴퓨터에 대한 IP주소나 도메인을 알아야한다. 그 주소를 입력해야 연결이 되며, 원격지 컴퓨터를 실행 시킨 후, 원격지 컴퓨터 화면에서 복제하고자 하는 동영상을 <그림 5>과 같이 실행을 하면서 동시에 접속한 컴퓨터에서 복제프로그램을 실행하여서 동영상을 복제하는 기

법이다.

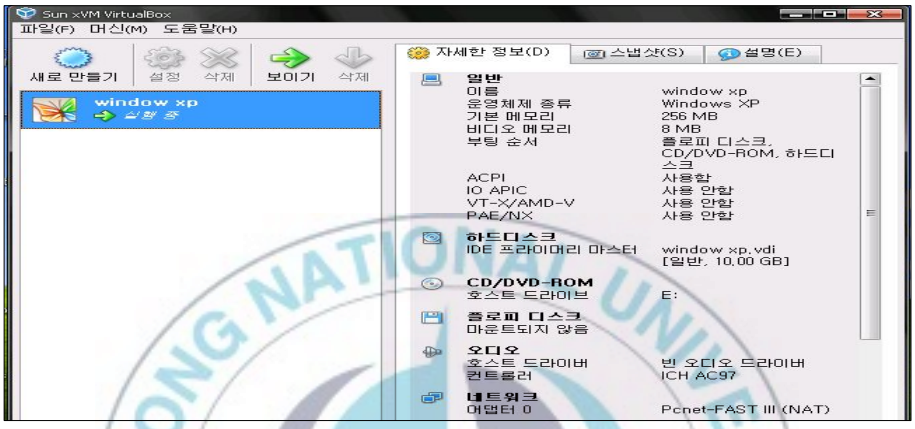


<그림 4> 원격 데스크톱 연결 프로그램

<그림 5> 원격접속 프로그램으로 복제하는 화면

다. 가상머신(OS)을 이용한 복제 기법

가상머신이란 <그림 6>와 같은 가상머신 프로그램을 실행해서 로컬 컴퓨터 안에 또 다른 운영체계를 설치하여 하나의 컴퓨터에



<그림 6> Sun xVMVirtualBox 가상머신프로그램

두 가지의 운영체계 시스템이 별도로 가동이 되는 것으로, 하나의 컴퓨터에 두 개 이상의 컴퓨터를 따로 실행할 수 있다. 화면상으로 보면 원격접속을 이용해서 원격지 컴퓨터를 실행한 모습과도 유사하다고 하겠다. 그러나 가상머신을 이용한 복제는 원격접속 기법과는 달리 자신의 컴퓨터에 또 다른 하나의 컴퓨터를 더 설치하는 기법으로 원격 컴퓨터에 대한 접속 정보 등은 없어도 무방하며, 원격지 컴퓨터의 사양에 따라 복제 성능이 좌우가 될 수 있지만, 가상머신 기법에서는 로컬 컴퓨터 자체 사양에 따라서 복제 성능이 좌우가 된다. 로컬 컴퓨터의 사양이 좋으면 복제 성능에도 좋은 영향을 가지게 된다.

<그림 7>과 같이 가상머신 프로그램을 실행하여 하나의 컴퓨터에서 두 개의 운영체계가 실행되고 있으며, 하나의 운영체계 내에

서 복제하고자 하는 동영상을 플레이하여 다른 운영체계 화면에서 복제프로그램을 동작하여 복제를 하는 장면이다.

<그림 7> 가상머신을 통한 영상 복제하는 화면

III. 미디어 콘텐츠 영상 복제방지 설계구현

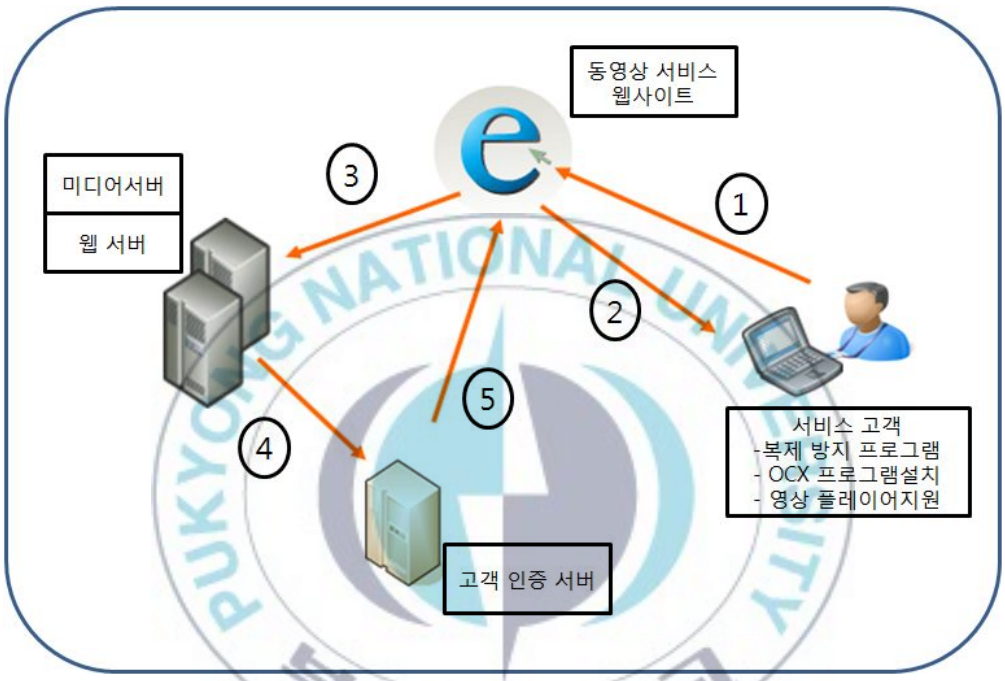
인터넷 웹 사이트에서 서비스나 실행되어 지는 동영상을 복제하는 방법으로는 첫째는 일반적인 방법으로 복제 프로그램을 사용하는 것이 있고, 두 번째는 원격접속 프로그램을 이용하여 복제하는 방법이 있으며, 세 번째는 가상머신을 이용하여 복제하는 방법이 있으며, 마지막으로 S-Video 단자를 이용하여 복제하는 방법이 있다. 일반적으로 미디어 콘텐츠 영상에 대해 복제를 방지하는 방법으로 첫 번째 방법인 복제 프로그램을 사용하지 못하도록 하는 것이 일반적으로 적용되고 있으며, 다른 방법에 대해서는 적용이 미비한 상태이다.

