情報保護學會論文誌
第15券 第2號, 2005. 4

웹 상에서 스테가노그라피 기법을 이용한 안전한 데이터베이스 보안 구현*

문 봉 근,†‡ 유 두 규, 고 명 선, 엄 기 원, 전 문 석
숭실대학교

An Implementation of Database Security Using Steganography in the Web

Bong-Keun Moon,†‡ Du-Gyu Ryoo, Myung-sun Ko, Ki-Won Eom, Moon-Seog Jun
Soongsil University

요 약

인터넷의 활용이 증가하면서 우리는 많은 양의 정보를 서로 공유하고 있으며, 다양한 형태의 데이터를 저장하는 데이터베이스의 사용이 증가하고 있다. 인터넷에서 다수의 사용자가 자료를 공유함에 있어서 인가되지 않은 사용자로부터 정보의 수정, 삭제, 조회로부터 보호하기 위하여 정보 보호 시스템이 절실히 요구되고 있다.

과거 데이터에 관한 보안은 대부분 여러 단계를 거치는 접근제어에 의존하는 소극적인 보안대책으로서, 비밀데이터의 내용을 원형 그대로 저장하고 있으므로 여러 가지 불법적인 공격에 대한 취약점을 갖고 있다.

본 논문에서는 웹 데이터베이스에서 특별히 보호가 요구되는 비밀 데이터 아이템의 내용을 불법적인 공격으로부터 보호하기 위해 스테가노그라피 기법을 이용한 데이터베이스를 구현하여 웹 상에서 불법 사용자가 데이터베이스의 내용을 획득하더라도 내용을 알 수 없어 완벽하게 데이터 아이템을 보호할 수 있다.

ABSTRACT

As the usage of Internet grows, we share many informations among the others and use more database systems for a various type of data. However, secure database system, which prevents the unauthorized users from modification, deletion, and access, is urgently required for sharing data in Internet.

Conventional technologies of a data security are passive methods which depend on several steps with an access control, and these methods are vulnerable against the illegal attack because attacker can see the plain text that is private message.

To prevent private data item for the special security from the malicious attack in web database, this paper is devoted to implement database system using steganography method, so we can protect the data item completely because attacker cannot know the secure message although he get the content of database.

Keywords : *Web, Steganography, Database*

접수일 : 2004년 8월 16일 ; 채택일 : 2005년 3월 15일
* 본 연구는 숭실대학교 교내연구비 지원으로 이루어짐.
† 주저자, ‡ 교신저자 : mbk2000@chol.com

Ⅰ. 서 론

인터넷의 활용이 증가하면서 우리는 많은 양의 정보를 서로 공유하고 있고, 다양한 형태의 데이터를 저장하는 데이터베이스의 사용이 증가되고 있다. 데이터베이스는 데이터의 불필요한 중복을 피하고 응용 프로그램에 사용하기 위하여 상호 관련된 데이터를 적절한 형태로 모은 것을 말한다.[1] 따라서 데이터베이스에서 데이터와 프로그램 상호간에 독립성을 유지해야 하고 데이터를 수정하거나 검색할 때는 공통적이고 합리적인 중앙 통제가 실시되어야 한다. 직접적으로 컴퓨터를 사용하는 사람이 늘어남에 따라 컴퓨터를 이용한 데이터베이스 정보의 합법적인 또는 불법적인 획득으로 개인의 사생활로부터 회사비밀, 국가비밀에 이르기까지 보안을 유지해야 할 중요한 자료가 노출될 수 있는 위험한 요소가 많이 존재하고 있다.

최근 데이터베이스 시스템이 점차적으로 조직 사회의 기능을 수행하기 위한 중심요소가 됨에 따라 다양한 집단의 사용자들에 의해 공유되고 사용되어 지기 위하여 컴퓨터 시스템에 저장된다. 여러 사용자가 자료를 공유함에 따라 데이터베이스에 저장된 정보를 인가 받지 않은 사용자로부터 정보의 사용, 악의적인 정보의 변경 및 자료의 노출을 방지하기 위하여 데이터베이스 보안 시스템이 절실히 요구되고 있다.[1]

데이터베이스 보안을 제어하는 방식에는 외적 보안(external security), 인터페이스 보안(interface security) 및 내적 보안(internal security) 등이 있다.[2] 외적 보안은 컴퓨터 시설 및 장치 등의 물리적 접근에 대한 통제를 말하며, 인터페이스 보안은 물리적 접근이 허용된 사용자에 대해 패스워드(password)와 같은 기법 등으로 인증(authentication)하는 것을 말한다. 내적 보안은 컴퓨터 시스템내의 여러 자원에 대한 사용자의 접근을 제어하고, 저장되어 있는 자료의 불법적인 노출을 방지하기 위하여 다음과 같은 4가지 측면이 고려되어야 한다.

