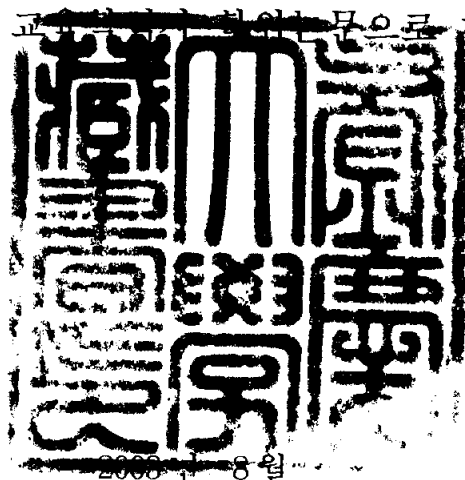


교육학 석사 학위 논문

이미지 워터마킹 벤치마킹 틀 평가에 관한 연구

지도교수 박 지 환

이 논문을 교육학 석사 학위논문으로 제출함



부경대학교 교육대학원

전 산 교 육 전 공

김 민 정

김민정의 교육학석사 학위논문을 인준함

2003년 6월 21일

주 심 공학박사 김 영 봉



위 원 공학박사 박 승 섭



위 원 공학박사 박 지 환



< 차 례 >

[표차례]	iii
[그림차례]	iv
[Abstract]	v
1. 서론	1
2. 디지털 워터마킹 기법	4
2.1 디지털 워터마킹의 정의	4
2.2 Cox 워터마킹 기법	5
2.3 WaterStamp	6
2.4 Digimarc	8
2.5 디지털 워터마킹의 평가 항목	9
3. 벤치마크 프로그램	12
3.1 Stirmark	12
3.2 Checkmark	16
3.3 JEWELS	21
4. 공격항목 분석 및 평가	25
5. 실험결과 및 고찰	29

5.1 Stirmark	29
5.2 Checkmark	30
5.3 JEWELS	32
5.4 고찰	33
6. 결론	36
[참고문헌]	38

< 표차례 >

[표 1] Cox 워터마킹 수행 스크립트	6
[표 2] Stirmark 공격항목의 parameter	14
[표 3] nongeometric 응용에 사용된 개별공격항목	19
[표 4] JEITA의 일반 영상처리 내성 평가항목과 기준	22
[표 5] Stirmark 공격의 워터마크 추출 결과	30
[표 6] Checkmark 공격의 워터마크 추출 결과	31
[표 7] JEWELS 공격의 워터마크 추출 결과	33

< 그림차례 >

[그림 1] 워터마크 삽입 과정	5
[그림 2] 워터마크의 검출/추출 과정	5
[그림 3] WaterStamp v0.9 실행 화면	7
[그림 4] WaterStamp v4.0 실행 화면	8
[그림 5] Digimarc 워터마크 삽입 화면	9
[그림 6] Kutter 등이 분류한 공격 방법	10
[그림 7] Voloshynovskiy 등이 분류한 공격 방법	11
[그림 8] Stirmark Test Platform 구조	16
[그림 9] 워터마킹 공격 분류	17
[그림 10] 응용에 따른 워터마킹 영상	18
[그림 11] Checkmark 결과 테이블 화면	32

A Study on Evaluation of Benchmarking Tools for Image Watermarking

Min-Jeong Kim

Graduate School of Education
Pukyung National University

Abstract

Digital Watermarking has been proposed as a viable solution to the need of copyright protection and authentication of multimedia data in a networked environment, because it makes possible to identify a author, owner, distributor, or authorized consumer of a document. Benchmarking tools have developed variously for digital Watermarking evaluation. There are Strimark, Checkmark, JEWELS, and Optimark in the Benchmarking tools. Stirmark Benchmarking tool is a representative one among existing benchmarking tools which evaluate robustness of digital watermarking algorithms for still images. In this paper, we evaluate existing watermarking algorithms with these Benchmarking tools, and make a comparative study of each tool's strength and weakness.

1. 서론

인터넷의 광범위한 보급에 따라 네트워크를 이용한 멀티미디어 콘텐츠(정지영상, 동영상, 오디오 등)의 유통, 판매가 본격화되고 있다. 그러나 멀티미디어 콘텐츠는 컴퓨터 상에서 모든 작업(작성, 편집, 복사, 배포 등)이 수행되고 또 그 취급이 용이하기 때문에 위법임에도 불구하고 무단으로 복제되기 쉬운 저작권 보호의 문제가 심각한 실정이다. 디지털 워터마킹은 암호화와 함께 디지털 콘텐츠의 저작권자 및 소유권자의 권익을 보호하기 위한 효율적인 방법 중의 하나이다. 디지털 콘텐츠의 저작권자나 소유권자를 보호하기 위해 삽입된 디지털 워터마크는 다양한 디지털 콘텐츠의 응용 및 활용에 따라 본의 아니게 손상을 입거나 변형될 우려가 있다. 또한, 디지털 콘텐츠를 불법으로 복제, 유통 및 사용하려는 사람들에 의하여 의도적으로 워터마크가 제거되거나 손상 및 변형될 수 있다. 이러한 워터마크에 대한 각종 손상, 변형 및 제거 등을 워터마크에 대한 공격(attack)이라고 한다.

디지털 워터마킹 기술의 평가는 크게 다음과 같은 세 가지 관점에서 이루어진다.

- 시각적 평가(visible evaluation) : 워터마크를 삽입하기 전의 원래의 영상과 워터마크가 삽입된 영상과의 품질 차이에 대한 평가이다.
- 강인성 평가(robustness evaluation) : 삽입된 워터마크가

다양한 공격에 대하여 얼마나 강하게 살아남을 수 있느냐 하는 관점에서의 평가이다.

- 용량 평가(capacity evaluation) : 삽입되는 워터마크에 얼마나 많은 정보를 넣을 수 있는가 하는 관점에서의 평가이다.

강인성도 높으면서 시각적 품질도 모두 높은 것이 이상적인 기술이지만 현재의 디지털 워터마킹 기술로는 이러한 것을 이루기는 매우 어려운 실정이므로 디지털 워터마킹의 목적 및 응용 분야를 고려하여 강인성과 시각적 품질간의 조정(trade-off)이 필요하다.

위의 세 가지 평가 이외에도 디지털 워터마킹의 목적 및 응용 분야에서 필요로 하는 요구사항을 만족시키는지의 여부를 고려하여 종합적인 평가가 이루어져야 한다.

워터마크의 강인성에 대한 체계적인 벤치마크 테스트를 수행하기 위해 워터마크 공격기법에 대한 연구가 활발히 진행되고 있다. 현재 널리 사용되고 있거나 또는 평가를 위해 개발중인 디지털 워터마킹의 벤치마킹 방법에는 Checkmark, Optimark, Certimark, JEWELS, Stirmark 등이 있다. 본 논문에서는 워터마킹 알고리즘 개발자들에게 자신이 개발한 알고리즘을 평가하고자 할 때 평가목적에 적합한 벤치마킹 평가 툴을 소개하고자 한다.

