내성을 강화한 data embedding기법

정 인 식, 권 오 진
세종대학교 전자공학과
전화 : 02-3408-3828 / 핸드폰 : 016-396-5843

Enhanced robust data embedding techniques

In-Shik Jeong, Oh-Jin Kwon
Dept. of Electronics Engineering, Sejong University
E-mail : always@image.sejong.ac.kr

Abstract

Data embedding has recently become important for protecting authority. In this paper, we propose a robust data embedding technique for images.

Our techniques are based on the convolution between message image and a random phase carrier. We add extra bits with carrier image to improve precision of detecting rate, moreover, we use block by block based cyclic correlation for the compensation of distortion. In experiment, we show that the proposed algorithm is robust to Stirmark 3.1. attacks.

Ⅰ. 서론

최근 인터넷에서 멀티미디어 컨텐츠의 사용량이 급격히 증가하고 있다. 이에 따라 멀티미디어 컨텐츠의 위·변조 및 불법 복제 또한 급격히 증가하고 있는 추세이다. 인터넷이란 매체가 개방적이고 현재의 네트워크 환경 및 사용자의 컴퓨터 환경이 급격하게 발전하기 때문에 이러한 불법적인 행위들은 매우 손쉽게 수행되어 진다. 최근 이러한 문제점을 해결할 수 있는 방편으로 data embedding 기법에 대한 연구가 활발하며 그 결과 또한 상당한 수준에 이르렀다. 이러한 결과들이 업계에서 속속 실질적인 제품으로 출시되고 있다. 그러나 대부분의 결과들이 Stirmark 공격에 내성을 보이지 못하는 것이 큰 문제가 되고 있다.

본 논문의 Ⅱ장에서는 지금까지 제시된 기법들을 Ⅲ장에서는 새로운 알고리즘을 설명한다. Ⅳ장에서는 Stirmark 공격 후 실험결과를 제시하고, 결론을 Ⅴ장에 서술한다.

Ⅱ. 지금까지 제시된 방법들

*Data embedding*의 가장 간단한 기법은 Least Significant Bit(LSB)를 이용하는 기법이다. 이것은 먼저 영상의 LSB를 제거한 후, 워터마킹 sequence를 LSB에 삽입하는 기법이다. 여기서 워터마킹 sequence는 '0'과 '1'로 구성된다. 그러나 LSB를 이용한 기법은 에러가 발생되지 않는 환경에서 사용해야하는 단점이 있다. LSB를 개선한 방법으로는 m-sequence를 이용한 기법이 있다. '0'과 '1' 대신에 '-1'과 '1'을 LSB에 삽

입하는 기법이다[1]. 더 나아가 m-sequence를 이용하는 기법을 2차원으로 확장하고 검출과정에서 원 영상과 data embedding된 영상을 cross correlation함으로써 JPEG compression에서도 robust한 결과를 나타냈다[2].

이런 기법들과 달리 transform domain에서 사용되는 기법들에는 Discrete Cosine Transform(DCT), Discrete Fourier Transform(DFT), Discrete Wavelet Transform(DWT)등을 사용하는 기법이 대표적이다.

먼저 DCT를 사용한 기법들을 살펴보면, DCT 계수의 에너지 정도에 따라 data가 삽입될 계수를 선택하고 그 계수를 증가 또는 감소시키는 기법이 있다[3]. n개의 random number를 생성하고 원 영상을 DCT 변환한 후 DCT 계수 중에서 DC값을 제외한 큰 magnitude값 n개에 생성시킨 random number를 삽입하는 기법이다[4]. DCT를 이용한 기법들의 가장 큰 장점은 JPEG, MPEG같이 DCT를 이용하여 압축을 하는 것들에 사용될 경우 내성이 상당히 높아진다는 점이다.

DFT를 이용하는 기법은 frequence domain에서 phase에 data를 삽입하는 기법과 Log Polar Mapping 등을 사용하여 Rotation, Scale, Translation(RST)에서 변화 없는 영역으로 다시 변환한 후 data를 삽입하는 기법들이 있다[5].

DWT를 이용하는 기법은 DWT의 성질인 다 해상도 분해, spatial-frequency domain에서 국지화가 잘 되고 원 영상이 DWT를 한 후 간결하게 표현되는 장점으로 인해서 최근 논문이 급속히 늘어나고 있는 추세이다[6].

Ⅲ. Data Embedding

3.1 Data embedding 기법

본 논문에서는 Honsinger의 data embedding기법을 기반으로 하였다[7].

