선택적 좌표를 이용한 부분 이미지 암호화 기법 연구

한창남, 김정재, 전문석
숭실대학교 일반대학원 컴퓨터학과
e-mail : pluto0142@ssu.ac.kr, argniss@nate.com, mjun@ssu.ac.kr

A Study of Method for Partial Image Encryption using Selective Coordinate

Chang-Nam Han, Jung-Jae Kim, Moon-Seog Jun
Dept of Computer Science, Soong-Sil University

요 약

멀티미디어 시대가 도래함에 따라 콘텐츠들이 인터넷을 통해 셀 수 없을 만큼 많은 양이 전송되어지고 있다. 하지만 콘텐츠를 전송할 때의 안전성과 보안성 및 저작권 문제 등은 아직도 보완해야 할 문제이다. 따라서 본 논문에서는 콘텐츠 중 이미지로 한정하여서 이 이미지의 부분의 좌표를 선택하여 그 부분만 암호화함으로써 이미지를 안전하게 보호할 수 있는 기법에 대해 연구하고자 한다.

1. 서론

21세기에 들어서 현대 사회가 멀티미디어 사회로 발전을 하면서 콘텐츠(이미지, 음악, 영상 등)들이 인터넷이라는 사이버공간을 통해 셀 수 없을 만큼 많은 양이 이동되고 있다. 그 전송매체가 될 수 있는 인터넷으로 사용자는 원하는 콘텐츠를 쉽게 검색할 수 있으며 인터넷으로 뉴스를 본다던지, 전자상거래를 이용할 수도 있으며 실생활에 잘 깃들어져 있어 친숙한 매체가 되었다. 하지만 인터넷이라는 매체를 이용해 콘텐츠를 전송할 때의 안전성, 보안성 및 콘텐츠의 저작권 문제 등은 아직도 보완해야 할 문제이다.

따라서 이러한 안전성, 보안성 및 콘텐츠의 저작권 문제에 대한 연구가 필요하다. 본 논문에서는 이러한 연구 중의 일환으로 콘텐츠 중의 하나인 이미지를 이용하여 그 이미지의 부분의 좌표를 선택하여 좌표에 해당하는 이미지의 영역을 암호화하고 DOI(Digital Object Identifier)를 삽입하여 DOI와 함께 그 영역의 키를 관리함으로써 콘텐츠를 보다 효율적으로 관리할 수 있는 방안에 대해 연구하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로 DOI(Digital Object Identifier)에 대해 살펴보고 3장에서는 선택적 좌표를 이용한 이미지 부분 암호화 기법에 대해 제안하며 4장에서는 결론을 기술한다.

2. 관련연구

2.1 DOI(Digital Object Identifier)

DOI(Digital Object Identifier)는 URN(Uniform Resource Names) 체계의 한 사례로서 디지털 콘텐츠에 대해 고유한 식별기호를 부여하고 이를 URL로 변환하여 인터넷상의 해당 정보의 위치에 접근할 수 있는 체계다. 1990년대 이후 인터넷의 보급이 확대되면서 다양한 콘텐츠가 인터넷을 통해 유통되기 시작하였는데 인터넷을 통해 유통되는 콘텐츠의 식별체계로서 ISBN이나 ISSN등의 기존의 식별체계가 한계가 있으며 URL 또한 콘텐츠 자체가 아니라 콘텐츠의 위치를 식별하는데 이용되기 때문에 콘텐츠의 고유한 식별시스템이 필요함으로 인해 DOI가 개발되게 되었다.

DOI의 구문은 4가지의 요소로 구성되어 있다. 열거, 기술, 변환, 정책으로 이루어져 있으며 열거

(enumeration)는 식별자를 할당하는 역할이며, 기술(description)은 DOI로 식별된 콘텐츠의 메타데이터(INDECS 체계)이고 변환(resolution)은 DOI의 해당 콘텐츠로의 변환(Handle System)이며 정책(policy)은 시스템의 운용을 관할하는 규칙이다.

DOI의 구문은 <Prefix>와 <Suffix>로 구성된다. Prefix는 <등록관리기관 번호>와 <등록기관 번호>로 구성되는데 등록관리기관 번호와 등록기관 번호는 “.”로 구분한다. Suffix는 Prefix가 끝난 다음 사선 뒤에 오게 되는데 등록기관이 자체적으로 부여한다. Suffix에는 통상 각 콘텐츠별 기존 식별코드를 선언하고 그 식별코드의 실제 값이 오게 된다. 다음 그림 1은 DOI 구문구조를 실례로 든 것이다.

doi:10.1082/TEST-KOSIM_PROC/1999-133-136

[그림 1] DOI의 구문구조

그림 1에서 “10.1082”는 Prefix가 되고 “TEST-KOSIM_PROC/1999-133-136”은 Suffix가 된다. Prefix는 전체적인 DOI 등록관리기관의 지정과 맞물려 ‘10.1082.10/1234’와 같이 두 번째 부분이 세분화될 수도 있다.

