클라우드 컴퓨팅 기반 스트리밍 미디어의 검색 가능 이미지 암호 시스템의 설계

차병래* · 김대규 · 김남호 · 최세일 · 김종원**

Design of Searchable Image Encryption System of Streaming Media based on Cloud Computing

Byung-Rae Cha* · Dae-Kyu Kim · Nam-Ho Kim · Se-Ill Choi · Jong-Won Kim**

요 약

본 논문에서는 클라우드 기반의 스트리밍 미디어의 보안 인증과 프라이버시를 제공하기 위한 검색 가능 이미지 암호 시스템을 설계한다. 검색 가능 암호 시스템의 기본 설계를 모태로 텍스트의 검색에서 확장하여 스트리밍 서비스의 검색을 가능하며, 암호화 및 CBIR 기술을 이용하여 개인의 프라이버시 및 보안 인증을 제공한다. Partial Story Cut과 Image Keyword 생성의 간략한 시뮬레이션을 통하여 스트리밍 서비스 기반의 검색 가능 암호 시스템의 가능성을 확인할 수 있다.

ABSTRACT

In this paper, we design searchable image encryption system to provide the privacy and authentication on streaming media based on cloud computing. The searchable encryption system is the matrix of searchable image encryption system by extending the streaming search from text search, the search of the streaming service is available, and supports personal privacy and authentication using encryption/decryption and CBIR technique. In simple simulation of post-cut and image keyword creation, we can verify the possibilities of the searchable image encryption system based on streaming service.

키워드

Searchable Image Encryption System, Streaming Media, Privacy, Cloud Computing
검색가능 이미지 암호 시스템, 스트리밍 미디어, 프라이버시, 클라우드 컴퓨팅

Ⅰ. 서 론

최근 IT 분야의 이슈를 보면, 클라우드 컴퓨팅과 빅 데이터(Big Data)가 여러 이슈들 중에 포함되어 있으며, 산·학· 연 활동이 활발히 진행 중에 있다. 컴퓨팅 환경 분야의 새로운 패러다임으로 클라우드 컴퓨팅이 거론되고 있으며, 활발한 소셜 네트워크에 의한 빅 데이터가 새로운 이슈로 부각되었다. 이 두 영역에 위치한 서비스가 스트리밍 서비스이며, 스트리밍 서비스에 의해 발생되는 빅 데이터 문제와 이에 관련된 추가적인 문제점들이 새로이 대두되고 있는 상황이다. 이러한 문제점들을 클라우드 컴퓨팅 기술로 극복하기 위한

* 광주과학기술원 정보통신공학과(brcha@nm.gist.ac.kr)
** 교신저자 : 광주과학기술원 정보통신공학과(jongwon@gist.ac.kr)
접수일자 : 2012. 06. 30 심사(수정)일자 : 2012. 07. 26 게재확정일자 : 2012. 08. 09

클라우드 컴퓨팅 기반의 스트리밍 서비스를 설계하고 한다. 본 연구의 목표는 클라우드 컴퓨팅 기반의 스트리밍 서비스를 지원하기 위한 StraaS(Streaming as a Service)를 설계를 목표로 한다.

기업마다 빅 데이터의 형태나 요구 사항은 매우 다양하고, 이에 따른 컴퓨팅 환경도 복잡해졌다. 특히 스토리지 입장에서는 단순히 데이터를 저장하는 것뿐만 아니라, 다양한 컴퓨팅 환경을 유기적으로 연동시켜야 한다는 점에서 가장 중요한 인프라이며, 전체 컴퓨팅 환경을 결정짓는 핵심 요소이다. Big Data의 효율적 활용을 위해서는 클라우드 컴퓨팅을 이용한 Big Data와 관련된 모든 영역에서 중요한 역할을 수행할 수 있으며, 클라우드 기반의 Hadoop, MapReduce 같은 솔루션이 Big Data의 복잡성을 해결이 가능하다. 또한 그림 1과 같이 클라우드 인프라의 컴퓨팅 자원에 의해서 실시간 분석이 가능하며, 네트워크 강화(scaling of network)를 통해 Big Data를 통한 가치 창출 기반 조성할 수 있다. 또한 기존 유무선 네트워크 및 주파수 인프라 관리 또한 복잡/다양한 Big Data에 맞게 대응 필요하다.