본 연구에서는 위의 일반적인 방법을 포함한 나머지 3가지 방법에 대해서 복제를 예방할 수 있는 시스템을 개발하였다. 복제프로그램을 방지하는 하는 모듈과 원격접속 프로그램을 이용한 불법복제를 방지할 수 있는 모듈과 가상머신 및 S-Video 단자를 이용한 불법복제 방지 등을 포함한 시스템 구성 및 처리되어지는 기법에 대해 설명한다.

1. 복제 방지를 위한 시스템 구성도

원격접속 프로그램으로 복제하는 방법에 대한 방지 모듈은 <그림 8>에서와 같이 복제 방지 S/W인 사용자 OCX-Player 프로그

램과 동영상을 관리하는 미디어서버, 고객의 정보 및 동영상 서비스를 제공하는 웹서버, 마지막으로 정상적인 서비스 유무를 점검하는 고객 인증 서버로 구성이 된다.



<그림 8> 복제 방지 서비스 시스템 구성도

1-1) 회원가입 및 복제 방지 프로그램 설치

<그림 8>의 시스템 구성의 흐름도를 보면 ①번 플로우에서 서비스 고객이 동영상 서비스 웹사이트에 회원 가입을 하고, ②번 플로우에서 사이트에서 제공하는 OCX 프로그램을 설치를 하면, 자동을 복제 방지 프로그램이 설치가 되고, 영상을 볼 수 있는 자체 개발한 플레이어가 설치가 된다. 복제 방지 프로그램에는 기본적으로 시중에 배포되어 있는 복제 프로그램들과 원격 접속 프로그램, 가

상머신에 대한 정보를 데이터베이스화하여 저장되어 있으며, 지속적으로 추가 프로그램들에 대한 정보를 추측해 나간다.

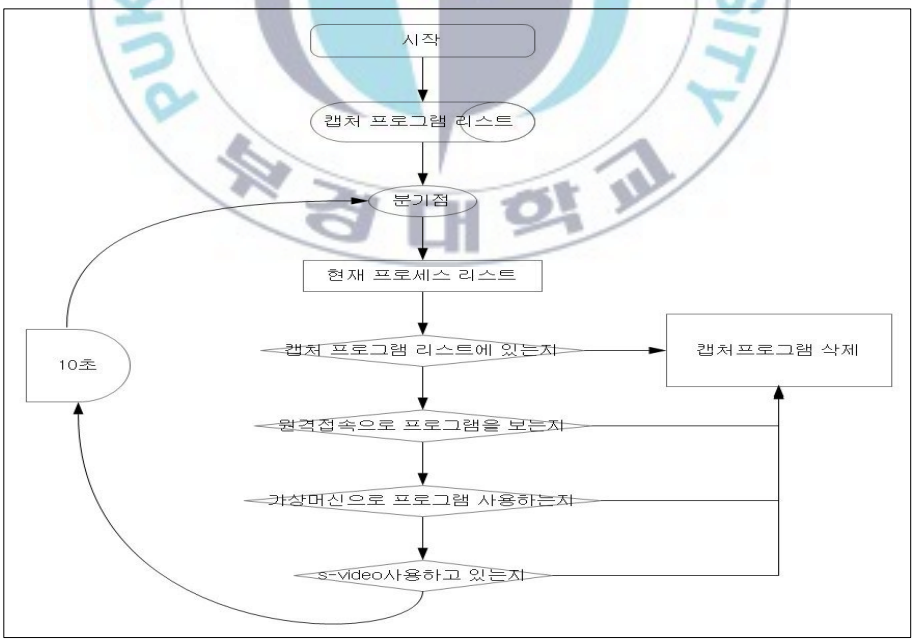
1-2) 복제를 시도할 시 처리 플로우

①번 플로우에서 동영상 서비스 사이트에 접속한 후 ③번 플로우를 통해 동영상 서비스를 제공을 받아 동영상 플레이어로 영상을 청취하면서, 만약 복제 프로그램 및 원격접속 프로그램, 가상머신 프로그램을 실행 시켜 복제를 시도하면, 복제 방지 프로그램에서 감지하거나 접속 경로가 정상적이지 못 할 경우에 ④번 플로우를 통해 고객 정보 및 감지 내용을 저장하고, 복제하려는 고객 화면을 증거 자료로 사용하기 위해 자동으로 다섯 정도의 이미지를 캡쳐해서 저장한다. 그런 후 ⑤번 플로우를 통해서 고객에서 복제 관련 프로그램 및 가상 머신이 작동한 것을 통보하고, 동시에 복제 관련 프로그램 및 가상 머신 프로그램의 작동을 차단시킨다.

