특집논문-01-6-1-07

스크린 마크 공격 : 새로운 정지영상 워터마킹 공격 기법

박 현 중*, 이 충 훈**, 이 흥 규**

Screen Mark Attack : A New Image Watermarking Attack

Hyun-Joong Park*, Choong-Hoon Lee** and Heung-Kyu Lee**

요 약

본 논문에서는 영상 워터마킹에 대한 새로운 공격 방법인 스크린 마크(Screen Mark) 공격 방법을 소개한다. 스크린 마크 공격 방법은 오버마크(overmark) 공격 방법을 응용한 공격 방법으로써, 워터마크가 삽입된 영상에 공격자의 워터마크를 삽입하여 워터마크 검출기가 정상적으로 작동하지 못하게 하는 공격 방법이다. 공개(public) 워터마킹 시스템에 오버마크 공격을 적용할 수 없는 것과는 달리, 제안한 공격 방법은 공개 워터마킹 시스템에도 적용할 수 있다. 제안한 공격 방법을 통하여 상용 워터마킹 시스템을 이용하여 워터마크를 삽입한 영상을 효과적으로 공격할 수 있었으며, 다른 워터마킹 공격 방법들을 이용하여 공격한 영상보다 보다 좋은 화질을 보인다.

Abstract

This paper describes a new watermarking attack algorithm, a screen mark attack. The screen mark attack is a modified overmarking attack, which attacks a watermarking system by inserting another watermark into a marked image. Overmarking attack has a problem that it cannot be applied to a public watermarking software that prohibits the watermark embedder from embedding another watermark into an already marked image. However, the proposed attack algorithm can be applied to such a public watermarking scheme. Test results show that the proposed watermarking attack algorithm is successful for commercial watermarking softwares and attacked images show better quality than images attacked by other attack tools.

I. 서 론

디지털 데이터 처리능력의 발달의 부작용으로 데이터의 불법복제 및 불법 유포가 용이해져 멀티미디어 데이터와 같은 대용량 데이터도 쉽게 복제가 가능해졌다. 멀티미디어의 저작권 문제와 불법복제 문제를 해결하기 위하여 암호화 기법이 이용되기는 하지만, 완벽한 해결책을 마련해 주지는 못하였다. 이와 같은 문제로 인하여 저작권을 보호하기 위한 새로운 방법으로 디지털 워터마킹이 소개되었다.

한편, 워터마크의 견고성에 대한 체계적인 벤치마크(benchmark)를 수행하기 위해 워터마크 공격 기법에 대한 연구가 활발히 진행되고 있다. 대표적인 워터마크 공격 벤치마킹 프로그램으로 StirMark와 Unzign을 들 수 있고[1][2], 그 외에도 영상처리와 같은 단순 공격과, 기하학적인 공격, 여러 개의 워터마크를 삽입하여 공격하는 오버마킹과 같은 모호성 공격[3], 워터마크를 통계적인 방법으로 추정하여 제거하는 공격 방법[4][5] 등 다양한 워터마킹 공격방법이 존재한다.

* SK Telecom, Platform Application 개발 팀
SK Telecom, Platform Application Development Team
** 한국과학기술원 전산학과/해킹 바이러스 연구센터
KAIST Computer Science Dept./Hacking and Virus research Center

※ 본 연구는 첨단정보기술 연구센터를 통하여 과학재단의 지원을 받았음.

본 논문은 정지영상을 위한 공개 워터마크 시스템에 대해 제 2의 워터마크를 삽입하여 워터마크 검출기가 올바른 워터마크를 검출할 수 없도록 하는 새로운 공격방법을 소개한다. 제안된 방법은 오버마킹 공격의 변형으로, 기존의 오버마킹 공격이 공개 워터마킹 시스템에 적용할 수 없다는 문제를 안고있는 반면에, 제안한 방법은 공개 워터마킹 시스템에도 적용할 수 있다.

본 논문의 구성은 다음과 같다. II장에서는 기존의 워터마킹 공격 방법들에 대하여 살펴보고, III장에서는 제안한 워터마킹 공격 방법에 대하여 설명한다. IV장에서는 제안한 방법이 효과적으로 워터마킹 시스템을 무력화시킴을 보이고, V장에서 결론을 맺는다.

II. 관련 연구

워터마킹 기술과 워터마크 공격 방법은 워터마크를 삽입하려고 하는 디지털 데이터(정지영상, 동영상, 오디오 등)에 따라 다양하다[3]. 본 장에서는 정지영상에 대한 워터마크 공격 방법에 관한 연구들을 살펴본다.