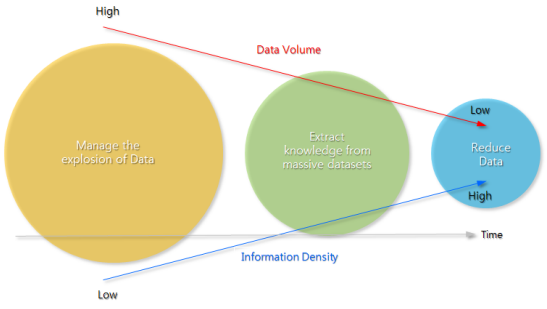

그림 1. Big Data를 통한 가치 창출
Fig. 1 Valued chain creation by Big Data

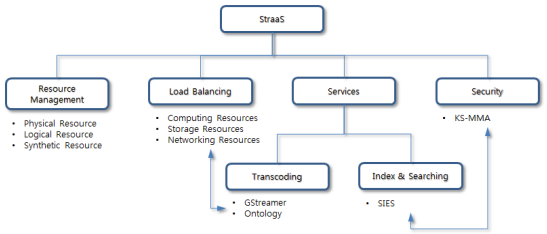

그림 2. StraaS 서비스의 개념도
Fig. 2 Concept diagram of StraaS service

클라우드 컴퓨팅 기반과 데이터 처리 기술을 이용하여 스트리밍 서비스를 제공하는 것을 StraaS라 정의하며, StraaS는 기존의 스트리밍 서비스를 클라우드 컴퓨팅 인프라의 컴퓨팅, 네트워킹, 그리고 스토리지 자원위에서 보안을 제공하며, 다양한 서비스를 위한 데이터 처리 기술을 서비스로 제공하는 서비스를 의미하며, 그림 2와 같이 나타낸다. StraaS는 클라우드 컴퓨팅 기반의 스트리밍 서비스를 제공하며, 임의의 제약조건에서도 클라우드 인프라의 컴퓨팅을 탄력적으로 운용하여 스트리밍 미디어의 변환, 색인/검색 및 압축 등의 다양한 서비스를 실시간으로 제공할 수 있다는 것이 StraaS의 특징이다. 검색 가능 암호 시스템(SES ; Searchable Encryption System)은 암호화된 자료를 복호화하지 않고도 원하는 자료를 검색할 수 있도록 하는 암호 기반 기술이다. 검색 가능 암호 시스템은 개인의 정보가 외부 저장 공간에 저장되면서 발생하는 여러 문제점에 대한 해결 방법으로 지금까지 많은 연구가 진행되었으며, StraaS의 기능 중의 하나인 SIES는 SES의 개념을 클라우드 컴퓨팅 기반의 스트리밍 미디어로 확장한 연구이다.

본 논문의 2장에서는 관련 연구로 검색 가능 암호 시스템의 개념과 기술동향을 기술한다. 3장에서는 검색가능 이미지 암호 시스템을 설계하며, 스트리밍 미디어에서의 색인과 패턴 정보, 스트리밍 미디어와 이미지 키워드의 암호 및 복호화, 그리고 SIES의 메타정보에 대해서 기술한다. 4장에서는 간단한 프로토타입을 코딩하여 스트리밍 미디어의 포스트 컷 분할과 이미지 키워드 생성에 관한 시뮬레이션으로 SIES의 가능성을 검증하며, 마지막으로 5장에서는 본 연구의 내용을 요약한다.

II. 관련 연구

본 연구의 관련 연구로는 검색 가능 암호 시스템의 개념과 기술 동향에 대해서 기술한다.

2.1 검색 가능 암호 시스템의 개념

정보를 안전하게 저장하기 위한 다른 방법으로 암호화를 생각할 수 있다. 즉, 외부 저장 공간에 저장할

정보를 안전성이 증명된 암호 시스템을 이용하여 암호화하는 것이다. 안전성이 증명된 암호 시스템은 복호화 키를 소유하지 못한 공격자가 암호문으로부터 실제 저장된 정보를 얻을 수 없다는 것을 보장한다. 따라서, 외부 침입자 또는 저장 공간의 소유자가 외부 저장 공간에 저장된 암호문에 접근했다하더라도 실제 의미 있는 정보를 얻지는 못한다는 것을 의미한다.

검색 가능 암호 시스템은 기존의 암호 기술과 같이 암호화된 정보에 대한 안정성을 보장하면서 동시에 특정 키워드를 포함하는 정보를 검색할 수 있도록 고안된 암호 기술이다. 데이터베이스에서 제공되는 다양한 기능 중 많은 경우가 특정 키워드를 포함하는 정보에 대한 검색을 바탕으로 이루어지기 때문에 검색 가능 암호 시스템은 앞에서 제기된 문제에 대한 해결 방안 중 하나로 여겨지고 있다. 또한 기본적인 검색 이외에도 범위 검색, conjunctive 검색 등의 다양한 검색 기능을 제공하는 검색 가능 암호 시스템[1-4]에 대한 연구도 진행 중이다.

검색 가능 암호 시스템에서 암호화의 대상인 정보를 문서(Document)라 부른다. 즉, 문서는 사용자가 숨기고 싶은 정보(Information)이다. 또한, 사용자가 자신이 원하는 문서를 검색하기 위해 서버에 제공하는 정보를 키워드(keyword)라고 부른다. 일반적으로 자료는 그 문서에 포함된 키워드들의 집합으로 (1)과 같이 정의된다.

$$D = \{ W_1, W_2, \cdots, W_n \} \quad (1)$$

검색 가능 암호 시스템은 키 생성(key generation), 암호화(build index), 트랩도어 생성(trapdoor generation), 검색(search)의 4가지 단계로 이루어지며, 그림 3과 같이 나타낸다.