본 논문의 구성은 2장에서 디지털 워터마킹의 정의 및 기존의 워터마킹 기법들에 대해 간략히 소개한다. 3장에서는 여러 벤치마킹 프로그램에 대해서 살펴보고 4장에서는 공격항목을

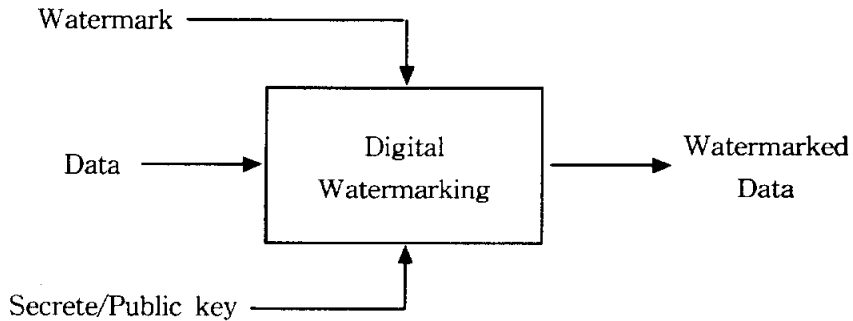
분석 및 평가하고, 5장에서 기존에 개발되어 있는 워터마킹 기법을 실제 영상에 적용한 후, 벤치마킹 툴을 이용하여 공격, 평가해 보고 각 벤치마킹 툴의 장,단점을 파악하고 한다. 마지막으로 6장에서는 결론 및 향후 연구과제를 제시한다.

2. 디지털 워터마킹 기법

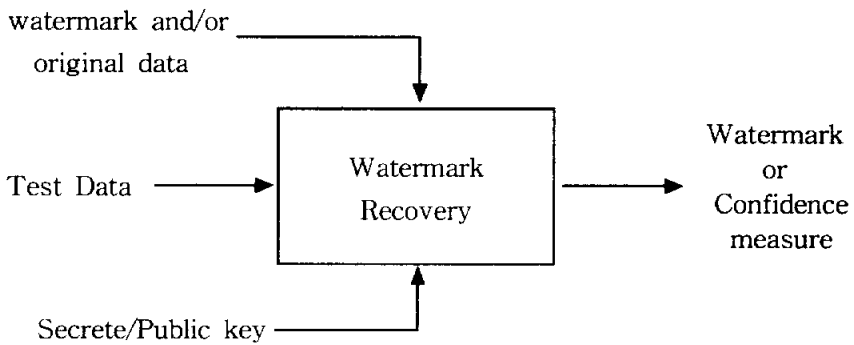
2.1 디지털 워터마킹의 정의

저작권 보호를 위해 멀티미디어에 인지되지 않도록 신호 또는 정보를 삽입하는 기술을 워터마킹이라고 하고 삽입되는 마크를 watermark라고 한다. 워터마크에 신는 정보는 제작자, 소유자, 판매자, 거래자의 고유번호 등이 되고 이는 멀티미디어의 불법 유통시 네트워크 상에서 역추적이 가능하게 한다. 워터마크는 여러 분야에서 응용이 되고 있는데 멀티미디어 저작물의 저작권 보호 뿐만 아니라 각종 저작물의 인증(변조가 없었음을 보장), 무단 배포 방지, 불법 배포자 확인, 소유권 확인 등에 이용된다.

디지털 워터마킹 알고리즘은 삽입 알고리즘과 검출/추출 (detection/extraction) 알고리즘으로 구성된다. 삽입 알고리즘은 원 영상 X 에 대하여, 워터마크 신호 W 와 사용자 키 k 가 주어졌을 때, 영상 X 에 키 k 를 이용하여 워터마크 W 가 삽입되어 워터마킹 영상 Y 를 얻게 된다. 워터마킹 검출 알고리즘은 검출시 원영상 X 가 필요한 경우와 그렇지 않은 경우로 분류될 수 있다. 검출시 원영상 X 가 필요한 경우는 원영상을 가진 저작자만이 워터마크를 추출할 수 있다.



<그림 1> 워터마크의 삽입 과정



<그림 2> 워터마크의 검출/추출 과정

2.2 Cox 워터마킹 기법

1997년도 IEEE에 발표되었던 “Secure spread spectrum watermarking for multimedia”, I.J.Cox, J.Kilian, T.Leighton, T.Shannon의 논문에서 소개된 알고리즘을 구현한 프로그램이다. 그리고 워터마크 검출시 원영상을 필요로 하는 non-blind 방식 워터마킹 알고리즘이다.

Cox의 기법을 사용한 워터마킹 프로그램은 'signature생성->워터마크 삽입->추출->비교' 4단계로 이루어져 있으며 DOS 기반 프로그램이다.

각 단계의 명령어는 표1과 같다.

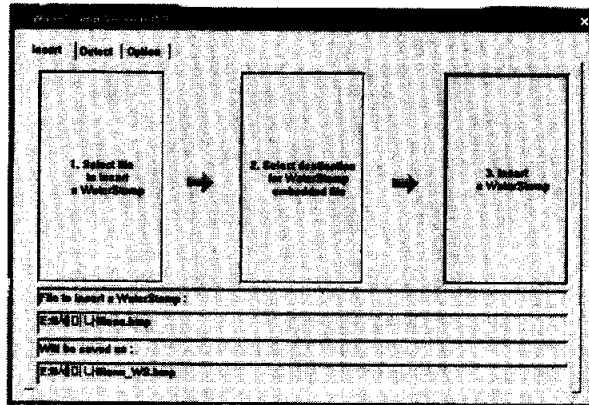
표1. Cox 워터마킹 수행 스크립트

<i>gen_cox_sig -n 1000 -o cox.sig</i>
<i>wm_cox_e -s cox.sig -o cox_lena.pgm lena.pgm</i>
<i>wm_cox_d -s cox.sig -i lena.pgm -o cox.wm cox_lena.pgm</i>
<i>cmp_cox_sig -s cox.sig cox.wm</i>

주의 할 것은 이 소스의 입출력은 PGM 파일 포맷의 512*512 크기 8비트 그레이 스케일만을 한정하고 있다.

2.3 WaterStamp

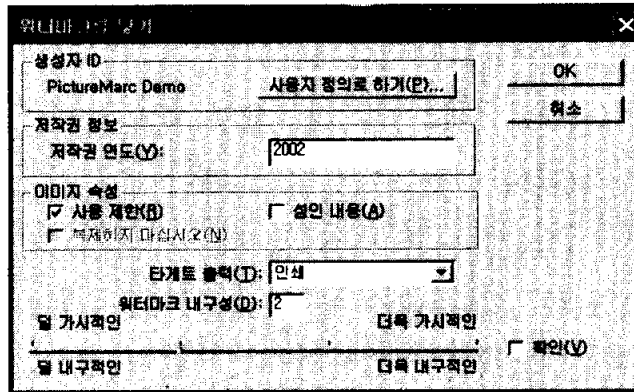
WaterStamp는 국내 워터마킹 전문 벤처기업인 디지털리얼 테크놀로지(주)에서 개발한 디지털 콘텐츠 보호 솔루션의 평가 버전이다. 윈도우 기반 프로그램이므로 쉽게 워터마크를 삽입, 추출할 수 있다. 테스트용 버전이므로 삽입되는 워터마크는 제작사에서 지정해 놓은 것으로 제한되어 있다. WaterStamp v0.9는 Cox 기법과 같이 추출 단계에서 원본 이미지가 필요한 non-blind 방식이다. WaterStamp 버전 0.9의 워터마크 삽입 실행 화면은 <그림 3>과 같다.



<그림 3> WaterStamp v0.9 실행 화면

2003년 1월에 버전 4.0이 테스트용으로 발표되었으며 버전 0.9와의 차이점은 버전 0.9에서는 추출시 원본 이미지가 필요한 non-blind 방식이었지만 4.0에서는 원본 이미지가 필요없는 blind 방식으로 구성되어 있다. 여러 개의 파일을 한꺼번에 워터마크를 embedding, detecting할 수 있는 batch 파일 기능이 추가되었으며 워터마킹 기법도 robust, Fingerprinting, Fragile, Steganography 4 종류로 테스트 해볼 수 있게 구성되어 있다. WaterStamp 버전 4.0의 워터마크 삽입 실행화면은 <그림 4>와 같다.

