

정지영상 워터마킹 평가 및 인증 기술

오원근 | TTA, 데이터연구반 위원
한국전자통신연구원 컴퓨터·소프트웨어연구소
김해광 | 세종대학교 소프트웨어공학과

1. 서론

인터넷 및 정보통신 기술의 발달로 우리 산업에서 콘텐츠 산업이 차지하는 비중이 날로 증가하고 있고, 질적으로도 중요한 위치를 차지하고 있다. 아울러 콘텐츠 관련 기술도 종래의 단순 요소기술에서 차세대 IT 환경의 발달과 더불어 복잡하면서도 관련 기술이 통합되는 추세이다. 즉, 초고속, 대용량, 유무선 통합 환경에서는 콘텐츠가 사용자 중심, 실감성, 이동성 및 저작권 보장이라는 특성을 갖게되며 이러한 형태의 콘텐츠를 생성/제작, 저장/관리, 보호/유통 및 서비스하는 새로운 기술의 개발이 필요하다.

특히, 매년 생성되는 모든 콘텐츠의 약 80%(1 엑사바이트, 10^{18} 바이트)를 차지하는 디지털 콘텐츠는, 그 특성상 내용의 손실없이 무한복제가 가능하기 때문에 인터넷상에서 유통될 때 디지털 콘텐츠의 저작권을 관리하는 기술이 절실하게 요구된다. 현재, 일반적으로 사용되어지고 있는 디지털 콘텐츠의 저작권 보호 기술 중 대표적인 기술이 DRM¹⁾ 기술인데, 이중에서도 디지털 콘텐츠에 저작권 정보를 삽입하거나 추출하여 콘

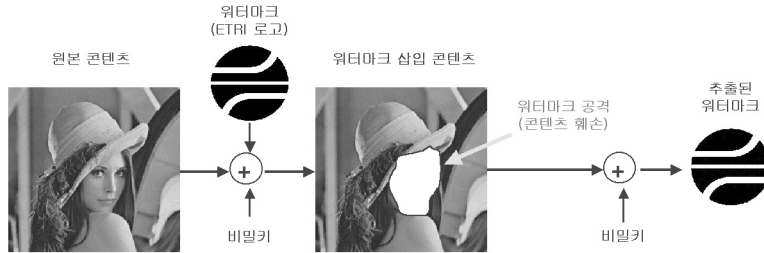
텐츠의 저작권을 보호하는 기술이 워터마킹 기술이다.

본고에서는 워터마킹 기술의 개요와, 정지영상에 대한 워터마킹 평가 및 인증에 대한 내용과 절차에 대해 설명한다.

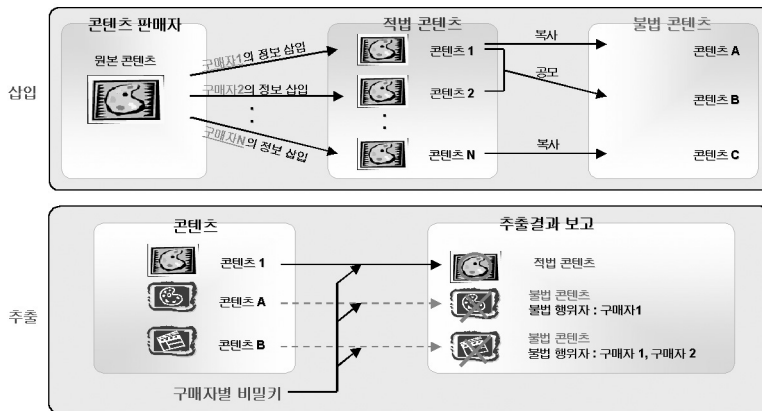
2. 워터마킹 기술의 개요

워터마킹 기술은, 크게 세가지 종류로 나눌 수 있는데, 콘텐츠의 삽입된 정보가 외부의 공격에도 견딜 수 있는 Robust 워터마킹(그림 2.1), 콘텐츠에 구매자 정보를 삽입하여 불법 복제시 해당 구매자를 추적할 수 있는 핑거 프린팅(그림 2.2) 그리고 콘텐츠를 의도적으로 훼손하거나 위·변조시 해당부분을 검출하여 인증과 무결성을 제공하는 Fragile 워터마킹(그림 2.3) 등이다.