그림 3. 검색 가능 암호 시스템의 기본 구성
Fig. 3 Basic structure of searchable encryption system

- 키 생성 단계 - 사용자가 앞으로 사용할 검색 가능 암호 시스템을 준비하는 단계.
- 색인 및 암호화 단계 - 사용자는 주어진 자료에 대해 자료 자체를 암호화한 문서와 색인된 키워드의 정보를 포함한 인덱스(index)를 생성하며, 암호문과 인덱스는 모두 서버에 저장되고, 암호화 단계에서 사용자의 키에 의해서 비밀 키 기반 검색 가능 암호 시스템(SSE)과 공개 키 기반 검색 가능 암호 시스템(PSE; Public-key Searchable Encryption)을 구분함.
- 트랩 도어 생성 단계 - 트랩 도어 생성 단계는 사용자에 의해서 실행되며 주어진 키워드에 해당하는 트랩 도어를 생성하며, 트랩 도어는 오직 사용자의 키로부터 생성이 가능.
- 검색 단계 - 마지막, 검색 단계는 주어진 트랩 도어에 대응하는 문서를 찾는 단계로 서버에 의해서 실행되며, 검색의 결과로 서버는 주어진 트랩 도어와 일치하는 문서의 암호문 또는 문서의 식별자(identifier)을 사용자에게 전달.

검색 가능 암호 시스템은 다음과 같은 요구 조건을 만족시켜야 한다. 우선 검색 단계에서는 주어진 트랩 도어와 일치하는 모든 문서들이 검색되어야 하며, 검색에서 발생할 수 있는 오류는 최소화되어야 한다. 여기에서 오류란 주어진 트랩 도어에 대응하는 키워드를 포함하고 있지 않은 문서가 검색 결과에 포함될 확률을 의미한다. 정보 보호 측면에서 볼 때, 검색 과정에서 유출되는 정보의 양은 가능하면 작아야 한다. 좀 더 구체적으로 주어진 트랩 도어와 관계없는 또는 일부 키워드만을 포함하는 문서에 대한 정보는 유출이 되어서는 안된다.

2.2 검색 가능 암호 시스템의 기술 동향

검색 가능 암호 시스템은 개인의 정보가 외부 저장 공간에 저장되면서 발생하는 여러 문제점에 대한 해결 방법으로 지금까지 많은 연구가 진행되었으며, 그림 4와 같이 사용자의 암호화 키에 의해 공개 키와 개인 키로 분류할 수 있다. [5]

개인 키 기반 SES의 Oblivious RAM은 1996년 R. Ostrovsky와 P. Golle [6, 7]에 의해서 제안되었으며, 기본적으로 검색 가능 암호 시스템으로 보기는 힘들지만, 추가적인 정보를 유출하지 않으면서 원하는 정보를 검색할 수 있는 검색 방식을 제안했다는 점에서 검색 가능 암호 시스템의 초기 형태라는 의미를 지닌

다. Hidden Search는 2000년 Song, Wagner, Perrig[8]에 의해서 제안된 시스템으로 평문의 정보를 유출하지 않으면서 검색할 수 있도록 고안되었으며, 명확한 안전성이 정의되지는 않았지만 초기의 검색 가능 암호 시스템이라 할 수 있다. 처음으로 안전성이 증명된 검색 가능 암호 시스템으로 2003년 Goh[9]가 Bloom filter를 사용하여 설계하였다. 또한 Goh는 처음으로 검색 가능 암호시스템에 대한 명확한 안전성 정의를 제시하였으며, 이를 이용하여 제안된 검색 가능 암호 시스템이 안전함을 증명하였다. 2005년 Chang 등이 제안한 방식[10]은 매우 작은 트랩 도어를 사용하는 등 검색 가능 암호 시스템에 대한 현실적인 요구를 반영하여 고안되었다. Curtmola[11] 등은 대칭키 기반 검색 가능 암호 시스템에 대한 기존의 adaptive security 정의를 새롭게 수정하였으며, 이를 바탕으로 새로운 검색 가능 암호 시스템인 SSE(Symmetric-key Searchable Encryption)를 제안하였다. SSE에 사용된 주요 기술은 해시 테이블과 링크드 리스트(linked list)이다. 기존에 제안된 모든 검색 가능 암호 기술이 서버에 저장된 모든 자료의 인덱스에 대해 검색을 수행하던 것에 비해서 SSE는 주어진 키워드에 대응하는 자료의 인덱스만을 검사한다.