1-3) 복제 방지 프로그램 기능

<그림 9>의 복제 방지 시스템 흐름도에서 보는 것과 같이 서비스 고객에게 설치되는 복제 방지 프로그램인 사용자 OCX-Player가 처리하는 기법은 1) 상용되고 있는 동영상 복제 프로그램을 데이터베이스화 하여 실시간으로 복제 프로그램이 구동하는지 여부를 감시하여 구동 시에 경고 메세지를 보내고, 동영상 서비스를 중단하여 복제되는 것을 방지한다. 2) 원격접속 프로그램을 이용하여 동영상을 복제하는 것을 감시한다. OCX-Player에서 실시간으로 원격

접속 프로그램의 사용 여부를 감시하여 원격접속 프로그램이 감지가 되면 동영상 서비스를 중단하여 복제되는 것을 방지한다. 3) 가상머신을 이용하여 동영상을 복제하는 것을 감시한다. OCX-Player에서 실시간으로 가상머신 사용 여부를 감시하여 가상머신이 감지가 되면 동영상 서비스를 중단하여 복제되는 것을 방지한다. 4) s-video 단자 사용유무 검사를 실시간으로 감시를 하여, 관련된 프로그램 및 프로세서가 가동할 시에 동영상 서비스를 중단하고, 실행되는 프로그램 및 프로세서를 차단을 시켜 불법으로 복제되는 것을 방지하도록 되어있다. 5) 인증모듈을 통해서는 정상적인 접속 경로로 미디어서버에 접속하는지 여부를 서버 주소 아이피와 포트 정보를 통해서 분석하여 인증여부를 결정한다. 인증을 받은 후에만 서비스를 정상적으로 받을 수 있도록 한다.

