Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 2 pp. 849-855, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.2.849

스크램블링 암호화 기법을 이용한 전자신분증 위변조 방지 기법

이광형[1*], 정용훈[1]
[1]서일대학교 인터넷정보과

A study of e-passport against forgeries using scrambling encryption method

Kwang-Hyoung Lee[1*] and Young-Hoon Jung[1]
[1]**Internet Information, Seoil College**

요 약 본 논문에서 제안하는 시스템은 기존 여권에서 가시적으로 확인이 가능한 개인정보 보호를 위하여 스크램블링 기법을 이용하여 안전성을 확보할 수 있게 되었다. 제안하는 시스템은 스크램블링 기법을 이용하여 개인정보 즉 여권번호와 사진을 스크램블링 기법을 이용하여 전자여권에 삽입된다. 제안하는 시스템에서 암·복호화를 하기 위해서는 사용자의 개인키와 발급인증기관의 개인키 모두가 있어야 암·복호화가 가능하므로 안전하며 처리속도 또한 전자여권 전체를 암·복호화 하지 않으므로 우수함을 입증하였다.

Abstract In this paper, a proposed system can be ensured safety using scrambling technique in order to protect personal information which identifies visually from the existing e-passport. This system inserts ID card number and photograph into e-passport using scrambling technique. In this system, we need user private key and CA private key to encrypt and decrypt which make it secure. And It show better performance in throughput by not encrypting or decrypting the whole e-passport.

Key Words : Scrambling technique, Electronic ID card, E-passport, Digital protection technology

1. 서론

최근 몇 년 사이의 급격한 인터넷의 발달과 보급은 디지털 생활에 많은 변화를 가져왔다. 초기 단순하고 간단한 자료나 정보의 취득이나 커뮤니티 활동에서 한발 더 나아가 쇼핑이나 금융, 수많은 콘텐츠의 이용 등 인터넷의 사용 목적 및 범위 또한 확장되어 왔다. 한국인터넷진흥원의 조사에 따르면 2006년 12월을 기준으로 국내의 6세 이상 인구의 74.8%가 최근 1개월 이내 1회 이상 인터넷을 사용한 것으로 나타났으며, 그 중 32.7%가 유료 콘텐츠를 이용하고 있는 것으로 조사되었다[1].

유료 콘텐츠의 이용자들이 주로 이용하는 콘텐츠의 종류와 이용정도에 대한 조사 결과 음악을 유료 콘텐츠로 이용하는 사용자가 75.7%로 가장 많았으며, 영화 및 방송을 유료 콘텐츠로 이용하는 경우가 42.5%에 달했고 기타 온라인 게임, 교육, 커뮤니티 등의 순으로 나타났다. 이러한 온라인 콘텐츠 사용의 보편화와 유료 콘텐츠 사용의 증가로 디지털 멀티미디어의 사용과 보급이 급증하고 있다. 뿐만 아니라 기존의 아날로그 데이터들이 디지털화되면서 각종 멀티미디어 매체 또한 기존의 아날로그 방식에서 디지털 방식으로 전환되어 가고 있다. 더불어 이러한 멀티미디어 서비스 및 콘텐츠의 보호에 대한 지적 재산권의 요구가 증가하고 있다.

대부분의 디지털 데이터는 불법 복제 및 유포가 매우 용이하다는 단점을 가지고 있고, 그러한 불법 행위의 정도가 심각한 문제로 대두되었다. 그중에서도 특히 디지털 비디오의 경우에는 위성이나 케이블, 인터넷 망과 같은 공개적인 경로를 통해 전송되므로 복제 및 무단 서비스 이용의 위험성이 더욱 크다. 따라서 디지털 멀티미디어 데이터에 대한 보호의 중요성이 커지고 있으며 이에 따

이 논문은 2010년 서일대학 학술연구비 지원에 의해 연구되었음.
*교신저자 : 이광형(dreamace@seoil.ac.kr)
접수일 11년 12월 16일 수정일 (1차 12년 01월 10일, 2차 12년 01월 30일) 게재확정일 12년 02월 10일

라 여러 가지 디지털 비디오 보호 기술에 대한 연구가 이루어지고 있다.

