이차원바코드를 이용한 공문서 위·변조 방지 확인 시스템 제안

류 기훈, 임 선영, 한 희일

한국외국어대학교 정보통신공학과

Proposal for systems of protecting and verifying fabrication on official documents using two-dimensional barcode

Ki-Hoon Ryu, Seon-Yeong Lim, Hee-il Hahn

Department of Information and Communications Engineering, Hankuk University of Foreign Studies
iceryu@naver.com

요약

이차원바코드 기술과 암호화 알고리즘을 이용하여 문서의 위·변조 등을 방지하고 문서의 상태를 기업체나 공공기관 등에서 쉽게 확인하여 판단할 수 있는 시스템을 제안한다. 모든 위·변조 확인이 필요한 문서에 암호화된 이차원바코드를 첨부한다. 확인자 측에서는 첨부된 이차원 바코드를 바코드 리더기로 인식하거나 이차원 바코드의 사진을 관련 인터넷 웹 사이트를 통해 문서의 위·변조를 판단한다.

키워드:

이차원 바코드; 위·변조 방지; 암호화

1. 서론

학·석·박사 등의 학위와 각종 문서의 위·변조가 사회 전반에 만연해 공공의 신뢰를 저하시키고 있다. 또한 부동산 매매 계약서에서 법원의 판결문에 이르기까지 각종 문서의 위·변조 역시 사회 각 부문에서 거침없이 자행되고 있다. 전국의 각 법원에 접수된 문서 위·변조 관련 범죄의 추이도 국가와 사회의 앞날을 걱정하지 않을 수 없게 한다. 대법원 집계에 따르면 2004년 5053건, 2005년 6733건 등으로 증가세에 있다. 또한 위·변조의 대상도 주민등록증, 토지 문서, 국제운전면허증 등으로 미치지 않은 곳이 없을 정도이다. 특급탁송화물로 밀반입하려다 인천공항세관에 적발된 위조 서류가 2004년 20건에서 지난해 80건 까지 증가하였고, 2007년도에도 6 월말 현재 국내 주요 대학의 졸업증명서 26건, 주민등록증 16건, 성적증명서 10건 등 모두 70건에 이르고 있다.

본 논문에서는 이차원 바코드와 암호화 알고리즘을 이용하여 문서의 위·변조 등을 방지하고 문서의 상태와 문서의 데이터를 기업체나 공공기관 등에서 쉽게 판단할 수 있는 시스템을 구현하고자 하였다. 문서 내에 있는 모든 데이터의 위·변조를 방지하기 위하여 데이터를 이차원 바코드로 변환 저장하여 문서에 표시한다. 또한 이차원 바코드의 보안을 위하여 이차원 바코드에 저장할 데이터를 암호화시킴으로써 문서의 안전성을 유지할 수 있다. 이차원 바코드는 전기적으로 연결되지 않은 두 컴퓨터 사이에서 데이터 교환 역할을 하고 데이터 이동을 쉽게 할 수 있어 이차원 바코드를 포함한 문서에 대한 신뢰성과 무결성을 보장받을 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 이차원 바코드와 암호화 알고리즘에 대하여 설명하고 3장에서는 시스템의 개요, 문서의 출력 과정, 출력된 문서의 검증 과정을 설명한다. 4장에서는 시스템 구현 및 결과 분석을 설명하고 5장에서 결론을 맺고 향후 연구방향을 제시한다.

