워터마크가 삽입된 이차원 바코드와 위·변조 방지 시스템

Forgery Protection System and 2D Bar-code inserted Watermark

이상경 · 고광은 · 심귀보*

SangKyung Lee, Kwang-Enu Ko and Kwee-Bo Sim*

중앙대학교 전자전기공학부

요 약

일반적으로 인쇄 문서의 위변조를 방지하기 위해 복사방지마크와 이차원 바코드가 많이 사용되고 있다. 하지만 이차원 바코드는 복사 방지 마크와 분리 배치되어 있어 사본 구별이 시각적으로 힘들고, 스캐너로만 인식할 수 있다는 단점이 있다. 따라서 본 논문은 이차원 바코드에 워터마크를 삽입해 시각뿐만 아니라 스캐너로 정확하게 구분 할 수 있는 위변조방지기술에 대해 연구했다. 복사 방지마크는 디지털 입출력 장치의 저주파 필터 특성으로 인해 특정 패턴이 소실되거나 변형되는 것을 이용해 패턴으로 만들었다. 원본과 사본을 스캔한 이미지의 히스토그램을 분석을 통해 성능검증을 했다. 그리고 이차원 바코드를 웹캠이나 핸드폰 카메라로 인식한 인증키로 온라인 서버에 접속해 내용을 확인하는 시스템을 제안했다.

키워드 : 위조 방지, 위조패턴, 이차원 바코드, bar-code, Watermark

Abstract

Generally, the copy protection mark and 2D bar-code techniques are widely used for forgery protection in printed public documents. But, it is hard to discriminate truth from the copy documents by using existing methods, because of that existing 2D-barcode is separated from the copy protection mark and it can be only recognized by specified optical barcord scanner. Therefore, in this paper, we proposed the forgery protection technique for discriminating truth from the copy document by using watermark inserted 2D-barcode, which can be accurately distinguished not only by naked eye, but also by scanner. The copy protection mark consists of deformed patterns that are caused by the lowpass filter characteristic of digital I/O device. From these, we verified the performance of the proposed techniques by applying the histogram analysis based on the original, copy, and scanned copy image of the printed documents. Also, we suggested 2D-barcode confirmation system which can be accessed through the online server by using certification key data which is detected by web-camera, cell phone camera.

Key Words : Anti-Counterfeiting, Anti-Counterfeiting pattern, 2D bar-code, bar-code, Watermark

1. 서 론

최근 디지털 인쇄 기술이 발전하면서 스캐너와 레이저프린터가 보편화 되었다. 이에 따라 일반인도 쉽게 위조할 할 수 있어 위조 품목이 주민등록증, 여권 등에서 벗어나 영어 성적 증명서, 통화 내역서, 처방전 까지 다양해지고 있다. 특히 처방전의 경우 항정신성 의약품과 같은 전문 의약품 을 일반인이 컬러프린터를 이용해 구입하는 사례가 증가 하고 있어, 금지하는 법률안이 최근 발의 되었다[1].

증가하는 위·변조 문제를 해결하기 위해 특수 잉크와 용지, 홀로그램 등이 사용되고 있다. 그 중에서 일반 프린터로 구현이 쉬운 이차원 바코드와 복사방지 마크를 함께 구성해 내용의 위·변조와 복사 방지를 하고 있다. 복사방지마크는 시각적으로 문서의 복사 유무를 식별하고, 바코드를 통해

내용의 위·변조를 확인한다. 하지만, 정교하게 위조가 되었을 때 스캐너와 같은 장비가 없으면 시각적으로 판별하기 힘들고, 바코드만 복사할 경우 사본과 구분하기 힘들다[2].

이를 해결하기 위해 일반 레이저 프린터와 스캐너에서 이차원 바코드에 복사방지마크 삽입해 시각적으로 확인을 하고, 정확한 확인을 위해서 핸드폰카메라나 스캐너를 사용하는 위·변조 시스템을 제안했었다[3]. 그리고 심볼에 패턴을 삽입해 시스템으로 구현 했다. 하지만 패턴이 단순하고 시각적으로 정확한 확인이 어려웠다[4].