2. 관련연구

2.1 디지털 보호 기술

디지털 데이터는 미디어 상호간의 유연한 운영과 다양한 기능을 가능하게 하는 장점이 있으나, 복제와 조작이 용이하며, 복제된 데이터와 원본을 구별하기 힘든 단점을 가진다. 이러한 단점은 저작권자의 지적 재산권에 손실을 입힐 수 있는 매우 중요한 문제로 이를 위해 디지털 데이터 보호 기술이 필요하다. 이러한 디지털 데이터 보호 기술에는 스테가노그래피, 워터마킹, 스크램블링 등이 있다. 표 1에서는 이러한 기술들을 비교 하고 있다[7-9].

[표 1] 디지털 보호 기술 비교
[Table 1] Comparison for digital protection technology

	스테가노그래피	워터마킹	스크램블링
영상인지	가능	가능	불가능
영상내용	의미없는내용	실제 정보	실제 정보
은닉정보	실제 정보	소유권, 라이센스	없음

2.2 스테가노그래피(Steganography)

스테가노그래피는 통신의 존재 자체를 숨기면서 통신하는 기술로서 스테가노그래피라는 용어는 '덮여있다'는 뜻의 'steganos'라는 그리스 언어와 '쓰기'를 나타내는 'graphia'라는 말의 합성어이다.

스테가노그래피는 전달하려는 실제 정보를 의미 없는 내용에 삽입하여 숨기는 기술로, 이러한 관점에서 워터마킹 기술과 유사한 특징을 가지고 있으나 차이가 있다.

스테가노그래피는 정보 은닉을 위해 가장 중요하며, 용량이 전송 효율을 결정하며 견고성은 비가시성에 비해 덜 중요하며 공개키 알고리즘을 사용한다.

스테가노그래피는 정보를 은닉하기 위해 보이지 않는 잉크, 점 크기의 작은 사진, 문자 정렬, 디지털 서명 등의 방법을 제공한다. 이러한 스테가노그래피의 목적은 제3자가 영상 안에 은닉된 정보가 있다는 것을 알지 못하게 하는 것이다. 표 2는 정보 특성에 따라 스테가고그래피의 분류이다.

[표 2] 정보 특성에 따른 스테가노그래피의 분류
[Table 2] A classification of steganography by a characteristic of information

	공유 정보	안전성	공격자 모델	문제점
수순 스테가노그래피	없음	삽입 및 추출	수동적	실례가 없음
비밀키 스테가노그래피	비밀키	키 또는 커버	수동적	키 공유
공개키 스테가노그래피	공개키	키	능동적	은닉정보 존재 유무결정이 어려움

2.3 워터마킹(Watermarking)

워터마킹 기술은 작품에 대한 메시지를 간직하기 위해 작품을 눈으로 구분할 수 없는 형태로 변경하는 작업을 말한다.

즉, 원래의 콘텐츠에 소유권이나 라이센스 등의 정보를 삽입하여 지적 재산권 보호와 불법 유통, 조작방지 등에 사용하는 기술이다. 일반적인 워터마킹 시스템은 다음 그림 1과 같다.

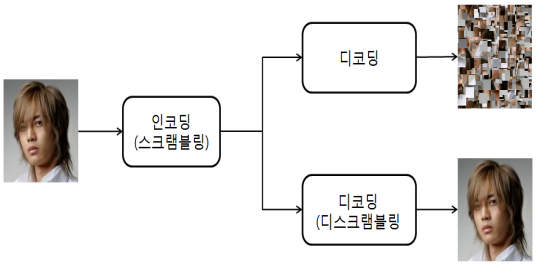
[그림 1] 워터마킹 시스템
[Fig. 1] Watermarkig system

일반적으로 워터마킹 시스템은 입력기와 검출기로 이루어지며, 입력기는 워터마크로서 입력하고자 하는 메시지와 마크를 삽입하려는 대상 이미지를 입력 값으로 가진다.