Honsinger의 논문에서 워터마크 message template $T(x,y)$는 message 영상과 carrier 영상의 convolution에 의하여 생성된다. Message 영상 $M(x,y)$는 iconic 영상 또는 사용자에게 입력받은 text를 bit화 시켜 이진 영상으로 생성된다. 이때 삽입되는 data는 64bit이고 10bit는 패리티로 추가된다. Carrier 영상 $C(x,y)$을 생성하는 가장 큰 목적은 message 영상의 에너지를 어떠한 곳에도 집중되지 않고 전체영상에 골고루 분포하도록 하는데 있다. Carrier 영상은 인위적으로 만든 phase와 magnitude의 Inverse Fast Fourier Transform(IFFT)에 의하여 만들어진다. 이때 에너지 집중을 막기 위하여 uniform random number를 생성하여 phase를 만들어 준다. 이때 key를 사용자에게 입력받아 생성한다. 이 key는 검출과정에서도 필요하다. Carrier 영상의 magnitude는 flat spectrum 또는 Contrast Sensitivity Function(CSF)에 의하여 생성된다. Flat spectrum은 Stirmark공격에 대응하기 위해 필요하고[8], CSF를 사용할 경우 검출률이 높아지고 비가시성이 높아진다. Data의 삽입의 원리는 다음과 같다.

$$I'(x,y)=I(x,y)+\alpha(M(x,y)*C(x,y)) \quad \text{.....(1)}$$

식(1)에서 '$*$'은 cyclic convolution으로 정의하고 α는 임의의 상수이고, $I(x,y)$와 $I'(x,y)$는 각각 원 영상과 워터마크가 삽입된 영상이다. 식(1)은 다음과 같이 쓸 수 있다.

$$I'(x,y)=I(x,y)+\alpha(T(x,y)) \quad \text{.....(2)}$$

식(2)은 message 영상과 carrier 영상을 cyclic convolution에 의하여 message template를 만들고 이것을 원 영상에 삽입하는 방식이다. 삽입과정을 좀더 자세히 살펴보면 다음과 같다.

1) 사용자의 key와 text를 입력받아 $C(x,y)$와 $M(x,y)$을 생성한다. 이때 $C(x,y)$와 $M(x,y)$의 크기는 임의적으로 조정할 수 있다. 본 논문에서는 128x128로 설정하였다.

2) $C(x,y)$와 $M(x,y)$의 cyclic convolution에 의하여 $T(x,y)$을 생성한다.

3) $T(x,y)$의 값이 $I(x,y)$의 값보다 크기 때문에 $T(x,y)$의 값을 α값에 의하여 비례적으로 축소시킨다.

4) $I(x,y)$을 128x128 블록으로 나눈다. 이것은 $C(x,y)$, $M(x,y)$, $T(x,y)$ 모두 128x128의 크기로 생성되었기 때문이다.

5) 축소된 $T(x,y)$을 각각의 블록에 더해준다.

이러한 과정에 의하여 data embedding이 이루어진다. 이때 주의할 점은 convolution과정이 FFT domain에서 이루어진다.

검출은 삽입의 역 과정으로, 그 원리는 다음과 같다.

$$M'(x,y)=I'(x,y)\otimes C(x,y) \quad \text{.....(3)}$$

식(3)에서 '$\otimes$'은 cyclic correlation으로 정의되고, $M'(x,y)$은 워터마크가 삽입된 영상에서 추출된 message 영상이다. $C(x,y)$의 성질을 보면

$$C(x,y)\otimes C(x,y)=\delta(x,y) \quad \text{.....(4)}$$

여기서 $\delta(x,y)$는 Dirac delta function이다. 또한 cyclic convolution 및 cyclic correlation은 교환법칙이

성립된다. 식(3)에 식(1)(4)과 교환법칙의 성질을 적용하면 다음과 같다.

$$M'(x,y) = \alpha M(x,y) * \delta(x,y) + I(x,y) \otimes C(x,y) \quad ..(5)$$

이상적인 경우 식(4)와 같이 carrier 영상의 autocorrelation은 delta function이 되고 원 영상과 carrier 영상의 cyclic correlation은 0이 나온다. 이것은 (5)식을 보면 앞 부분 $\alpha M(x,y) * \delta(x,y)$는 $\alpha M(x,y)$가 되고 뒷 부분 $I(x,y) \otimes C(x,y)$는 0이 된다. 따라서 $M'(x,y) = \alpha M(x,y)$가 된다. 이것이 이상적인 경우이다. 그러나 실제의 경우에선 전자는 delta function에 거의 가까운 값이 나오는 반면, 후자는 0이 아닌 값들이 존재한다. 이것은 잡음으로 볼 수 있다. 검출과정을 자세히 살펴보면 다음과 같다.