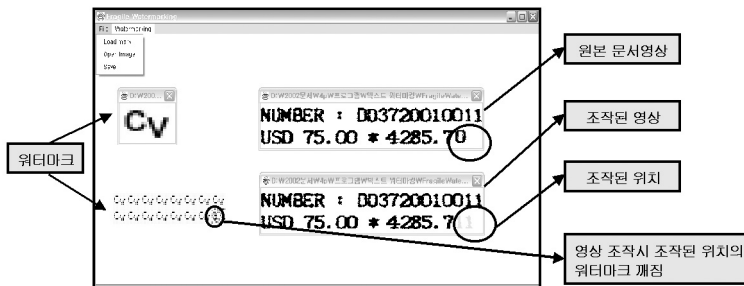
1) DRM(디지털 저작권 관리 : Digital Rights Management) : 디지털 콘텐츠의 불법 유통과 복제를 방지하고 적법한 사용자가 콘텐츠를 사용케 하며, 과금 서비스 등을 통해 디지털 콘텐츠의 저작권을 관리하는 기술.



<그림 2.1> 워터마크 삽입 및 추출(워터마킹)



<그림 2.2> 핑거프린팅 기술



<그림 2.3> Fragile 워터마킹 기술

이들 워터마킹 기술들은 목적에 따라 신호처리, 영상처리, 컴퓨터 그래픽스, 통신, 전산학, 인지과학 등 여러분야의 기초기술들이 복합적으로 사용되고 있으며, 원래의 목적에 따라 의도적/비의도적인 워터마크의 손상, 변형 및 제거 등으로부터 강인성을 보장받아

야 한다. 여기서, 워터마크에 대한 각종 손상, 변형 및 제거 등을 워터마크에 대한 공격(attack)이라고 한다. 다시 말해서 워터마킹의 공격이란 워터마크가 삽입된 디지털 콘텐츠를 조작하여 워터마크 신호를 제거하거나, 워터마크 신호를 검출할 수 없게 만들거나, 또는

위조된 워터마크를 만들어 삽입한 사람이 저작권 및 소유권을 주장할 수 없도록 하는 것을 말한다.

따라서, 워터마킹 기술을 개발하고 설계하는데 있어서 워터마크를 손상, 변형 및 제거할 수 있는 다양한 공격들에는 어떤 것들이 있는지를 파악하고 다양한 공격에 효율적으로 동작하는지에 대한 평가가 이루어져야 한다. 디지털 워터마크의 평가는 크게 1) 시각적 관점(visibility evaluation), 2) 강인성 평가(robustness evaluation), 3) 용량 평가(capacity evaluation) 등의 3가지 관점에서 이루어진다.

현재 다양한 공격에 대한 디지털 워터마킹 기술을 완벽하게 평가하는 방법은 나와있지 않은 상황이며,

실제로도 평가에 필요한 요구조건을 모두 만족시키는 대단히 어려운 일이다. 따라서, 디지털 워터마킹 기술의 평가는 디지털 워터마킹의 활용분야 및 목적에 따라 평가하는 것이 바람직하다. 현재 가장 많이 사용되고 있는 워터마킹 평가를 위한 벤치마킹 방법으로는 StirMark, CertiMark 및 CheckMark 등이 있다.

한편, 워터마킹이 적용되는 미디어는, 텍스트(e-Book, 전자문서), 동영상(VOD, 인터넷 TV, 교육 콘텐츠), 정지영상(인터넷 신문, 의료영상, 디지털 사진), 오디오(AOD, 인터넷 음악), 그래픽(2/3D 데이터, VR) 등이며, 활용분야도 매우 다양하다(표 1 참조).

