Diagonal 프로파일을 이용한 텍스트 문서의 디지털 워터마킹

정숙이, 김은실, 박지환
부경대학교 전자계산학과

Digital Watermarking for Text Document Using Diagonal Profile

Sook Yi Jeong, Eun Sil Kim, Ji Hwan Park
Dept. of Computer Science, Pukyong Nat'l University

요 약

인터넷과 같은 개방형 컴퓨터 네트워크의 발전에 따라 오디오, 이미지, 비디오 또는 텍스트 문서와 같은 멀티미디어 데이터에 대해 어느 정도의 열화없이도 지적 재산권의 불법적인 이용이 가능해 졌다. 본 논문에서는 불법으로 배포되거나 복제되는 텍스트 문서의 저작권 보호를 위한 워터마킹 스킴을 제안한다. 이 스킴에서는 텍스트 문서 이미지에 대한 diagonal 프로파일을 이용하여 문서상에 원소유자의 비밀정보 즉, 저작권 정보를 삽입하여 불법 복제를 억제하기 위한 새로운 워터마킹 및 추출 방법을 소개한다. 이 방법에 따르면 diagonal 프로파일의 특성으로 인해 공격자에 의한 워터마크의 제거나 문서의 형태 변경을 쉽게 검출할 수 있다.

1. 서론

오늘날, 컴퓨터 네트워크의 속도 향상과 통신 서비스의 보급으로 인해, 인가되지 않은 사용자에 의한 멀티미디어 데이터의 접근 및 변경이 가능하게 되었다. 종래에는 이들 중요한 자원의 적절한 보호를 위해 암호 기술을 바탕으로한 많은 스킴들이 제안되어 왔지만, 복호된 디지털 데이터에 대한 복사나 재 배포에 관한 근본적인 문제들을 해결할 수는 없었다. 특히, 이들 네트워크를 통한 문서 데이터의 배포는 각 수신자의 필요에 따른 멀티미디어 데이터들의 변경 또는 위조를 가능하게 하였다. 따라서, 인가되지 않은 문서의 복사나 배포를 억제하기 위해 배포된 문서에 저작권 정보를 삽입하는 방법을 정보 은닉(information hiding)이라 한다. 정보 은닉은 중요한 정보를 의미가 있는 데이터에 삽입시켜 정보를 전송하는 방법으로 정보 자체를 랜덤한 형태로 전송하는 암호화와는 달리 중요한 정보의 삽입 여부 또한 알 수 없도록 하여 불법 배포자를 지정할 수 있도록 한다. 이러한 저작권 보호의 방법에는 원 소유자의 비밀 정보, 즉 디지털 데이터를 그대로 유지시키면서 저작권 정보를 삽입하는 디지털 워터마킹이라는 기술이 있으며, 디지털 데이터에 저작권 정보를 삽입하여 불법으로 유통되거나 복제된 디지털 데이터를 발견할 경우, 그 데이터의 정보를 추출하여 불법으로 배포시킨 소유자를 확인할 수 있는 fingerprinting[1] 등이 있다.

일반적으로 원 소유자의 비밀정보를 담고있는 워터마크는 시각적으로 제 3자에 의해 구별될 수 없어야 하고 AD/DA 변환, 샘플링 및 양자화와 같은 신호처리나 회전, 확대/축소, 크로핑(cropping)과 같은 기하학적인 왜곡 현상에 견고해야 한다. 또한 워터마크는 결탁 공격이나 위조에 대한 견고성을 지녀야 하며, 워터마크 추출에 있어서 모호성을 지니지 않아야 한다는 특성을 가지고 있다.

본 논문에서는 저작권 보호를 위해 텍스트 문서에 적용할 수 있는 디지털 워터마킹 방법을 제안한다. 우선, 2장에서는 텍스트 문서를 위한 디지털 워터마킹 방법에 대해 알아보고, 3장에서는 본 논문에서 제안하는 diagonal 프로파일 및 이들 워터마크의 삽입 및 추출 방법에 대해 소개한다. 마지막으로 4장에서는 본 제안 방식에 대한 결론 및 향후 연구 과제를 간략하게 소개한다.