2. 이차원 바코드와 암호화

2.1 이차원 바코드

바코드는 데이터를 표현하고 이를 취하는 수단과 방법의 경제성과 편리성, 그리고 바코드 자체 구조의 높은

데이터 신뢰성을 가지고 있다. 또한 여러 산업 분야의 다양한 환경에서 데이터를 수집하고 관리하는 데에 다른 어떤 자동인식(automation identification) 기술보다도 뛰어난 적응성을 갖추고 있다. 사용이 확대되면서 폐쇄적으로 응용되던 체계에서 벗어나 동일 산업계 간 또는 여러 계열 산업계 간이나 국가나 국제 간에 공통으로 응용될 수 있는 개방형 체계를 지향한다. 전기적으로 연결 되어 있지 않은 두 컴퓨터 사이에서 바코드는 데이터 교환의 가교역할을 할 수 있기 때문에 데이터 브리지의 개념을 지닌다. 하나의 컴퓨터 시스템에서 출력된 데이터 파일은 이차원 바코드로 표현되어 타 컴퓨터 시스템에서 키보드를 치지 않고 재입력이 가능하다. 그러므로 모든 산업 분야의 다양한 응용 분야에서 데이터를 신속하고 정확하게 수집할 수 있는 최적의 도구로 저렴하고 용이하게 데이터를 표현할 수 있고 각각의 응용 환경에 맞는 시스템을 이용하여 오류 없는 데이터를 실시간으로 수집하고 처리 할 수 있다.

2.1.1 이차원 바코드의 종류

데이터 구성 방법에 따라 크게 다층형 바코드(stacked bar code)와 매트릭스형 코드(matrix code)로 나뉜다. 다층형 바코드가 종래의 선형 일차원 바코드를 종축(y 방향)으로 누적해 놓은 형태인 점에 반하여 매트릭스형 코드는 정방향의 검고 흰 요소들을 모자이크 식으로 배열하는 형태이므로 보다 더 새로운 구조라고 할 수 있다.

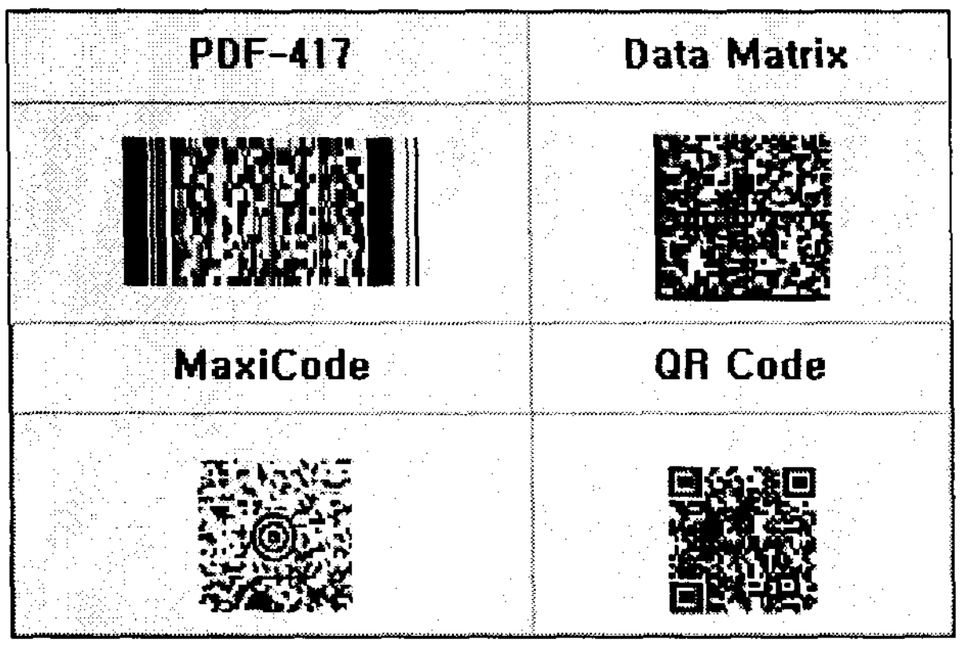


그림 1. 국제 ISO표준 이차원 바코드의 종류

KS 마크를 획득한 이차원바코드는 그림 1에 제시한 바와 같이 미국에서 개발된 PDF417, Data matrix, Maxicode와 일본에서 개발된 QR code 등이 있다. 본 논문에서 채택한 이차원 바코드는 QR code로서 일반 글자의 경우 1,817 문자, 알파벳과 숫자의 경우 4,296 문자, 숫자만 사용할 경우 7,089 문자까지 기록할 수 있다.