와 같다.



<그림 5> Digimarc 워터마크 삽입 화면

2.5 디지털 워터마킹의 평가 항목

디지털 워터마킹 기술에 대해서 워터마크의 해독이나 제거, 위조 등의 공격에 대한 안전성을 검토해야 한다. 유효한 공격 수단이나 공격방향이 명확히 되면 그 공격에 견딜 수 있는 워터마킹 기술이 개발되어 더욱 신뢰할 수 있는 알고리즘을 찾아 낼수 있기 때문이다.

디지털 워터마킹을 평가하는 경우, 여러 가지 측면에서 판단해야 한다. 고려하고 있는 디지털 콘텐츠의 이용방법과 밀접한 관계가 있지만, 아래와 같은 항목에 대하여 고려 할 필요가 있다.

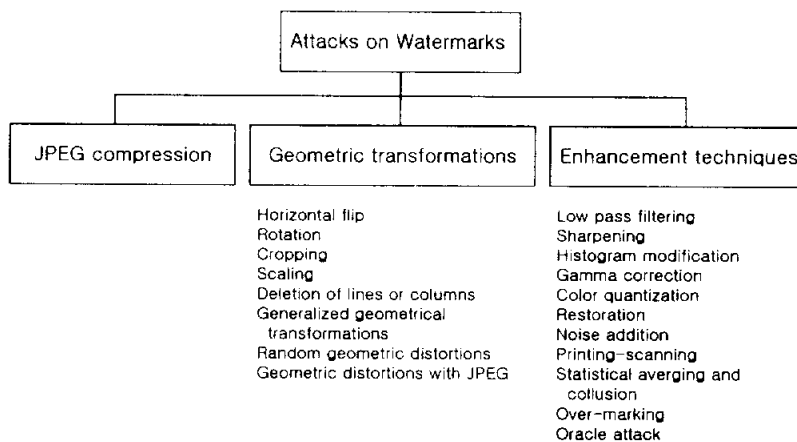
- (1) 디지털 워터마킹에 대한 공격
- (2) 영상처리 등에 의해 워터마크가 제거될 위험성

- (3) 삽입된 워터마크 정보 중 비공개의를 부분을 누설, 고침, 위장할 위험성
- (4) 복수의 공모에 의한 결탁공격
- (5) 화질, 음질 등의 평가
- (6) 압축 등에 의한 내성 평가
- (7) 워터마크의 삽입 및 검출 시간
- (8) 디지털 워터마킹의 동작환경

이것은 디지털 워터마킹 기술 평가항목의 중요한 요소들이다.

워터마크의 공격의 종류에 대한 분류방법은 다양하다.

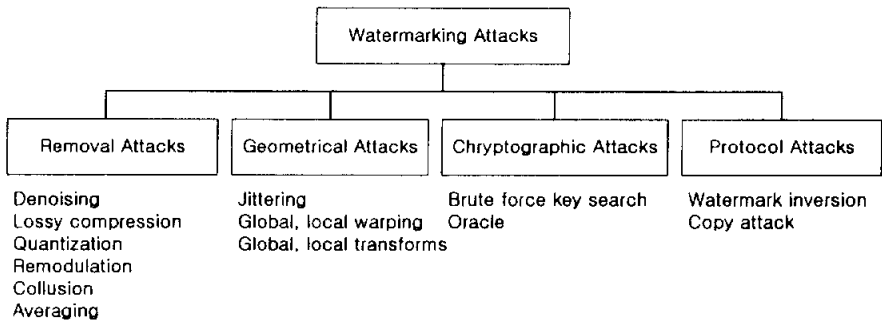
<그림 6>는 Kutter 등의 분류한 공격방법으로 크게 JPEG 압축, 기하학적 변환, 신호처리 공격으로 분류할 수 있다.



<그림 6> Kutter 등이 분류한 공격방법

또 다른 최근의 분류로 Voloshynovskiy 등은 <그림 7>과 같

이 공격방법을 분류하고 있다. 전체적으로는 소거공격, 기하학적 공격, 암호학적 공격, 프로토콜 공격으로 분류하고 있다. 암호학적으로는 키를 찾아내는 방법, 신탁 등이 포함되고 프로토콜 공격에는 카피 공격 등이 새로이 추가되었다. 이와 같이 다양한 공격방법이 계속 등장하고 있음을 확인할 수 있다.



<그림7> Voloshynovskiy 등이 분류한 공격방법

3. 벤치마크 프로그램

디지털 이미지 워터마킹 알고리즘의 강인성 평가는 다른 매체에 대한 알고리즘보다 활발히 연구가 진행되고 있으며, 몇 가지 벤치마킹 프로그램들이 발표되어 있다. 삽입된 워터마크를 공격하는 것은 영상을 조작하여 삽입된 워터마크 신호를 제거하거나, 원 저작자조차 검출할 수 없게 만들거나 위조된 워터마크 신호를 재 삽입하여 소유권 주장을 할 수 없게 만드는 방법이다. 대표적인 벤치마킹 프로그램으로 Stirmark, Checkmark 그리고 JEWELS 등이 있다.

3.1 Stirmark

Stirmark는 정지영상(still image)에 대한 디지털 워터마킹 기술을 평가하기 위한 방법으로써 캠브리지 대학에서 개발된 벤치마킹 방법이다. 1997년 11월에 버전 1.0이 나왔으며 현재는 버전 4.0이 나와 있는 상황이다. Stirmark는 현존 벤치마킹 방법들 중 가장 대표적인 것으로서 강인성에 주안점을 둔 벤치마킹 방법이다.

3.1.1 공격의 종류

Stirmark는 워터마킹 공격항목을 아래와 같이 크게 4가지로

분류할 수 있다.

(1) JPEG Compression

(2) Geometric transforms

Affine, Rescale, Rotation, SmallRandomDisortions,
RotationScale, RotationCrop

(3) Signal Processing

AddNoise, ConvFilter, MedianCut, Selfsimilarities

(4) Special Transforms

Flip, Cropping, RemoveLines, Rotaion 90°, 180°, 270°

Rescale은 영상을 확대 및 축소하는 공격이다. RotationCrop은 회전에 의해 발생한 공백 제거하는 공격이며 영상크기가 감소하게 된다. 반면 RotationScale은 RotationCrop의 결과를 원 영상의 크기로 다시 scaling하는 공격으로 원 영상과 영상 크기가 동일하게 된다. SmallRandomDisortions은 각 pixel 위치 값에 아주 작은 랜덤값을 더하여 이동시키는 것으로, 즉 바둑판 모양의 좌표를 임의로 흔드는 공격이다. 각 공격에 대한 파라미터 값과 설명은 표 2에서 확인할수 있다.