입력기로부터 산출된 값은 워터마크 검출기의 입력 값으로 주어지며, 대부분의 검출기에서는 워터마크가 존재하는지와 메시지가 입력되어 있는 산출 값이 있는지를 결정하는 역할을 한다[5].

2.4 스크램블링(Scrambling)

스크램블링 기술은 원본 영상 데이터를 특정한 키에 의해 변형 또는 암호화하여 전송함으로써, 특정한 키를 가진 수신자만이 정상적으로 영상을 복원할 수 있도록 하는 기술을 말한다. 따라서 원본 영상을 복원할 수 있는 키를 가진 허가된 사용자들만이 스크램블링으로 인해 왜곡된 영상을 원래의 영상으로 복원할 수 있고 허가되지 않은 수신자는 수신된 영상을 복호화 하더라도, 원래의 영상이 아닌 스크램블링 과정을 거쳐 왜곡된 영상을 보게 됨으로써 정당한 수신자의 권리를 보호할 수 있다. 다음 그림 2는 일반적인 스크램블링 시스템 이다[2-4].



[그림 2] 스크램블링 시스템
[Fig. 2] Scrambling system

2.5 기존 스크램블링 기법

스크램블링은 크게 공간 영역에서의 스크램블링 방법과 주파수 영역에서의 스크램블링 방법, 그리고 그 외의 움직임 벡터를 이용한 방법, 암호화 알고리즘을 이용한 방법 등으로 나눈다[6,10].

2.5.1 공간 영역에서의 스크램블링 방법

화면에 출력되는 공간 영역에서 영상을 직접적으로 왜곡하는 방법으로 일반적으로 많이 사용하는 방법이다. 공간 영역에서의 스크램블링 기법에는 라인 역전, 라인 반전, 라인 치환, 컷 앤 로테이트 스크램블링 기법이 있다.

가) 라인 역전 스크램블링 방법(Line Reversal Scrambling)
가장 단순한 스크램블링 방법으로 스캔 라인(scan line)을 끝에서 끝으로 오른쪽(R)을 왼쪽(L)으로 왼쪽을 오른쪽으로 뒤집는다. 디지털 데이터의 전송 순서를 뒤집는 방식 역시 이 방법에 속한다. 구현이 간단하지만 보안성이 매우 낮다.

나) 라인 반전 스크램블링 방법(Line Inversion Scrambling)
각각의 스캔 라인에 대한 광도 값을 얻어서 흑과 백을 바꾼다. 광도 값을 반전시켜서 전체 영상이나 일부 스캔 라인을 왜곡시킨다. 구현이 간단하지만 품질이 좋지 않고, 영상의 왜곡 정도가 미미하고 보안성 역시 낮다.

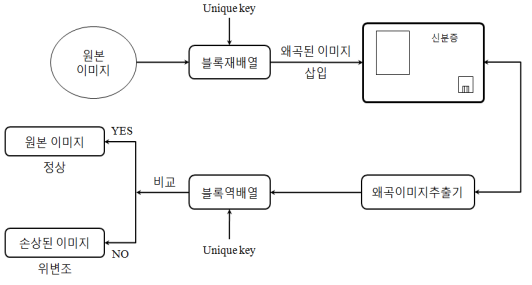
2.5.2 주파수 영역에서의 스크램블링 방법

공간 영역보다 주파수 영역에서의 스크램블링이 더 효율적일 수 있다. 따라서 최근에는 DCT(Discrete Cosine Transform), DFT(Discrete Fourier Transform), DWT(Discrete Wavelet Transform) 같은 주파수 영역에서의 스크램블링에 대한 연구가 활발하게 이루어지고 있다. 주파수 영역에서의 스크램블링 방법에는 DCT 기반의 스크램블링 방법, 웨이블릿 기반의 스크램블링 방법, 비트 스크램블링 방법 등이 있다.

3. 제안시스템

본 논문에서 제안하는 시스템은 사용자의 개인정보 유출사고를 방지하기 위해 신분증에 가시적으로 표현되어 있는 개인정보를 스크램블링 기법을 이용하여 암호화하고 이를 비가시적으로 표현하는 방법이다.