1) $I'(x,y)$을 128x128 블록으로 나눈다.
2) 각 블록에서 같은 위치에 있는 화소 값을 모두 더해준다.
3) 사용자로부터 key를 받아 $C(x,y)$을 생성한다.
4) 2)의 결과와 3)의 결과를 cyclic correlation한다.

이러한 과정에 의하여 사용자가 입력한 text 또는 iconic 영상을 검출할 수 있다. 검출과정도 삽입과정과 같이 cyclic correlation을 FFT domain에서 수행한다.

3.2 내성을 강화한 data embedding

3.1 장에서 Honsinger가 제안한 data embedding 기법에 대하여 알아보았다. Honsinger의 기법에서는 Stirmark에 대하여 내성을 갖기 위해서 carrier 영상 생성 시 phase를 uniform random number로 사용한다고 3.1 장에서 언급하였다. CSF는 검출률 및 비가시성에는 좋은 장점을 갖지만 Stirmark에는 검출이 되지 않는 단점이 있다. 또한 Honsinger가 제안한 기법은 Stirmark에 적용 후 affine correlation을 적용하여 검출하는 방식이다. 더 나아가 affine correlation으로 검출이 되지 않으면 신호 대 잡음비를 개선하여 검출하는 방식을 사용하고 있다. 본 논문에서는 워터마크가 삽입된 영상의 비가시성은 조금 감소되지만 왜곡된 정도의 정확한 검출이 가능한 기법을 사용한다.

Honsinger의 알고리즘에서는 사용자에게 입력받거나 또는 Uniform Resource Locator(URL) 등을 bit화 시켜 임의적, 정방형, 원형의 message 영상을 만들었다. 그중 원형이 공격 후 검출과정에서 가장 좋은 결과를 나타낸다. 원형의 message 영상은 그림 1. 같다. 그림 1.에서 message 영상은 '0'과 '1'로 이루어진 이진 영상이다. 이것은 64bit의 data를 포함하고 10bit의 패리티를 추가하여 오류발생 시에도 검출률을 높이는데 이용된다.

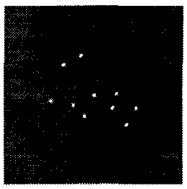


그림 1. Message 영상의 예

본 논문에서는 그림 1.에서 원형 점들의 반지름을 감소시켜 그림 2.와 같이 그 개수를 100개 정도로 늘린다.

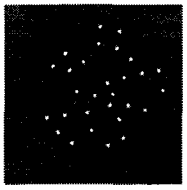


그림 2. 확장된 message 영상의 예

그림 2.에서도 data는 64bit, 패리티는 10bit 총 74bit를 사용한다. 나머지는 '0'을 삽입한다. 이러한 과정은 검출과정에서 cyclic correlation의 정확도를 높이기 위함이다. 확장된 message 영상을 $M'(x,y)$로 정의한다. 그림 2.와 같이 message 영상을 만든 후 3.1장의 삽입 과정보다 α값을 증가시켜 원 영상에 워터마크를 삽입한다. 검출과정은 다음과 같다.

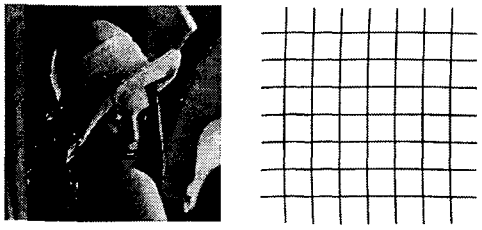
1) $M'(x,y)$을 생성한다. 이때 원형의 각 점들은 모두 '0'으로 삽입한다.
2) 사용자로부터 key를 받아 $C(x,y)$을 생성한다.
3) 1)의 결과와 2)의결과를 cyclic convolution을 수행한다.
4) $I'(x,y)$을 128x128 블록으로 나눈다.
5) 각 블록에 대하여 3)의 결과와 cyclic correlation을 수행 후 각 블록의 최대값인 peak를 찾는다.
6) 왜곡된 영상을 복원한다.
7) 복원된 영상을 128x128 블록으로 나누고, 블록의 같은 위치에 있는 각 화소 값을 더해준다.
8) 7)의 결과와 2)의 결과를 cyclic correlation한다.