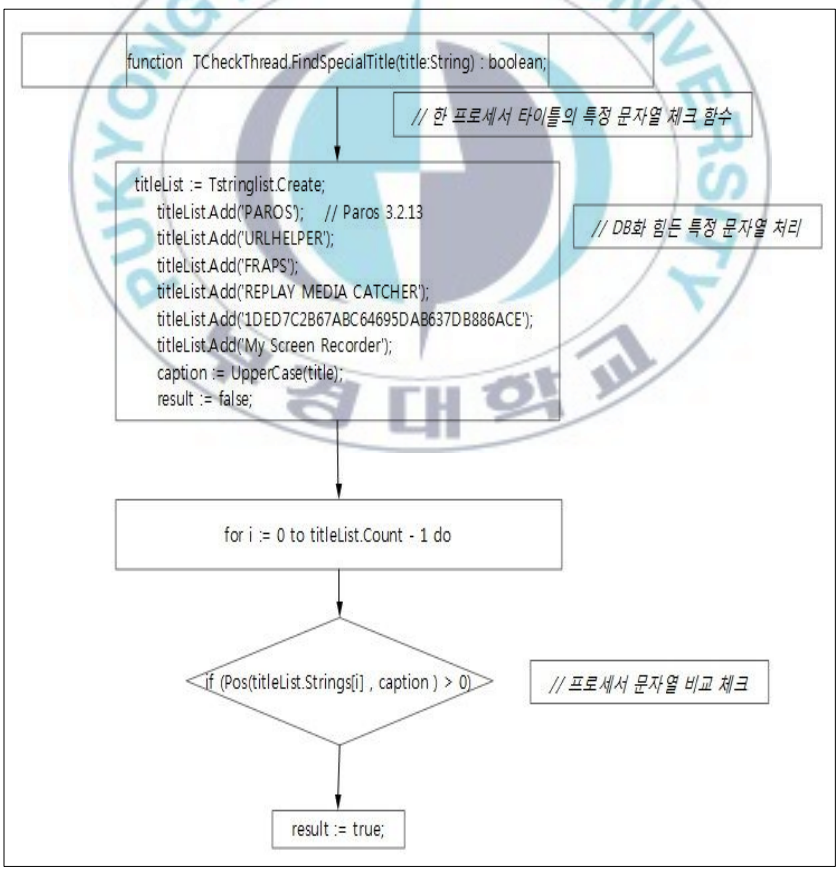


<그림 9> 복제 방지 시스템 흐름도

2. 복제 방지를 위한 모듈별 프로그램 기법

2-1) 복제 프로그램 처리 프로그램

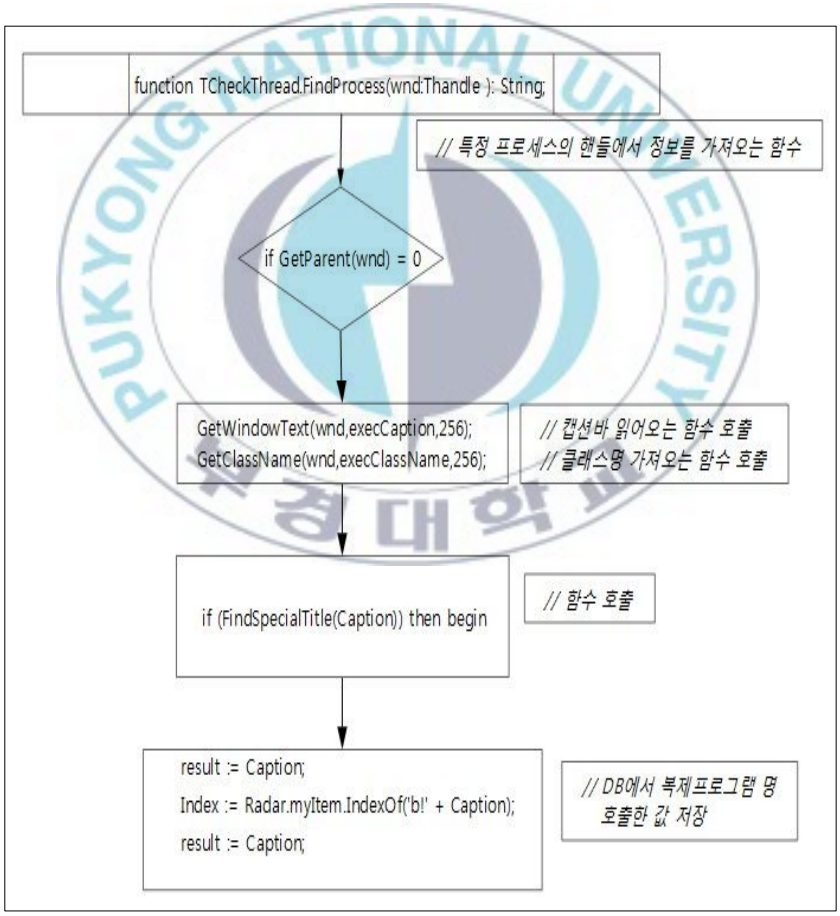
복제 프로그램은 수시로 개발되어 배포가 되기 때문에 데이터베이스화해서 처리를 해야 한다. 따라서 본 논문은 <그림 10>과 같이 다양한 사이트에서 개발된 특정한 복제 프로그램을 서버 시스템에 등록하여 처리할 수 있도록 개발하였다. 아래 흐름도는 복제 프로그램의 리스트에 등록된 이름이 발견될 경우 복제 프로그램의 실행을 금지하도록 처리하는 과정을 나타내고 있다.



<그림 10> 복제 프로그램 등록 처리

2-2) 복제 프로그램 처리 프로그램

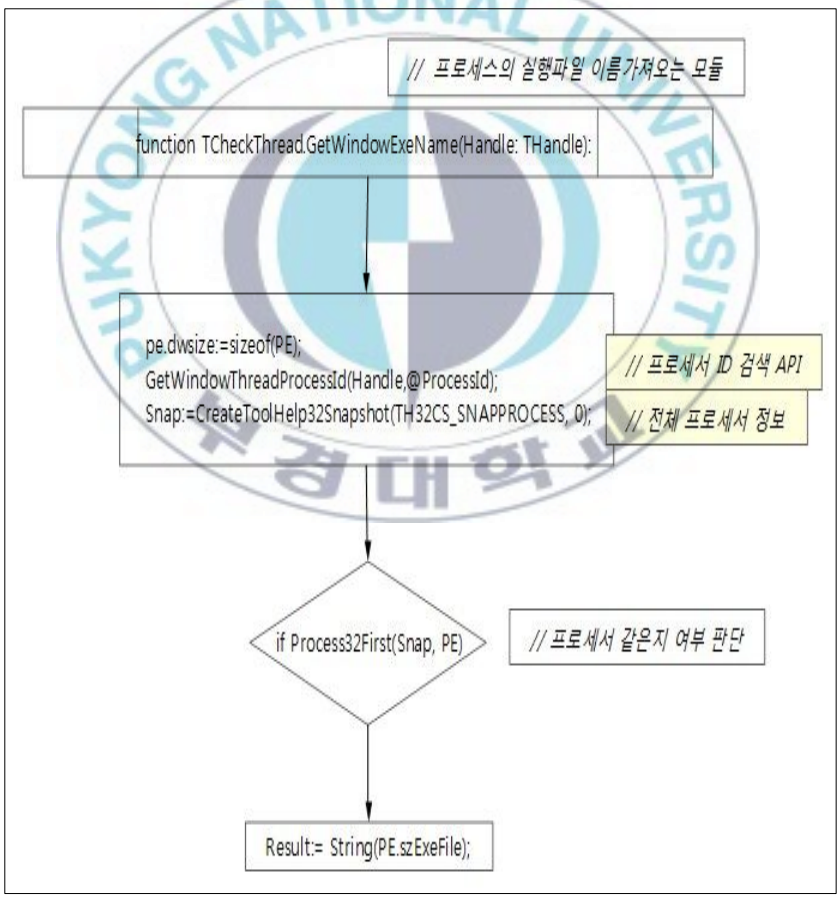
데이터베이스화 되어진 복제 프로그램 목록을 참조하야 현재 실행되어지는 동영상 서비스의 컴퓨터에서 복제 프로그램의 프로세서가 실행되고 있는지의 여부를 실시간으로 검색 및 처리하는 과정이 필요하다. <그림 11>과 같이 복제 프로그램의 프로세서를 실시간으로 검색 및 처리하는 과정을 나타내고 있다.