2.2 암호화

암호화(Encryption)는 시큐리티에 대처하는 가장 강력한 수단이다. 암호화는 데이터의 내용이 불명확하도록 본래의 데이터를 재구성하여 암호문을 만드는 것이다. 이 때 사용되는 데이터의 재구성 방법을 암호화 알고리즘이라 한다. 암호화 알고리즘에서는 암호화의 비밀성을 높이기 위해 키(key)를 사용한다. 암호화의 목적으로는 허가된 사람에게만 내용 열람을 가능하게 하는 기밀성과 데이터의 불법 변조를 방지하기 위한 무결성, 상대의 신원을 확인하는 인증, 이미 발생한 사건에 대한 증명을 위한 부인 방지 등이 있다.

2.1.1 AES 암호화 알고리즘

AES(Advanced Encryption Standard)는 200 년 2 월에 미국 NIST (National Institute of Standard and Technology)에 의해 연방 정보처리 표준 (FIPS 197, Federal Information Processing Standard)으로 지정된 대칭 키 암호화 방식으로서, 적어도 향후 20~30 년 정도까지는 안전성이 보장된 차세대 암호화 표준이다.

AES 는 효율, 보안, 성능, 구현, 유연성 면을 고려할 때 기존 암호화 표준인 3-DES 에 비해 탁월한 차이를 보이고 있다. AES 는 대칭 키 블록 암호화 알고리즘으로서, 블록 크기는 16, 24 또는 32 바이트가 사용가능하며, 각각의 블록 크기에 역시 16, 24 또는 32 바이트의 키를 사용할 수 있도록 되어 있다. 또한 16 바이트(128 비트) 블록에 16 바이트(128 비트) 키를 사용할 때 최적의 효율을 낼 수 있도록 고안되어 있다.

3. 공문서 위·변조 방지 시스템 설계

본 논문에서는 이차원바코드를 이용하여 발급된 공문서의 무결성과 위·변조 방지를 위한 공문서 위·변조 방지시스템을 제안하였다. 오프라인 환경에서 문서에 대한 무결성과 위·변조에 대한 검증은 쉽지 않다.

본 시스템에서는 현재 물류 시스템에서 효율적인 물품관리를 위해 사용 중인 바코드를 응용하여 오프라인 환경에서 출력된 공문서의 신뢰성을 보장하고자 하였다.

이차원바코드는 공문서의 내용뿐만 아니라 전자서명 및 사진의 이미지 정보까지 저장할 수 있다. 그러나 이차원바코드도 위·변조가 가능하므로 저장할 정보를 AES 암호화 알고리즘을 이용하여 암호화한 후 저장하도록 설계하였다.

3.1. 공문서 출력모듈 설계

기업과 공공기관의 공문서와 같은 전자 문서, 병원의 처방전, 기타 영수증 등의 문서를 출력하면 문서의 위·변조가 가능하여 무결성을 입증을 할 수 없기 때문에 신뢰성이 저하되는 문제점을 안고 있다. 출력된 공문서의 신뢰성과 무결성을 보장하기 위해 AES 암호화 기술과 이차원바코드 기술을 사용하였다. 제안한 시스템에서는 공문서의 내용을 AES 암호화 기술로 암호화한 후 이차원바코드로 변환하여 공문서와 함께 출력한다. 그림 2는 공문서 출력과정을 보여주고 있다.