본 논문에서는 글자를 이차원 바코드에 삽입해 시각적으로 인식할 수 있게 하고, 스캐너로 스캐닝한 원본과 사본의 히스토그램 차이를 통해 복사 유무를 구별하는 위변조 시스템에 대해 연구했다. 이를 바탕으로 인증키를 이차원 바코드에 저장해 문서 위·변조를 방지하는 시스템을 제안했다.

2. 인쇄물 위·변조 방지 관련 연구 문제점

2.1 워터마크

디지털워터마킹은 글자나 그림과 같이 소유권을 나타낼

접수일자 : 2010년 10월 21일

완료일자 : 2010년 11월 16일

* 교신 저자

※ 본 논문은 본 학회 2010년도 추계학술대회에서 선정된 우수논문입니다.

수 있는 데이터를 저작물에 삽입하고 추출하는 모든 기술적인 방법을 말한다. 원본 데이터의 손실이 적고, 사람이 시각 또는 청각으로 인식할 수 없게 삽입된다[5]. 특히, 스마트폰과 E-Book, 컬러프린터와 같은 디지털 콘텐츠가 보편화되면서 저작물을 쉽게 복제, 수정이 배포 가능해졌다. 이에 따라 1990년 K. Tanaka 등에 의해서 개발된 디지털워터마킹이 디지털콘텐츠 저작권보호에 사용되고 있다[6]. 압축, 잡음, 회전 그리고 이미지프로세싱등과 같은 공격에 강인하게 삽입할 수 있는 연구가 진행되고 있다. 인쇄출력물에 관한 연구는 미흡하지만 LPM (Log-Polar Map) 샘플링에서 검출 성능향상을 위해 유전알고리즘으로 최대 표본 반지름을 지정하고, 삽입 주파수를 실험적으로 선택해 워터마크가 1차 출력물에서만 검출 되도록 하는 연구가 있었다[7]. 하지만 바코드에 적용하기 위해서는 다양한 주파수 대역을 가진 이미지를 생성한 후 삽입 주파수를 결정하는 복잡한 과정을 필요하고 바코드 생성할 때 마다 심볼의 개수와 위치가 달라져 적용하기 어렵다.

2.2 이차원 바코드

이차원 바코드는 데이터를 점으로 표현하고 매트릭스 형태로 배열해 영문기준으로 1500자 이상 저장 할 수 있다. 따라서 온라인 연결이 없어도 내용 위·변 확인이 가능하다. 하지만 전자민원과 같이 높은 보안이 필요한 경우는 온라인과 연계되어 활용되고 있다. 이차원 바코드의 인식은 핸드폰카메라나 웹캠 같은 영상장치와 스캐너 또는 전용리더기로 인식이 가능하다[8]. 이러한 장점 때문에 이차원 바코드를 이용해 공문서에 삽입해 위·변조 방지를 제안한 연구가 있었지만[8]. 실제로 위·변조에 사용되는 바코드는 고밀도 바코드가 사용되기 때문에 스캐너로만 데이터를 읽을 수 있고, 바코드만 복사해서 위조에 사용할 경우 검사할 수 있는 기술이 없다. 실제로 사본은 인식이 안 된다고 주장했던 처방전 바코드도 자동인식 장치가 정상적으로 인식했다[9].

3. 제안 시스템

3.1 워터마크 생성

워터마크는 스캐너의 특성을 이용해 사본과 원본사이에 차이가 발생하도록 Survival패턴과 Delete패턴을 만들어 사용했다. 그림 1과 같이 비스듬한 직선을 복사하거나 스캐너로 스캔할 경우 CCD센서에 픽셀을 정확하게 매칭할 수 없어 불연속한 점이 나타난다. 이 문제를 해결하기 위해 다양한 스캔 엔진이 개발되고 있지만 그림 2의 시각형과 같이 저주파 필터효과 때문에 흐려지는 화질 저하가 나타난다[10].

그림 1. 라인 CCD의 이미지 처리 문제
Fig. 1. Image process problem in line ccd

또한 위조를 막기 위해서는 Survival패턴과 Delete패턴을 시각적으로 구별하기 힘들어야 한다. 이를 위해 시각 시스템이 두 물체사이를 구별하기 필요한 최소 차이를 설명한

JND(Just Noticeable Difference)를 이용했으며, 식 (1)과 같이 나타낸다.

$$JND = \frac{\Delta I}{I} \times 100[\%] \quad (1)$$

JDN은 영상의 강도인 luminance성분에 I에 대한 강도 변화 ΔI 로 나타낸다. 시각시스템이 인식할 수 있는 최소차이는 일반적으로 2%이상 때 가능하다고 알려져 있다. 이 변화 폭이 너무 크면 적용이 어렵지만 적정 범위 내에서는 일정하게 나타난다[11].