2. 텍스트 문서를 위한 디지털 워터마킹

텍스트 문서를 위한 디지털 워터마킹 기술은 크게 공간 도메인에서의 워터마킹과 주파수 도메인에서의 워터마킹 기법으로 나눌 수 있다. 먼저, 공간 도메인에서의 워터마킹 방법에는 규칙적인 문서의 워드와 라인을 미세하게 이동시켜 워터마크를 삽입하는 방법[2],[4]-[6],[9]으로 워터마크의 삽입에 따른 변형을 거의 식별할 수 없다. 특히, [2]에서는 각 문서마다 유일한 워터마크를 삽입하여 불법으로 배포한 인가된 수신자가 누구인지를 식별하기 위한 방법들을 제안하고 있으며, [3]에서는 암호학적인 프로토콜을 사용하여 전자 문서의 안전한 배포를 위한 시스템을 제안하고 있다. 이 방법에 따르면 삽입된 워터마크는 복사, 스캐닝, 팩스에 의해 왜곡되더라도 centriod 검출이나 원 문서와 왜곡된 문서의 차이를 근거로 하는 상관관계 검출, 그리고 에지(edge)와 같은 특징들을 근거로 워터마크를 검출하는 특징검출 방법들을 이용하여 삽입된 워터마크를 검출할 수 있다. 첫째, centriod 검출 방법은 라인과 워드 모두에 적용할 수 있으나 잡음이 존재할 경우의 검출 성능에 있어서는 라인 쉬프팅 방법이 더 효율적이나, 검출을 위해서는 워터마크되지 않은 원래의 문서가 필요하다. 둘째, 상관관계 검출은 워드 쉬프팅 방법에 있어서 검출 성능이 뛰어나지만, 역시 검출을 위해서는 워터마크 되지 않은 원래의 워터마크 되지 않은 문서가 필요하다. 마지막으로 특징 검출에 있어서는 라인 쉬프팅 방법에 효율적이며, 위 두 가지 검출 방법과는 달리 원 문서는 필요하지 않지만 잡음이 존재할 경우 그 검출 성능이 현저히 감소되는 단점을 지니고 있다.

공간 도메인에서의 또 다른 방법은 삽입할 워터마크를 seal[10][11]이라는 이미지를 사용하여 랜덤하게 매핑시킴으로써 어느 정도 문서의 열화가 발생하더라도 복원된 워터마크 정보는 식별할 수 있는 점에 착안한 방법이 소개되고 있다.

위와는 달리, 주파수 도메인에서의 삽입 방법[7]에는 Cox et. al이 제안한 방법[8]을 바탕으로 워드/라인 쉬프팅 방법으로 저작권 정보를 삽입한다. 그리고 삽입된 워터마크의 검출은 워터마크된 문서를 주파수 도메인으로 변형하여 워터마크 성분을 추출하며, 원 소유자의 워터마크된 문서로부터 추출한 워터마크 정보와 불법으로 유통되는 문서의 워터마크 정보에 대한 유사도를 측정하여 불법 복제 여부를 판단한다. 그러나, 이 방법은 잡음에는 견고하나 기하학적인 왜곡에 영향을 받게 되는 단점이 있다.

3. Diagonal 프로파일을 이용한 제안 방식

이 장에서는 본 논문에서 제안하고자 하는 diagonal 프로파일을 이용한 워터마킹 방법을 소개한다. 우선, (i, j)의 위치에 있는 픽셀 값을 $f(i, j)$라고 할 때 2차원 평면에서의 텍스트 문서의 전체 이미지 $n \times m$은과 어떤 워드는 각각 식 (2)와 (3)에서와 같이 구성된다고 가정한다.

$$f(i,j) \in \{0,1\},\ i=0,\ldots,n-1,\ j=0,\ldots,m-1 \quad (1)$$

where, n and m is width and height of a entire image, respectively.

$$f(x,y) \in \{0,1\},\ x=0,\ldots,w-1\ y=0,\ldots,h-1 \quad (2)$$

where, w and h is width and height of any word respectively.

Diagonal 프로파일은 어떤 이미지의 행과 열에 대한 현재 픽셀 값에 대해 식 (3)을 적용하여 히스토그램 버켓에 대한 인덱스 k를 계산하여 구성한다. 그림1은 이미지에 대한 diagonal 프로파일을 구성한 것이다.

$$k = i - j + r - 1,\ 0 \le k \le n + m - 1 \quad (3)$$

$$where,\ r = \begin{cases} r = m, & \text{if } n > m \\ r = n, & otherwise \end{cases}$$

이렇게 구성된 diagonal 프로파일은 k는 $0 \sim n+m-2$의 범위를 가지므로 총 $n+m-1$개의 버켓 수를 가지게 된다.