〈표 1〉 워터마킹 기술의 활용분야

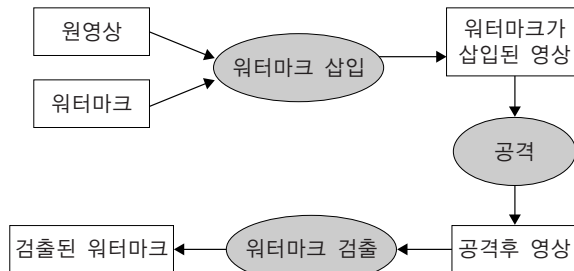
활용분야	활용목적
저작권 보호 (Copyright Protection)	콘텐츠에 삽입된 워터마크를 이용하여 저작권 정보를 제공하며 저작권이 침해된 경우 소유권 증명에 이용
핑거 프린팅 (Fingerprinting)	콘텐츠를 배포할 때 공급받는 사용자의 정보를 함께 삽입하여 불법 복제의 근원지를 추적하는데 이용
데이터 인증 (data authentication)	쉽게 깨지는 워터마크를 이용하여 콘텐츠의 변형 및 위조여부를 판단하며 변형 및 위조된 위치도 확인가능
비밀통신 (Data Hiding)	워터마크를 이용하여 콘텐츠 데이터에 제3자가 확인할 수 없는 비밀 메시지의 삽입 가능
신분증 위변조 방지	여권, 면허증 등 신분증의 사진에 워터마크를 삽입하여 위조여부를 검사하고 위·변조를 방지
인터넷 티켓 판매	인터넷 우표, 영화 표, 상품권 등 인터넷을 통한 티켓을 발매할 때 복제를 막을 수 있도록 워터마크를 사용한 보안 서비스
Off-line code	Off-line 광고 영상(ex : 명암) 속에 워터마크를 삽입하여 on-line 정보와 연결하거나 바코드와 같은 정보제공
복제방지 (Copy control)	워터마크 정보를 이용하여 복제장치(예 : DVD)를 제어하여 불법복제의 근원지를 추적하는데 이용
방송 모니터링 (Broadcast monitoring)	상업광고에 워터마크를 삽입하고, 이를 자동화된 모니터링 시스템이 검출함으로써 계약대로 방송되는지를 확인하는데 이용
장비제어 (Device control)	장비의 실행제어를 위한 워터마크 이용. 예를 들어 방송 동기화, 비디오 연동 자동제어 인형 등
의료보안 (Medical Safety)	의료 영상에 워터마크를 삽입하여 정보의 무결성과 환자의 정보를 안전하게 확인
인덱싱(Indexing)	콘텐츠에 메타데이터 삽입

3. 정지영상 워터마킹 평가 및 인증

정지영상 워터마킹 기술은 현재의 성능으로 볼 때 하나의 범용 워터마킹 기술 혹은 여러개의 응용에 대응한 워터마킹 기술을 평가하는 것은 적합하지 않다. 따라서 여기서는 현재의 혹은 앞으로 나올 워터마킹 기술들의 평가를 위한 인증서의 규격을 정하여, 사용자가 워터마킹 기술의 인증서의 내용을 토대로 자신의 목적에 따라 선택하여 사용할 수 있도록 하는데 평가의 목적을 두었다.

3.1 정지영상 워터마킹 처리구조

정지영상 워터마킹 기술은 <그림 3.1>과 같은 구조



<그림 3.1> 정지영상 워터마크 처리구조

<표 2> 정지영상 워터마크 성능평가 항목

성능 항목	내용
가시성	정지영상에 워터마크를 삽입했을 경우, 인간의 시각으로는 워터마크의 존재여부를 알 수 없어야 한다.
강인성	신호처리 등의 의도되거나 의도되지 않은 변형 공격을 받았을 경우에도 정지영상에 삽입되어 있는 워터마크의 존재를 검출할 수 있어야 하며, 허가되지 않은 압축을 정확하게 검출할 수 있어야 한다.
Tamper 내구성	고의적으로 워터마크를 제거하기 위해 데이터의 일부를 파내는 것을 방지할 수 있어야 한다.
신뢰성	워터마크가 삽입되었을 때는 삽입된 것을 정확히 찾아야 하며, 삽입되지 않았을 때는 삽입되지 않았다고 해야 하는 제한(신뢰도)을 의미한다.
갱신성	원래의 워터마크에 새로운 워터마크의 추가가 가능하다.
계산 복잡성	워터마크의 삽입과 검출의 구현과 수행이 간단하다.
압축 효율성	워터마크 삽입이후, 압축 효율이 떨어지지 않는다.
기밀성	삽입된 워터마크의 정보를 판독할 수 없다.

를 기반으로 사용된다. 워터마크 정보는 원 영상에 워터마크 삽입과정을 통하여 삽입된다. 이러한 워터마크가 삽입된 영상은 의도되거나 의도되지 않은 다양한 경로의 변환 공격을 겪을 수 있다. 이러한 변환 공격에 의해 변형된 영상이 공격 후 영상이다. 공격 후 영상으로부터 워터마크 검출과정에 의해 검출된 워터마크는 원래의 워터마크의 정보를 유지하도록 하는 것이 기본적인 워터마킹 기술의 성능이다.