위 2가지 스캔과 프린터의 특성 실험을 통해 만든 4가지 심볼 패턴을 사용해 바코드 이미지를 생성했다. 시각적인 변화를 살펴보면 일반 이차원 바코드의 사본을 스캔한 이미지(그림 2의 (d))는 원본을 스캔한 이미지(그림 2의 (c))보다 흐리게 나타났고, 보정한 사본 이미지(그림 2의 (e))는 레벨 값 조정만으로 원본과 비슷하게 복원되었다. 제안한 이차원 바코드는 보정한 이미지(그림 2의 (c))에서 거의 모든 패턴이 사라져 확연한 차이를 보여 시각적으로 구별할 수 있었다. 사본스캔이미지(그림 2의 (b))에서는 심볼패턴 일부가 사라졌지만, 효과가 작고 정확한 원본을 알고 있어야 한다.

구분	원본스캔	사본스캔	보정 사본
제안 바코드			
일반 바코드			

그림 2. 스캐닝 결과

Fig. 2. Results after scanning.

히스토그램 분포에서는 심볼에만 적용했기 때문에 그림 3에서처럼 원본과 사본에서 차이를 나타냈지만, 일반 이차원 바코드와 비슷하게 나타나 스캐너를 통해 구별하기 힘들었다. 특히 보정한 사본을 스캔한 이미지는 히스토그램 분포가 원본과 비슷하게 복원되었다.

그림 3. 스캔 히스토그램

Fig. 3. Scanning histogram

이를 해결하기 위해 본 논문에서는 그림 4의 (a)와 같이 '본'과 같은 글자를 삽입하고, 배경에도 워터마크를 적용한 바코드 생성 방법을 제안했다. 글자의 가독성과 워터마크의 효과가 높은 패턴을 찾기 위해 글자부분에 적용한 패턴(그림 4의 (b))과 미적용 패턴(그림 4의 (c))으로 나누어 생성했다.

그림 4. 바코드 이미지 예제
Fig. 4. Example of bar-code image

3.2 암호화

암호화는 평문 중 일부를 선택해 배열로 만들어 XOR 연을 한 후 패턴 코드표에 따라 재배치하는 방법을 사용했다. 선택된 비트는 XOR 연산 후 코드표에 따라 값이 변환 된다. 변환 과정은 그림 5의 순서도와 기본 용어정의 후 예를 통해 자세히 설명했다. 복호화는 반대과정 이므로 생략했다.

그림 5. 암호화 과정
Fig. 5. Encryption process.

3.2.1 패턴-선택표와 코드표

암호화를 위해 XOR bit 암호화를 위한 코드표와 2차 변환된 데이터를 재배치하는 패턴-선택표가 사용된다.

첫 번째로 코드 비트는 XOR 연산을 위해 사용된 비트를 암호화 하기위한 변환 코드표이다. 선택된 bit에 해당되는 코드 값을 사용자 또는 관리자가 정의할 수 있고, bit 수는 같게 작성한다. XOR bit는 다음에 나오는 표 2의 패턴-선택표에 의해 정의 된다. 4개의 선택표 일 때 정의 해놓은 표1을 예로 들면 선택 bit가 '0001'이면 '0111'으로 변환된다.

표 1. 코드표 예제

Table 1. Example of code table

Data	Code	Data	Code	Data	Code	Data	Code
0000	0010	0100	1011	1000	1111	1100	1110
0001	0111	0101	0110	1001	1100	1101	1000
0010	1001	0110	1010	1010	0100	1110	0011
0011	0001	0111	0000	1011	0101	1111	1101

두 번째로 패턴-선택표는 암호문을 만들기 위해 필요한 패턴을 모아 놓은 표이다. 구성은 표 2와 같이 재배치 할 패턴을 선택하는 Select bit와 XOR 연산위해 사용할 입력 데이터의 번호를 나타는 XOR bit, 2차 변환된 데이터를 재배치하는데 사용되는 패턴으로 되어 있다. 패턴에 포함된 ID bit와 Select bit 의 bit 번호는 같아야 복호화가 가능하며, 유출 사고나 또는 임의로 사용하는 경우와 같이 필요에 따라 쉽게 표를 변경함으로써 쉽게 대처할 수 있다.