본 논문에서 제안하는 알고리즘은 먼저 신분증에서 주민등록번호, 주소 등 개인정보에 해당하는 부분을 스크램블링 기법을 이용하여 픽셀 단위로 나누고 이를 블록 재배열 알고리즘과 암호화 키(Encryption key)를 이용하여 암호화 한다. 암호화된 전자신분증을 제3자가 습득해도 개인정보에 해당하는 부분은 모두 암호화 되어 있으므로 암호화키와 블록 재배열 알고리즘 모두를 알아야만 개인정보를 습득할 수 있다. 제안하는 시스템의 전체 구조는 그림 3과 같다.



[그림 3] 제안하는 시스템 전체 구성
[Fig. 3] Total constitution of a proposed system

제안하는 시스템에서는 스크램블링 기법을 이용하여 신분증에서 개인정보에 해당하는 부분을 블록 재배열 알

고리즘과 암호화 키를 이용하여 암호화한다. 암호화하는 개인정보 영역을 픽셀 단위로 나누고 이를 블록 재배열 알고리즘을 이용하여 암호화한다.

위변조 여부 확인은 이미지 추출기를 이용하여 전자 신분증 내부의 스마트 칩에 있는 암호화된 이미지를 추출하여 블록 역배열 알고리즘과 복호화 키를 이용하여 원본 이미지로 복호화하며, 복호화된 이미지를 비교하여 원본 이미지와 일치 여부를 확인하고 위변조 사실을 확인할 수 있다.

3.1 블록 재배열 알고리즘

블록 재배열은 먼저 암호화할 원본 이미지를 로드하게 된다. 로드된 이미지를 암호화하기 위해 몇 픽셀 단위로 원본 이미지를 나눌 것인지를 결정한다. 여기서 픽셀의 단위는 송・수신자 간에 미리 약속된 사이즈로 나누어야 수신자가 수신된 암호화된 이미지를 복호화할 경우 손상되지 않은 원본 이미지를 획득 할 수 있다.

원본 이미지가 한 가지 색상일 경우 픽셀 단위로 자르게 되면, 원본 이미지와 암호화된 이미지가 동일하게 나타나므로 사용자가 암호화된 이미지와 원본 이미지를 구분할 수 없다. 그러므로 모두 동일한 색상일 경우를 대비하여 컬러(color)값을 변환하여 동일한 색상의 이미지도 블록 재배열 알고리즘을 통하여 암호화할 경우 동일한 색이 아닌 그림 4와 같이 다양한 색상값으로 변경된다.

[그림 4] 동일 색상 이미지
[Fig. 4] The same hue image

이렇듯 이미지 암호화에 필요한 것은 사용자의 고유 암호화 키(U key)와 시스템 고유의 암호화키(S key), 암호화 키의 길이(Length)이다. 암호화의 키는 (식 1)과 같이 생성한다.

사용자의 고유키와 시스템의 고유키로 연접한 값으로 설정한다.

$$Key1 = (Ukey \oplus Skey) \qquad (식\ 1)$$

또한 키의 길이는 (식 2)와 같이 설정한다. (식 2)에서 이미지에 해당하는 암호화 키의 길이는 원본 이미지의 가로 X 세로 길이에 6을 곱한 값이며, 이때 6을 곱한 이유는 RRGGBB에서 사용되는RGB 색상의 길이가 6byte이기 때문이다.

$$Key_{length} = (image_{width}) \times (image_{height}) \times 6 \qquad (식\ 2)$$

예로 1024 * 768의 이미지를 (식 1)에서 나온 키 Key1(“HB2744142A“)로 암호화 할 경우, 키의 길이는 다음과 같다.