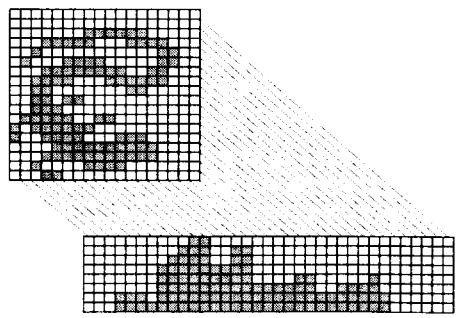

그림 1. 텍스트 이미지에 대한 diagonal 프로파일

3.1 워터 마크 삽입 과정

본 제안 방식에 있어서, 문서의 저작권자가 저작권 정보를 생성하기 위해 자신의 비밀 정보를 선택하여 워터마크를 삽입하는 알고리즘은 다음과 같으며, 그 과정을 그림2에 간략하게 나타내었다.

[step1] 비밀정보 $S_i \in \{0, 1\}$를 구성

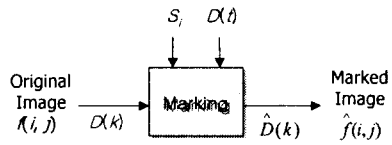

그림 2. 워터마크 삽입 과정

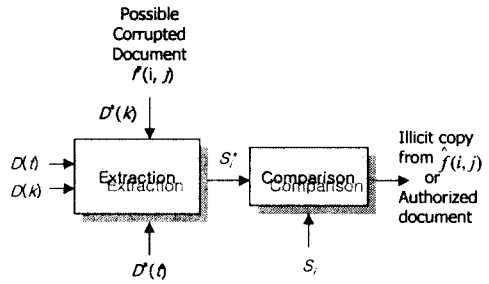

그림 3. 워터마크 추출 과정

[step2] $f(i, j)$의 diagonal 프로파일 $D(k)$를 생성

$$D(k)=\begin{cases} D(k)+1, & \text{if } f(i,j)=1 \\ D(k), & otherwise \end{cases} \quad (4)$$

$$where,\ k=i-j+r-1\ (0\le k\le n+m-1),$$
$$0\le i\le n-1,\ 0\le j\le m-1,$$
$$r=\begin{cases} r=m, & \text{if } n>m \\ r=n, & otherwise \end{cases}$$

[step3] S_i를 삽입하기 위해 랜덤하게 선택된 워드를 $f(x, y)$라고 할 때, $f(x, y)$의 diagonal 프로파일 $D(t)$를 생성

$$D(t)=\begin{cases} D(t)+1, & \text{if } f(x,y)=1 \\ D(t), & otherwise \end{cases} \quad (5)$$

$$where,\ t=i-j+r-1\ (0\le t\le w+h-1),$$
$$0\le x\le w-1,\ 0\le y\le h-1,$$
$$r=\begin{cases} r=h, & \text{if } w>h \\ r=w, & otherwise \end{cases}$$

[step4] 구성된 $D(t)$에서 워터마크 삽입위치를 다음과 같은 조건에 따라 랜덤하게 선택하여 삽입

- $D(t)$를 두 블록(b_l, b_r)으로 나누어
  S_i = '0' : b_l의 임의의 위치에 1 픽셀 삽입
  S_i = '1' : b_r의 임의의 위치에 1 픽셀 삽입
- 선택된 위치는 원 텍스트 문서 이미지상의 동일한 인덱스를 가지는 '흑' 픽셀 값에 인접한 경우의 픽셀
- 선택된 위치가 '흑'의 픽셀 값을 가지는 경우는 제외
- 삽입된 위치가 다시 선택되는 것을 방지하기 위해 해당 삽입 워드의 위치를 테이블에 기억하여 충돌을 방지

[step5] S_i를 모두 삽입할 때까지 step3~4를 반복

[step6] 워터마크된 전체 텍스트 문서의 diagonal 프로파일 $\hat{D}(k)$를 생성

[step7] $\hat{D}(k)$로 부터 워터마크된 문서 $\hat{f}(i,j)$를 생성

[step2]와 [setp6]에서 $D(k)$와 $\hat{D}(k)$를 생성하는 것은 앞에서 언급한 워드 쉬프팅과 라인 쉬프팅에서와 같이공격자에 의해 임의의 위치가 변경될 경우, 해당 변경 위치의 프로파일 만이 변경되는 것과는 달리, 공격자에 의해 워터마크된 텍스트 문서가 약간이라도 변경될 경우 diagonal 프로파일의 특성상 전체 프로파일의 변경에 영향을 미치므로 워터마크 검출에 있어서의 검출 성능을 높일 수 있으며, 노이즈에 의해 왜곡되는 경우 워터마크의 보정에도 사용될 수 있다.