본 장의 구성은 다음과 같다. 워터마크의 공격에 대한 정의를 1절에서, 워터마크 공격의 유형별 분류는 2절에서 알아본다.

1. 워터마킹 공격의 정의

워터마킹 공격이란 워터마크가 삽입된 정지영상을 조작하여 워터마크 신호를 제거하거나, 워터마크 신호를 검출할 수 없게 만들거나, 또는 위조된 워터마크를 만들어 워터마크를 삽입한 사람이 소유권을 주장할 수 없게 만드는 방법이다.

2. 워터마크 공격의 유형별 분류

본 논문에서는 [4]에서 사용을 했던 워터마크 공격(Watermark Attack)의 분류 방법을 사용하여 설명한다. 이 방법에서는 다음과 같이 크게 4개의 서로 다른 워터마크 공격 방법으로 분류한다.

2.1 단순 공격(Simple Attack)

단순공격은 파형 공격(Waveform Attack) 또는 잡음 공격(Noise Attack)이라고 일컬어지기도 하며, 워터마크를 축출하거나 제거하려는 어떤 시도도 없이 단순히 워터마크가 삽입된 영상 전체를 조작하여 워터마크에 손상을 가하는 공격을 말한다. 단순공격의 예로 선형(Linear) 또는 일반적인 비선형(Non-linear) 필터링, MPEG과 JPEG같이 파형에 기초로 한 압축방법, 잡음 삽입, 크러핑(Cropping), 화소(Pixel) 영역에서의 양자화(Quantization), 아날로그로 변환, 그리고 감마 교정(Gamma Correction) 등을 들 수 있다.

2.2 검출불능 공격

검출불능 공격(Detection-disable Attack)은 동기성 공격(Synchronization Attack)이라고 일컬어지기도 하며, 삽입된 워터마크와 워터마크 패턴의 상관관계(Correlation)를 제거하여 워터마크 검출기가 워터마크를 검출할 수 없게 만드는 공격을 말한다. 검출불능 공격의 대표적인 예는 영상 확대(Zooming), 영상 회전(Rotation), 영상부분 축출(Subsampling), 픽셀들의 삽입 및 제거, 영상 이동(Shifting) 그리고 다른 기하학적인 변환 등을 들 수 있다.

2.3 모호성 공격(Ambiguity Attack)

모호성 공격은 위조 워터마크 공격(Fake-watermark Attack), 반전 공격(Inversion Attack), 또는 데드락 공격(Deadlock Attack)이라고 일컬어지기도 하며, 위조 원형 영상을 만들거나 위조 워터마크를 만들어서 워터마크를 검출할 때 혼동을 일으키게 하는 공격을 말한다[2]. 모호성 공격의 대표적인 예로 하나 또는 그 이상의 워터마크를 삽입하여 최초의 워터마크가 무엇인지 알 수 없게 만들어 영상의 소유권에 대한 혼란을 일으키는 반전 공격(Inversion Attack)을 들 수 있다[5].

2.4 제거 공격(Removal Attack)

제거 공격(Removal Attack)은 워터마크가 삽입된 영상을 분석한 후 워터마크를 추정하거나 워터마크가 삽입되기 전의 영상을 추정하여 워터마크를 제거하거나 워터마크를 무용지물로 만드는 공격을 말한다. 제거 공격의 대표적인 예는 결탁 공격(Collusion Attack)[6], 비선형 필터 연산을 이용한 공격[7] 등을 들 수 있다.

III. 스크린 마크 공격

본 장에서는 오버마킹 공격 방법의 기본적인 아이디어를 응용한 스크린 마크 공격 방법이라는 새로운 형태의 정지 영상 워터마킹 공격 방법을 제안한다. 오버마킹 공격 기법이란 이미 워터마크가 삽입되어 있는 데이터에 또 다

른 워터마크를 삽입하여, 실제 데이터의 저작자가 누구인지 판별할 수 없도록 하는 공격 방법이다. 일반적으로 공개(public) 워터마킹 시스템은 워터마크를 삽입하기 전, 데이터에 다른 워터마크가 삽입되어 있는 지를 조사한 후 워터마크를 삽입하는 방법을 취하기 때문에, 이미 워터마크가 삽입되어 있는 영상에 또 다른 워터마크를 삽입하는 오버마킹 공격 방법을 적용할 수 없다. 본 논문에서는 위와 같은 공개 워터마킹 시스템에 또 다른 워터마크를 삽입할 수 있는 공격 방법을 제안하고, 이전에 삽입된 워터마크의 기능을 방해하는 새로운 마크를 삽입한다는 의미에서 스크린 마크 공격이라 칭한다. 본 논문에서 제안한 방법은 워터마킹의 개념 자체를 이용하는 공격 방법이기 때문에 프로토콜 공격 기법에 해당하며, 따라서 공격 대상이 되는 워터마킹 시스템의 알고리즘에 무관하게 공격을 가할 수 있다.