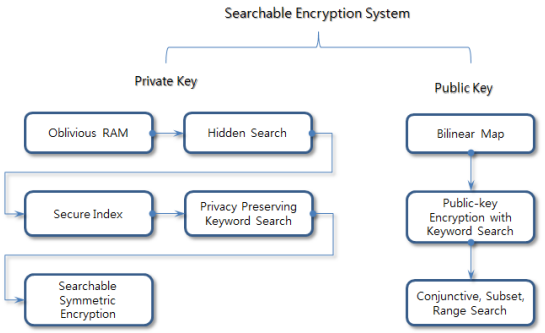

그림 4. 개인 키와 공개 키에 의한 SES 분류
Fig. 4 SES classification by private key and public key

공개키 기반의 검색 가능 암호 시스템은 공개키 기반 암호의 장점을 이어 받아 시스템의 공개 정보만을 이용하여 누구나 암호문을 생성할 수 있도록 한다. 따라서 자료의 제공자와 사용자가 동일하던 대칭키 기반의 시스템보다 더 많은 응용 범위를 가진다. 지금까지 다양한 공개키 기반 검색 가능 암호시스템이 제안되었는데, 최근의 결과들은 대부분 시스템의 설계에 겹선형 사상(bilinear map)을 사용하였다. 겹선형 사상은 타원곡선 위에서 정의된 Weil pairing 또는 Tate pairing으로 대표되며, 겹선형 사상은 Joux가 삼자간 키 공유 시스템에 처음 사용한 이후 다양한 암호 응용 프로토콜의 설계에 사용되고 있다. Boneh 등[12]은 처음으로 공개키 기반의 검색 가능 암호 시스템의 정의를 제시하였으며, 이를 만족하는 최초의 공개키 기반 검색 가능 암호 시스템을 제안하였다. 이들은 두 개의 알고리듬을 소개하였는데, 이 중 하나에서 겹선형 사상을 사용하였고, 다른 하나는 trapdoor permutation을 사용하여 시스템을 구성하였다. 또한 검색 가능 암호 시스템에 대한 안전성 모델을 완성하였다. 2007년 Boneh와 Waters[13]는 다양한 부가 검색 기능을 지니는 공개키 기반 검색 가능 암호 시스템을 제안하였다. 이들은 일반적인 키워드 인덱스에 대해 효율적으로 conjunctive 검색을 수행할 수 있도록 시스템을 고안하였고, 키워드 인덱스의 결합을 통해서 subset과 범위 검색을 효율적으로 처리하였다.

III. 검색 가능 이미지 암호 시스템의 설계

본 장에서는 스트리밍 미디어의 검색 가능 이미지 암호 시스템을 설계한다. 먼저, 스트리밍 미디어에 대한 1차 색인 및 패턴 정보 추출 절차를 기술하며, 또한 1차 키와 2차 키에 의한 스트리밍 미디어의 암호 및 복호화 과정에 대해서 기술한다.

3.1 검색 가능 이미지 암호 시스템

검색 가능 암호 시스템은 암호화된 자료를 복호화하지 않고도 원하는 자료를 검색할 수 있는 암호 기반 기술이라면 검색 대상을 텍스트에서 이미지로 확장하여 검색 가능 이미지 암호 시스템(SIES)을 설계한다. 검색 가능 암호 시스템은 개인의 정보가 외부 저장 공간에 저장되면서 발생하는 프라이버시 등의 여러 문제점에 대한 해결 방법으로 지금까지 많은 연구가 진행되었으나, 본 연구에서는 이미지로 확장하여 StraaS에서 검색 가능 이미지 암호 서비스를 제공한다.

SES에서 정보를 포함하는 문서와 키워드를 이용해

서 숨기고 싶은 정보를 암호화하고, 사용자가 자신이 원하는 암호화된 문서를 검색하기 위해 서버에 제공하는 정보를 키워드를 이용하여 검색한다. 제안하는 SIES에서는 문서를 스트리밍 미디어로, 문서에 포함된 키워드는 스트리밍 미디어의 여러 이미지들로 확장한다. 즉, SES의 (1)을 (2)로 확장하여 정의한다.

$$Streaming\ Media = \{ IMG_1, IMG_2, \cdots, IMG_n \} \quad (2)$$

SIES는 SES와 동일하게 키 생성(key generation), 색인 및 암호화(build index), 트랩도어 생성(trapdoor generation), 검색(search)의 4가지 단계로 이루어지며, 키 생성 단계에서 약간의 전처리(Pre-processing)가 추가된다. 키 생성 단계에서 사용자가 앞으로 사용할 검색 가능 이미지 암호 시스템을 준비하는 단계이며, 이 부분이 KS-MMA[14]가 키 생성 단계를 대처하게 되며, 그림 5에 나타낸다.