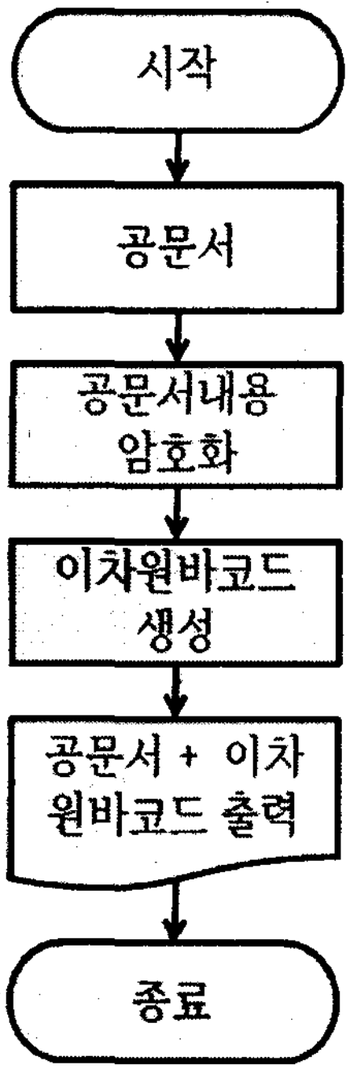


그림 2. 공문서 출력 순서도

3.2 출력문서 검증모듈 설계

공문서와 공문서의 내용이 암호화되어 변환된 이차원바코드가 함께 출력된 문서는 상대방에게 전달된다. 전달 받은 문서의 무결성 및 위·변조 확인을 위하여 그림 3에 제시한 과정에 따라 처리한다. 우선, 문서에 인쇄된 이차원바코드를 스캐닝하여 이를 해독한 후 복호화하여 원래의 데이터로 변환시킨다. 복원된 공문서의 내용과 출력된 공문서의 내용을 서로 비교함으로써 위·변조 검사를 할 수 있다.