Attacks	Parameter
PSNR	0,10,20,...,100
AddNoise	0,20,40,60,80,100
JPEG 압축	15,20,25,30,35,40,50,60,70,80,90,100
MedianCut	3,5,7,9(filter size)
ConvFilter	1(Gaussian filetring) 2(Sharpening)
SelfSimilarities	1,2,3
RemoveLines	10,20,30,...,100(randomly remove lines rows/columns)
Cropping	1,2,5,10,15,20,25,50,75(ratio)
Rescale	50,75,90,110,150,200(ratio)
Rotation	-2,-1,-0.75,-0.5,-0.25,0.25,0.5,0.75,1,2 5,10,15,30,45,90(angles in degrees)
RotationCrop	-2,-1,-0.75,-0.5,-0.25,0.25,0.5,0.75,1,2 (angles in degrees)
RotationScale	-2,-1,-0.75,-0.5,-0.25,0.25,0.5,0.75,1,2 (angles in degrees)
Affine	mat1 = 1 0 0 0.01 1 0
	mat2 = 1 0 0 0.05 1 0
	mat3 = 1 0.01 0 0 1 0
	mat4 = 1 0.05 0 0.05 1 0
	mat5 = 1 0.01 0 0.01 1 0
	mat5 = 1 0.05 0 0.05 1 0
Affine	mat6 = 1.010 0.013 0 0.009 1.011 0
	mat7 = 1.007 0.010 0 0.010 1.012 0
	mat8 = 1.013 0.008 0 0.011 1.008 0
SmallRandom Distortions	0.95, 1, 1.05 1.1
LatestSmallRandom Distortions	0.95, 1, 1.05 1.1

표 2. Stirmark 공격항목의 parameter

3.1.2 Stirmark의 구성

Stirmark 벤치마킹은 정지영상에 대한 디지털 워터마킹 기술을 평가하기 위한 방법으로 캠브리지 대학에서 개발하였으며 1997년 11월에 버전 1.0이 나왔으며, 그후 여러 차례의 수정을 통해 1999년도에 버전 3.1이 발표되었으며 현재는 버전 4.0이 나와있는 상황이다. 버전 3.1에서는 pgm, ppm, jpg 이미지 포맷이 지원되었으나 버전 4.0에서는 bmp, ppm, jpg 이미지 포맷이 지원되는 차이점이 있다. Stirmark 벤치마킹 툴은 다음 사이트에 가면 소스가 공개되어 있고 다운로드 받을 수 있다. <http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/>

Stirmark의 구조는 <그림 8>과 같이 구성되어 있으며 공격하고자 하는 영상을 Media의 Input 폴더에 넣고 Bin 폴더의 Benchmark의 실행 파일을 실행하게 되면 한 파일에 대해 16개 테스트에 의해 115개의 공격된 영상이 Output 폴더에 생성되어 있음을 알 수 있다. 단, 입력 영상이 버전 3.1에서는 ppm, pgm, jpg or jpeg 이었는데 반해 버전 4.0에서는 ppm, bmp, jpg or jpeg으로 제한되어 있다. 각 테스트에 대한 파라미터들은 Profiles 폴더에서 확인할 수 있다.

/Bin/	Benchmark/	the benchmarking tool itself	
	Libraries/	libraries sent by users	
Profiles/		profiles are text configuration files describing the test to be applied(one profile per application and per 'robustness' level)	
Media/	Input/	Images/	Set1/ samples sorted according to some criteria
			Set2/
			...
		Sounds/	Set1/
			Set2/
			...
	Output/		Same substructure is created for input

<그림 8> Stirmark Test Platform 구조

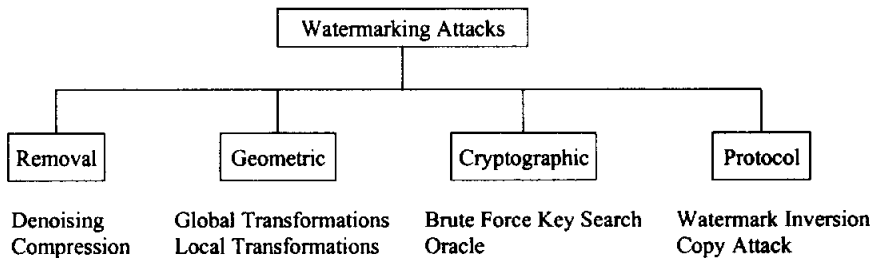
3.2 Checkmark

Checkmark는 워터마킹 기술의 평가를 위한 벤치마킹 툴로서 Geneva 대학에서 개발하였으며 2001년 6월에 버전 1.0이 발표되었고 2001년 12월에 버전 1.2가 개발되어 현재 사용되고 있다.

3.2.1 Checkmark의 구성

Checkmark에서는 워터마킹 공격항목을 4개의 레벨로 구분

하여 분류하고 있다. 첫 번째 레벨은 공격그룹(attack group)으로 <그림 9>과 같이 4개의 항목으로 구성되어 있다. 두 번째 레벨은 공격형태(attack type)로 그림 8에서 Removal 그룹은 Denoising, Compression 등의 여러 공격형태로 구성되어 있다. 세 번째 레벨은 공격클래스(attack class)로 Denoising 타입은 ML (maximum likelihood), MAP(maximum posteriori probability)와 같은 클래스로 구성되어 있다. 네 번째 레벨은 개별공격(individual attack)으로 각 클래스는 하나 혹은 그 이상의 개별 공격으로 구성되어 있다. 예를 들면 MAP 공격 클래스는 Wiener filtering, soft thresholding 등의 개별공격으로 구성되어 있다.



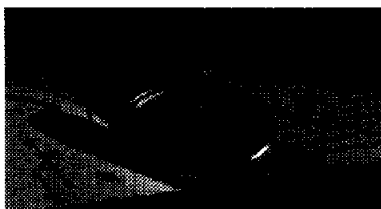
<그림 9> 워터마킹 공격 분류

또한, Checkmark는 응용에 따라서 공격방법을 6가지로 분류하고 있다. 다시 말해 22개의 공격 클래스를 적용 워터마킹 영상의 응용에 따라 6개의 응용항목에 적절히 분류하고 있다.

- (1) nongeometiric (46개의 개별공격)
- (2) copyright (382개의 개별공격)
- (3) banknote (178개의 개별공격)

- (4) logo (77개의 개별공격)
- (5) medical (45개의 개별공격)
- (6) video (193개의 개별공격)

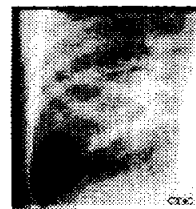
위 응용의 분류에서 medical 영상과 logo 영상의 경우를 제외한 나머지는 같은 분류의 영상으로 처리하고 있다.



일반영상



로고영상



의료영상

<그림 10> 응용에 따른 워터마킹 영상

3.2.2 실행 방법

Checkmark는 Matlab으로 구현된 프로그램으로 크게 4개의 중요한 파일함수로 구성되어 있다.

- (1) getconfig.m (경로설정)

워터마크된 영상 혹은 공격된 영상의 경로설정, 응용종류 설정, 워터마킹 기법 설정 등을 수행한다.

- (2) runCheckmark.m (공격수행)

워터마크된 각종 영상에 대해서 응용종류에 따라 공격을 수행하여 JPEG파일 포맷으로 출력한다.

- (3) testDetector.m (XML파일 포맷으로 결과출력)

이 파일함수에서 워터마킹의 추출모듈을 사용자가 삽입하여 수많은 공격영상에 대한 결과처리를 일괄적으로 수행할

수 있다.

(4) parseresults.m (HTML문서로 결과를 출력)

testDetector.m에서 출력된 XML파일의 결과를 바탕으로 HTML문서로 출력한다. 아래 표3은 nongeometric 응용에 사용된 개별공격 항목들이다.