3. 제안하는 기법

제안하는 기법은 크게 세 가지로 나눌 수 있다. 색상 정보 값을 변경하는 과정, 제안하는 Image Package 구성도, 제안내용의 전체 시스템이다.

3.1 색상 정보 값 변경

본 시스템의 암호화 과정 중의 하나인 색상 정보 값 변경이다. 이미지의 어느 한 영역을 암호화 할 때 좌표를 통해 이미지의 부분을 선택해 해당되는 부분의 색상 정보 값을 변화시켜 그 값으로 암호화를 진행한다. 다음 그림 2는 이미지의 색상 정보 값을 변환시키는 함수이다.

$$\sum_{x=n_{th}_x}^{n_{th}_x Width} \sum_{y=n_{th}_y}^{n_{th}_y Height} (X,Y)_{image_ColorValue}$$

[그림 2] Image_translation

그림 2의 Image_translation 연산에서 이미지의 좌표 값을 지정하면 이미지의 색상 값을 변환하게 된다.

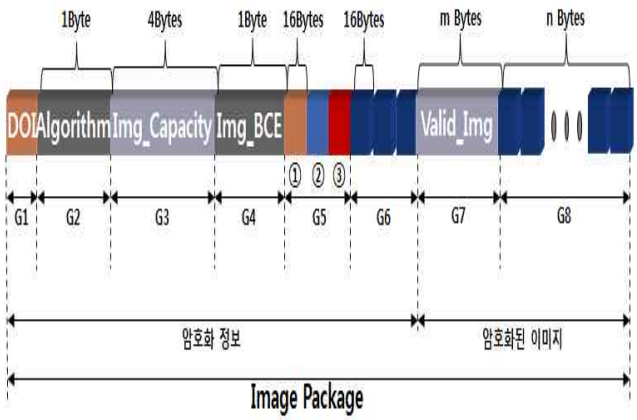
B0412597DCEA...

[그림 3] 색상 정보 값

그림 3은 그림 2의 Image_translation 연산을 하고 난 후의 색상 정보 값이다.

3.2 Image_Package 구성도

다음 그림 4는 암호화된 이미지의 Image Package 구성도이다.



[그림 4] Image Package 구성도

그림 4는 암호화된 이미지 파일의 내부 구조를 나타낸 것이다. <G1>은 DOI 정보가 들어간다. DOI는 KMS에서 이미지에 부여하는 식별자로서 추후 영역의 키를 요청받을 때 검색하는 식별자로서 사용되어진다. <G2>는 알고리즘이다. 어떠한 알고리즘으로 이미지의 영역을 암호화할지 결정한다. <G3>는 암호화된 이미지 전체의 용량이다. 암호화한 후의 이미지 용량이 어느 정도인지를 나타낸다. <G4>는 암호화된 영역(블록)의 개수를 나타낸다. 그림 5의 이미지 영역 암호화를 예시로 했을 때 <G4>의 값은 3이 된다. <G5>는 암호화할 부분의 정보가 들어간다. 암호화 할 영역의 시작점의 좌표, 좌표를 기준으로 높이와 너비를 얼마만큼 잡아서 암호화를 할 것인지 등의 정보를 나타내준다. 그림 5의 이미지를 예로 들었을 때 ①, ②, ③의 순서대로 좌표 값을 넣어준다. <G6>는 패딩 사이즈이다. 이미지 블록을

암호화했을 때 일정한 단위로 블록을 나누고 남는 부분이나 모자라는 부분에 대해서 패딩을 채워서 암호화를 하는데 그 부분을 나타낸다. <G7>은 암호화 한 후의 유효 이미지 용량을 나타내고 <G8>은 암호화 후의 패딩 데이터를 나타낸다. 각 그룹에 대한 표현은 표 1을 참조하면 된다.