본 논문에서 제안된 공격 방법은 크게, 공격자의 워터마크인 스크린 마크를 생성하는 1단계와, 스크린 마크를 공격하고자 하는 영상에 삽입하는 2단계로 나뉜다. 스크린 마크를 생성하는 과정은 1절에서 그리고 생성된 스크린 마크를 이용하여 공격하는 방법은 2절에서 각각 설명한다.

1. 스크린 마크 생성과정

제안한 공격 방법은 워터마크가 삽입된 영상에 공격자의 새로운 마크를 삽입하는 방법이다. 본 방법을 이용하여 워터마킹 시스템을 공격하려면, 공격자의 워터마크(스크린 마크)가 필요하다. 워터마킹 시스템이 한 개인에 대하여 모든 영상에 동일한 워터마크를 삽입하는 형태라면, 공격자는 공격하고자 하는 영상이 아닌 다른 영상에 워터마크를 삽입하고 워터마크가 삽입된 영상과 원 영상과의 차이를 이용하여 공격자 자신의 워터마크를 쉽게 생성해 낼 수 있고, 이 워터마크를 공격하고자 하는 영상에 합성으로써 쉽게 오버마킹과 같은 공격을 가할 수 있다. 그러나, 워터마킹 시스템이 동일한 사람에 대하여 영상마다 다른 워터마크를 삽입하는 형태라면, 즉, 영상에 종속적인(dependent) 워터마크를 삽입하는 상태라면, 한 영상을 위하여 생성된 워터마크는 다른 영상에 적용 할 수 없는 워터마크이므로, 이와 같은 방법으로는 공격에 실패하게 된다. 본 절에서는 영상에 종속적인 워터마크를 삽입하는 워터마킹 시스템에서도 유효한 워터마크로 인식될 수 있는 공격자의 워터마크를 생성하는 방법에 대하여 설명한다.

공격자의 워터마크인 스크린 마크의 생성과정은 크게 피 공격자의 워터마크가 삽입된 영상에서 워터마크를 제거하는 1단계와 워터마크가 제거된 영상을 이용하여 공격자의 워터마크인 스크린 마크를 생성하는 2단계로 나눌 수 있다. 1단계에서는 반복적인 필터링 공격을 가하여 영상으로부터 피 공격자의 워터마크를 제거하는 오라클(oracle) 공격 방법을 적용하여 워터마크를 제거한다[8][9]. 스크린 마크 생성에 관한 개념 도는 그림 1과 같으며, 생성과정은 다음과 같다. 본 과정에서는 Alice의 워터마크가 삽입된 영상 X에 Mallory가 공격을 가한다고 가정한다.

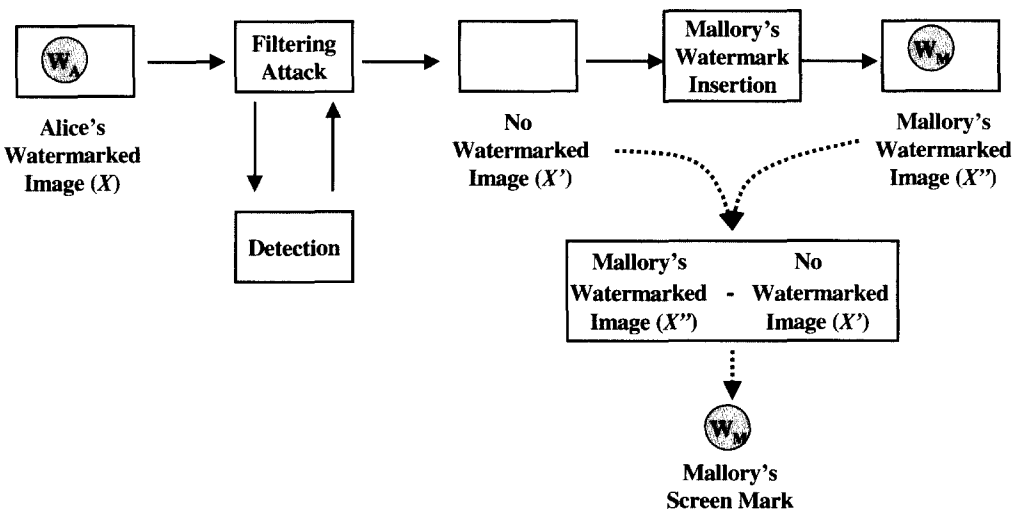


그림 1. 스크린 마크의 생성과정
Fig. 1. Screen mark generation

① 공격대상 영상 (피 공격자인 Alice의 워터마크(W_A)가 삽입되어있는 영상) X에 블러링과 같은 필터링(filtering) 공격을 미세하게 가한다.