3.2 정지영상 워터마킹 성능평가 항목

정지영상 워터마킹 기술의 성능평가 항목은 <표 2>에서 보이고 있다.

3.3 정지영상 성능평가 내용

3.3.1 강인성

강인성은 7절에서 정의하고 있는 각 시험 공격에 대해 삽입된 워터마크와 검출된 워터마크의 비율의 통계를 사용하여 평가한다. 다음의 세 가지 방식의 성능 측정치를 사용한다.

비트 정보 손실율 = 검출 워터마크 비트수/삽입된 워터마크 비트수

바이트 정보 손실율 = 검출 워터마크 바이트수/삽입된 워터마크 바이트 수

무손실 워터마크 정보 검출율 = 에러가 전혀 없으면 1, 그렇지 않으면 0

3.3.2 비가시성

워터마크가 삽입된 영상에 대해 5명의 임의로 선정된 전문가로부터 가시성을 1부터 3까지(1 : 눈에 뵈, 2 : 중간, 3 : 눈에 띄지 않음)의 등급을 받고 이의 통계치를 사용

3.3.3 삽입 정보량

공격후 90%까지 살아 남는 워터마크 비트수를 삽입 정보량으로 한다.

3.3.4 삽입 계산 복잡성

인증대상의 워터마크 제품의 워터마크 삽입 계산 복잡성을 명령어와 사용 메모리 양으로 낸다.

3.3.5 검출 계산 복잡성

인증대상의 워터마크 제품의 워터마크 검출의 계산 복잡성을 명령어와 사용 메모리 양으로 낸다.

3.4 정지영상 공격의 내용

3.4.1 필수공격

다음의 공격은 모든 시험 정지영상에 대해서 필수적으로 실시한다.

a) 회전공격 : 1도, 4도, 7도, 15도, 16도, 30도, 37도, 45도

b) 이동공격 : 0.1픽셀, 0.2픽셀, 0.3 픽셀, 0.4 픽셀, 0.5 픽셀

c) 업샘플링 : 1:1.1, 1:1.4, 1:1.5, 1:1.6, 1:2, 1:3, 1:4

d) 다운 샘플링 : 1:0.9, 1:0.8, 1:0.7, 1:0.5, 1:0.4, 1:0.2, 1:0.1

e) 필터링 : 스무딩(smoothing) 필터링, 샤프닝(sharpening) 필터링, 미디언(median) 필터링을 적용한다.

미디언(median) 필터링은 3x3, 4x4, 5x5의 윈도우 사이즈를 사용한다.

가우시안 필터와 샤프닝 필터는 다음의 마스크를 사용한다.

$$h = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{bmatrix} \text{ 가우시안 필터} \quad h = \begin{bmatrix} 0 & -1 & 0 \\ -1 & 5 & -1 \\ 0 & -1 & 0 \end{bmatrix} \text{ 샤프닝 필터}$$

f) 클리핑 : 영상의 가장자리를 전체 영상에서 가로, 세로 1/10, 2/10, 3/10, 4/10, 5/10를 제거한다.

g) D/A 와 A/D 변환

h) 압축 : JPEG 압축으로서 QP 4, 6, 7, 10, 15, 20에 대하여 압축을 한다.

GIF 압축을 한다.

i) 화면율(aspect ratio) 변형 : 영상의 수평/수직 스

케일 요소를 다르게 적용하여 변형한다.

j) 수평 플립 : 영상을 좌우 방향으로 플립한다.

k) 쉬어링(shearing) : X축 및 Y축으로 (0, 1), (0, 5), (1, 0), (5, 0), (1, 1), (5, 5) 만큼 변형한다. (x, y) 괄호 안의 파라미터는 각각 X축 및 Y축을 가리키며 X축으로 x% 만큼을, Y축으로 y% 만큼을 이동한다.

l) 선형 기하 변형 : 일반 선형 기하 변형식은 다음과 같이 표현된다.

$$x' = ax + by$$

$$y' = cx + dy$$

각각의 계수 (a, b, c, d)에 대해 다음의 값들을 취해 선형 기하변형 한다. (1.010, 0.013, 0.009, 1.011), (1.007, 0.010, 0.010, 1.0120), (1.013, 0.008, 0.011, 1.008)

3.4.2 선택 공격

3.4.1의 필수 공격의 조합으로 평가대상자가 연속적인 공격을 가할 수 있다.

