암호화와 워터마킹 기법을 이용한 디지털 이미지의 안전한 전송

변성철° 안병하
광주과학기술원 기전공학과
{scbyun°, bayhay}@kjist.ac.kr

Secure Transmission of Digital images using Cryptography and Watermarking Techniques

Sungcheal Byun° Byungha Ahn
Dept. of Mechatronics, Kwang-Ju Institute of Science and Technology

요 약

본 논문에서는 디지털 이미지를 대칭 및 비대칭 암호화와 워터마킹 기법을 사용하여 안전하게 전송하는 방법을 제안한다. 제안된 기법은 디지털 이미지의 안전한 전송을 위하여 필수적인 네가지 조건 즉, 비밀성, 인증, 무결성, 부인방지 기능을 제공한다. 비대칭 키 암호화 기법은 전자서명의 발행과 대칭키의 암호화를 위해 사용하고, 대칭키 암호화 기법은 워터마크가 삽입된 디지털 이미지를 암호화 하는데 사용하며, 워터마킹 기법은 전송하고자 하는 디지털 이미지에 전자서명을 삽입하기 위해 사용한다. 제안한 방법의 장점은 전자서명이 별도의 파일로 첨부되는 기존의 전송방식과는 달리 암호화된 디지털 데이터와 전자서명이 동일한 파일 내에 존재하게 되는 것이다.

1. 서론

공공 네트웍을 통한 디지털 데이터의 안전한 교환을 위하여 네가지 요구조건을 충족해야 한다. i) 비밀성 : 오직 보내는 사람과 받는 사람만 데이터를 읽을 수 있다. ii) 인증 : 수신자는 데이터의 발신자를 확인할 수 있다. iii) 무결성 : 수신자는 데이터가 전송중에 변경되었는지 확인할 수 있다. iv) 부인방지 : 발신자는 데이터가 본인으로부터 송신되었다는 것을 부인할 수 없다. 전자서명은 위의 4가지 요구조건중 비밀성을 제외한 모두를 충족시킬 수 있는 수단이다. 비밀성은 비인가자의 무단 접근을 방지하기 위하여 키에 의해서 달성가능하다.

디지털 데이터에 워터마크를 삽입함으로써 방송 모니터링, 저작권 증명, 거래추적, 저작물 인증, 복사 제어, 장치 제어등과 같은 다양한 응용분야에 적용 가능하다[1]. 응용분야에 따라서 디지털 데이터 보호방법도 다양하게 적용된다. 지난 수년간 많은 수의 워터마킹 알고리즘이 제안되었는데 그 중 디지털 데이터의 인증과 무결성에 관한 대표적인 알고리즘은 다음과 같다.

Friedman[2]은 신뢰할 수 있는 디지털 카메라를 제안 하였다. 촬영된 이미지에 전자서명을 삽입함으로써 이미지가 조작 되었는지 여부와 어느 카메라에 의해서 촬영되었는지 확인이 가능하도록 하였다. Yeung and Mintzer[3]는 이미지의 무결성을 확인하기 위하여 의사 랜덤 시퀀스와 수정된 에러 확산 방법을 제안하였다. Wong and Memon[4]은 이미지 인증을 위하여 비밀키와 공개키를 이용한 워터마킹 기법을 제안하였다.

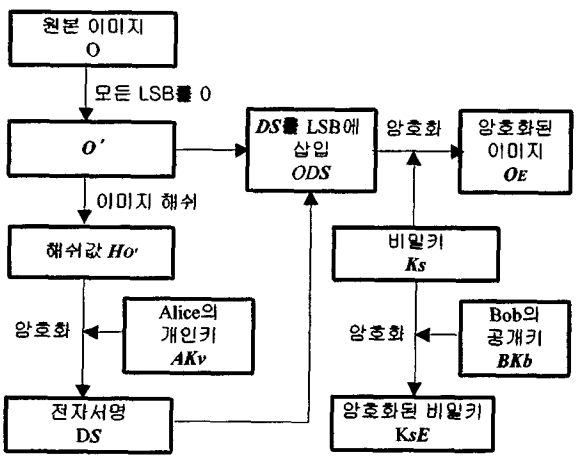
본 논문에서는 대칭 및 비대칭 암호화와 워터마킹 기법을 사용하여 디지털 데이터를 안전하게 전송하는 방법을 제안 하였다. 데이터의 안전한 교환을 위하여 사용중인 기존의 방법은 데이터를 전송할 때 암호화된 원문, 전자서명, 전자봉투의 세가지 파일을 동시에 보낸다. 제안한 방법은 전자서명을 암호화된 원문에 삽입하여 보냄으로써 더욱 안전한 디지털 데이터의 전송방법을 제공한다.