<그림 11> 복제 프로그램 명 호출 처리

2-3) 프로그램 프로세스 감지 처리 프로그램

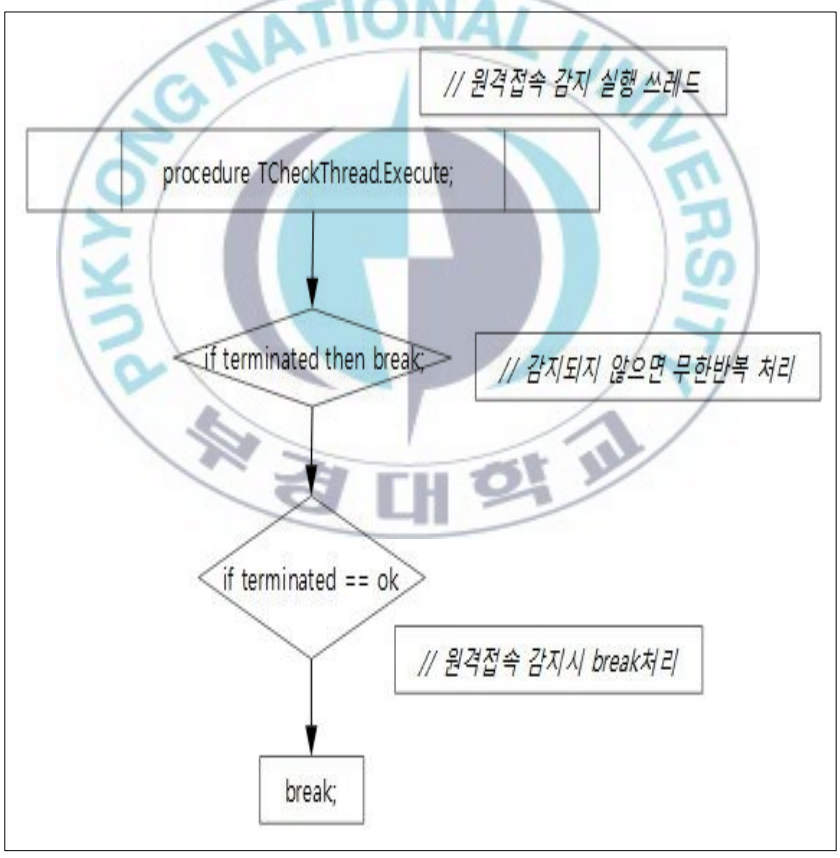
복제 프로그램만 데이터베이스화 하는 것이 아니라, 원격접속 프로그램과 가상머신 프로그램에 대해서도 데이터베이스화 작업을 하여 구축을 해야 한다. 따라서 본 논문은 <그림 12>와 같이 복제 프로그램의 프로세서뿐만 아니라 원격접속 프로세서와 가상머신 프로세서에 대해서도 감지하여 처리할 수 있도록 개발하였다. 아래 흐름도는 각 종 프로그램의 프로세서들이 발견될 경우 복제 프로그램의 실행을 금지하도록 처리하는 과정을 나타내고 있다.



<그림 12> 프로세서 실행 파일 검색 처리

2-4) 원격접속 감지 처리 프로그램

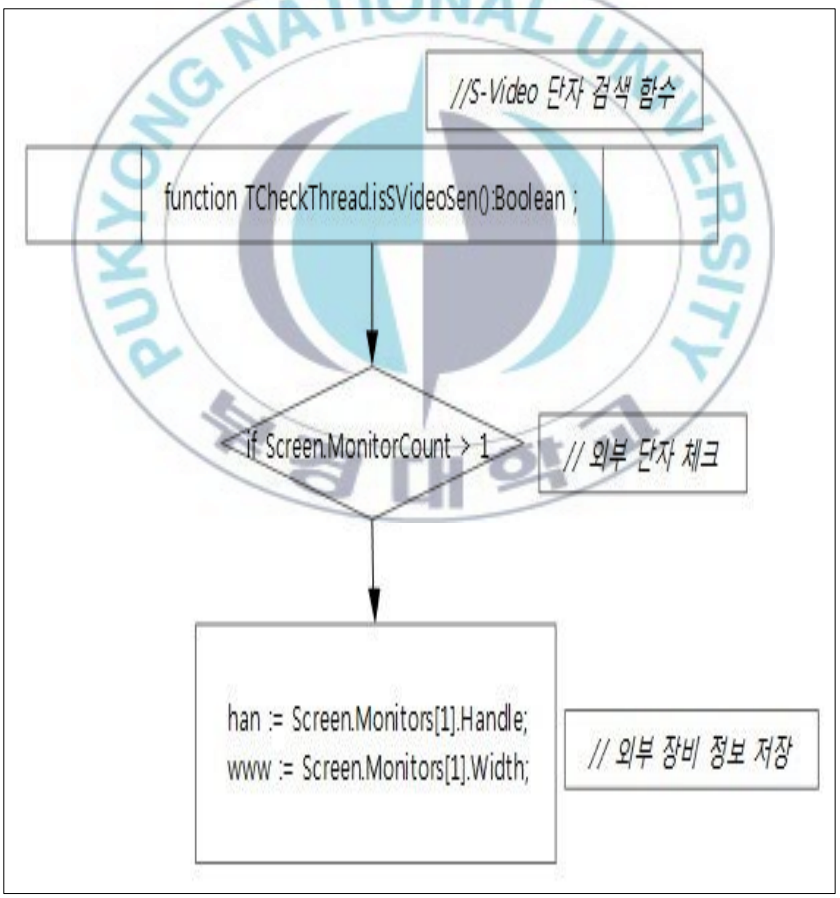
일반 고객이 자신의 컴퓨터에서 동영상 서비스를 받고 있는 동안 동영상 서비스를 받고 있는 컴퓨터 내에 원격으로 접속하는 프로세서가 있는지를 Termiated API를 이용하여 무한반복하며 실시간으로 감지하도록 개발한 프로그램이 <그림 13>과 같이 구현되고 있다. 아래 흐름도에서 원격접속이 발견될 경우 원격접속 프로그램의 실행을 금지하도록 처리하는 과정을 나타내고 있다.



<그림 13> 원격 접속 감지 처리

2-5) S-Video 단자 감지 처리 프로그램

동영상 서비스를 받고 있는 동안 동영상 서비스를 받고 있는 컴퓨터 내에 외부의 S-Video 단자를 사용하여 복제를 할 수 있으므로 S-Video 단자로 접속하는 프로세서가 있는지를 Screen API를 이용하여 실시간으로 감지하도록 개발한 프로그램이 <그림 14>과 같이 구현되고 있다. 아래 흐름도에서 외부단자의 개수를 실시간으로 점검하여 발견될 경우 외부단자의 실행을 금지하도록 처리하는 과정을 나타내고 있다.