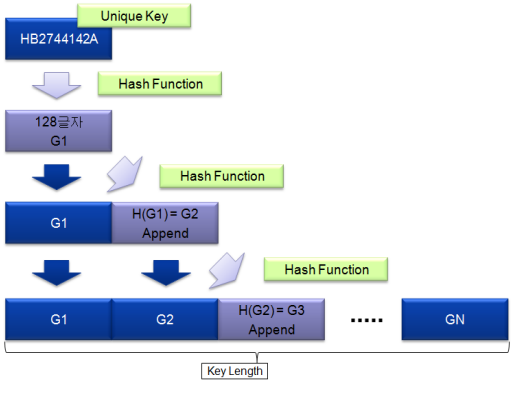
Key_{length} = 1024 * 768 * 6 = 4,718,592

4,718,592만큼의 키 길이를 구하기 위해서는 해쉬함수가 필요하며, 만약 해쉬함수(Sha-512)를 사용한다고 가정을 하면,

Sha-512(“HB2744142A”) =
”0ebe77fead7a4b6a7a6c81b7ec05861fd88d9df6d4adfd6459fb57f8b277814f547c9137ee1dbacd559c278fe326cb6e54ba371acf4629d9dcb437b20279903f“

이다.

하지만 Sha-512(“HB2744142A”)의 문자 길이는 128이다. 이를 4, 718,592 만큼의 길이로 만들기 위해서는 재귀적 호출함수를 이용하여 만들 수 있다. 즉 해쉬 결과값을 다시 해쉬함수를 이용하여 연접시켜 사용하며, 그림 5와 같다. 먼저 암호화키를 해시함수로 연산하여 얻은 결과 128글자를 G1이라 하고, G1을 다시 해시함수 수행하여 얻어진 128글자를 G2라 한다. G3는 G2를 해시함수를 수행하여 얻은 결과이며, 이와 같은 과정을 GN 까지 반복 수행한다.



[그림 5] 암호화 키 생성 방법
[Fig. 5] Generation Method Encrypt Key

이렇게 얻어진 암호화키를 Key2 (G1 ~ GN까지 연산한 키)라고 가정하고, (식 2)와 같이 원본 이미지에 대입시켜 암호화 한다.

$$Image\_Encrypt = (Original_{image} + Key2) \bmod 256 \quad \text{(식 3)}$$

원본 이미지(Original$_{image}$)는 (0,0) 픽셀의 RGB색상부터 (1023, 767)까지의 RGB 색상까지 나열하면 Key2의 길이와 같다. 이를 2byte씩 묶어 식(2)와 같이 연산을 하게되면 원본영상과는 다른 이미지가 생성되게 된다. 이렇게 생성된 이미지가 암호화된 이미지이다.

즉 처음 키였던 Key1 = “HB2744142A”였으며, 이를 이용하여 새로운 암호화된 이미지를 저장함과 동시에 원본이미지와의 무결성을 보호하게 된다.

원본 암호화키(“HB2744142A”)의 경우는 전자신분증을 관리하는 시스템의 공개키 알고리즘으로 암호화 하여 안전성을 고려하도록 한다.

또한 속도 향상을 위해 원본 이미지 전체가 아닌 부분설정을 통해서도 가능하다. 이는 1024 X 768 크기의 이미지에서 (100, 100)부터 (500, 300)크기만을 설정하여 암호화 할 수도 있다. 이는 사용자의 원본 이미지에 주요부분만을 설정하여 암호화가 가능하기 때문에 시스템 오버헤드 측면을 고려하여 설정할 수 있는 특징도 있다.

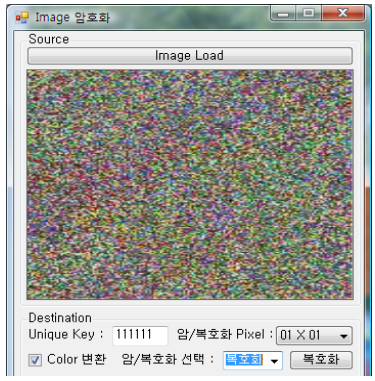
이와 같이 전자신분증에서 사용자의 개인정보와 이미지 정보를 블록 재배열 알고리즘을 통하여 암호화하여 신분증에 삽입된다.