표 2. 패턴-선택표 예제

Table 2. Example of pattern-Select table

Select bit	XOR Bit	Pattern
0	0	4~7
0	1	12~15
1	0	8~11
1	1	20~23

3.2.2 암호화 과정

그림 6은 표 1의 코드표와 표 2의 패턴-선택표를 이용해 28bit크기를 갖는 입력 데이터인 "0101 1100 0100 1000 1001 1011 1011"을 암호화하는 과정이다.

그림 6. 암호화 과정 예
Fig. 6. Example of encryption process.

- 1) "0101110001001000100110111011"을 입력받는다.
- 2) 패턴-선택표 중에서 한 개의 패턴 코드를 선택 해 사용한다. 표2의 "01"패턴을 선택했다.
- 3) 패턴-선택표의 XOR bit 인 15~12번 bit와 입력데이터를 XOR 연산하여 1차 변환한다.
- 4) 3)에서 선택한 XOR bit를 표1의 코드 값으로 변환한다. 선택 bit가 "1000"이므로 "1111"이 된다.
- 5) 4)에서 변환한 값을 1차 데이터의 XOR bit 자리인 15~12번 bit자리에 삽입한다.
- 6) 패턴-선택표에 따라 2차 변환 된 데이터에서 해당되는 값을 찾아 위치시킨다. 예를 들어 패턴의 번호가 "7, 6, 21, 20, 19" 이면 , 2차 변환 데이터 7번과 6번 bit는 "00"이고, 20번~19번 bit는 "001"이므로, 두 값을 합친 "00001"값이 된다.
- 7) 마지막으로 암호문을 저장한다.

3.2.2 패턴

패턴은 2차 변환 된 값을 재배치시키기 위한 bit번호를 나타내는 표이다. 기본구성은 그림 7의 (a)와 같이 XOR 연산 된 데이터를 재배치하기 위해 임의의 크기로 나눈 bit조각인 Slice와 패턴-선택표의 Select bit로 되어 있다. 만약 2개 이상의 패턴으로 구성 할 때는 그림 7의 (b)처럼 각각의 패턴을 구별하기위해 ID bit가 추가된다.

(a) 1개 패턴 구조

(b) 데이터를 2개의 패턴에 저장 하는 경우

그림 7. 패턴 구조

Fig. 7. Formation of pattern

패턴은 크게 실제 데이터를 저장하는 정보 패턴과 의미 없는 데이터인 허위 정보 패턴으로 구성되지만, 저장 효율성을 위해 정보패턴만 사용했다. 패턴을 생성하는 규칙은 다음과 같이 정의 된다.

<공통 규칙>

- 1) 암호문의 기본 구성은 Slice, Select bit이며, 2개 이상의 패턴으로 생성할 경우 만 ID가 추가된다.
- 2) 순서에 의해 암호화 되는 것이므로 사용자 또는 관리자가 Slice, Select bit, ID bit의 위치를 설정 할 수 있다. 그리고 패턴과 Slice의 bit 개수도 입력 데이터에 따라 자유롭게 설정할 수 있다.
- 3) 단, 패턴-선택표내에서는 전체 암호문 bit수와 할당된 ID, Select bit의 bit수는 같아야한다.
- 4) 그리고 동일한 패턴표 내에서는 Select bit와 ID bit 위치는 같고, Slice 순서와 크기는 틀려야한다.
- 5) 한 개 패턴으로 생성 할 경우 Code bit는 인접해도 상관없으나 나누어 배치하는 것을 권장한다.

<2개 이상의 암호문 생성규칙>

- 1) 생성하는 암호문의 수는 ID bit로 표현 가능한 개수 내에서 생성 할 수 있다.
- 2) ID bit는 1bit 단위로 분할해 배치하고, 인접해 있으면 순서를 유추할 있으므로 나누어 배치한다.
- 3) Select bit는 암호문에 각각 1bit씩 삽입한다.