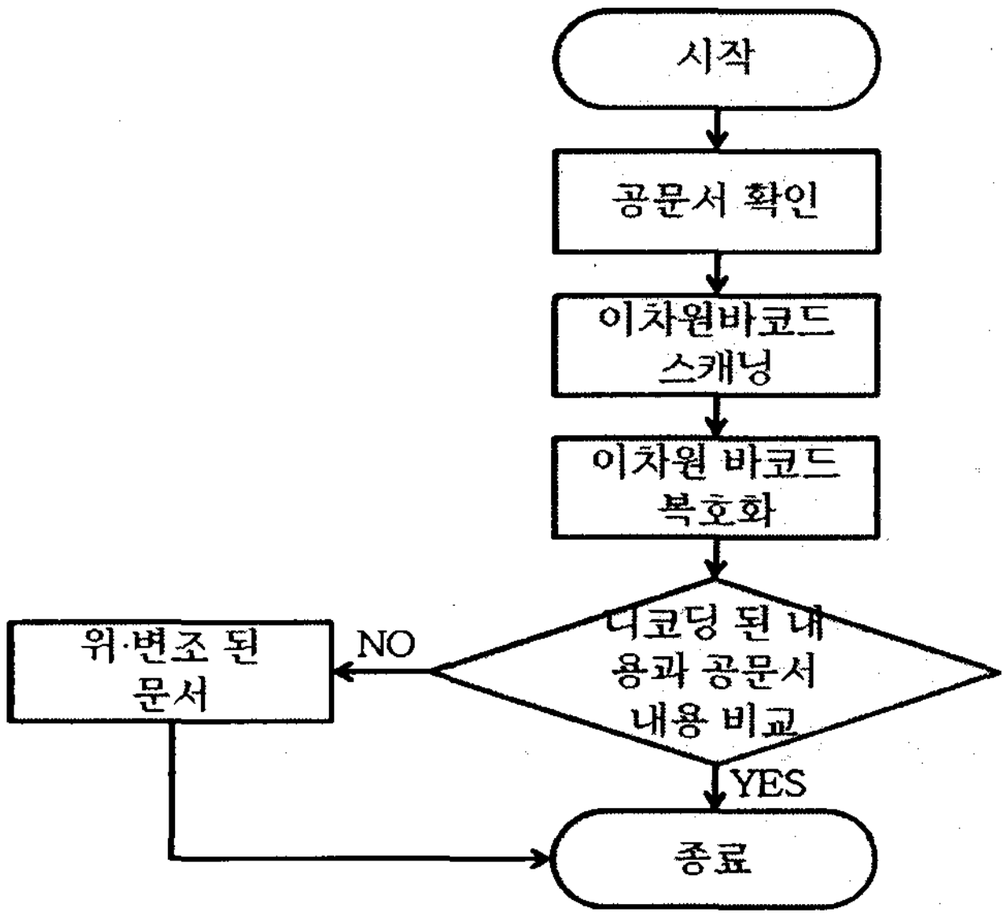


그림 3. 출력된 공문서 검증 흐름도

4. 공문서 위·변조 방지 시스템 구현

본 논문에서는 재학증명서를 예로 들어 구현하였다. 재학증명서에 포함된 모든 데이터를 암호화한 다음 이차원바코드로 변환하여 출력된 재학증명서의 신뢰성과 무결성을 갖도록 하였다.

4.1. 재학증명서 출력과 검증 구현 결과

그림 4는 본 논문에서 제안한 공문서(재학증명서) 위·변조 시스템의 초기화면을 보여주고 있다. 검색 버튼을 통해 학번이나 주민등록번호로 재학생의 데이터를 검색할 수 있다.

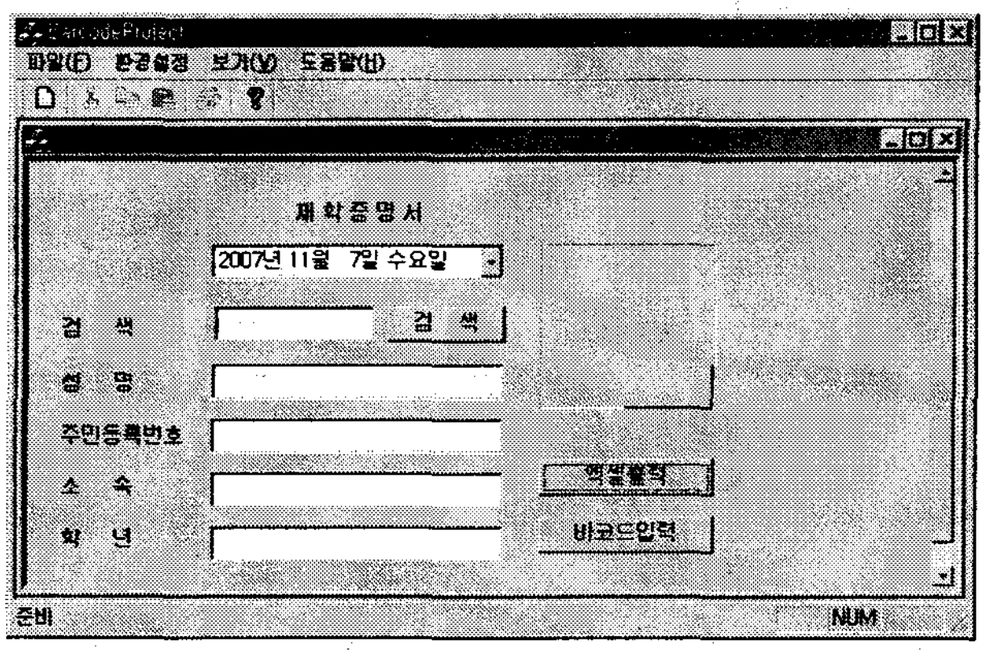


그림 4. 위·변조 시스템 초기 화면

검색을 통해 찾은 데이터는 엑셀출력 버튼을 통해 재학증명서를 출력할 수 있다. 바코드 입력 버튼은 바코드 리더기를 통해 출력된 재학증명서의 이차원바코드를 스캐닝하여 화면에 출력한다.