▶reSample(1)

subGroup	CType	CFactor	down sample	up sample
sampltdownup1	J	100.00	0.75	1.33
sampltdownup2	J	100.00	0.50	2.00
sampltdownup3	J	100.00	0.75	1.30
sampltdownup4	J	100.00	0.50	1.90

▶Wavelet(10)

subGroup	CType	CFactor
waveletcompression1	W	0.10
waveletcompression1	W	0.20
waveletcompression1	W	0.30
waveletcompression1	W	0.40
waveletcompression1	W	0.50
waveletcompression1	W	0.60
waveletcompression1	W	0.80
waveletcompression1	W	1.50
waveletcompression1	W	3.50
waveletcompression1	W	8.00

▶Remodulation(4)

subGroup	CType	CFactor	window
dpr1	J	100.00	3.00
dpr2	J	100.00	5.00
dprcorr1	J	100.00	3.00
dprcorr2	J	100.00	5.00

▶ML(7)

subGroup	CType	CFactor	window
medfilt1	J	100.00	2.00
medfilt2	J	100.00	3.00
medfilt3	J	100.00	4.00
trimmedmean1	J	100.00	3.00
trimmedmean2	J	100.00	5.00
medpoint1	J	100.00	3.00
midpoint2	J	100.00	5.00

►MAP(6)

subGroup	CType	CFactor	window
hardthresh1	J	100.00	3.00
hardthresh2	J	100.00	5.00
softthresh1	J	100.00	3.00
softthresh2	J	100.00	5.00
wiener1	J	100.00	3.00
wiener2	J	100.00	5.00

►JPEG(12)

subGroup	CType	CFactor
jpegcompression1	J	10.00
jpegcompression1	J	15.00
jpegcompression1	J	25.00
jpegcompression1	J	30.00
jpegcompression1	J	40.00
jpegcompression1	J	50.00
jpegcompression1	J	60.00
jpegcompression1	J	75.00
jpegcompression1	J	80.00
jpegcompression1	J	85.00
jpegcompression1	J	90.00
jpegcompression1	J	100.00

►Filtering(3)

subGroup	CType	CFactor	window
gaussian1	J	100.00	3.00
gaussian2	J	100.00	5.00
sharpening1	J	100.00	5.00

►Copy(1)

subGroup	CType	CFactor
copy1	J	100.00

▶ColorReduce(2)

subGroup	CType	CFactor
dither1	J	100.00
thresh1	J	100.00

표3. nongeometric 응용에 사용된 개별공격항목

3.3 JEWELS

JEWELS는 일본 전자정보기술산업협회(JEITA)에서 워터마크 평가 지원 시스템(JEWELS)으로 개발하여, 정지영상의 저작권 보호 및 이용자의 이용 범위에 대한 가이드 라인 설정을 목적으로 디지털 워터마킹 기술의 안전성 평가를 위한 벤치마킹 프로그램이다. JEWELS는 전체적으로 11개 항목의 내성평가와 15가지의 영상 변환공격을 포함하고 있다. 각 항목들은 여러 개의 파라미터를 가지면서 다양한 공격이 가능하도록 구성되어 있다.

일반 영상처리 내성의 평가항목은 디지털화 된 영상으로서 영상조정을 목적으로 하는 처리 중에서 선택한다. 또한 평가의 실용성을 고려하고 평가 작업을 간략화 할 수 있도록 대표되는 영상처리 파라메타의 조합으로 설정한다. 이는 물론 실제의 영상처리에서는 다양한 영상처리 기법을 복잡하게 조합하여 처리하는 경우가 많지만 이 모든 것을 다루기는 어렵기 때문이다. 디지털 워터마크의 사용환경에 따라서는 이렇게 설정하

는 일반 영상처리 내성 평가항목과 기준이 적절하지 않을 수 있다. 그래서 디지털 워터마크를 이용하는 사용자가 사용목적에 맞게 임의의 영상처리를 추가할 수 있는 평가구조로서 유연성을 가지도록 구성하는 것이 바람직할 것이다. 또 특수 영상처리 내성의 평가항목에 관해서는 디지털 워터마킹 기법마다 공격효과가 있는 기법이 다르고 동시에 내성의 강약이 달라지게 되기 때문에 특정하는 것은 어렵다.

여기서는 특수 영상처리에 대해서는 다루지 않고 일반 영상처리에 대한 내성 평가항목과 기준에 대해서 알아보기로 한다.

디지털 워터마킹은 오류 정정 부호가 조합되어 있는 경우가 많고 일반적으로는 삽입 정보량이 적을수록 높은 오류 정정 기능을 가진다고 생각할 수 있다. 그러나 디지털 워터마킹 기술이 비공개인 경우 이 구별은 할 수 없기 때문에 여기서는 오류 정정 부호를 포함한 내성을 평가한다. JEITA에서 제안하고 있는 평가항목과 기준을 표4에 정리하여 나타낸다.

평 가 항 목		평 가 방 법
1	※ 파일형식 변환 (a) 디지털 워터마크를 full color 영상에 삽입하는 것	
	인덱스 칼라	시험영상에 워터마크를 삽입하고 사용 팔레트에 「Web」을 선택해서 Indexed Color로 하고 다시 Full Color 영상으로 변환하여 평가한다.

평 가 항 목		평 가 방 법
2	JPEG 압축	시험영상에 워터마크를 삽입하고, JPEG 파일로 압축, 저장 보존한다. 이것을 신장해서 평가한다. YCrCb의 축소는 4 : 2 : 0 (수평, 수직 동시에 1/2로 서브샘플링)을 이용하고, 양자화 테이블로는 표준 예를 사용한다. 압축률(영상 파일크기)은(a) 1/5 (b) 1/10 (c) 1/20 (d) 1/40 에 대해 평가한다. 단 신장후의 영상의 가로, 세로의 화소값을 각각, w, h로 했을 때 압축률의 계산은 아래 식(1)로 정의한다. $[\text{압축률}] = [\text{JPEG파일의크기(byte)}] / (w \times h \times 3) \quad (1)$
(b)워터마크를 JPEG 압축 영상에 삽입하는 방법		
3	JPEG 압축 /신장	시험영상을 1/8의 파일크기의 JPEG 파일로 압축하고 워터마크를 삽입한다. 이것을 일단 full color 영상으로 신장 후 다시 JPEG 압축에 의해 상기의 압축률로 압축하고, 평가한다.
4	트리밍	워터마크를 삽입한 시험 영상의 중심을 고정하고 (a) 3/4 (b) 1/2 (c) 1/3 (d) 1/4의 축척으로 동일 가로, 세로의 비로 트리밍한 영상을 평가한다.
5	확대	상기 트리밍 영상을 원 영상 크기로 확대한 영상을 평가한다. 확대 처리로는 선형 보간을 사용한다
6	축소	워터마크를 삽입한 시험영상의 중심을 고정하고 (a) 3/4 (b) 1/2 (c) 1/3 (d) 1/4의 축척으로 축소했을 때의 내성을 조사한다. 축소 처리로는 선형 보간을 사용.
7	계조 변환	시험영상에 워터마크를 삽입하고 그 RGB 신호에 대해, 식(2)을 이용하여 계조변환을 행했을 때의 내성을 평가한다. 계수 a로는 (a) 0.5 (b) 0.75 (c) 1.25 (d) 1.5 를 사용한다. 시험 영상 픽셀값 : I_{xy}, 처리후 영상 픽셀값 : O_{xy}, 임의의 파라메타 : a $O_{xy} = 255 \cdot \left(\frac{I_{xy}}{255} \right)^a \quad (2)$