3.2 워터 마크 추출 과정

삽입된 워터마크의 추출에 앞서, 본 방식에서는 단순히 워터마크된 문서의 변경 여부만을 검출하고자 하는 경우에는 워터마크된 문서의 diagonal 프로파일 $\hat{D}(k)$와 불법으로 유통되어 변경되었을 가능성이 있는 문서 $f'(i, j)$의 diagonal 프로파일 $D'(k)$에 대한 각각의 프로파일만을 비교하여도 변경여부를 검출할 수 있다. 그러면, 삽입된 워터마크의 추출 과정을 살펴보자. 그림 3은 그 과정을 간략하게 나타낸 것이다.

[step1] 불법으로 유통되어 변경되었을 가능성이 있는 문서를 획득하여 디지털화된 문서 $f'(i, j)$를 생성

[step2] $f'(i, j)$의 diagonal 프로파일 $D'(k)$를 생성.

[step3] 랜덤하게 선택된 워터마크 삽입 위치를 가지고 그 위치에 해당하는 $D'(t)$를 생성

[step4] step3을 반복하여 비밀정보 S_k'를 추출

- $S_k = S_k'$: 원 소유자로부터 인가된 텍스트 문서
- $S_k \neq S_k'$: $\hat{f}(i,j)$로부터 불법 복제되거나 변경된 텍스트 문서

4. 실험 결과

원 소유자의 비밀정보 S_k를 삽입하여 워터마크된

People often ask questions like why we need standards. First, we can safely assume that there must be good reasons, otherwise, the international community would be wasting millions of dollars for standard development processess. Let us find out what these reasons are. A standard is like an official language. People may speak many different languages in a country. However, in order to make it easy for people to communicate with each other, one language at least must be chosen as the official language for the country. The key words, easy to

그림 1. 원 텍스트 이미지(1822×644, 8라인, 91워드)

People often ask questions like why we need standards. First, we can safely assume that there must be good reasons, otherwise, the international community would be wasting millions of dollars for standard development processess. Let us find out what these reasons are. A standard is like an official language. People may speak many different languages in a country. However, in order to make it easy for people to communicate with each other, one language at least must be chosen as the official language for the country. The key words, easy to

그림 5. 워터마크된 이미지(8비트×15워드(120비트)삽입)

People often ask questions like why we need standards. First, we can safely assume that there must be good reasons, otherwise, the international community would be wasting millions of dollars for standard development processess. Let us find out what these reasons are. A standard is like an official language. People may speak many different languages in a country. However, in order to make it easy for people to communicate with each other, one language at least must be chosen as the official language for the country. The key words, easy to