② 워터마크 검출기를 이용하여 Alice의 워터마크가 검출되는지를 확인한다. 만일, Alice의 워터마크가 검출되면 ①을 Alice의 워터마크가 추출되지 않을 때까지 반복 수행하여, Alice의 워터마크가 제거된 영상 X'를 얻는다[8][9].

③ 공격자인 Mallory는 Alice가 사용한 워터마킹 시스템을 이용하여 영상 X'에 자신의 워터마크(W_M)를 삽입하여 영상 X"를 얻는다. 영상 X'에는 워터마크가 제거된 상태이므로 공개워터마킹 시스템에서도 워터마크를 삽입할 수 있게된다.

④ Mallory는 자신의 워터마크가 삽입된 영상 X"과 삽입되지 않은 영상 X'를 이용하여 두 영상의 차이를 구함으로써, 해당 영상에 대한 자신의 워터마크 신호(W_M)를 구할 수 있다. 이를 스크린 마크라 칭한다. 스크린 마크 W_M은 Alice가 사용한 워터마킹 시스템을 이용하여 생성하였고, Alice의 영상 X를 통하여 얻은 마크이기 때문에, 영상에 종속적인 워터마크를 삽입하는 워터마킹 시스템에서도 영상 X에 대하여 유효한 워터마크로 사용될 수 있다.

2. 스크린 마크의 삽입 및 공격

1 절에서 생성한 Mallory의 스크린 마크를 이미 Alice의 워터마크가 삽입되어 있는 영상에 삽입하여 공격하는 과정은 그림 2와 같다.

스크린 마크 생성과정을 통해서 얻은 Mallory의 마크 W_M를 가중치(α)를 이용하여 신호의 강도를 조절한 후, Alice의 워터마크가 삽입된 영상(X)과 합성하여 스크린 마크 공격 영상(X*)을 생성한다. 이런 식으로 합성된 영상(X*)에는 Alice의 워터마크 신호(W_A)와 Mallory의 워터마크 신호(W_M)가 동시에 존재하는 형태가 되어, 워터마크 추출기는 정상적인 저작권자를 판별 할 수 없게 된다.

본 논문에서 제안하는 공격 방법은 프로토콜 공격 방법의 일종으로, 공격하고자하는 워터마킹 시스템의 알고리즘이나 기법 등과 상관없이 공격을 가할 수 있고, 따라서, 피공격자인 Alice의 워터마크와 공격자인 Mallory의 워터마크의 형태에 대한 정보는 필요치 않다. 정상적인 공격을 위하여 Mallory의 워터마크는 위의 과정과 같이 Alice가 워터마크를 삽입하는데 이용했던 워터마킹 시스템과 Alice의 워터마크가 삽입된 영상을 통하여 추출해내어야 한다는 전제조건만 만족시키면 본 공격 방법을 적용할 수 있다.

3. 스크린 마크의 가중치

Alice의 워터마크가 삽입된 영상에 가중치(weight factor)를 곱하여 얻은 스크린 마크를 삽입하여 스크린 마크 공격을 이용하여 공격한 영상X*는 식 (1)과 같이 표현할 수 있다.

$$X^* = X + \alpha W_M = X^o + W_A + \alpha W_M \qquad (1)$$

X*에 대한 워터마크 검출 결과는 가중치α에 따라서 달라질 수 있다. 따라서 가중치를 적당히 크게 하여, 워터마크검출기가 Mallory의 워터마크만을 검출하거나, 두 워터마크가 모두 검출되거나 둘 중 아무 것도 검출하지 못하도록 하여야 한다. 가중치는 새로 삽입하는 마크의 강도뿐 아니라 영상의 화질에도 영향을 미치므로, 영상의 화질 저하를 최소화하도록 적절히 조절하는 것이 필요하다.