평가항목		평가방법
8	사영 변환	위터마크를 삽입한 시험영상을 사영변환한 때의 내성을 평가한다. 좌표변환은 아래의 계산식으로 행하고 선형 보간을 사용한다. 파라메타 (a, b)는 (a) (5, 1) (b) (10, 3) (c) (20, 6) (d) (30, 9)로 한다. 원영상의 가로, 세로의 화소수를 각각 w, h, 임의의 화소의 좌표를 x, y, 변환후의 좌표를 X, Y로 했을 때, 이하의 좌표변환식으로 나타낼 수 있다. $x = X + \frac{aw(h - Y)(1 - \frac{2X}{w} - \frac{b}{100})}{200h} \quad (3)$ $y = \frac{200Y - 2aY(1 - \frac{Y}{2h})}{200 - a} \quad (4)$
9	공간 주파수 변환	위터마크를 삽입한 시험영상에 공간주파수 변환을 실시한 후의 내성을 평가한다. (a)와 (b)는 블러링 처리 (c), (d)는 에지 강조 처리에 해당한다.
10	프린터/ 스캔	위터마크를 삽입한 시험영상을 a배로 하고 오차 확산 처리에 의해 2치화를 행한다. 다음으로 2치화된 영상을 중간조 영상으로서 선형 보간에 의해 축소하고, 1/a (원 영상 크기)로 하고 이 영상을 평가한다. 파라메타 a로서 (a) 3 (b) 2 (c) 1.5 (d) 1을 사용하고 회전량은 시계 방향으로 0.5도 한다.
11	중첩 합성	블랜드 파라메타를 (a) 0.8 (b) 0.6 (c) 0.4 (d) 0.2 로 했을 때의 내성을 평가한다. 여기서 G를 정수로 하고 $L^*=50$ 에 해당하는 117을 이용한다.

표 4. JEITA의 일반 영상처리 내성 평가항목과 기준

4. 공격항목 분석 및 평가

벤치마킹 툴의 공격항목에 대한 각 파라미터 값은 앞선 3장에서 나타낸 <표 2,3,4>를 참조하도록 한다.

4.1 회전공격

영상전체를 한 축을 중심으로 회전시키는 공격을 말한다.

- Stirmark : Rotation, RotationScale, RotationCrop
- Checkmark : Rotation, RotationScale
- JEWELS : Rotation

4.2 스케일링 공격

영상의 전체를 일정한 비율로 확대하거나 축소하는 공격을 말한다.

- Stirmark : Rescale
- Checkmark : Scale, Resample
- JEWELS : 확대(MAGNIFY),축소(REDUCE)

4.3 클리핑 공격

영상 일부를 잘라내는 공격을 말한다.

- Stirmark : Cropping
- Checkmark : Cropping
- JEWELS : Trimming

4.4 변환 공격

- Stirmark : Affine(shearing, general affine transformations)
- Checkmark : Shearing
- JEWELS : 해당 공격 없음

4.5 필터링 공격

필터링 처리에는 Gaussian 필터링, Sharpening 필터링, Median 필터링 등이 있다.

- Stirmark : MedianCut, ConvFilter
- Checkmark : Filtering, ML
- JEWELS : 공간주파수 변경 필터

4.6 압축 공격

- Stirmark : JPEG
- Checkmark : JPEG, Wavelet
- JEWELS : JPEG압축(Compress), JPEG압축->JPEG신장(Compress_De), JPEG신장->JPEG압축(DeCompress)

4.7 소거 공격

- Stirmark : RemoveLines
- Checkmark : Row_col
- JEWELS : 해당공격 없음

4.8 Stirmark에만 있는 공격

- SmallRandomDisortions/LatestSmallRandomDisortions : 각 pixel 위치값에 아주 작은 랜덤값을 더하여 이동시키는 공격. 즉 바둑판 모양의 좌표를 임의로 혼드는 공격이다
- AddNoise/SelfSimilarites

4.9 Checkmark에만 있는 공격

- Projective transformations
- Modeling of video distortions based on projective transformations
- Warping
- Copy
- Template removal
- Denoising (midpoint, trimmed mean, soft and hard thresholding, wiener filtering)
- Denoising followed by perceptual remodulation
- Non-linear line removal
- Collage

4.10 JEWELS에만 있는 공격

- Gradation
- 프린트/스캔
- 합성영상

4.11 평가

JPEG 압축이나 Rescale 공격에서는 Stirmark나 Checkmark나 파라미터가 거의 똑같음을 알수 있다. 그리고 Shearing을 포함한 Affine 변환 공격은 Stirmark가 파라미터나 종류가 많고 필터링 공격은 Checkmark가 종류가 약간 많음을 알수 있다. 그리고 Rotation 공격은 Stirmark가 회전각도가 다양한 반면 Checkmark는 간단한 몇 개 각도로 테스트해 볼수 있다. 기하학적인 공격에서는 Stirmark가 파라미터가 다양하므로 세밀한 공격을 해볼수 있으며 Checkmark는 각 응용에 따라 공격항목이 다르므로 각 응용에 맞게 공격을 할수 있다. 그리고 JEWELS는 Stirmark와 Checkmark에서 할수 없는 몇가지 공격을 간단히 수행할수 있는 장점이 있다.

5. 실험결과 및 고찰

5.1 Stirmark

Stirmark 버전 4.0에서는 PGM 파일 포맷을 입력 영상으로 지원하지 않으므로 실험 영상인 lena.bmp 파일을 PGM 포맷으로 변경하였다. 그리고 Cox 워터마킹을 수행하여 생성된 워터마크 삽입 파일을 다시 BMP 포맷으로 변경하여 공격한 후 생성된 공격영상들을 다시 PGM 포맷으로 변경하여 추출하는 단계가 부가적으로 필요하였다.

표5는 Stirmark 4.0을 이용하여 공격한 후 추출한 결과 테이블이다. 여기서 (A)는 Cox 기법, (B)는 WaterStamp (C)는 Digimarc 프로그램을 나타낸다. 여기서 (B)WaterStamp는 버전 0.9와 4.0에서 테스트되었으며 버전 4.0에서는 워터마크 삽입강도를 정할 수 있으므로 삽입강도 30,70,100에서 테스트되었음을 괄호로 나타내었다. 각 공격 항목에서 숫자는 parameter에 변화를 주어서 여러 가지로 공격된 것을 나타낸다. 예를 들어 JPEG 압축은 parameter 값이 15,20,25,30,35,40,50,60,70,80,90,100으로 총 12가지 공격이 이루어졌음을 나타낸다. Cox 기법은 비교 단계에서 Correlation 이 0.2 이상이면 워터마크가 살아 남은 것으로 간주한다. JPEG 압축, Rescale, MeidanCut, RemoveLines 공격항목에서는 3가지 프로그램 모두 대체로 강인함을 알 수 있다.