여기서 $I'(x,y)$은 워터마크 삽입 후에 Stirmark 공격을 한 영상이다. 과정 1)에서 $M'(x,y)$는 $M(x,y)$에 비하여 화소 개수가 최대 74만큼 차이가 있다. 이것은 전체 화소의 개수가 16384에 비하여 상당히 작은 수이다. 이러한 이유에 의하여 $M(x,y)$와 $C(x,y)$을 cyclic convolution하여 생성된 값과 $M'(x,y)$와 $C(x,y)$을 cyclic convolution에 의하여 생성된 값이 상당히 유사

한 점을 이용하였다. 과정 4),5)는 Stirmark 공격 후 영상의 왜곡 정도를 알아보기 위함이다. Stirmark 공격이 없다면 4),5)번 과정을 수행했을 때 각 블록의 가장 첫 번째 위치에서 peak가 발생할 것이다. 그러나 $I'(x,y)$은 4),5)번의 과정을 거치면 peak들이 왜곡된 만큼 이동하여 나타난다. 과정 6)에서 peak들 중 정방형에 가까운 4점을 찾아 128x128로 복원한다. 과정 4),5)를 수행하면 전체 블록의 약 60%정도만 정방형으로 나타난다. 그러나 왜곡된 정도가 정확히 검출 가능하므로 60%의 블록만 있어도 복원후 사용자가 입력한 text를 검출 할 수 있다.

Ⅳ. 실험 결과

본 장에서는 Stirmark 3.1에서 "no option"으로 실험하였다. 다음의 결과는 Lena 1024x1024영상을 이용한 결과이다.



(a) Stirmark 공격 후 워터마크 삽입된 영상　　(b) Stirmark 공격 후 격자영상

그림 3. Stirmark 공격 후 영상

그림 3. (a)은 시각적으로 원 영상과 큰 차이를 느낄 수 없다. 그러나 격자영상을 사용하면 그림 4.(b)처럼 확연히 왜곡된 것을 알 수 있다. 그림 4.는 3.2장의 과정 4)5)를 수행 후의 결과이다.

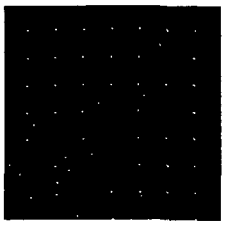


그림 4. 제안된 방법에 의한 peak 검출

그림 4.에서 각 점들은 그림 3. (b)에서 교차하는 지점이다. Stirmark 공격 없이 삽입 검출하는 경우 각 128x128 블록마다 peak가 발생한다. 그림 4.에서 peak 점들 중 128x128 블록에 유사한 4점들을 128x128 블록으로 수정 후 검출할 수 있다. 또한 어떠한 지점에 peak가 전혀 다른 곳에 나타나는 경우 상하좌우에 있는 peak를 이용하여 위치를 예측할 수 있다.

Ⅴ. 결론

본 논문은 Stirmark에 내성을 가지는 data embedding 기법을 제시하였다. 이것은 워터마크를 만들기 위한 message 영상 생성과정에서 data에 잉여 비트를 추가해 cyclic correlation의 정확도를 높였고, 공격받은 영상에 대하여 블록 별로 cyclic correlation을 수행하여 각 블록의 왜곡된 정도를 정확히 알 수 있기 때문에 왜곡된 정도를 보상할 수 있다. 이러한 과정에 의하여 워터마크가 삽입된 영상은 Stirmark 공격을 받아도 정상적으로 text가 검출 가능하다.

본 논문에서는 기존의 기법을 개선시켜 내성을 강화하였다. 그러나 α값 증가로 인해 비가시성이 낮아지기 때문에 비가시성 보다는 강한 내성을 요하는 용도로 사용하는 것이 더욱 적합하다.

참고문헌

[1] R. van Schyndel, A. Tirkel, and C. Osborne, "A digital Watermark," in *IEEE Proceeding of ICASSP*. Vol. II, pp. 86-90. 1994

[2] R. Wolfgang and E. Delp, "A watermark for digital images," in *IEEE Proceeding of the ICIP*, pp. 219-222, 1996.

[3] J. O'Ruanaidh, C. Dautzenberg, and F. Boland, "Watermarking digital images for copyright protection", in *Proc. Inst. Elect. Eng. Vis. Image Signal Processing*, Vol. 143, no. 4, pp. 250-256, Aug. 1996.

[4] J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, Vol. 6, no. 12, pp. 1673-1687, 1997.

[5] J. O'Ruanaidh, T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Process.*, Vol. 66, no. 3, pp. 303-317, 1998.

[7] C. Honsinger, "Data embedding using phase dispersion," *IEE Seminar on Secure Images and Image Authentication*, pp. 5/1-5/7, 2000

[8] http://www.cl.cam.ac.uk/users/fapp2/watermarking/stirmark/index.html