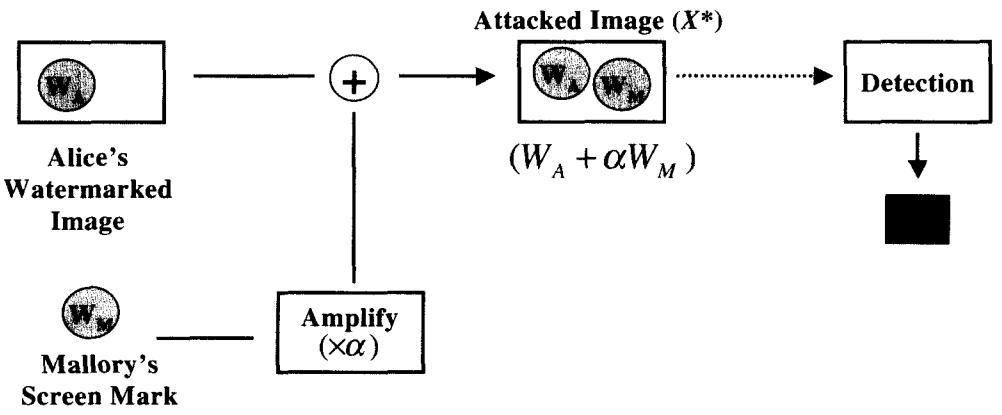


그림 2. 스크린 마크의 삽입을 통한 공격과정
Fig. 2. Attack process by screen mark insertion

Ⅳ. 성능 평가

1. 검출 능력 평가

스크린 마크 공격 기법의 평가를 위하여 상용 워터마킹 소프트웨어를 이용하여 테스트하였다. 사용한 워터마킹 소프트웨어는 Digimarc사의 Picturemarc 1.6.84와 Signum Technologies사의 Suresign 3.1으로, 가장 잘 알려진 영상 워터마킹 소프트웨어이다. 두 소프트웨어 모두 공개 워터마킹 기법을 사용하여, 사용자의 키를 요구하지 않고 워터마크 삽입 추출이 가능하며, 워터마크 신호로써 사용자의 ID 정보를 삽입 추출한다. 두 워터마킹 시스템 모두 영상에 이미 워터마크가 삽입되어있으면, 새로운 워터마크를 삽입하지 못하도록 하는 기능이 있다. Picturemarc는 Suresign에 비하여 회전, 절삭, 확대/축소 등의 기하학적 공격에 강하고, Suresign은 상대적으로 압축이나, 필터링 등에 강한 것으로 평가된다[1].

테스트에 이용한 영상은 Balloon, Baboon, F16, Fishing Boat, Lena, Papers, Watch, Waterfall, Western House, Zebra등 10개의 256x256 크기의 흑백 영상이다. 먼저 한 사람의 워터마크를 생성하여 삽입한 후, 제안된 방법으로 또 다른 사람의 워터마크를 생성하여 삽입한 후 워터마크의 검출 결과를 테스트하였다. 이때, 식 1에서의 가중치 α를 변화시켜가며 워터마크 추출 실험을 행하여, 공격에 성공하여 먼저 삽입한 워터마크가 검출되지 않는 α값을 조사하였다. 결과는 표 1과 같다. 표 1에서 가중치가 α_1보다 작을 때는 원 저작자의 워터마크가 검출되었고, $\alpha_1 \sim \alpha_2$의 구간에서는 워터마크가 검출되기는 하나 누구의 워터마크인지를 판별할 수 없다는 결과가 나오며, α_2보다 가중치를 크게 하여 공격하였을 경우에는 공격자의 워터마크가 추출되어 공격이 성공적으로 이루어짐을 알 수 있었다. 표에서 α_1과 α_2의 값이 같은 경우는 누구의 워터마크인지를 판별할 수 없는 경우는 발생하지 않고 바로 공격자의 워터마크가 추출된 경우이다.

표 1. 가중치에 따른 검출 능력 평가
Table 1. Watermark detection test according to embedding strength

Watermarking Software	영상 / 가중치	1	2	3	4	5	6	7	8	9	10
Picturemarc	α_1	1.7	2.5	1.4	2.0	2.0	1.8	1.5	2.0	2.0	2.0
	α_2	2.1	3.0	2.0	2.0	2.1	2.0	2.0	2.1	2.1	2.0
Suresign	α_1	1.1	1.4	0.7	0.7	1.0	0.6	1.0	1.0	0.8	1.0
	α_2	1.8	3.0	1.4	1.5	1.5	1.1	1.4	1.6	1.4	1.5

