Stirmark를 이용한 영상 워터마킹 평가 연구

김민정*, 박지환**
*부경대학교 교육대학원 전산교육전공
**부경대학교 전자컴퓨터정보통신공학부

A Study on Image Watermarking Evaluation with Stirmark

Min-Jeong Kim*, Ji-Hwan Park**
Dept. of Computer Education, Pukyong National University
Div. of Electronic, Computer & Telecom. Eng., Pukyong National Univ.

요 약

디지털 워터마킹 평가를 위한 벤치마킹 방법이 여러 가지 개발되고 있다. 특히 Stirmark 벤치마킹은 정지영상에 대한 디지털 워터마킹 기술을 평가하기 위한 방법으로 현존 벤치마킹 방법들 중 가장 대표적인 것으로서 강인성에 주안점을 둔 방법이다. 본 논문에서는 Stirmark의 공격 종류와 Stirmark를 이용하여 기존에 개발되어 있는 여러 가지 워터마킹 기법을 평가하고자 한다.

1. 서 론

디지털 워터마킹은 암호화와 함께 디지털 컨텐츠의 저작권자 및 소유권자의 권익을 보호하기 위한 효율적인 방법 중의 하나이다. 디지털 컨텐츠의 저작권자나 소유권자를 보호하기 위해 삽입된 디지털 워터마크는 다양한 디지털 컨텐츠의 응용 및 활용에 따라 본의 아니게 손상을 입거나 변형될 우려가 있다. 또한, 디지털 컨텐츠를 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[1,2].

- 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.

현재 널리 사용되고 있거나 또는 평가를 위해 개발중인 디지털 워터마킹의 벤치마킹 방법에는 Checkmark[3],Optimark[4],Certimark[5],JEWELS[6], Stirmark[7] 등이 있다.

본 논문은 2장에서 Stirmark의 구성을 알아보고, 3장에서 기존에 개발되어 있는 워터마킹 기법을 실제 영

본 연구는 SEDICA 지원에 의해 수행되었음.

상에 적용한 후, Stirmark를 이용하여 공격, 평가하고자 한다.

2. Stirmark[7-9]

Stirmark는 정지영상(still image)에 대한 디지털 워터마킹 기술을 평가하기 위한 방법으로서 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.

2.1 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°

2.2 Stirmark의 구성

그림1. Stirmark Test Platform 구조

/ 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

Stirmark 벤치마킹 툴은 다음 사이트에 가면 소스가 공개되어 있고 다운로드 받을 수 있다.

http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/

Stirmark의 구조는 표1과 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.

3. 실험 및 평가 결과

Stirmark는 평가를 위해 어떤 특정한 워터마킹 기법을 정해놓고 있지는 않다. 즉 사용자가 개발한 모든 워터마킹 기법을 대상으로 알고리즘을 평가할 수 있다. 본 논문에서는 테스트를 위해 [10]에서 소개되고 있는 Cox의 기법과 상용화 단계에 있는 [11]의 테스트용 WaterStamp 0.9 버전과 그래픽 에디터 프로그램인 Adobe Photoshop 6.0의 필터에 있는 Digimarc를 사용하여 워터마킹 삽입 및 추출을 수행하였다.

3.1 Cox 워터마킹 기법

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

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

주의 할 것은 [10]에서 소개되어지는 이 소스의 입출력은 PGM 파일 포맷의 512*512 크기 8비트 그레이 스케일만을 한정하고 있다. 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.

3.2 WaterStamp v0.9 & Digimarc

WaterStamp 버전 0.9와 Adobe Photoshop 버전 6.0의 Digimarc는 윈도우 기반 프로그램이므로 쉽게 워

터마크를 삽입, 추출할 수 있다. 테스트용 버전이므로 삽입되는 워터마크는 제작사에서 지정해 놓은 것으로 제한되어 있다. WaterStamp는 Cox 기법과 같이 추출 단계에서 원본 이미지가 필요한 non-blind 방식이고 Digimarc는 원본 이미지가 필요 없는 blind 방식임을 알수 있다. Digimarc에서는 내성을 1~4까지 입력 가능하다. 숫자가 클수록 내성은 강하고 화질은 떨어진다. 본 논문에서는 내성을 2로 정하여 워터마크를 삽입하였다. WaterStamp의 워터마크 실행 화면과 Digimarc의 워터마크 삽입 화면은 그림2, 3과 같다.