그림 8은 위 규칙을 이용해 만든 패턴 예제 이다.

그림 8. 패턴 예제
Fig. 8. Example of pattern

3.3 바코드생성과 워터마크 삽입

앞에서 설명한 암호화와 워터 마크를 이용해 바코드를 생성하는 과정이다. 워터마크효과를 먼저 검증하기 위해 오류 검출 코드는 생략하고, Code-word는 ASCII코드로 사용했다. 그림 9와 같은 순서로 진행되며, 자세한 생성 과정은 다음과 같다.

그림 9. 워터마크 삽입된 바코드 부호화
Fig. 9. Watermarked bar-code encoding.

- 1) 문자 또는 숫자 데이터를 입력 받는다.
- 2) 입력 받은 데이터를 Code-word로 변환 한다.
- 3) 변환한 Code-word 대한 오류검출코드를 생성한다.
- 4) 암호 코드표에서 사용할 암호코드를 선택한다.

- 5) 암호 코드표에 따라 암호화한다.
- 6) 워터마크가 삽입된 이차원바코드를 생성한다.

4. 이차원 바코드의 복사 방지 검증 실험

4.1 실험방법

이차원 바코드 생성 프로그램을 그림 10과 같이 2개의 패턴-선택표를 사용해 생성했으며, 암호화된 2원 배열 값 중에서 '1'인 값에 심볼을 배치했다. 워터마크의 성능검증이 선행되어 하기 때문에 암호의 성능과 안정성 검증 실험은 진행하지 않았다.

그림 10. 바코드 생성 과정
Fig. 10. 2D bar-code generation process

생성된 바코드의 워터 마크 성능검증 실험은 HP사의 3970 스캐너와 laserjet 2300 레이저 프린터를 사용했다. 사본은 원본을 600dpi로 스캔 후 레이저 프린터로 수정 없이 출력한 사본과 레벨 값을 사용해 진하게 보정해 출력한 보정사본을 사용했다.

이차원 바코드 이미지는 그림 11과 같이 가시성과 워터마크 효과를 높이기 위해 심볼 모양과 색상이 다른 이미지를 만들어 사용했다. 실험은 복합기와 복사기에서 보편적으로 사용되는 해상도인 600dpi에서 워터마크 성능을 검증했다. 이 중에서 2개를 선택해 스캐너를 통한 빠른 데이터 처리와 복사방지마크의 검출 가능성을 200dpi 스캔 실험을 통해 확인했다.

그림 11. 사용한 바코드 이미지
Fig. 11. Used bar-code image

4.2 600 dpi 스캔 비교

삽입된 워터마크의 복사 방지 효과검증을 위해 원본이미지와 사본이미지를 해상도 600dpi에서 스캔한 후 특징을 그림 12와 같이 히스토그램을 통해 분석했다. 우선 특징을 살펴보면, 다음과 같다

첫 번째로 배경과 심볼 사이에 간섭 없이 데이터를 읽을 수 있다. 픽셀 분포가 원본에서는 심볼이 60에서 100사이

이고, 배경은 220에서 255사이에 있어 경계가 명확하다. 따라서 심볼과 배경 영역을 임계 값 기준으로 쉽게 이진화해 분리 할 수 있다.

두 번째로 사본이미지의 배경영역에서 효과가 크게 나타났다. 사본스캔에서 배경영역 230에서 250사이에 높게 나타나 원본과 큰 차이를 보였다. 특히 그림 12의 (c)나 (e)처럼 고르게 분포할 경우 2배 이상의 증가했고, 그림 12의 (g)나 (f) 같이 범위가 바뀌었다.

세 번째로 그림 12의 (f)와 같이 불완전한 형태가 좋은 효과를 보여줬다. 동그라미나 사각형의 경우 픽셀 값 분포가 대부분 높은 쪽으로 이동해 인쇄 품질이 나쁘거나 토너 부족과 같은 화질저하 문제와 구분이 어렵다. 하지만 불완전한 형태의 심볼은 그림 12의 (f)에서처럼 원본에서는 60에서 100사이에 밀집해 있었지만 사본에서는 높은 값으로 이동하면서 넓게 분포된다.