그림 5. 검색 가능 이미지 암호 시스템의 기본 구성
Fig. 5 Basic structure of searchable image encryption system

키 생성 단계에서 각 사용자는 자신의 키를 생성하여 저장하고 암호 시스템의 공개 정보는 서버나 다른 사용자들에게 공개한다. 여기에서는 KS-MMA가 키 생성 단계 기능을 수행한다. 암호화 단계에서 사용자의 스트리밍 미디어를 암호화하고, 스트리밍 미디어에 포함된 이미지 키워드를 포함한 인덱스(index)를 생성한다. 암호화된 스트리밍 미디어와 이미지 키워드의 인덱스는 모두 클라우드의 스토리지에 저장되며, 암호화 단계에서사용자의 키는 KS-MMA가 제공한다. 트랩 도어 생성 단계는 사용자의 권한에 의해서 주어진 이미지 키워드에 해당하는 트랩 도어를 생성한다. 트랩 도어는 오직 사용자의 키로 부터 생성이 가능하다. 마지막, 검색 단계는 주어진 트랩 도어에 대응하는 스트리밍 미디어를 찾는 단계로 클라우드의 스토리지에서 검색된다. 검색의 결과로 서버는 주어진 트랩 도어와 일치하는 암호화된 스트리밍 미디어 또는 암호화된 스트리밍 미디어들의 식별자(Identifier)을 사용자에게 전달한다.

3.2 1차 색인 & 패턴 정보

StraaS의 SIES는 실시간으로 생성된 스트리밍 미디어를 분석하여 다양한 색인 및 정보를 생성한다. 이 데이터 처리과정에서는 1차 색인과 패턴 정보들을 생성하게 된다. 1차 색인은 스트리밍 미디어를 클라우드 컴퓨팅의 컴퓨팅 자원을 이용하여 Image Processing의 CBIR을 수행하여 생성하게 되며, 색인 외에 생성된 추가정보를 이용하여 패턴 정보를 구성하게 된다. 이와 같은 절차를 그림 6에 간략하게 나타낸다.

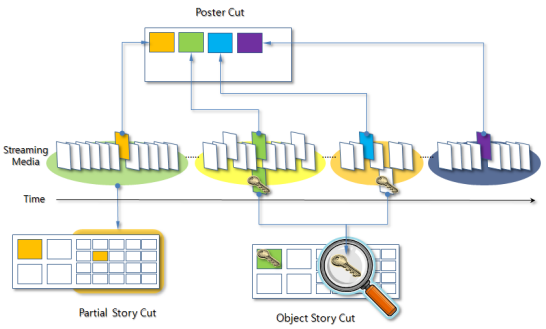

그림 6. SIES의 1차 색인 과정
Fig. 6 1st Index processing of SIES

1차 색인 정보로는 크게 Poster Cut과 Partial Story Cut으로 구성된다. Partial Story Cut은 Image Processing에 의해서 스트리밍 미디어를 임의의 크기의 스트리밍 미디어로 영역 설정 및 분할하며, 분할된 스트리밍의 평균에 해당하는 대표 이미지를 선택하는 과정이다. 그리고 Poster Cut은 Partial Story Cut의 대표 또는 평균 이미지를 Tiled Display 형태로 스트리밍 미디어를 요약된 정보를 추출하고, 색인을 생성한다. 특히 Poster Cut은 검색 가능한 암호화 시스템의 검색을 위한 이미지 키워드로 사용된다.

3.3 1차 키와 2차 키에 의한 암호화 과정

스트리밍 미디어와 이미지 키워드에 대한 1차 키와 2차 키에 의한 암호화 과정을 설명한다. 그림 7의 (a)는 스트리밍 미디어를 나타내며, 그림 7의 (b)는 이미

지 프로세싱에 의해서 선택된 이미지 키워드를 나타낸다.

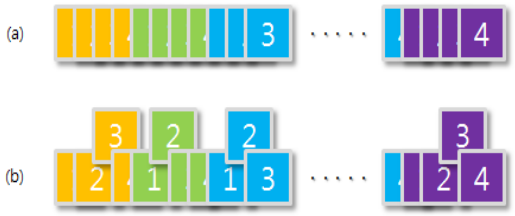

그림 7. 스트리밍 미디어와 스트리밍 미디어에서 선택된 이미지 키워드
Fig. 7 Streaming media and selected image keyword in streaming media

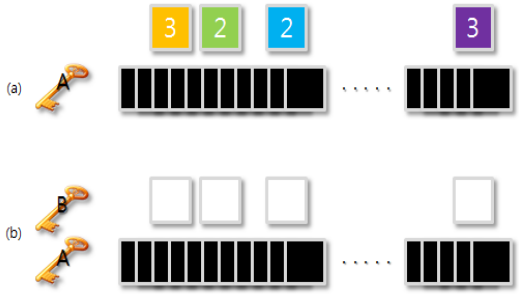

그림 8. 1차 키에 의한 스트리밍 미디어의 암호화와 2차 키에 의한 이미지 키워드의 암호화
Fig. 8 Streaming media encryption by 1st key and emcryption of image keyword by 2nd key

인증된 사용자는 KS-MMA에서는 1차 키 집합과 2차 키를 할당받고, 암호화를 수행하게 된다. 1차 키 집합 A는 암호화 키들의 집합으로 스트리밍 미디어의 Partial Story Cut을 암호화하고, 2차 키 B는 이미지 키워드를 포함하는 Poster Cut을 암호화하며, 그림 8의 (a)와 (b)가 이러한 상황을 나타낸다. 모든 스트리밍 미디어와 이미지 키워드는 암호화되어 유지 및 관리된다.