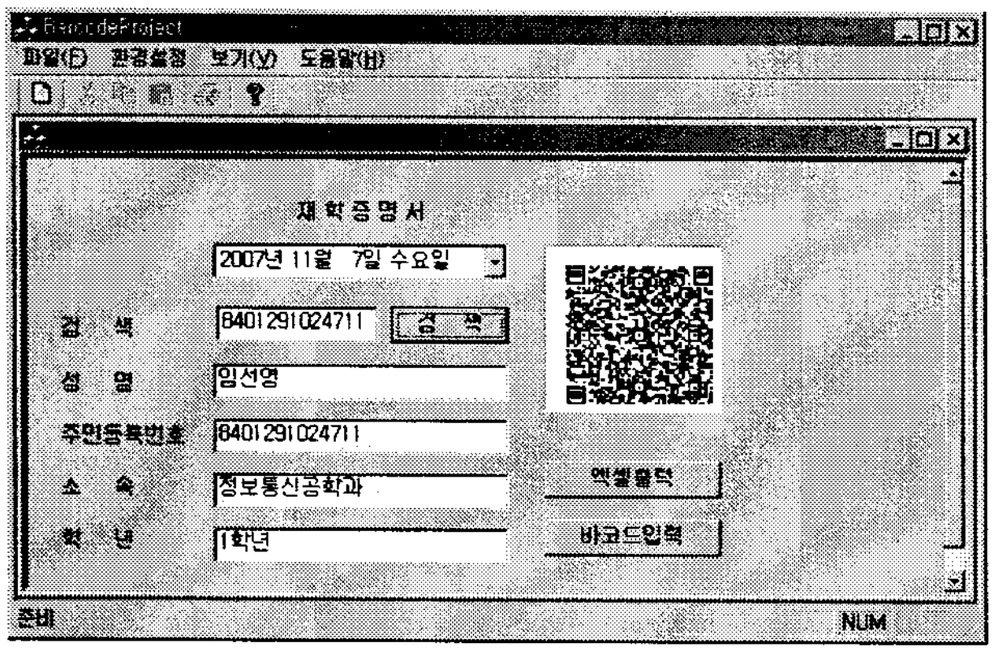
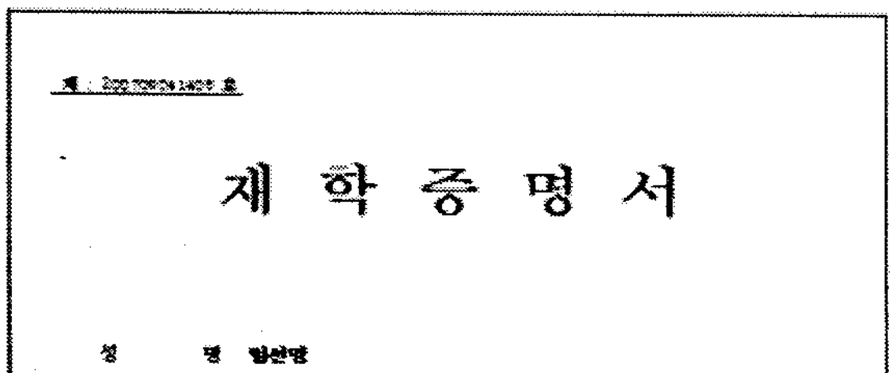


그림 5. 데이터 검색과 이차원바코드 생성과정

그림 5는 검색을 통해 찾은 재학생의 데이터를 화면에 출력하고 재학생의 데이터를 암호화하여 이차원 바코드로 변환해서 화면에 출력한 결과를 보여주고 있다.



재 학 증 명 서

성 명 임선영

주민등록번호 840129-1024711

소 속 한국외국어대학교대학원DSP랩

학 년 1학년

위의 사실을 증명합니다.

2007년 09월 04일

한국외국어대학교 총 장

그림 6. 출력된 재학증명서

제안한 공문서 위·변조 방지 확인 시스템을 통해 출력된 재학증명서는 그림 6에 제시한 바와 같다. 재학증명서 하단에 포함된 이차원 바코드에는 암호화된 재학생의 데이터가 저장되어 있다. 이 이차원바코드를 해독하여 복호화한 다음, 그 결과를 원문의 내용과 비교함으로써 문서의 위·변조를 확인할 수 있다.