그림 12. 600dpi에서 스캔한 결과
Fig. 12. Scanned in 600dpi

4.3 200dpi 스캔 비교

600dpi에서 심볼과 배경에서 큰 효과를 나타낸 2개의 바코드 이미지를 선택 해 200dpi로 스캔 후 600dpi 실험과 같이 히스토그램으로 분석했다. 실험에 사용한 바코드 그림 11의 (c)와 그림 11의 (f)를 선택했다. 추가적으로 보정 사본을 추가해 비교했다.

우선 히스토그램을 살펴보면 그림 13에서 같이 사본의 심볼과 배경 영역의 분포가 600dpi 스캔 실험과 비슷하게 나타났다. 하지만 진하게 보정한 사본은 그림 13에서처럼 배경부분의 노이즈가 증가해 픽셀 값의 분포가 150에서 200 사이에 넓게 나타났다. 심볼 영역에서는 비슷하게 복원이 되어 보완이 필요하다.

그림 13. 200dpi에서 스캔한 결과
Fig. 13. Scanned in 200dpi.

두 번째로 시각적 변화에서는 그림 14의 (b)에서처럼 사본 스캔은 패턴 패턴이 세로 줄무늬 형태로 변형 되었다. 그리고 사본 스캔에서는 배경 패턴이 삽입 안 된 글씨 부분에 노이즈가 증가 했다. 보정이 안 되거나 흐리게 출력한 경우 배경 패턴이 세로 형태로 변형되거나 사라졌다. '본'글자의 가독성은 그림 14의 (e)와 그림 14의 (h)에서 좋았지만, 보정된 사본에서는 패턴이 뭉개져 원본과 차이를 보여 구분이 가능하다. 그리고 정확하게 글자를 읽기는 어려워 개선이 어려워 개선이 필요하다.

그림 14. 200dpi에서 스캔한 결과
Fig. 14. Scanned in 200 dpi.

5. 활용 시스템 제안

앞에 실험을 스캐너와 시각을 통해 바코드의 복사 유무를 확인할 수 있음을 확인 했다. 그리고 위터마크가 삽입되면서 크기가 증가해 저장효율이 낮다. 하지만 웹캠이나 핸드폰카메라로 인식이 가능해 활용성이 높다. 특히 핸드폰의 경우 항상 온라인으로 연결되어 실시간 확인이 가능하다. 따라서 인증키를 이차원 바코드에 저장해 문서 발급하고, 온라인을 통해 문서 인증하는 시스템을 제안했다.

5.1 발급 시스템

발급 시스템은 그림 15와 같이 웹사이트나 전용 프로그램을 사용해 발급요청이 이루어지고, 출력은 레이저 프린터 사용한다. 발급시스템의 특징은 사용자가 발급요청을 하게 되면 모든 내용이 아닌 생성된 인증키를 제안된 이차원 바코드에 저장한다. 발급 과정에서 문서 종류나 사용자의 선택으로 문서 확인 기간 또는 횟수 등을 지정해 인증키의 보관 기간을 제한하거나 조회 횟수를 표시 할 수 있다.

그림 15. 발급시스템
Fig. 15. Issuance System

5.2 인증시스템

인증시스템은 그림 16과 같이 스캐너와 웹캠이나 핸드폰 카메라와 같은 영상장치를 이용해 제안된 이차원 바코드를 인식하고, 온라인으로 연결된 인증시스템에 접속해 문서 인증을 받는다. 장점으로는 스캐너의 경우 자동급지장치(ADF, Automatic Document Feeder)를 이용해 다량의 문서와 복사유무를 빠르게 구별할 수 있다. 핸드폰을 사용할 경우는 항상 온라인으로 연결되어 있어 실시간 확인이 가능하다. 하지만 시각적으로 복사유무를 확인해하므로 조회 횟수 표시나 유효 보존기간과 같은 제한 조치가 필요하다.

그림 16. 인증 시스템

Fig. 16. Certification system

6. 결 론

이차원 바코드에 워터마크를 적용하고, 시각으로 확인하기 위해 '본'과 같은 글자를 삽입시스템을 제안했다. 워터마크 성능을 히스토그램 분석을 통해 일반 프린터와 스캐너에서 성능을 확인했다.