3.2 블록 역배열 알고리즘

블록 역배열 알고리즘은 암호화의 역으로 먼저 왜곡이미지추출기를 통하여 전자신분증의 스마트 칩에서 암호화된 이미지를 추출한다. 추출된 이미지는 블록 역배열 알고리즘과 복호화 키를 이용하여 원본 이미지로 복호화한다. 이때 블록 역배열 알고리즘과 암호화 키 모두가 일치해야 정확한 원본 이미지로 복호화할 수 있다.

그림 5는 왜곡이미지추출기를 통해 암호화된 이미지를 블록 역배열 알고리즘을 이용하여 원본 이미지로 복호화하는 과정을 나타낸다.

불법 사용자가 블록 역배열 알고리즘을 알고 있다 고 가정할 때 복호화 키를 알지 못하면 원본 이미지를 복원할 수 없다. 또한 복호화키를 알고 있어도 블록 역배열 알고리즘을 알지 못하면 원본 이미지로 복호화가 불가능하다.

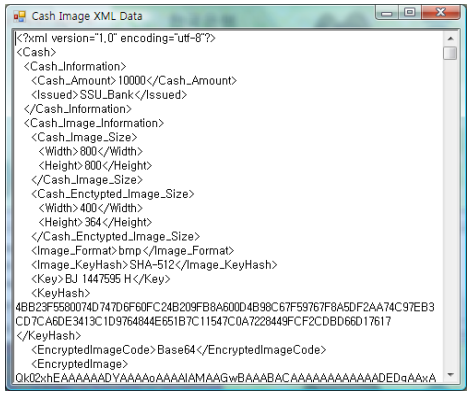


[그림 5] 블록 역배열 알고리즘
[Fig. 5] Block reverse arrangement algorithm

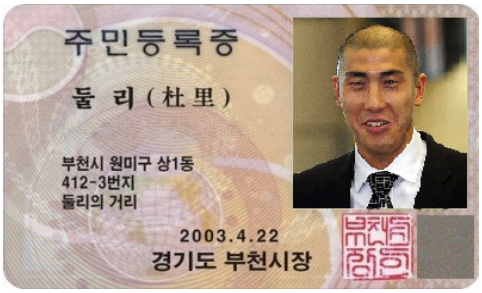
4. 성능평가

4.1 안전성에 대한 평가

현재 사용되고 있는 신분증에서는 사용자의 개인정보를 가시적으로 표현된다. 그러므로 사용자가 신분증을 분실할 경우 개인정보가 노출될 수 있는 단점을 가진다. 또한 전자여권의 경우도 마찬가지로 개인정보가 그대로 노출되어 있으므로, 여권 도난 사고가 빈번하게 발생하고 있으며 이를 이용하여 제3자에게 판매를 하거나 악의적인 목적으로 사용될 수 있다. 제안하는 시스템은 사용자가 신분증을 분실했을 경우 제3자가 이를 습득하여도 개인정보는 신분증 내에 암호화하여 스마트 칩에 저장되므로 개인정보 유출에 대한 사고를 방지할 수 있다. 또한 신분증을 불법 복제하여 사용할 경우 이를 쉽게 판별할 수 있다. 다음 그림 6은 신분증에서 암호화된 부분의 정보를 나타내며, 그림 7은 암호화된 개인정보 및 이미지 정보가 삽입된 신분증을 보여준다.



[그림 6] 암호화된 전자신분증 정보
[Fig. 6] An encrypted electronic ID card information



[그림 7] 암호화된 전자신분증
[Fig. 7] An encrypted electronic ID card

4.2 위·변조 방지

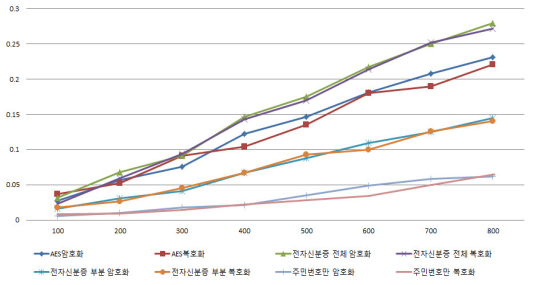
모든 전자신분증은 일련번호 발행 절차를 거치기 때문에 신청한 인증서와 일련번호 없이는 어떠한 경우에도 권한이 부여된 발급인증기관 이외에는 전자신분증 발행이 불가능하며, 발급인증기관에서도 사용자 동의 없이 불법적인 전자신분증을 발행할 수 없다.