그림2. WaterStamp 실행 화면

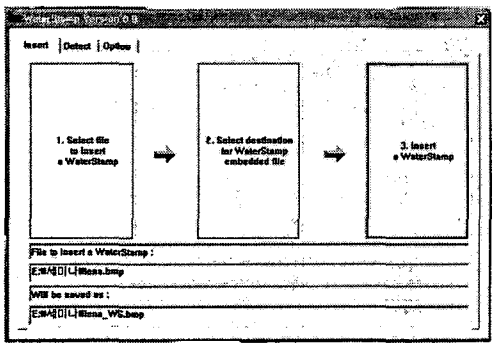
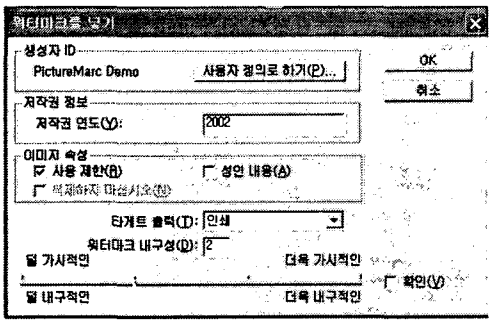


그림3. Digimarc 워터마크 삽입 화면



3.3 평가 결과

표2는 Stirmark 4.0을 이용하여 공격한 후 추출한 결과 테이블이다. 여기서 (A)는 Cox 기법, (B)는 WaterStamp v 0.9 (C)는 Digimarc 프로그램을 나타낸다. 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. 각 공격 항목의 parameter값은 부록에 보인다. Cox 기법은 비교 단계에서 Correlation 이 0.2 이상이면 워터마크가 살아 남은 것으로 간주한다. 워터마크가 살아남은 확률을 보면 (A)는 78%, (B)는 84%, (C)는 49%로 나타났다. JPEG 압축, Rescale, MeidanCut, RemoveLines 공격항목에서는 3가지 프로그램 모두 대체로 강인함을 알 수 있다.

표2. 공격에 대한 워터마크 추출 결과

구분	Attacks	A	B	C
JPEG	JPEG압축	12/12	12/12	11/12
Geometric Transforms	Afine	7/8	6/8	3/8
	Rescale	6/6	6/6	6/6
	Rotation	9/15	9/15	2/15
	SamllRandom Disortions	4/4	4/4	0/4
	LatestSamllRandom Disortions	4/4	0/4	0/4
	RotaionScale	10/10	8/10	2/10
	RotationCrop	10/10	8/10	2/10
Signal Processing	AddNoise	2/6	6/6	1/6
	ConvFilter	1/2	2/2	2/2
	MedianCut	4/4	4/4	3/4
	Selfsimilarities	0/3	3/3	2/3
Special Transforms	Cropping	0/9	7/9	0/9
	RemoveLines	10/10	10/10	10/10
	Rotation 90°	0/1	1/1	0/1
PSNR	-	11/11	11/11	11/11
합계		90/115	97/115	56/115

4. 결 론

워터마킹 기법에 대한 공격 벤치마킹 툴인 Stirmark의 기본 구성을 살펴보고, 각 워터마크 삽입 추출 프로그램을 사용하여 Stirmark를 이용하여 평가해 보았다. Stirmark 버전 4.0의 특징을 보면 워터마킹 기술은 서로 다른 목적으로 많은 응용 분야에 적용되기 때문에 벤치마킹 전에 사용 목적과 대상을 선택하도록 하고 있다. 즉 영상의 품질, 계수, 강인성, 공격의 강도 등을 적용하여 벤치 마킹을 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. 이런 Stirmark의 단점을 보완하고 각 응용 분야에 맞게 프로파일을 구성한 벤치마킹 프로그램 개발이 국내에서도 이루어지어야 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] http://watermarking.unige.ch/Checkmark/

[4] http://poseidon.csd.auth.gr/optimark/

[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/

[부록] - Stirmark 공격항목의 parameter

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
LatestSmallRandomDistortions	0.95, 1, 1.05 1.1