3.4 2차 키와 1차 키에 의한 복호화 과정

스트리밍 미디어와 이미지 키워드에 대한 2차 키와 1차 키에 의한 복호화 과정을 설명한다. 인증된 사용자는 KS-MMA에서 할당받은 2차 키를 이용하여 이미지 키워드를 복호화를 수행하게 되며, 그림 9의 (a)와 같이 나타낸다. 인증된 사용자가 선택한 이미지 키워드에 해당하는 Poster Cut 영역의 이미지 키워드에 해당하는 Partial Story Cut을 1차 키 집합을 이용하여 복호화를 수행하게 되며, 그림 9의 (b)가 이러한 상황을 보여주고 있다.

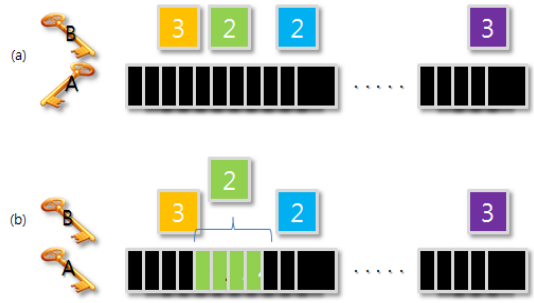

그림 9. 2차 키에 의한 이미지 키워드의 복호화와 1차 키에 의한 스트리밍 미디어의 복호화
Fig. 9 Decryption of image keyword by 2nd key and decryption of streaming media by 1st key

Ⅳ. 프로토타입의 가능성 시뮬레이션

SIES의 프로토타입을 Matlab으로 코딩하여 스트리밍 미디어의 이미지 키워드 생성과 포스터 컷 생성을 위한 스트리밍 미디어의 분할에 의한 가능성을 시뮬레이션 한다.

4.1 이미지 키워드 생성

스트리밍 미디어를 분석하여 스트리밍 미디어를 ㄷ구성하는 이미지들의 중앙값에 해당하는 대표 이미지를 선택하며, 선택된 이미지를 이미지 키워드로 사용한다[15]. 그림 10은 Matlab을 이용하여 임시적으로 샘플 스트리밍 미디어를 생성한 것이며, 그림 11은 샘플 스트리밍 미디어의 RGB에 의한 변이 추이를 나타낸 것이다. 그림 12는 샘플 스트리밍 미디어의 평균값에 의한 선택된 이미지 키워드를 나타낸 것이며, 그림 7의 (b)에 나타낸 이미지 키워드의 실체를 보여준다.