3.4.3 시험 정지영상 데이터 베이스

시험 정지영상 데이터 베이스는 총 80장으로 구성하며 각 영상 크기별로 QCIF 영상 20장, CIF 20장, SVGA 20장, HDTV 20장으로 구성한다. 시험 정지영상 데이터베이스는 HDTV 영상 20장을 화면의 복잡성, 사용 색 등을 고려하며 서로 다른 영상특성을 갖는 것으로 선정한 후 이 HDTV 영상 20장을 다운 샘플링하여 SVGA, CIF, QCIF 영상 20장을 만들어서 정지영상 데이터베이스를 구축한다.

3.4.4 시험 워터마크 정보 데이터베이스

시험 워터마크 정보는 8x8, 16x16, 32x32, 64x64 크기의 로고 이미지 4장과 32비트 정보, 16비트 정보, 8비트 정보를 선정하여 성능평가를 위한 시험 워터마크 정보로 사용한다.

3.5 정지영상 워터마킹 인증

정지영상의 워터마킹 인증을 위해서는 다음과 같은 절차를 밟아야 한다.

- 1) 워터마킹 인증신청자는 인증신청서 및 인증대상인 워터마킹 제품을 인증기관에 송부한다.
- 2) 인증기관은, 제출된 워터마킹 제품에 대해 규격에서 제정한 워터마크 데이터-워터마킹 제품의 삽입 알고리즘을 사용하여 시험 정지영상 데이터베이스의 정지영상-를 삽입한다.
- 3) 다음은 규격에서 제정한 다양한 공격 알고리즘을 사용하여 공격한 후 결과영상에 대해 인증신청자가 제출한 워터마킹 검출 알고리즘을 사용하여 삽입된 워터마크에 대해 검출 신뢰성에 대한 통계를 산출한다.
- 4) 마지막으로, 워터마킹 인증기관은 신뢰성 정보와 함께, 워터마킹 제품의 계산 복잡성, 용량 등의 정보를 인증서(표 3)에 포함하여 인증 신청기관에 보낸다.

〈표 3〉 인증서 양식

인증기관 정보	인증기관 명			
	인증기관 주소			
	인증기관 일련번호			
인증 신청자 정보	인증 신청자 명			
	인증 신청자 주소			
	인증 신청자 식별 번호			
워터마킹 제품 일반 정보	워터마킹 제품 식별 번호			
	특허(선택)			
	알고리즘 설명			
	대상문서 대상 응용			
워터마킹 성능	강인성	회전		
		이동		
		샘플링	UP	
			DOWN	
		필터링	Gaussian	
			Median	
			Sharpening	
		클립핑		
		D/A, A/D 변환		
		압축	JPEG	
			GIF	
		화면을		
		수평 플립		
		쉬어링		
	선형 기하 변형			
	삽입정보량	회전		
		이동		
		업 샘플링	UP	
			DOWN	
		필터링	Gaussian	
			Median	
			Sharpening	
		클립핑		
		D/A, A/D 변환		
		압축	JPEG	
			GIF	
		화면을		
		수평 플립		
쉬어링				
선형 기하 변형				
가시성				
워터마크 삽입 복잡성	계산 속도			
	사용 메모리			
워터마크 검출 복잡성	계산 속도			
	사용 메모리			

4. 정지영상 워터마킹 인증의 자동화

앞 절에서 설명한 정지영상 워터마킹의 인증을 위해서는, 다양한 워터마킹 기술에 대한 평가절차를 반복하여야 하며, 평가결과에 대한 안정성과 신뢰성을 확보하기 위해서는 같은 워터마킹 제품에 대해서도 성능 실험을 수차례 실행하는 것이 바람직하다.

이를 위해서는 워터마킹 인증의 절차를 자동화하는 것이 효율적인데, 인증기관에 설치된 평가 엔진에 연구실의 연구, 개발자나 산업체의 제품 개발자 및 수요자가 인터넷을 통해 쉽게 접근, 평가를 받을 수 있게 된다. 이는 워터마킹 기술이나 제품의 평가가 객관적으로 이루어질 수 있어 평가결과를 상호 신뢰할 수 있게 됨을 의미한다. 워터마킹 인증의 자동화를 위해서는 다음과 같은 체계 및 환경의 개발이 필요하다.