그림 7. 워터마크된 이미지(8비트×91워드(728비트)삽입

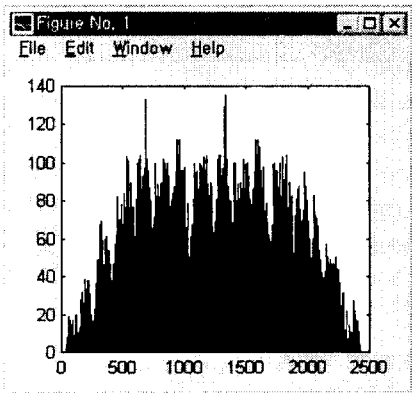

그림 8. 그림 (4)의 diagonal 프로파일

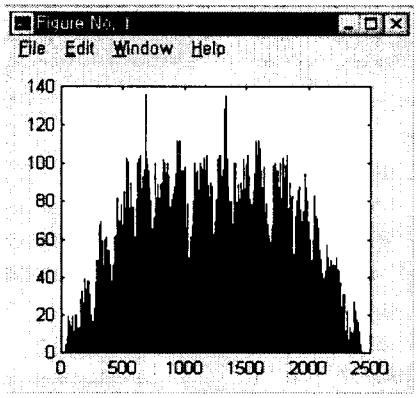

그림 9. 그림 (5)의 diagonal 프로파일

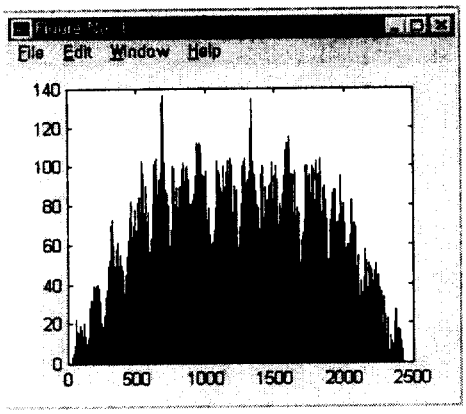

그림 10. 그림 (7)의 diagonal 프로파일

텍스트 문서와 워터마크 되지 않은 텍스트 문서를 비교하고, 삽입된 비밀 정보 S_k의 추출하였다. 텍스트 문서는 12 포인트 Times New Roman 서체로 구성되었으며, 8개의 라인과 91개의 워드로 구성된 1822×644 크기의 이미지를 HP5200C(150dpi)로 스캔하여 문서 이미지를 읽어들여 실험하였다. 또한 본 실험에서 삽입한 비밀정보 S_i는 15바이트와 91바이트의 영문자로 구성하였다. 그림 4~10은 실험에서 사용한 원 텍스트 문서 이미지와 워터마크된 이미지 및 diagonal 프로파일을 나타낸 것이다.

5. 결론 및 고찰

본 논문에서는 diagonal 프로파일을 이용하여 원 소유자의 비밀 정보를 삽입시켜 텍스트 문서에 적용할 수 있는 새로운 워터마킹 및 추출 방법을 소개하였다. 워터마크가 삽입된 위치를 알고자 하거나 워터마크를 제거하기 위해 텍스트 문서에 대한 임의의 위치를 변경할 경우, 그 문서의 원 소유자는 변경되었을 가능성이 있는 문서의 diagonal 프로파일과 원 문서의 diagonal 프로파일을 비교함으로써 변경여부를 검출할 할 수 있다. 더 나아가 원 소유자가 삽입한 비밀 정보를 추출하여 유통된 문서가 불법 복사된 문서인지 여부를 판단할 수 있었다. 워터마크는 랜덤하게 삽입되므로 공격자는 워터마크 삽입 위치를 알지 못하게 된다.

또한 본 논문에서 제안된 방법에 2장에서 소개된 검출 방법들을 적용하여 기존 텍스트 워터마킹을 위한 제안된 방법들에서의 검출 방법들 간의 성능 비교 분석이 필요할 것으로 사료된다.

[참고문헌]

[1] N. Wagner, "Fingerprinting", Proc. of the IEEE Symposium on Security and Privacy, pp. 18-22, April. 1983.

[2] J. Brassil, S. Low, N. Maxemchuk, L. O'Gorman, "Electrnoic Marking and Identification Technique to discourage document copying", IEEE J. Selected Area Commun., pp. 1495-1504, Vol. 13, Oct. 1995

[3] A. K. Choudhury, N. F. Mexemchuk, S. Paul, "Copyright Protection for Electronic Publishing over Computer Networks", IEEE Network, pp. 12-21, Vol. 9, May, 1995. [4] S. H. Low, N. F.

[4] Mexemchuk, A. M. Lapone, "Document Identification for Copyright Protection Using Centroid Detection", IEEE Trans. on Communication, pp. 372-383, Vol. 46, No. 3, Mar. 1998.

[5] S. H. Low, A. M. Lapone, N. F. Mexemchuk, "Performance Comparison of Two Text Marking and Detection Methods", IEEE J. Selected Areas Communication., pp. 2057-2062, Vol. 16, No. 14, May. 1998.

[6] J. T. Brassil, Steven H. Low, N. F. Mexemchuk, "Copyright Protection for the Electronic Distribution of Text Documents", Proc. of the IEEE, Vol. 87, No. 7, July 1999.

[7] Yong Liu, Jonatha Mant, Edward Wong, Steven Low, "Marking and Detection of Text Documents Using Transform-domain Techniques", SPIE Vol. 3657, San Jose, California, Jan. 1999

[8] I. Cox, J. Kilian, T. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on Image Processing, Vol. 6, No. 12, pp. 1673-1687, 1997

[9] Yasuhiro Nakamura, Kenio Matsui, "著作權保護のための電子文書のハードコーヒの署名の埋め込み", 정보처리학회 논문지, Vol. 36, No. 8, Aug. 1995

[10] Yasuhiro Nakamura, Kenio Matsui, "和文書へのシール畵像による透かし", 정보처리학회 논문지, Vol. 38, No. 11, Nov. 1997

[11] M. Iwakiri, Y. Murakami, W. Piyapisuit, Y. Nakamura, K. Matsui, "電子文書のテキスト復元機能を持つ印章方式", SCIS2000-D54, Okinawa, Japan, Jan. 2000