구분	Attacks	A	B				C
			V0.9	V4.0 (30)	V4.0 (70)	V4.0 (100)	
JPEG	JPEG압축(12)	12	12	1	1	2	12
Geometric Transforms	Afine(8)	7	6	0	0	0	4
	Rescale(6)	6	6	3	3	6	6
	Rotation(15)	9	9	9	9	10	2
	SamllRandom Disortions(4)	4	4	0	0	0	0
	LatestSamllRandom Disortions(4)	4	0	0	0	0	0
	RotaionScale(10)	10	8	9	9	8	5
	RotationCrop(10)	10	8	8	8	8	2
Signal Processing	AddNoise(6)	2	6	1	1	1	1
	ConvFilter(2)	1	2	1	1	2	2
	MedianCut(4)	4	4	1	1	2	3
	Selfsimilarities(3)	0	3	2	2	2	2
Special Transforms	Cropping(9)	0	7	2	2	2	0
	RemoveLines(10)	10	10	8	8	7	10
	Rotation 90°(1)	0	1	0	0	0	0
PSNR측정	PSNR(11)	11	11	11	11	11	11
합계(115)		90	97	57	57	61	60

표5. Stirmark 공격의 워터마크 추출 결과

5.2 Checkmark

워터마킹 방법은 마찬가지로 Cox방법과 WaterStamp, Digimarc 세가지 방법이고 Checkmark 응용항목은 nongeometric 항목으로 하나의 영상에 46개 공격이 수행되었다. Cox 방법에서의 추출과정은 상관도 값이 0.2보다 크면 추출성공으로 간주한다. 표6은 46개의 개별공격에 대한 각 워터

마킹 방법에 대한 추출결과를 나타내고 있다. Cox 방법은 100% 추출성공률을 보인 것으로 Checkmark 공격에 강인함을 알수 있고 반면 Adobe Photoshop 6.0 의 Digimarc는 거의 모든공격에 추출이 되지 않아 Checkmark 공격에 약함을 알수 있다.

Attacks	A	B				C
		V0.9	V4.0 (30)	V4.0 (70)	V4.0 (100)	
reSample(1)	1	1	0	0	1	0
Wavelet(10)	10	10	3	3	3	0
Remodulation(4)	4	4	0	0	4	0
ML(7)	7	7	0	0	0	0
MAP(6)	6	6	0	0	5	0
JPEG(12)	12	12	1	1	3	1
Filtering(3)	3	3	3	3	3	0
Copy(1)	1	0	0	0	0	0
ColorReduce(2)	2	0	0	0	0	0
합계(46)	46	44	7	7	19	1

표6. Checkmark 공격의 워터마크 추출
결과(nongeometric)

그리고 <그림 11>은 checkmark에서 nongeometric응용에 대한 결과테이블을 HTML문서로 표현된 화면이다.

Checkmark version 1.2

Technology : cox_1 ; Application : nongeometric

Attacks/Images	im1	im2	im3	im4	im5	Avg
Remodulation(4)	4 100%	4 100%	4 100%	4 100%	4 100%	100%
MAP(6)	6 100%	6 100%	6 100%	6 100%	6 100%	100%
JPEG(12)	12 100%	12 100%	12 100%	12 100%	12 100%	100%
Filtering(3)	3 100%	3 100%	3 100%	3 100%	3 100%	100%
Copy(1)	1 100%	1 100%	1 100%	1 100%	1 100%	100%
Wavelet(10)	7 70%	10 100%	10 100%	9 90%	10 100%	92%
ML(7)	5 71%	7 100%	7 100%	6 86%	7 100%	91%
reSample(1)	0 0%	0 0%	0 0%	0 0%	0 0%	0%
ColorReduce(2)	0 0%	0 0%	0 0%	0 0%	0 0%	0%
Average (230)	71%	78%	78%	75%	78%	76%

Total number of attacks: 230
Number detected: 208
Percent detected: 90%

<그림 11> Checkmark 결과테이블 화면

5.3 JEWELS

실험하고자 하는 영상에 대한 공격 항목을 job제어파일.jcl로 만들고 JEWELS.EXE를 실행시킨다. 예를 들어 reduce 공격에 대한 작업을 reduce.jcl로 만들고 lena.bmp 파일을 공격하고자 한다면 입력창에서 -J reduce.jcl lena 를 입력하면 lena 이미지에 reduce 공격이 이루어지게 되며 공격된 영상들이 생성되게 된다. 표7은 JEWELS을 이용하여 공격한 후 추출한 결과 테이블이다. 마찬가지로 테스트에 사용된 워터마킹 알고리즘들

은 Strimark에서 사용되었던 (A)cox기법, (B)WaterStamp, (C)digimarc 이다. cox 프로그램은 trimming, 확대, 사영 변경 공격을 제외한 모든 공격에 강인함을 확인할 수 있고, WaterStamp 프로그램은 사영 변경, 프린트/스캔 공격을 제외한 공격에 강인함을 알수 있다. 반면 digimarc 프로그램은 trimming, 확대, 사영 변경, 프린트/스캔 공격에 취약함을 확인할수 있다.

Attacks	A	B				C
		V0.9	V4.0 (30)	V4.0 (70)	V4.0 (100)	
JPEG압축(1)	1	1	0	1	1	1
JPEG압축->JPEG신장(4)	4	4	1	1	2	4
JPEG신장->JPEG압축(1)	1	1	0	1	1	1
trimming(4)	0	2	3	3	3	1
확대(4)	0	3	1	2	2	0
축소(4)	4	4	1	2	2	4
계조변경(4)	4	4	4	4	4	4
사영변경 (4)	1	2	0	0	0	0
공간주파수변경(4)	4	4	4	4	4	4
프린트/스캔 (4)	4	0	0	0	0	0
합계(34)	23	25	14	18	19	19

표7. JEWELS 공격의 워터마크 추출 결과

5.4 고찰

Stirmark 버전 4.0의 특징을 보면 워터마킹 기술은 서로 다

른 목적으로 많은 응용 분야에 적용되기 때문에 벤치마킹 전에 사용 목적과 대상을 선택하도록 하고 있다. 즉 영상의 품질, 계수, 강인성, 공격의 강도 등을 적용하여 벤치마킹을 실시한다. 하지만 Stirmark 벤치마킹은 단순한 디지털 영상 처리 및 기하학적 변형에 의한 공격들이 주를 이루고 있기 때문에 영상 및 워터마크의 통계적 특성 등을 분석하여 공격을 가하는 보다 지능적인 공격에 대해서는 평가가 제대로 이루어지지 않는 단점을 가지고 있다. 그리고 척도로 이용되는 PSNR은 시각적인 척도로는 부적합하며 삽입, 추출에 걸리는 시간을 고려하지 않고 이미지의 사전정보를 고려하지 않은 문제점들을 가지고 있다. 반면 Checkmark는 출력 양식을 XML 포맷으로 나타내며 결과 테이블은 HTML 문서로 작성이 되어 눈으로 평가 결과를 비교적 용이하게 확인 가능한 장점이 있다. 또 새로운 화질 평가 방법으로 weighted PSNR과 Watson metric을 도입하고 있다.

JEWELS는 각각의 응용분야에 따라 평가 프로파일을 달리 설정하여 특성에 맞게 평가하고 작업파일을 사용자가 구성해 사용자의 목적에 맞게 공격할 수 있는 유연성이 있다.

워터마킹 알고리즘을 개발한 개발자가 강인성을 평가해보기 위해 벤치마킹 툴을 쓰고자 할때 응용분야가 확실히 정해져있고 알고리즘이 Matlab으로 구현이 용이하다면 Checkmark를 사용하면 워터마킹 삽입 추출까지 벤치마킹 툴에서 이루어질 수 있으며 추출시 일일이 알고리즘에서 확인하지 않고 추출 결과를 HTML 문서로 쉽게 결과를 확인 할수 있다. 하지만

구현된 알고리즘이 Matlab으로 구현이 어렵고 강인성 부분에서 기하학적인 공격방법으로 세부적으로 평가하고자 한다면 Stirmark를 권하고자 한다. Stirmark는 각 공격항목에 대해 여러 가지의 파라미터들이 설정되어있으므로 세밀히 평가할수 있다. 그리고 지금 현재 <http://stirmark.kaist.ac.kr/menu.html> 이 사이트에 가면 자신이 개발한 알고리즘을 Stirmark 4.0 엔진에서 웹에서 평가할수 있도록 서비스가 제공되고 있다. 단 자신의 알고리즘을 워터마킹 라이브러리(*.dll)로 업로드 시켜야 테스트해 볼수 있도록 되어있다. 그리고 자신의 알고리즘을 기하학적인 공격뿐 아니라 두루두루 간단히 테스트 하고자 한다면 JEWELS를 권하고자 한다. JEWELS에서는 자신이 테스트 하고자 하는 공격항목과 파라미터를 사용자가 작업파일 .jcl로 만들어 테스트 할수 있으므로 사용자의 구미에 맞게 쉽게 테스트 할수 있는 장점이 있다.