2. 화질 평가

본 논문에서 제안한 스크린 마크 공격 기법의 화질을 평가하기 위하여, 워터마킹 공격 및 벤치마크 프로그램으로 잘 알려진 Stirmark와 Unzign과 비교하였다. Stirmak는 영상이 출력된 후 스캐닝을 통하여 재 입력되는 과정을 시뮬레이션 한 공격 방법으로써, 영상에 국부적으로 기하학

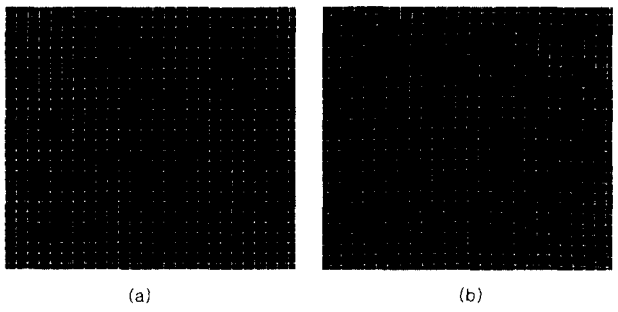


그림 3. Stirmark의 공격 결과 : (a) Stirmark 공격전, (b) Stirmark 공격후
Fig. 3. Stirmark attack result : (a) Before Stirmark attack, (b) After Stirmark attack

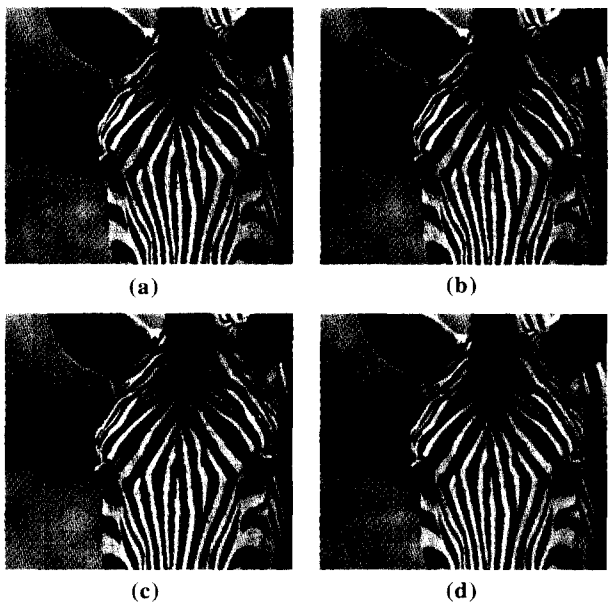


그림 4. 공격 방법들의 화질 비교, (a) 워터마크가 삽입된 영상, (b) 스크린 마크를 이용하여 공격한 영상, (c) Stirmark를 이용하여 공격한 영상, (d) Unzign을 이용하여 공격한 영상
Fig. 4. Image quality comparison (a) Marked image, (b) Image attacked by screen mark, (c) Image attacked by Stirmark, (d) Image attacked by Unzign

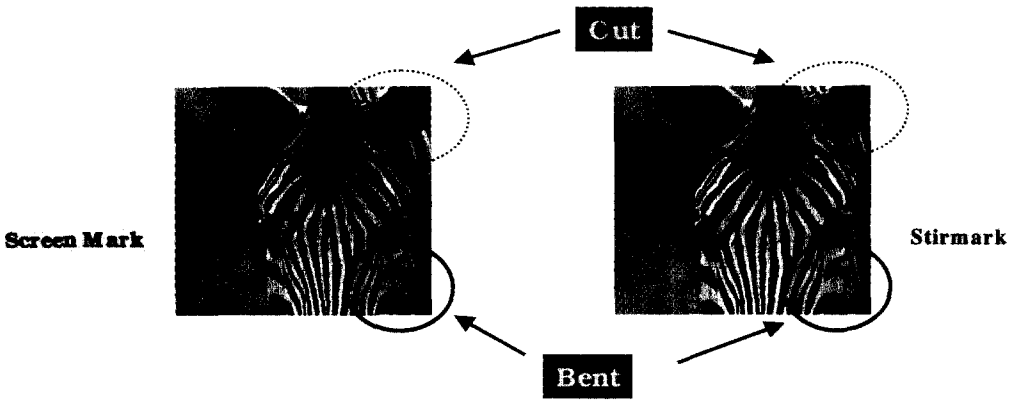


그림 5. 스크린 마크와 Stirmark의 비교
Fig. 5. Comparison between screen mark attack and Stirmark