<그림 14> S-Video 외부 단자 감지 처리

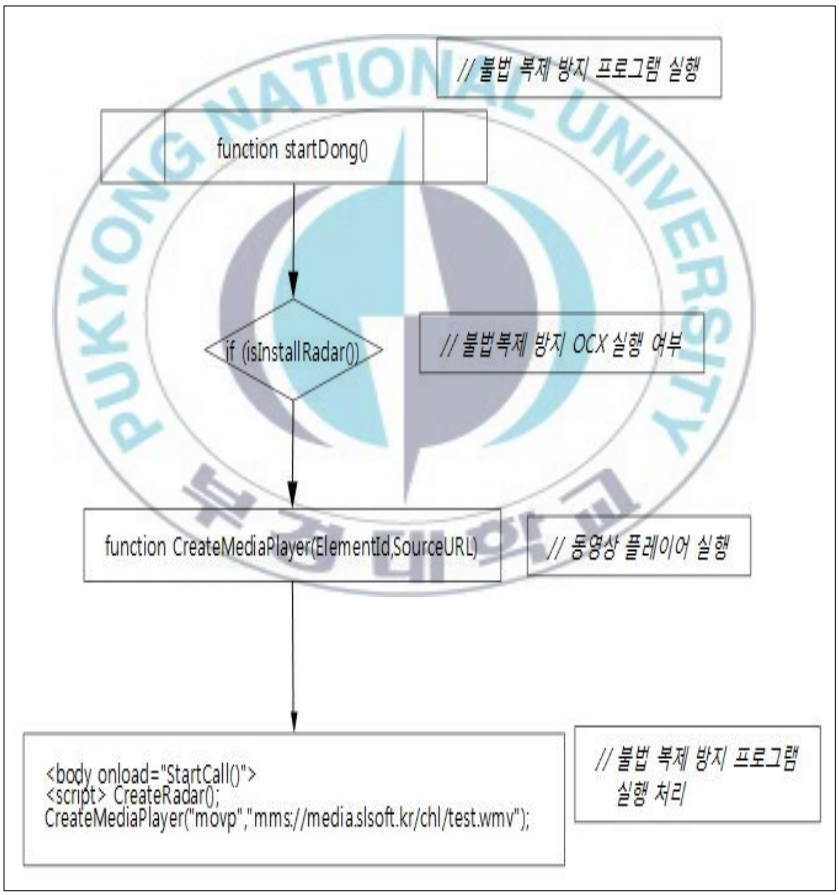
2-6) 가상머신(OS)실행 유무를 감지 처리 프로그램

<그림 14>와 같이 가상머신의 실행 유무를 감지할 때에는 Registry를 이용하여 개발하였다. 가상머신 프로세서의 특성을 분석하여 특정한 값을 적용하여 감지하는 방식으로 아래 흐름도에서 Registry의 유무와 키 값을 감지하여 가상머신이 발견될 경우 가상머신프로그램의 실행을 금지하도록 처리하는 과정을 나타내고 있다.

<그림 15> 가상머신(OS) 감지 처리

2-7) 복제 방지 프로그램 실행 HTML

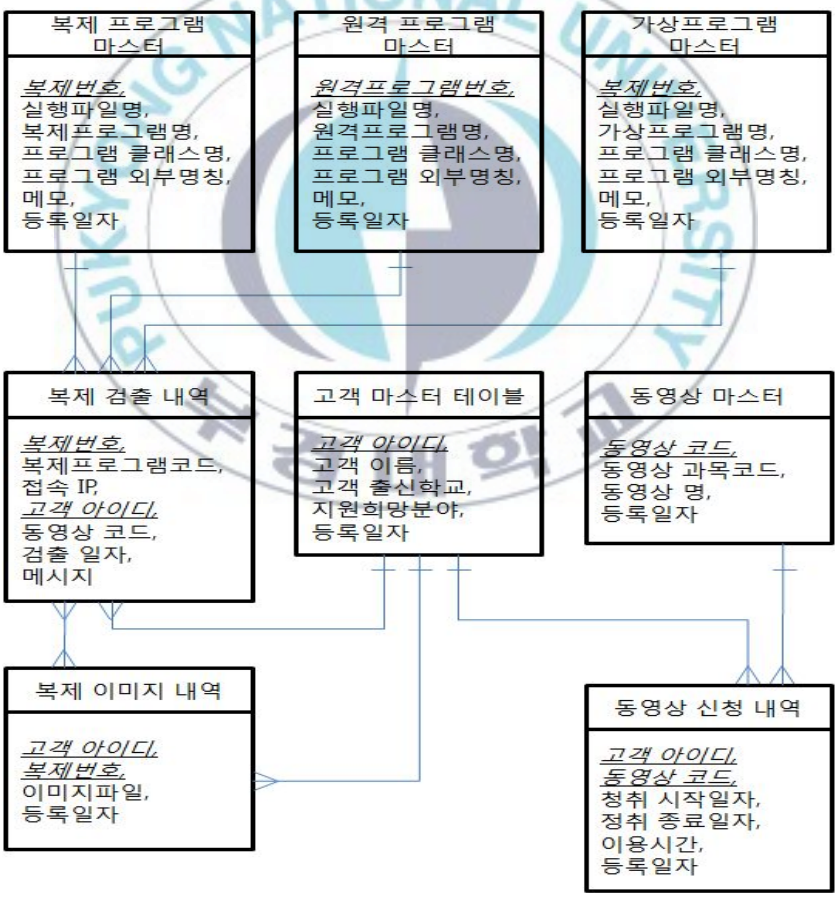
<그림 16>은 일반 고객이 동영상 서비스를 받고자 웹사이트에 가입을 하여, 사이트에서 제공되는 동영상 서비스를 받을 때에 불법 복제 방지 프로그램의 설치 여부를 점검하여 불법복제를 하지 못하도록 불법복제 방지 프로그램이 자동으로 설치되도록 개발한 흐름도이다.