6. 결론

디지털화된 멀티미디어 데이터의 사용증가와 컴퓨터 상에서의 유통이 용이해짐에 따라 저작권을 보호하기 위한 방법으로 디지털 워터마킹 기법이 활발히 연구되고 있으며, 저작권 보호뿐만 아니라 인증/무결성, 불법 유통자 추적 등 그 응용분야도 점차적으로 늘어나고 있다. 이렇게 워터마킹에 대한 국제적 관심은 급증하고 있지만 이를 지원할 표준화 활동은 많지 않다.

강인하고 유용한 워터마크를 개발 및 평가하는데 도움이 될 수 있도록 본 논문에서는 기존에 개발되어있는 cox기법, Waterstamp, Digimarc 3가지 워터마킹 기법의 소개와 디지털 워터마킹 평가항목에는 어떤 것이 있는지, 공격방법은 어떻게 분류되었는지 간단히 알아보고 이러한 워터마킹 기법에 대한 공격 벤치마킹 툴인 Stirmark, Checkmark, JEWELS의 기본 구성 및 소개를 하였다. 벤치마킹 툴에서 사용되는 공격항목을 회전, 스케일링, 클리핑, 변환, 필터링, 압축, 소거 공격으로 분류를 하고 각 벤치마킹 툴에만 있는 공격에는 어떤 것이 있는지 분석을 하고 어떤 공격에는 어떤 툴을 사용하는 것이 유용한지 평가를 하였다. 그리고 2장에서 소개된 각 워터마크 삽입 및 추출 프로그램을 사용하여 Stirmark, Checkmark, JEWELS 3개의 벤치마킹 툴을 이용하여 실험을 하였다.

Stirmark는 주로 단순한 신호처리 및 기하학적 공격들로 이루어져있지만 강인성 부분에서 평가하고자 할 때 각 공격항목

에 파라미터가 많으므로 세밀히 공격할 수 있는 장점이 있었으며 Checkmark는 알고리즘이 Matlab으로 구현이 가능하면 삽입,추출 과정이 벤치마킹 툴 속에 포함되어 공격에 대한 검출 결과가 XML 및 HTML 문서로 출력이 되므로 결과에 대한 정리가 간단한 장점이 있다. JEWELS는 Stirmark와 Checkmark에 없는 Gradation, 프린트/스캔, 합성영상 공격이 있어 색다른 공격을 할 수 있다.

테스트에 사용된 알고리즘들이 각기 다른 기법들로 개발되었기 때문에 향후 연구과제로 같은 기준을 가지고 있는 알고리즘들을 대상으로 각 벤치마킹 툴을 사용하여 공격을 하여 벤치마킹 툴에 대한 장,단점에 대해서 좀더 명확한 평가를 할 수 있도록 하여야 할 것이다. 그리고 앞서 살펴본 바와 같이 여러 벤치마킹 툴의 단점을 보완하고 장점을 살려 각 응용분야에 맞게 프로파일을 구성한 벤치마킹 프로그램 개발 및 평가기준이 국내에서도 이루어져야 할 것이다.

<참고문헌>

1. 이명호, 워터마킹 기술 분석 및 공격법 연구 최종보고서, 한국전자통신연구원, Jan. 2002
2. G. C. Langelaar, I. Setyawan and R. L. Lagendijk, "Watermarking Digital Image and Video Data: A State-of-the-art Overview", IEEE Signal Processing Magazine, Vol.17, No.5, pp.20-46, Sept. 2000.
3. I.Cox, J.Kilian, F.T.Leighton, and T.Shannon, "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, vol.6, pp.1673-1687, 1997.
4. <http://watermarking.unige.ch/Checkmark/>
5. <http://vision.unige.ch/certimark/>
6. <http://www.jeita.or.jp>
7. <http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/>
8. M. Kutter, F Petitcolas "A Fair Benchmark for Image Watermarking Systems." Proc. of SPIE: Security and Watermarking of Multimedia Contents, Vol.3657, pp. 226-239, 1999.
9. 김형중, "디지털 워터마킹 기술현황 분석 및 기능규격 제안 최종보고서", 한국디지털콘텐츠포럼, Jan. 2002
10. <http://www.cosy.sbg.ac.at/~pmeerw/Watermarking>
11. <http://www.digitreal.com/>
12. 강현호, 임쌍학, 박지환, "Checkmark를 이용한 디지털 워

터마킹 평가 연구”, 한국멀티미디어학회 논문집, Nov. 2002

13. 김민정, 박지환, “Stirmark를 이용한 영상 워터마킹 평가 연구”, 한국멀티미디어학회 논문집, Nov. 2002

14. 김은실, 손윤경, 박지환 “디지털 워터마킹 평가에 관한 고찰”, 한국멀티미디어학회지, Vol 5-1

15. 이진홍, 임태훈, 박지환, “디지털 워터마킹 알고리즘 평가 프로파일에 관한 연구”, 한국멀티미디어학회 논문집, Nov. 2002

감사의 글

대학원에 진학하겠다고 서울에서 다니던 직장을 그만두고 귀향한지 어느덧 3년이 지나 교육대학원 졸업을 앞두고 있습니다. 부족한 점이 많은 저에게 무사히 논문을 마칠 수 있도록 곁에서 도움을 주신 모든 분들의 격려에 감사드립니다.

먼저, 한국멀티미디어학회 사무국에서 업무를 하면서 학업을 마치도록 배려해주시고 3년여 동안 관심으로 지도해주신 박지환 교수님께 진심으로 감사의 말씀을 전합니다. 그리고, 심사를 맡아 주신 김영봉 교수님과 박승섭 교수님께 감사드리고, 박만곤 교수님, 여정모 교수님, 윤성대 교수님, 김창수 교수님, 이경현 교수님, 박홍복 교수님, 정순호 교수님께 감사드립니다.

학회업무를 제일 많이 도와줬던 동기 소진이, 후배 순혜, 정애, 그리고 여러 가지 일 때문에 많이 신경을 못 써드렸던 동기 임쌍학 선생님, 항상 친절하게 응대해주었던 이미나 대학원 조교에게도 감사의 마음을 전합니다. 멀티미디어 압축 및 보호 연구실의 모든 일반대학원, 교육대학원, 산업대학원의 선·후배 여러분께도 감사드리며, 특히, 이번 졸업논문에 있어서 여러 가지 조언을 해주셨던 강현호 선배님께 감사드립니다.

일과 공부를 병행하는데 어려움이 없도록 배려하고 격려해주신 한국멀티미디어학회 회장님, 총무이사님, 재무이사님 등 운영위원님께도 이 논문을 빌어 감사말씀 드립니다.

끝으로, 먼 곳에서 정신적인 힘이 되어주었던 오빠와 군대에서 열심히 훈련을 받고 있을 동생, 그리고 모든 투정과 짜증을 다 받아주시고 딸의 미래 걱정에 잠 못 이루시던 사랑하는 부모님께 이 논문을 바칩니다.

2003.7. 김민성