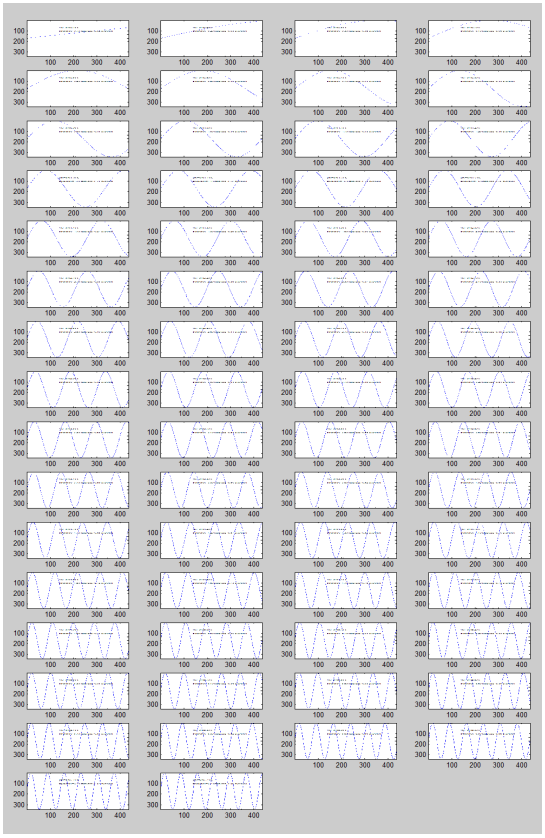

그림 10. 샘플 스트리밍 미디어
Fig. 10 Sample streaming media

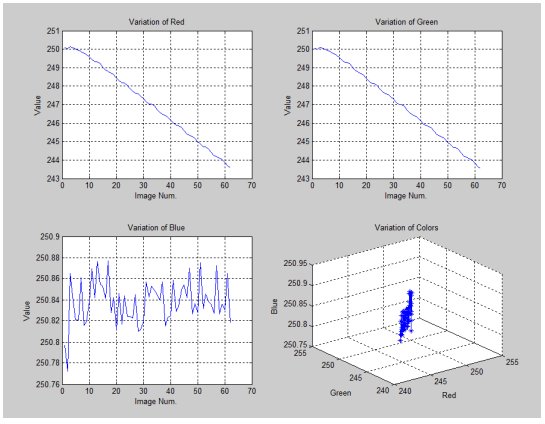

그림 11. 샘플 스트리밍 미디어의 변이 추이
Fig. 11 Variation transition of sample streaming media

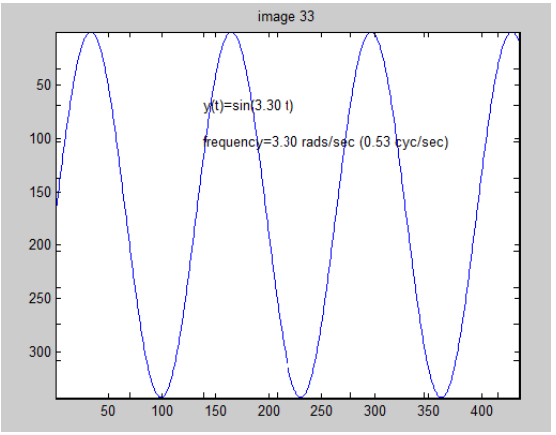

그림 12. 샘플 스트리밍 미디어에서 추출된 이미지 키워드
Fig. 12 Extracted image keyword from sample streaming media

4.2 Partial Story Cut 생성을 위한 스트리밍 미디어의 분할

대용량의 스트리밍 미디어를 검색하기 위한 색인을 위해서는 이미지 키워드와 스트리밍 미디어를 시간 영역으로 partial story cut을 생성하기 위해서는 스트리밍 미디어의 분할이 필요하다.

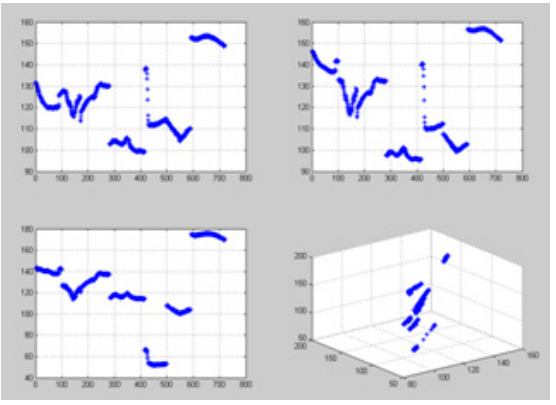

그림 13. partial story cut을 위한 RGB 분석
Fig. 13 RGB analysis for partial story cut

그림 13은 720 프레임의 스트리밍 미디어를 RGB 영역에서 분석하였으며, 결과적으로 3차원 공간에서 7개의 partial story cut 영역을 추출하였다. 그림 14는 7개

영역들의 시작 이미지와 끝 이미지를 나타낸 것이다.

그림 14. 스트리밍 이미지의 partial story cut 의 영역 분할
Fig. 14 Area division of partial story cut of streaming images

V. 결 론

본 논문은 클라우드 컴퓨팅 기반의 스트리밍 서비스에 대한 StraaS 서비스를 정의하며, StraaS 서비스의 기능 중의 SIES에 대한 제안 및 설계에 대한 연구이다. SIES는 스트리밍 미디어의 암호 및 복호화에 의해서 인증 및 프라이버시를 제공할 수 있으며, 스트리밍 미디어의 색인을 위한 이미지 키워드를 생성하고, 이미지 키워드는 스트리밍 미디어의 임의의 영역의 일부분을 참조한다. 인증에 의해서 이미지 키워드에 접근이 가능하게 되며, 이미지 키워드를 선택에 의해서 해당되는 스트리밍 미디어의 일부분 영역에 접근하게 되므로 부분적으로 프라이버시를 제공하게 된다. 제안된 SIES의 프로토타입 모듈에 의한 스트리밍 미디어의 Partial Story Cut을 위한 영역 분할과 이미지 키워드 생성을 시뮬레이션하여 가능성을 검증하였다.

참고 문헌

[1] P. Golle, J. Staddon, and B. Waters, “Secure Conjunctive Keyword Search over Encrypted Data,” In Applied Cryptography and Network Security Conference, pp. 24-31, 2004.

[2] B. Waters, D. Balfanz, G. Durfee, and D. Smetters, “Building an Encrypted and Searchable Auditlog,” NDSS, pp. 1-10, 2004.

[3] R. Ostrovsky and W. Skeith, “Private Searching on Streaming Data,” Crypto, pp. 397-430, 2005.