<그림 16> 불법 복제 방지 프로그램 실행

3. 복제 방지 시스템의 ER다이어그램

불법복제 방지 시스템의 간략한 데이터베이스 ER다이어그램(Entity-Relationship Diagram)를 <그림 17>에서와 같이 보면, 고객정보 마스터 테이블을 축으로 하여 마스터 테이블인 복제프로그램 정보 마스터, 원격접속프로그램 정보 마스터, 가상머신 프로그램 정보 마스터와 내역테이블인 고객별 복제내역 테이블, 고객별 복제 이미지내역 테이블 등으로 구성된 복제 방지 시스템의 ER다이어그램이다.



<그림 17> 복제 방지 시스템 ER다이어그램

IV. 분석 및 평가

1. 분석 및 평가

본 논문은 기존 콘텐츠 보호를 위해 콘텐츠 속에 삽입시켜 저작권을 보호하는 목적으로 연구 개발된 복제 방지 기술인 워터마킹 기법과 DRM 기법에 대해서 살펴보았고, 또한 다양한 형태의 SW을 이용하여 어떠한 방식으로 디지털 콘텐츠들을 복제하는지에 대해서도 살펴보았다.

기존 콘텐츠 보호를 위한 기법들은 콘텐츠 속에 삽입시켜 저작권을 보호하는 목적이므로 다른 사람과 공유하지 않고, 개인적으로 사용하게 될 경우에는 저작권에 대해 보호가 불가능하다. 따라서 디지털 콘텐츠를 SW 프로그램으로 복제하여 개인적으로 소장하여 사용하는 것에 대한 저작권의 보호를 하는 것이 중요하다고 하겠다.

본 논문은 [표 4]와 같이 이러한 복제 SW 프로그램들의 유형에 따라 분석한 결과에 따라 첫째는 일반적인 방법으로 복제 프로그램을 사용하여 복제하는 기법에 대해 복제 프로그램들을 데이터베이스화하여 복제 프로그램의 접근 여부를 감지하여서 차단하도록 개발하였다. 두 번째는 원격접속 프로그램을 사용하여 복제하는 기법에 대해 원격 접속 감지 모듈을 구동하여서 차단하도록 개발하였다. 세 번째는 가상머신 프로그램을 사용하여 복제하는 기법에 대

해 가상머신 접속 감지 모듈을 구동하여서 차단하도록 개발하였다. 마지막으로 S-Video 단자를 사용하여 복제하는 기법에 대해서도 S-Video 단자의 사용 여부를 감지하여 차단하도록 개발하였다.

[표 4]에서 보는 것과 같이 D사와 Y사의 프로그램은 원격접속 복제나 가상머신 접속 복제, S-Video 외부 단자를 이용한 복제에 대해서 불법으로 복제가 가능하였다. 본 논문의 연구 개발에서는 다양한 복제 유형에 대해서도 복제를 방지할 수 있다는 측면에서 의의가 있다.

[표 4] 복제 유형에 따른 타사 제품과의 복제가능 비교 분석

제품 / 복제 유형	D사 S/W	Y사 S/W	개발 S/W
복제 프로그램	복제 불가	복제 불가	복제 불가
원격접속 방법	복제가능	복제가능	복제 불가
가상머신 방법	복제가능	복제가능	복제 불가
S-VIDEO 기법	복제 가능	복제 가능	복제 불가

2. 향후 연구 과제

현재까지의 연구는 디지털 콘텐츠에 대한 복제 방지 기법들과 PC 환경에서 배포되어 지는 복제 프로그램들에 대해서 연구가 이루고 있다. 향후 연구에서는 스마트폰이나 넷북, 전자북, PMP 등

다양한 하드웨어 환경에서 제공되는 디지털 콘텐츠에 대해서도 콘텐츠가 필요한 사람에 의해서 기기에 맞는 복제 프로그램이 개발되어 불법으로 복제를 할 것이다. 이에 대비해서 각각의 하드웨어마다 개발된 복제 프로그램의 특성을 분석해서 각각의 하드웨어에 맞는 복제 방지하는 프로그램을 지속적으로 연구 개발이 필요하다.

V. 결론

최근 스마트폰의 활성화로 디지털 콘텐츠의 활용은 점차 증가하고 있다. 이러한 관점에서 영상 디지털 콘텐츠의 무단 복제는 지적 소유권의 문제뿐만 아니라 개발자의 경쟁력을 약화시키기 때문에 이와 관련된 연구의 필요성은 더욱 증대되고 있다. 본 연구도 이러한 현실을 고려하여 디지털 콘텐츠의 불법 복제를 예방할 수 있는 기법을 개발하고, 이를 현장에서 사용할 수 있는 방법을 연구하였다. 현재 다양한 디지털 콘텐츠의 불법 복제율은 매우 심각한 상태에 있다. 음악 콘텐츠, 영상 콘텐츠, 게임 콘텐츠, 교육용 콘텐츠, 만화 콘텐츠 등의 콘텐츠를 제작/판매하는 업체들은 불법 복제로 인한 경제적 손실이 막대함으로 디지털 콘텐츠 보안 솔루션을 적용하여 불법복제 방지에 많은 노력을 하고 있다. 그러나 기존의 디지털 콘텐츠 보안 솔루션들은 특정한 상황에서 복제를 예방하는 기술들이 개발되어 있지만, 여러 가지 유형을 고려한 복합적인 복제방지 솔류션을 지원하는데 한계를 가지고 있다. 따라서 본 연구에서는 교육용 콘텐츠의 다양한 복제 유형을 분석하과, 이들을 현장에서 사용할 수 있는 디지털 콘텐츠의 불법복제 솔류선을 아래와 같은 내용으로 개발하였다.