현재 전자신분증을 복제하여 사용할 경우 이를 막을 수 있는 방법으로는 진·위폐 감별기가 있어야하며, 육안으로 식별하기 쉽지 않으면 많은 시간과 비용이 발생할 수 있다.

불법 복제된 전자신분증을 사용할 경우 암호화한 암호화키를 획득하지 못한다면 전자신분증을 복호화 할 수 없으므로 사용이 불가능하다. 이는 시스템의 고유키인 S Key를 획득하지 못했기 때문이다.

4.3 기존 스크램블링 기법과 암·복호화 속도 비교

기존 AES 암호화 알고리즘으로 암호화한 것과 제안하는 스크램블링 기법의 속도를 비교하였으며, 이미지 파일 크기가 각기 다른 파일들을 비교 평가 하였다. 기존 AES 알고리즘 보다 제안하는 암호화 기법이 전자신분증 이미지 전체를 암호화 할 경우 상대적으로 암·복호화 속도가 느린 것을 확인하였다. 그러나 전자신분증의 이미지 크기를 절반이나 일부분 암·복호화할 경우 AES 알고리즘과 처리 속도는 비슷하다. 그러나 제안하는 시스템에서 전자신분증 이미지의 주민등록번호와 사진 부분만 암호화 할 경우 처리속도가 약 40% 향상되었음을 확인할 수 있었다. 이와 같은 결과로 볼 때 고성능 프로세스에서 병렬연산이 가능하게끔 되어 있지만 연산능력이 떨어지는 모바일 디바이스에서는 스크램블링 암호화 기법이 처리량이 많은 암호화 기법과 비교하여 영상그래픽 비트의 값만을 변경하는 특징을 가지므로 저사양 기기에 적합하다. 그림 8은 기존 AES 알고리즘과 제안하는 기법을 이용한 암·복호화 속도를 비교하고 있다.



[그림 8] 기존 시스템과 제안하는 시스템 영상 처리 속도 분석
[Fig. 8] Pircture process performance analysis between an existing system and proposed system

5. 결론

본 논문에서는 스크램블링 기법을 이용하여 전자신분증에서 개인정보를 보호할 수 있는 암호화 시스템을 제안하였다.

현재 사용하고 있는 여권이나 신분증은 분실 시 개인정보가 유출되어 개인정보 침해 사고로 이어질 수 있다. 이러한 개인정보 침해 사고를 막기 위한 개인정보 보호 기술이 필요하다.

전자신분증은 발급인증기관으로부터 정상적인 경로를 통해 발급 받은 사용자만이 사용이 가능해야 하며, 이를 불법 복제하거나 위·변조 했을 경우 전자신분증을 안전하게 보호하는 기술이 필요하다.

기존 신분증에서는 개인정보를 가시적으로 확인이 가능하여 분실 시 신분증을 습득한 제3자가 악의적인 목적으로 사용이 가능하며, 위·변조가 가능한 심각한 문제가 발생할 수 있다.

그러므로 기존의 신분증에서 이와 같은 단점을 극복하고자 개인정보 보호에 대한 연구가 진행되고 있다.

본 논문에서 전자신분증에 대한 인증 부분은 발급인증기관의 전자서명과 사용자의 인증 두 가지로 나눌 수 있다. 발급인증기관의 인증은 발급인증기관의 개인키로 전자서명하여 인증하며, 사용자 인증은 사용자의 개인키와 공인인증서를 이용하여 생성된 전자서명으로 인증하게 된다.

암호화된 전자신분증은 발급인증기관의 전자서명과 사용자 전자서명을 함께 발급함으로써 부인 방지 및 무결성 등을 보장할 수 있으며, 암호화 속도 역시 파일 전체가 아닌 부분적으로 암호화를 하게 되므로 속도가 빠

르며 암호화 강도 또한 향상된 기법을 제안하였다. 전자신분증의 위·변조 여부를 확인하기 위해서는 인증기관을 통해 암호화된 정보를 복호화하여 개인정보와 이미지 정보의 일치 여부를 확인하여 확인할 수 있다.