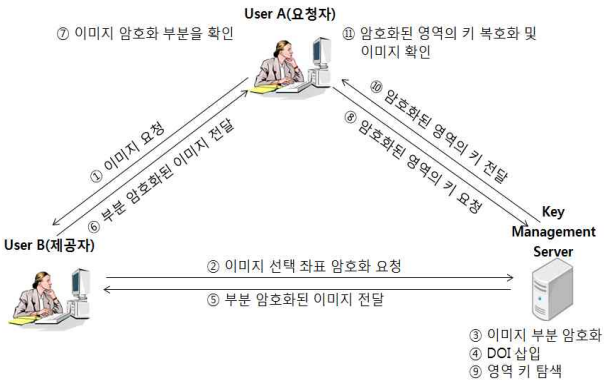
[표 1] Image Package 그룹별 설명

그룹			표현	설명
Image Package	암호화 정보	<G1>	DOI	디지털 객체 식별자
		<G2>	Algorithm	암호화 알고리즘
		<G3>	Img_Capacity	암호화된 이미지 전체의 용량
		<G4>	Img_BCE	암호화 블록의 개수
		<G5>	Coordinator	암호화할 부분의 정보 (기준점, Width, Height값)
		<G6>	Padding_Size	패딩 사이즈
	암호화된 이미지	<G7>	Valid_Img	유효 이미지
		<G8>	E_Padding	암호화 후의 패딩 데이터

[그림 5] 암호화된 이미지

3.3 전체 구성도

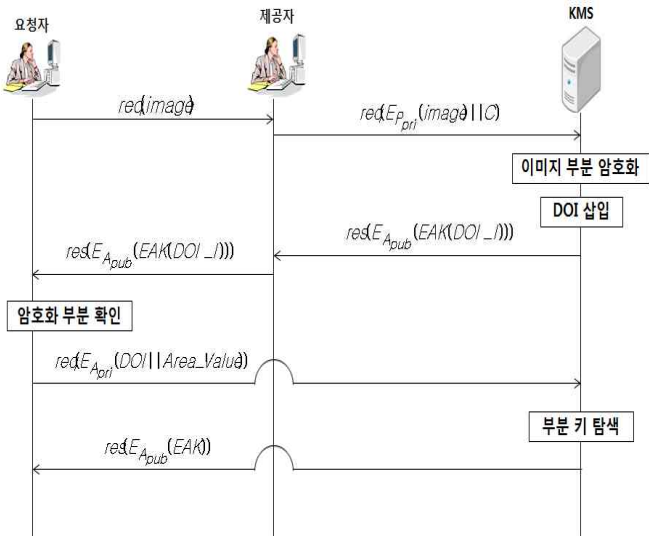
제안하는 전체 구성도는 다음 그림 6와 같다.



[그림 6] 제안하는 이미지 부분 영역 암호화 기법

그림 6에서 요청자(User A)는 제공자(User B)에게 자신이 원하는 이미지를 요청한다. 제공자는 KMS(Key Management Server)에게 이미지와 함께 원하는 좌표를 보내어 이 좌표에 해당하는 이미지의 영역을 암호화해달라는 요청을 한다. KMS는 제공자의 신원을 확인한 후에 이미지를 받아서 요청받은 좌표 로 그 영역을 암호화하고 영역을 암호화한 이미지에 DOI(Digital Object Identifier)를 삽입한다. KMS는 DOI와 함께 암호화한 영역의 키 값을 DB에 보관하여 1:1로 매칭하여 관리하게 된다. 이 후 KMS는 암호화한 이미지를 제공자에게 전달한다. 여기서 KMS가 이미지의 요청자에게 곧바로 이미지를 전달하지 않는 이유는 제공자가 접속을 하고 있지 않을 때를 대비하기 위해서이며 또 한 가지는 KMS가 아직 요청자의 신원을 확인하지 않았기 때문이기도 하다. 제공자는 요청자의 요청이 있을 때까지 암호화된 이미지를 가지고 있다가 요청자의 요청이 있은 후 암호화된 이미지를 전달한다. 요청자는 이미지에 암호화된 부분을 확인한 후에 KMS에게 암호화된 영역의 키를 요청을 한다. KMS는 요청자의 신원을 확인한 후에 DOI를 이용하여 DB에서 영역의 키를 찾아 그 키를 요청자에게 전달해준다. 이미지의 요청자는 영역의 키를 받아서 이미지를 복호화한 후에 이미지 완본을 확인하게 된다.

다음 그림 7은 제안하는 시스템의 흐름도이다.