우선, 600dpi 실험에서는 첫 번째로 배경과 심볼 사이에 간섭 없이 데이터를 읽을 수 있다. 두 번째로 사본이미지의 배경영역에서 효과가 크게 나타났다. 세 번째로 그림 12의 (f)와 같이 불완전한 형태가 좋은 효과를 나타내 스캐너와 시각적으로 워터마크를 구별할 수 있음을 확인했다. 이 같은 특성은 200dpi에서도 비슷하게 나타났다. 특히 스캐너에서 배경영역의 히스토그램이 보정사본과 사본 스캔 이미지에서 큰 변화보였고, 시각적으로는 배경 노이즈가 증가하거나 패턴이 세로로 변형되었다. 따라서 복사 유무를 스캐너와 시각적으로 구별할 수 있음을 확인했다. 하지만 삽입된 글자의 가독성과 심볼영역에서의 효과는 개선이 필요하다.

마지막으로 복사방지 마크가 적용된 바코드에 인증키를 저장해 문서를 발급하고 문서 인증하는 시스템을 제안했다. 워터마크삽입으로 바코드의 크기가 커지지만, 핸드폰 카메라로 문서인증할 수 있어 활용도가 높다. 스캐너의 경우 자동급지장치를 사용할 수 있고, 복사유무를 구별할 수 있어 많은 문서를 신속한 처리가 가능하다.

향후 과제에서는 스캐너를 통한 사본검출알고리즘과 이차원 바코드 복호화를 프로그램으로 구현하고, 검증하는 실험이 필요하다.

참 고 문 헌

- [1] 쿠키건강, "처방전 위·변조시 5년이하 징역", Available: health.kukinews.com, 2010, [Accessed: march 16, 2010]
- [2] 부산일보, "인터넷 통한 위조 증명서 불법 거래 실태", Available: http://www.busan.com, 2010, [Accessed: jun 16, 2010]
- [3] 이상경, 고광은, 심귀보, "워터마크기반의 이차원 바코드 위조방지기술 개발", 한국지능시스템학회, 2010년도 춘계 학술발표논문집 제20권 제1호, pp.414-417, 2010.
- [4] 이상경, 고광은, 심귀보, "위·변조 확인과 복사방지를 위한 이차원 바코드 시스템 연구", 한국지능시스템학회, 2010년도 추계 학술발표논문집 제20권 제2호, pp.209-212, 2010.
- [5] 이정기, 허진, 이광, 이호영, 이준, "디지털 이미지의 웨이블릿 워터 마킹", 한국 콘텐츠 학회, vol. 3, 2005.
- [6] 류기훈, 임선영, 한희일, "이차원바코드를 이용한 공문서 위·변조 방지 확인 시스템 제안", 한국지능정보시스템학회, 2007년 추계학술대회 논문집, pp.444-448, 2007.
- [7] 정성환, 이신주, 배종욱, 김준형, "인쇄된 문서의 위조 방지를 위한 워터마킹 모델 연구", 정보 통신 부, 2005.
- [8] 육성원, 이동인, 박성준, "인터넷 증명서 발급 기술", 정보보호학회지, 제 14권 제5호, pp.1-7, 2004.
- [9] 데일리팜, "위·변조 복사처방, 2D바코드도 '속수무책'", Available: www.dreamdrug.com, 2009, [Accessed: march 10, 2010]
- [10] 김규태, 김종원, 최중욱, "온라인 증명서 발급을 위한 복제방지 코드 패턴의 생성", 한국정보과학회, 1995년도 춘계 학술발표논문집, 제22권 제1호, pp.317-320, 1995.
- [11] Milan Sonka, "Eye Physiology", Available: www.engineering.uiowa.edu/~aip/Lectures, 2002, [Accessed: march 10, 2010]

저 자 소 개

이상경 (SangKyung Lee)

2010년 : 세명대학교 전자공학부 공학사
2010년 ~ 현재 : 중앙대학교 대학원 전자전기공학부 석사과정

관심분야 : Robot for the disabled, GPGPU, Intention Recognition, Intelligent System

고광은(Kwang-Eun Ko)

중앙대학교 전자전기공학부 석박사통합과정
[제20권 3호 (2010년 6월호) 참조]

심귀보 (Kwee-Bo Sim)

중앙대학교 전자전기공학부 교수
[제20권 4호 (2010년 8월호) 참조]