적 변형을 일으켜 워터마크를 추출하지 못하도록 하는 공격 방법이다. 그림 3은 격자모양의 영상에 Stirmark로 공격을 가했을 때 발생되는 변형을 나타낸다. Unzign은 기하학적 변형과 필터링을 혼합한 형태의 공격 방법으로, 영상을 Unzign을 이용하여 공격할 경우 몽롱화(blurring)현상이 발생한다. 그림 4는 Zebra영상에 워터마크를 삽입한 영상과, 본 논문에서 제안한 스크린 마크 공격 기법으로 공격한 영상, 그리고, Stirmark 와 Unzign으로 공격한 영상을 나타낸다. 육안으로 관찰하였을 때에는 스크린 마크 공격과, Stirmark를 이용하여 공격한 영상은 좋은 화질을 나타내었으나, 필터링 공격을 가하는 Unzign의 경우 공격한 영상에 몽롱화 현상이 일어나 화질이 많이 저하됨을 알 수 있다. Stirmark의 경우 육안으로 보기에 화질 자체는 좋은 결과를 보여주지만, 공격 방법의 특성상 그림 5와 같이 영상을 왜곡시키는 현상이 나타난다. 그림 5의 Stirmark로 공격한 영상을 보면, 우측상단의 귀 부분이 약간 잘려나간 것과, 우측하단의 얼룩말의 얼굴부분이 조금 더 넓어진 것을 관찰할 수 있다. 따라서 Stirmark 공격 방법을 이용하여 사람의 얼굴 사진이나 영상 내 객체의 형태가 중요한 정보를 가지는 영상을 공격할 경우 육안으로 구별 가능한 정도의 품질 저하가 발생할 수 있다.

그림 6과 그림 7은 각각 Picturemarc를 이용하여 워터마크가 삽입된 영상과, Suresign을 이용하여 워터마크가 삽입된 영상에, 스크린 마크 공격과, Stirmark, Unzign으로 공격을 가한 후의 화질을 PSNR로 비교한 것이다. 세 가지 공격 방법 모두 공격에 성공하여 정상적인 워터마크가 추출되지 않았을 때의 화질을 평가한 것으로, 육안 테스트에서는 Unzign이 가장 좋지 않은 화질을 보였으나, PSNR의 경우 비교대상이 되는 두 영상의 동일위치의 화소 쌍을 비교하여 화질을 평가하므로, 영상을 기하학적으로 왜곡시키는 Stirmark가 가장 안 좋은 결과를 나타내었다. 그림에서 살펴볼 수 있듯이, 제안된 공격 방법으로 공격한 영상

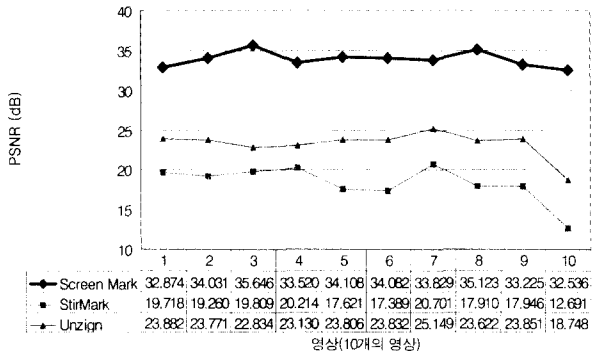


그림 6. Picturemarc에 대한 공격 후 화질 비교
Fig. 6. Image quality test of attacked Picturemarc images

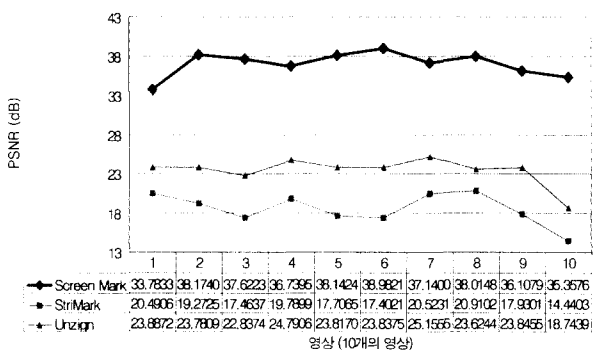


그림 7. Suresign에 대한 공격 후 화질 비교
Fig. 7. Image quality test of attacked Suresign images

들이 Picturemarc의 경우 Unzign으로 공격한 영상보다 평균 10.64dB, Stirmark으로 공격한 영상보다 평균 15.57dB 만큼 좋은 결과를 나타내며, Suresign의 경우 스크린 마크로 공격한 영상이 Unzign으로 공격한 영상보다 평균 13.57dB, Stirmark으로 공격한 영상보다 18.41dB만큼 좋은 결과를 나타낸다.