복제 유형에 따라 첫째, 일반적으로 많이 사용하는 복제프로그램을 사용해서 복제하는 것을 방지하였다. 둘째, 원격접속 프로그램을 사용해서 복제하는 것을 방지하였다. 셋째, 가성머신을 통해 접속하여 디지털 콘텐츠를 복제하는 것을 방지하였다. 넷째, S-Video 단

자를 사용해 외부 기기에서 디지털 콘텐츠를 복제하는 것을 방지하는 기법을 제시하였다.

본 연구에서 개발한 미디어 콘텐츠 영상 불법복제 방지 프로그램은 교육기관이나 산업체에서 고가의 영상 교육용 컨텐츠를 불법으로 복제되거나 활용되는 것을 방지할 수 있다는 측면에서 사회적으로 건전한 디지털 문화가 형성되어지고, 경제적으로는 디지털 콘텐츠 사업이 더욱 더 활성화될 수 있는 기반 연구가 되었다. 그러나 본 연구의 결과들은 최근의 스마트폰이나 BcN과 같은 다양한 통신 환경을 모두 고려하지 않고 있기 때문에 보다 다양한 시스템 환경의 불법 복제에 대한 범위를 넓혀서 적용할 수 있는 확장된 연구가 필요하다.

[참고문헌]

[1] 김창영, “국내 디지털콘텐츠 유통실태 조사", 한국소프트웨어진흥원, pp.7~12, 2007.

[2] 나채식, “온라인상 불법저작물 대책 및 개선방향”, 국회입법조사처, pp.3~14, 2009.

[3] 김태중, "디지털 콘텐트 보호를 위한 강인한 웨이블릿 기반 로고 워터마킹 알고리즘", 경희대 정보통신전문대학원, pp.6~31, 2008 02.

[4] M. Kutter, F. Jordan, and F. Bosson, "Digital signature of solor images using amplitude modulation", Proc. of SPIE, Vol. 3022, pp.518~526, 1997.

[5] K. I. Hashida and A. Shiozaki, "A method of embedding robust watermarks into digital color images", IEICE Trans. Fundamentals, Vol. E81-A, No. 10, pp. 2133-3237, Oct. 1998.

[6] Iain E. G. Richardson, Video codec design, John Wiley & Sons, pp. 127-133, 2002

[7] A. V. Oppenheim, R. W. Schafer, J. R. Buck, Discrete-time signal processing, Prentice-Hall, pp.541-588, 1999

K. I. Hashida and A. Shiozaki, "A method of embedding robust

[8] 강현배, 김대경, 서진근, “웨이블릿이론과응용”, 아카넷, pp.42-65, 2001

[9] http://www.jpeg.org

[10] 이호석, 김준기, “알기쉬운MPEG-2”, 홍릉과학출판사, 2002.

[11] Iain E.G Richardson, “H.264 and MPEG-4”, John Wiley &Sons, 2003.

[12] F. Hartung and M.Kutter, "Multimedia Watermarking Techniques," Proc. of the IEEE, Vol. 87, No. 7, pp.1079~1107, 1999.

[13] A. Tirkel et al. "Electronic Water Mark," in Proc. DICTA 1993, pp. 666~672, 1993.

[14] 강호갑, “DRM 최신 국제표준 기술사양 분석 및 세계 유명제품 동향과 전망에 관한 연구”, 2004.

[15] 한국방송영상산업진흥원[편], "디지털방송 콘텐츠 보호를 위한 복제방지 기술에 관한 연구", 방송위원회, pp.74~82, 2006.

[16] TechSmith, http://www.techsmith.com/

[17] 안카메라, http://www.ancamera.com/

감 사 의 글

본 논문이 완성되기까지 지도와 격려를 해주신 김창수 지도교수님께 깊은 감사를 드립니다. 저의 미비한 논문을 심사하시면서 세심한 검토와 지도를 해주신 이경현 교수님과 김종남 교수님께 감사드립니다.

그리고, 대학원에서 공부하는 동안 항상 힘이 되어준 김무경, 조혜정, 최은희, 김태현, 윤정한 동기님들께 진심으로 감사드립니다. 자료수집과 시스템 구현에 도움을 주신 (주)스타트라인의 이정호 부장님과 안주선 팀장님께 감사하며, 늘 아낌없이 조언을 해 주신 (주)리얼허브의 이강석 사장님께도 감사드립니다. 항상 마음의 도움을 주고 격려해주신 모든 분들께 감사의 마음을 전합니다.

마지막으로 오늘이 있기까지 정성으로 보살펴주신 어머님과 장모님, 그리고 힘들고 어려울 때 마다 항상 따뜻한 미소를 잃지 않고 격려해준 사랑하는 아내와 논문이 무엇인지, 어떤 내용인지, 계속 물어보며 궁금해 하던 사랑스러운 딸 다은이와 함께 이 기쁨을 나누고 싶습니다.

끝으로 저희들 곁을 먼저 떠나신 아버님과 고인이 되신 장인을 그리며 두분 영전에 이 책을 바칩니다.