이차원바코드가 포함된 재학증명서를 그림 7에 나타낸 바와 같이 스캔하여 이를 해독하면 그 내용은 암호화 여부에 따라 그림 8과 같이 나타난다. 따라서, 암호화 키를 알지 못하면 바코드의 내용을 읽을 수 없어 위·변조가 불가능하도록 하였다.

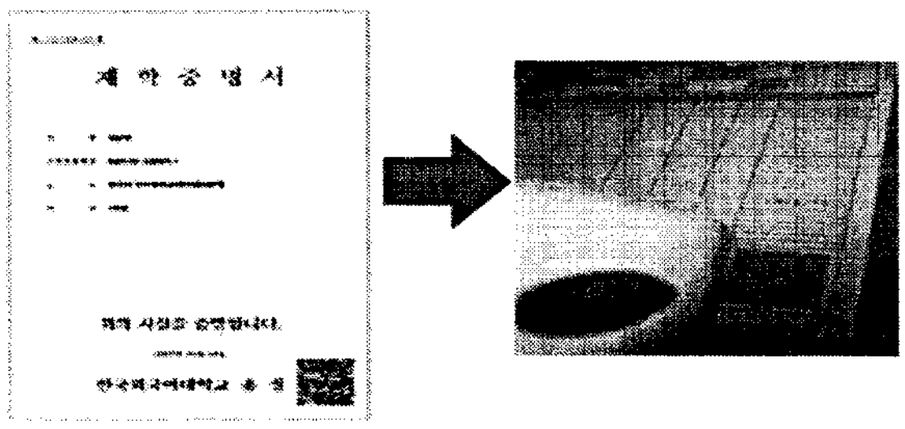


그림 7. 바코드 스캔 작업

	바코더 리더기 스캔을 통한 내용
암호화 전	#LICENSE#20070910001#NAME#임선영#IDNO#840129-1111111#POSITION#한국외국어대학교대학원DSP랩#GRADE#1학년#
암호화 후	#LICENSE# jg?뭢뼈y? #NAME# +뼈y?L#?ㄱ낐e$ #IDNO# 綵?B?ㅓ뭢[v?? #POSITION# n?윑S얺8>x?1?xrg i)'츘~][? #GRADE# 뗇?jg섀 Q}X?

그림 8. 암호화 유무에 따른 데이터 변화

4.2. 결과 분석

출력 후 문서의 안정성은 암호화된 데이터를 이차원 바코드로 변환함으로써 유지된다. 또한 대용량인 이차원 바코드의 장점을 살려 재학증명서의 내용도 저장할 수 있으므로 출력된 문서와 이차원바코드의 비교를 통해 위·변조 여부를 바로 파악할 수 있다. 또한 컴퓨터 사이에서 데이터의 교환 역할을 하고 데이터 이동을 쉽게 할 수 있다. 기존의 문서의 위·변조 및 복잡한 확인절차의 문제점을 암호화된 데이터에 대한 이차원바코드를 통해 해결할 수 있다.

5. 결론

본 논문에서는 이차원 바코드와 암호화 알고리즘(AES)을 이용하여 문서의 신뢰성과 무결성 보장을 위하여 문서의 출력모듈과 검증모듈을 설계하여 구현하였다. 공문서 이외에도 개인 신분 관련 증명서나

예매 시스템 등, 위·변조 가능성이 있는 분야에서도 본 논문에서 제안한 시스템을 적용할 수 있다.

참고 문헌

[1] 장승주. International Symbology Specification-QR Code, 1998 년.

[2] 강주성외, "현대암호학" (국가보안기술연구소, 2000)

[3] 원동호,김세헌."정보보호 관리 및 정책", 생능출판사 2002.

[4] 원동호, 이만영 외 5 명."현대 암호학 및 응용", 생능출판사 2002.

[5] 한국정보보호학회, "현대 암호학 및 응용" (한국정보보호진흥원, 2002)

[6] http://www.webcode.co.kr/changwon/education

[7] 오호근, "최신 바코드 기술 및 응용", 성안당