- 1) 워터마킹 활용분야의 체계적 분류
- 2) 활용분야에 적합한 평가기준 설정 및 평가체계 구축
- 3) 평가환경(신희처리, D/B 톨) 및 처리결과 분석체계 구축
- 4) 통계처리 방법론 개발 및 환경구축(스프레드 시트, 통계처리 패키지 등 활용)
- 5) 평가수행 및 평가결과 분석체계 구축

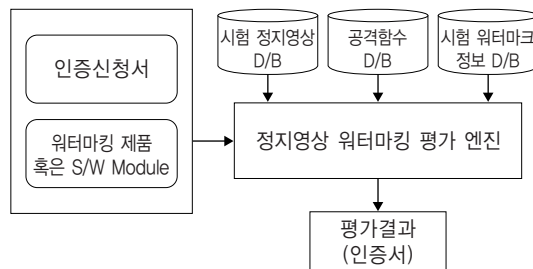
(그림 4.1)은 자동화된 평가 환경의 구조를 나타낸다.

5. 결론

본 고에서는, 정지영상에 대한 워터마킹의 성능을 평가하고 평가결과를 인증하는 기술 및 체계에 대하여 설명하였다. 정지영상 워터마킹을 평가하고 인증하는 목적은, 기존 혹은 향후에 개발될 관련 기술의 성능을 객관적, 체계적으로 비교, 분석하여 1) 기술 개발자들에게는 보다 우수한 워터마킹 기술의 개발을, 2) 수요자에게는 자신이 원하는 기술의 선택을, 3) 평가자에게는 공정한 평가를 가능하게 하는 것이다.

워터마킹 기술은 아직까지 수익성이 큰 비즈니스 모델이 없는 관계로 대부분의 관련 회사들이 경영상의 어려움을 겪고 있는 것이 현실이다. 그러나 최근 범 정부차원으로 추진되고 있는 신성장동력사업에 디지털 콘텐츠 분야가 큰 역할을 할 것이고, 이 기술에 대한 수요가 점차 크게 늘고 있기 때문에 우수한 기술의 개발은 필수적으로 요구될 것이다.

향후 이러한 기술적, 사회적 요구에 부응해서 보다 많은 정지영상 워터마킹 기술 및 제품들이 체계적인 평가, 인증을 통해 검증을 받고 상용화를 이룸으로써 국내의 워터마킹 시장과 산업이 활성화되었으면 한다.



〈그림 4.1〉 정지영상 워터마킹 인증 자동화 체계

참고문헌

- [1] 김명준, 오원근 외, “차세대 콘텐츠 기술 개발 계획에 관한 연구”, 정보통신기술개발기획연구 최종보고서, 2001. 8
- [2] 홍진우, 서영호 외, “디지털 콘텐츠 관리 기술 개발”, 정보통신부 선도기술개발과제 최종보고서, 2003. 2
- [3] 윤기승, 서영호 외, “DRM 기반 하의 디지털 콘텐츠 유통 솔루션 개발”, 정보통신부 선도기술개발과제 최종보고서, 2003. 11
- [4] 김해광, 오원근, “정지영상 워터마킹 인증”, TTA 표준 기고서, 2003. 10
- [5] Hae-Kwang Kim, Kwang-Bum Jin and Weon-Geun Oh, “Standard efforts for still image watermarking certification in Korea”, ISO/IEC JTC1/SC29/WG11 MPEG2003/M10083
- [6] Evaluation Tools for Persistent Association Technologies WD 4.0, ISO/IEC JTC 1/SC 29/WG 11/N6047
- [7] 유원영, “DCT기반의 적응적 비디오 워터마킹 알고리즘”, 전북대학교 박사학위 논문, 2002. 9
- [8] 홍진우, 석종원, 주상현, 서영호, “디지털 워터마킹 기술 성능 평가를 위한 벤치마킹 도구 분석 및 평가시안 - StirMark, CertiMark 및 CheckMark를 중심으로 -, 2001. 1
- [9] <http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/>
- [10] <http://www.certimark.org>
- [11] <http://www.checkmark.com>
- [12] 오상훈 외, “2002년도 SEDICA 운영 및 활성화 사업(최종보고서)”, 한국소프트웨어진흥원, 2002. 12 