[그림 7] 제안하는 시스템의 흐름도

A : 요청자 P : 제공자 pri : 개인키 pub : 공개키
EAK : 암호화한 영역의 키 C : 좌표 Area_Value : 영역 값

요청자는 제공자에게 이미지를 요청하는 메시지를 보낸다. 이미지 요청 메시지를 받은 제공자는 KMS에게 이미지의 좌표와 함께 자신의 개인키로 서명하여 이미지를 암호화하여 보낸다. 이미지를 받은 KMS는 이미지와 좌표를 받고 제공자를 확인한 후에 제공자에게서 받은 좌표를 이미지에 적용시켜 좌표에 맞는 이미지의 영역을 암호화한다. 그 후에 DOI를 삽입하여 그 DOI와 함께 암호화한 키를 DB에 1:1 매칭하는 형식으로 보관하게 된다. KMS는 영역 암호화한 이미지를 요청자의 공개키로 암호화하여 제공자에게 전송하게 된다. 요청자에게 바로 전송하지 않는 이유는 요청자가 바로 응답하지 않을 수도 있기 때문이며 또한 KMS가 요청자의 신원을 알 수 없는 이유이기도 하다. 그 이유로 인해 제공자에게 먼저 전송하게 되는 것이다. 이미지를 받은 제공자는 요청자의 요청이 있은 후에 암호화된 이미지를 전송하게 된다. 이미지를 받은 요청자는 자신의 개인키로 복호화하여 이미지를 확인하게 된다. 암호화된 이미지를 확인한 요청자는 KMS에게 자신의 개인키로 서명하여 암호화된 영역의 키를 요청하는 메시지를 전송한다. 메시지를 수신한 KMS는 요청자를 확인한 후 DB에서 DOI를 이용해 영역의 키를 찾는다. 영역의 키를 찾은 KMS는 요청자의 공개키로 영역의 키를 암호화하여 요청자에게 전송하게 된다. 영역의 키를 받은 요청자는 그 키로 이미지의 암호화된 영역을 복호화하여 완전한 이미지를 받아볼 수 있게 된다.

위에서 제안한 암호화 기법은 이미지의 좌표를 지정해 그 영역만을 부분적으로 암호화하여서 이미지의 암호화 및 복호화 시간을 단축하고 KMS의 부하를 감소시키는 장점을 가진다. 또한 암호화된 이미지에 DOI를 삽입함으로써 KMS의 DB에서 이미지 및 부분키 관리가 용이해진다.

또한 기존의 이미지 암호화 기법에서는 대칭키보다 속도가 느린 해시 알고리즘을 사용하였다. 하지만 이 해시 알고리즘을 이용할 시 해시체인 기법을 이용하여 키를 생성하는 과정에서부터 시스템에 오버헤드가 발생하게 된다. 본 논문에서 제안하는 시스템은 이미 검증되어진 암호화 알고리즘(대칭키 / 비대칭키)을 이용하며 파일 스트림을 암호화하는 것이 아니라 색상 정보 값을 암호화하여서 기존의 이미지 속성을 변화시키는 것이 아니기 때문에 어디에서든 이미지를 불러와서 확인할 수 있는 장점이 있다.

4. 결론 및 향후 계획

현대 사회가 멀티미디어 사회로 진행되어지면서 콘텐츠들이 인터넷이라는 정보의 바다에서 무수히 많이 생겨나게 되었다. 이 콘텐츠들을 사용자는 쉽게 검색하고 자유로이 전송할 수 있다. 하지만 콘텐츠를 전송할 때의 안전성, 보안성 및 저작권 문제 등은 아직도 해결해야 하는 문제로 남아있다.

본 논문에서는 콘텐츠 중 이미지를 예로 들어서 이미지를 좌표화해서 지정된 좌표의 영역만을 암호화하고 그 영역의 키를 이미지의 DOI(디지털 객체 식별자)를 통해 효율적으로 관리할 수 있게 하였다. 이미지를 전체를 암호화하는 것이 아니라 좌표에 따른 영역만을 암호화함으로써 상대적으로 부하가 적고 KMS에서 DOI와 함께 이미지 영역의 키를 관리함으로서 보다 효율적으로 키를 관리할 수 있다는 장점이 있다.

향후에는 이 시스템을 구현하여서 이전의 해시 알고리즘을 사용해 이미지 암호화를 한 것과 성능을 평가해보고 콘텐츠의 다른 부분에서도 DOI를 이용해 암호화된 데이터를 관리할 수 있는 방안에 대해서도 연구할 예정이다.

참고문헌

[1] 정상원, 오상훈, 한국데이터베이스진흥센터, “디지털 콘텐츠 식별 시스템(DOI)의 구축”, 2002년 제7회 한국정보관리학회 학술대회

[2] N.Paskin, "Digital Object Identifier", McGraw-Hill, 2003

[3] DOI Name Information and Guidelines, Crossref, 2009

[4] 정용훈, 모바일 환경에서 스크램블링 기법을 이용한 새로운 전자화폐 부분 암호화, 2009