제안한 시스템의 성능평가를 위해 구현한 후 AES 알고리즘과 비교 하였을 경우 암호화 강도가 향상되었으며, 암호화 부분에 따라 수행 시간이 향상되었음을 확인할 수 있었다.

전자신분증을 암호화 하는데 있어 이미지 전체, 반쪽, 일부분으로 나누어 실험한 결과 암호화 속도는 AES 알고리즘을 이용한 암호화에 비해 수행 속도가 향상되었다. 또한 암호화키를 분실할 경우 제안하는 암호화기법에서는 암호화키를 획득하여도 개인키가 없으므로 암호화된 전자신분증을 복호화 할 수 없다. 또한 개인키를 획득해도 스크램블링 기법을 알지 못한다면 암호화된 개인정보를 복호화 할 수 없으므로 암호화 강도 또한 향상되었다.

향후 문서 부분증명 내용 보안과 같은 멀티미디어 콘텐츠 분야에 활용할 수 있으며 연구가 필요하다.

References

[1] jung Y.H, “A New Partial Encryption of e-cash using Scrambling Technical in Mobile Environmemt”, Soongsil Unv. a doctoral dissertation, 2009.

[2] Kim. M .H, “Development of Scrambling Algorithm Using Reordering Macroblocks and Public-key Encryption", Seoil National University of Technology, master's thesis, 2008.

[3] Bloch, M., “Channel scrambling for secrecy”, Information Theory, 2009. ISIT 2009. IEEE International Symposium on June. 28. 2009-July. 3. 2009. Page(s):2452 - 2456.

[4] Hong Peng, YanBin Lin, Yuanzhi Wang, “An Information Hiding Algorithm Based on Blocks and Scrambling”, Artificial Intelligence, 2009. JCAI '09. International Joint Conference on 25-26 April 2009 Page(s):327 - 329.

[5] I. J. Cox, “Digital Watermarking” Morgan Kauffmann Publishers, 2002.

[6] Ito, I,; Kiya, H., “Phase scrambling for blind image matching”, Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on 19-24 April. 2009. Page(s):1521 - 1524.

[7] John Linn, “Trust Models and Management in Public Key Infrastructures”, Technical Notes and Reports of RSA Laboratories, November. 2000.

[8] Moni Naor and Kobbi Nissim, “Certificate Revocation and Certificate Update”, Proceedings of the 7th USENIX Security Symposium, pp.217-228, 1998.

[9] Antonio F.Gomez. Gregorio Marinez. Oscar Canovas., “New Security services based on PKI”, Future Generation Computer Systems, 2003.

[10] Corron, N.J. Reed, B.R. Blakely, J.N. Myneni, K. Pethel, S.D., “Chaotic scrambling for wireless analog video”, Southeastcon, 2009. SOUTHEASTCON '09. IEEE 5-8 March. 2009. Page(s):38 - 43.

이 광 형(Kwang-Hyoung Lee) **[종신회원]**

- 1998년 2월 : 광주대학교 컴퓨터공학과 졸업(공학사)
- 2002년 2월 : 숭실대학교 컴퓨터공학과 (공학석사)
- 2005년 2원 : 숭실대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학 인터넷정보과 부교수

<관심분야>
멀티미디어 데이터 검색, 영상처리, 멀티미디어 보안, DRM, USN, 학습콘텐츠

정 용 훈(Young-Hoon Jung) **[정회원]**

- 2004년 2월 : 숭실대학교 전자계산원 멀티미디어학과(공학사)
- 2006년 8월 : 숭실대학교 컴퓨터공학과 석사졸업(공학석사)
- 2010년 2월 : 숭실대학교 컴퓨터공학과 박사졸업(공학박사)
- 2011년 3월 : 서일대학교 인터넷정보과 전임교수

<관심분야>
암호학, 멀티미디어 보안, DRM, RFID 응용