2. 대칭 및 비대칭 암호화와 워터마킹 기법을 이용한 데이터 전송 방법

본 논문에서는 디지털 이미지를 전송하려고 하는 대상으로 가정하여 논의하였다. 이 방법은 다른 멀티미디어 데이터에도 확장 적용 가능하다.

2.1 워터마크 삽입 및 암호화

원본이미지에 대한 워터마크의 삽입 및 암호화 방법은 <그림 1>에 있다. 디지털 이미지에 있어서 LSB는 대부분 잡음성분이다. 따라서 이 영역에 워터마크를 삽입하면 원본이미지의 화질저하를 최소한으로 줄일 수 있다. 먼저 원본이미지의 모든 최소중요비트(Least Significant Bit, LSB)를 0으로 바꾼후 디지털이미지의 해쉬값을 계산한다. 해쉬 알고리즘이 가져야 할 필수조건은 해쉬값으로부터 원본이미지를 추정할 수 없고, 두개의 다른 이미지로부터 동일한 해쉬값이 발생하지 않아야 한다. 해쉬 알고리즘으로는 MD5, 국내 표준인 HAS160, 미 연방 표준인 SHA1&2, 그리고 유럽에서 많이 사용되고 있는 Ripemd등을 사용할 수 있다.



<그림 1> 워터마크 삽입 및 암호화 블록 다이어그램

계산된 해쉬값을 Alice의 개인키로 암호화 하면 이것을 전자서명이라 한다. 전자서명을 원본이미지의 LSB에 대체하고, 전자서명이 삽입된 원본이미지를 비밀키로 암호화한다. 여기에서 비밀키는 임의로 선택되어지며 Bob의 공개키로 암호화된다. 워터마크의 삽입 및 암호화에 대한 수학적 표현은 식(1)에 나타나 있다.

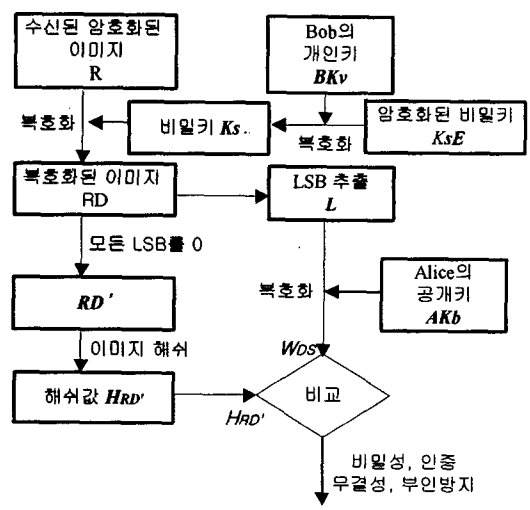
$$
\begin{aligned}
H_{O'} &= ID(O') \\
DS &= E_{AKv}(H_{O'}) \\
O_E &= E_{KS}(O_{DS}) \\
K_{SE} &= E_{BKb}(K_S)
\end{aligned}
\qquad (1)
$$

여기에서

O'	모든 LSB를 0으로 바꾼 원본 이미지;
ID	이미지 해쉬;
HO'	이미지 O'의 해쉬값;
E_{AKv}	Alice의 개인키를 이용한 암호화;
DS	전자서명;
O_{DS}	전자서명으로 LSB를 대체한 원본 이미지;
E_{KS}	비밀키로 암호화;
O_E	워터마크가 삽입되고 암호화된 이미지;
K_S	비밀키;
E_{BKb}	Bob의 공개키를 이용한 암호화;
K_{SE}	암호화된 비밀키.