[4] J. Bethencourt, H. Chan, A. Perrig, E. Shi, and D. Song, “Anonymous Multi-Attribute Encryption with Range Query Conditional Decryption,” Technical Report, C.M.U. pp. 1-38, 2006.

[5] 조남수, 홍도원, “검색 가능 암호 시스템 기술 동향,” 전자통신동향분석, 23권, 4호, pp. 1-9, 8월, 2008년.

[6] R. Ostrovsky, “Software Protection and Simulations on Oblivious RAMs,” ACM Symp. on Theory of Computing, Baltimore, MAryland, USA, May 14-16, pp. 514-523, 1990.

[7] P. Golle and R. Ostrovsky, “Software Protection and Simulation on Oblivious RAMs,” Journal of ACM, Vol. 43, No. 3, pp. 431-473, 1996.

[8] D. Song, D. Wagner, and A. Perrig, “Practical Techniques for Searching on Encrypted Data,” IEEE Symp. on Security and Privacy, 2000.

[9] E. J. Goh, “Secure Indexes,” Technical Report 2003/216, IACR ePrint Crpytography Archive, 2003.

[10] Y. C. Chang and M. Mitzenmacher, “Privacy Preserving Keyword Searches on Remote Encrypted Data,” In Applied Cryptography and Network Security Conf., pp. 391-421, 2005.

[11] R. Curtmola, J. Garay, S. Kamara, and R. Ost-

rovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," ACMCCS, pp. 79-88, 2006.
[12] D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," Eurocrypt, LNCS 3027, pp. 506-522, 2004.
[13] D. Boneh and B. Waters, "Conjunctive, Subset and Range Queries on Encrypted Data," Theory of Cryptography Conf., pp. 1-29 , 2007.
[14] 차병래, 한경헌, 이지민, 안영은, 류재민, "다자간 정합 인증 시스템의 설계", 2009 한국정보기술학회 하계 학술대회, pp. 458-462, 6월, 12일, 2009.
[15] 차병래, 김대규, 김남호, 최세일, "검색 가능 이미지 암호 시스템의 개념 설계", 한국전자통신학회 춘계학술대회, pp. 217-220, 6월, 8일, 2012.

저자 소개

차병래(Byung-Rae Cha)

2004년 2월 국립 목포대학교 컴퓨터 공학과(공학박사)
2005년 3월~2009년 2월: 호남대학교 컴퓨터공학과 전임강사
2009년 9월-현재 광주과학기술원 정보통신공학부 연구조교수
※ 관심분야 : 정보보안, Intrusion Detection System, 신경망, OTP, 클라우드 컴퓨팅, Future Internet 등

김대규(Dae-Kyu Kim)

1998년~2001년 밀레니엄 버그 전산 전문가
1999년~2001년 해양수산연구정보센터 개발실장
2008년~현재 ㈜아젠텍, 수석연구원
2009년~현재 M-RFID 표준화 및 관련 기술 개발
2010년~현재 감성ICT산업협회, 정회원
현재 (주)아젠텍 S/W 개발실 실장
※ 관심분야 : 모바일-RFID/NFC 기술 개발, 클라우드 컴퓨팅, 감성기술개발

김남호(Nam-Ho Kim)

1997년 8월 포항공과대학교 정보통신학과(공학석사)
2000년 8월 전남대학교 전산통계학과 (박사수료)
1991년 4월~1998년 2월 포스데이타(주)
1998년 3월~현재 호남대학교 인터넷콘텐츠학과 부교수
※ 관심분야 : 데이타마이닝, 유비쿼터스 컴퓨팅, 가상현실 응용, 생체인증 등

최세일(Se-Ill Choi)

1984년 한양대학교 전자공학과 졸업(공학사)
1989년 플로리다공과대학교 대학원 전산학과 졸업(공학석사)
2002년 모나쉬대학교 대학원 전산학과 졸업(공학박사)
1984년~1992년 LG전자, 삼성전자 선임연구원
1993년~현재 호남대학교 컴퓨터공학과 교수
※ 관심분야 : 소프트웨어공학, 전자상거래

김종원(Jong-Won Kim)

1987년 서울대학교 제어계측공학과 학사
1989년 서울대학교 제어계측공학과 석사
1994년 서울대학교 제어계측공학과 박사
1994년 3월~1999년 7월: 공주대학교 전자공학과 조교수
1998년 12월~2001년 7월 미국 Univ. of Southern California, Los Angeles, CA, EE-System Department 연구조교수
2000년 7월~2001년 6월 미국 InterVideo Inc., Fremont, CA, 개발 자문
2001년~현재 광주과학기술원 정보통신공학과 교수
※ 관심분야 : Networked Media Systems and Protocols focusing "Dynamic Composition of Immersive Media-oriented Services over the Wire/Wireless IP Convergence Networks".