V. 결론 및 향후 연구 방향

본 논문에서는 공개(Public) 워터마크이며 견고한(Robust) 워터마크 시스템을 공격하는 새로운 워터마크 공격 기법인 스크린 마크 공격에 대하여 소개하였다. 제안한 방법은 상용 워터마킹 소프트웨어를 이용하여 워터마크가 삽입된 영상을 효과적으로 공격하여 기존에 삽입된 워터마크를 추출할 수 없도록 하였으며, 공격한 영상의 화질 면에서도 기존의 벤치마크 도구인 Stirmark와 Unzign을 이용하여 공격한 영상보다 뛰어난 결과를 보였다.

앞으로는 무엇보다도 스크린 마크 공격 기법을 극복할 수 있는 새로운 워터마크 알고리즘을 연구 개발하고 현재까지 알려지지 않은 워터마크 공격 기법에 대한 연구를 통해서 미래에 요구되는 강인한 워터마크 알고리즘 연구 개발에 도움을 줄 수 있도록 워터마크 공격 기법에 대한 연구가 활발히 이루어져야 한다.

참 고 문 헌

[1] StirMark Version 3.1 Watermark Robustness Test Software. [Oline]. Available :http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/

[2] Unzign Watermarking Removal Software. [Online]. Available WWW: http://www.cl.cam.ac.uk/~fapp2/watermarking/image_watermarking/unzign/

[3] Frank Harung and Marin Kutter, "Multimedia Watermarking Techniques," *Proceedings of the IEEE*, Vol. 87, No. 7, pp. 1079-1107, Jul. 1999

[4] F.Hartung, J. K. Su, and B. Girod, "Spread spectrum watermarking: Malicious Attacks and counterattacks," *Proc. SPIE Security and Watermarking of Multimedia Contents 99, San Jose, CA*, pp. 147-158, Jan. 1999.

[5] S. Craver, N. Memon, B. L. Yeo, and M. Yeung, "Can invisible watermarks resolve rightful ownerships?," *IBM, IBM Res. Rep. RC 20509*, Jul. 1996.

[6] H. S. Stone, "Analysis of attacks on image watermarks with randomized coefficients," *NEC Res. Inst., Princeton, NJ, Tech. Rep.*, May 1996.

[7] Gerhard.C Langelaar, Jan Biemond, Reginald L. Lagendijk, "Removing spatial spread spectrum watermarks by non-linear filtering," *Proc. Europ. Signal Processing Conf. (EU-SIPCO) '98), Rhodes, Greece*, pp. 2281-2284, Sep. 1998.

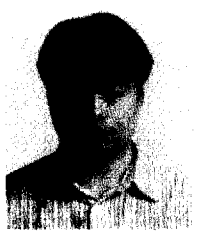
[8] Perrig, A., "A Copyright Protection Environment for Digital Images," *Diploma dissertation*, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, Feb. 1997.

[9] Linnartz, J.-P. M. G., and M. van Dijk, "Analysis of the Sensitivity Attack Against Electronic Watermarks in Images," *Proceedings of the Second International Workshop of Information Hiding*, vol. 1525 of Lecture Notes in Computer Science, Springer, pp. 258-272, 1998.

저 자 소 개

박 현 중

1999년 : 숭실대학교 컴퓨터공학부 학사
2001년 : 한국과학기술원 전산학과 석사
현재 : SK Telecom Platform Application 개발팀 연구원
주관심분야 : Real-time image transcoding, Wireless network



이 충 훈

1996년 : 동국대학교 컴퓨터공학과 학사
1998년 : 한국과학기술원 전산학과 석사
현재 : 한국과학기술원 전산학과 박사과정
주관심분야 : 디지털 워터마킹, 멀티미디어 저작권 보호기술

이 홍 규

1978년 : 서울대학교 전자공학과 학사
1981년 : 한국과학원 전산학과 석사
1984년 : 한국과학기술원 전산학과 박사
1984년~1986년 : Univ. of Michigan, Researcher
1986년~현재 : 한국과학기술원 전산학과 교수
1990년~1997년 : 인공위성 연구센터 연구기획 실장
2000년~현재 : DRM-Korea 보호기술 분과 위원장
E-mail : hklee@casaturn.kaist.ac.kr
Web : http://caio.kaist.ac.kr
주관심분야 : 디지털 영상 워터마킹, 멀티미디어 저작권 보호기술, 네트워크 보안