2.2 워터마크 추출 및 검증

수신된 이미지에 대한 워터마크의 추출 및 검증 절차는 <그림 2>에 있다.



<그림 2> 워터마크 추출 및 확인 블록 다이어그램

워터마크를 추출하고 확인하기 위해서 먼저 암호화된 이미지와 함께 전송된 비밀키를 Bob의 개인키로 복호화한다. 수신된 이미지를 이 비밀키를 사용하여 복호화하고 LSB에 있는 정보를 추출한다. 추출된 LSB의 정보는 Alice의 공개키로 복호화한 다음 이미지의 LSB를 0으로 대체한 후 계산된 해쉬값과 비교한다. 만약 두 값이 동일

하다면 수신된 이미지는 송신된 이미지와 동일하다는 것을 의미한다. 워터마크의 추출 및 검증을 위한 수학식은 식(2)와 같다.

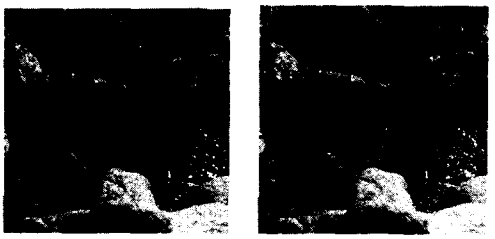
$$\begin{aligned} K_S &= D_{BKv}(K_{SE}) \\ R_D &= D_{Ks}(R) \\ HR_D' &= ID(R_D') \\ W_{DS} &= D_{AKb}(L) \end{aligned} \quad (2)$$

여기에서

K_{SE}	암호화된 비밀키;
D_{BKv}	Bob의 개인키를 이용한 복호화;
K_S	비밀키;
R	수신된 이미지;
D_{Ks}	비밀키를 이용한 복호화;
R_D	복호화된 이미지;
R_D'	모든 LSB를 0으로 바꾼 수신된 이미지;
ID	이미지 해쉬;
HR_D'	이미지 R_D'의 해쉬값;
L	추출된 LSB;
D_{AKb}	Alice의 공개키를 이용한 복호화;
W_{DS}	복호화된 LSB.

3. 실험 및 결론

본 논문에서는 제안된 방법을 검증하기 위하여 일련의 실험을 수행 하였다. 실험 대상 이미지로 <그림 3> (a)와 같이 256x256 크기의 "rocks" 이미지를 사용하였고 워터마크가 삽입된 이미지는 <그림 3> (b)와 같이 원본 이미지와 차이가 없다. 해쉬값을 계산하기 위한 알고리즘으로는 국내 표준인 HAS160을 사용하였다. 워터마킹된 이미지를 조작하지 않은 경우와 압축, 필터링, 확대, 축소, 픽셀값 변화, 일부분 잘림등과 같은 조작에 대한 실험을 통하여 <표 1>에서 보는 바와 같이 이미지에 대한 조작이 없었고 적절한 암호화 및 복호화 키를 사용했을 경우에만 비밀성, 인증, 무결성, 부인방지 요구조건을 충족시킨다는 것을 보였다.



(a) (b)

<그림 3> 원본 이미지(a)와 워터마크 삽입된 이미지(b)

<표 1> 다양한 이미지 조작에 대한 요구조건의 충족도

구분	비밀성, 무결성 인증, 부인방지	
	예	아니오
이미지 조작 없음, 정확한 키 사용	O	
압축		O
필터링		O
확대,축소		O
픽셀값 변화		O
일부분 잘림		O

4. 참고문헌

[1] I.J. Cox, M.L. Miller, and J.A. Bloom, Digital watermarking, Morgan Kaufmann Publishers, 2001.

[2] G.L. Friedman, "The trustworthy digital camera: Restoring credibility to the photographic image", IEEE Trans. Cons. Electron., vol. 39, pp. 905-910, 1993.

[3] M.M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification", Proc. ICIP, pp. 680-683, 1997.

[4] P.W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification", IEEE Trans. Image Processing, vol. 10, pp. 1593-1601, 2001.