- 첫째, 데이터 객체(object)에 대한 접근을 제어하는 접근 제어
- 둘째, 객체에서 다른 객체로의 정보 유출을 제어하는 정보 흐름 제어
- 셋째, 통계 정보와 같은 객체로부터의 은밀한 데이터(confidential data)의 추론을 제어하는 추론 제어
- 넷째, 접근 제어, 정보 흐름 제어, 추론 제어로도 방지할 수 없는 돌발적인 또는 악의적인 정보의 유출에 대비한 민감한 데이터(sensitive data)의 암호화를 위한 암호 제어

이와 같은 4가지 제어 기법은 서로 상이한 측면을 제어하므로 어느 하나도 다른 기능을 대신할 수 없는 상호 보완적인 기능을 지니고 있다. 4가지 측면을 모두 고려하다면 비용과 실용성에 많은 문제점이 있어 완벽한 보안 장치를 설계한다는 것은 현실적으로 거의 불가능하다. 데이터베이스 보안이라 하면, 데이터베이스 내에 저장된 데이터에 대한 누설, 변경 및 파괴로부터 데이터 또는 데이터베이스를 보호하는 것을 말한다.[2]

현재 가장 널리 사용되고 있는 데이터베이스 보안 시스템은 대부분 여러 단계를 거치는 접근 제어에 의존하고 있는 소극적인 보안 대책으로 여러 형태의 공격을 받을 수 있는 단점을 가지고 있다.[3]

본 논문에서는 데이터베이스에서 특별히 보호가 요구되는 데이터 아이템을 스테가노그라피 기법을 적용하여 연구한다. 제안된 스테가노그라피 기법은 데이터 아이템 단위의 내용을 스테가노그라피 기법을 적용하여 스테가노그라피화 함으로써 권한을 부여받은 자만이 키에 의하여 데이터 아이템의 내용을 볼 수 있도록 하며, 여러 형태의 공격으로부터 보호받을 수 있도록 한다. 제안된 스테가노그라피 기법은 윈도우 XP 운영체제에서 MySQL DBMS를 Java 및 JSP 언어로 구현하는 것을 기본으로 한다.

본 논문의 구성은 1장 서론에 이어 2장에서는 스테가노그라피를 기술하였으며, 3장에서는 제안 시스템의 구현을 위한 스테가노그라피 적용 단계와 알고리즘을 기술하였고, 4장에서는 구현과 결과 분석을 기술하였으며, 5장은 결론으로 본 연구의 끝을 맺으며 앞으로의 연구 방향 및 개선점을 제시하였다.

Ⅱ. 스테가노그라피

스테가노그라피는 메시지의 존재를 숨기면서 통신하는 기술로서, 어떤 송신자와 수신자 사이에 통신이 일어나고 있다는 사실을 숨기는 것을 의미한다. 스테가노그라피는 비밀 메시지의 존재를 숨기는 다양한 통신 방법을 제공하는데, 여기에는 보이지 않는 잉크, 점 크기의 작은 사진, 문자 정렬, 디지털 서명, 은밀한 채널, 분산 스펙트럼 통신 등이 있다.[4] 스테

가노그라피의 목적은 제 3자가 평범한 메시지 안에 비밀 메시지가 존재한다는 사실을 알지 못하도록 숨기는 것이다.

2.1 스테가노그라피 은닉 방법

스테가노그라피의 데이터 은닉 방법은 삽입 방법에 따라 두 가지로 분류할 수 있다.[4,5]

첫째, 공간 영역(spatial domain)에 데이터를 은닉하는 방법이다. 이 방법은 커버 객체에 영향을 미치지 않는 일정한 영역에 비밀 데이터를 삽입하는 방법이다.[6]

둘째, 주파수 영역(frequency domain)에 데이터를 은닉하는 방법이다. DFT, DCT 또는 DWT 같은 알고리즘을 이용하여 커버 객체를 주파수 변환한 후, 비밀 데이터를 삽입하는 방법이다. 장단점을 비교하면 다음 표 1과 같다.[7,8]

본 논문에서 제안하는 웹 상에서 스테가노그라피 기법을 이용한 안전한 데이터베이스 보안 구현은 공간 영역에 데이터를 은닉하는 방법이다.

〔표 1〕 스테가노그라피 은닉방법 장단점

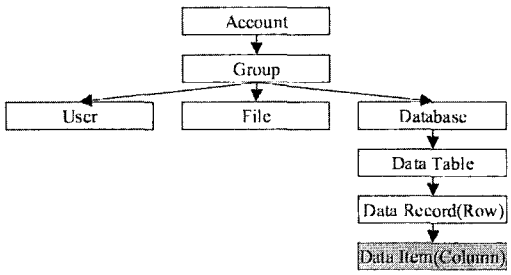
구분	공간영역 데이터 은닉방법	주파수영역 데이터 은닉방법
장점	-. 변환 식을 사용하지 않음 -. 연산 속도가 빠름	-. 영상 처리가 쉬움 -. 외부 공격에 강함
단점	-. 영상 처리가 어려움 -. 잡음 등의 외부 공격에 약함	-. 변환 식을 사용함 -. 연산 속도가 많이 소요됨
응용 분야	-. 데이터 양이 큰 동영상	-. 작은 크기의 단일 영상이나 음성

2.2 암호화와 스테가노그라피의 차이점

암호화와 스테가노그라피의 차이점은 암호화는 비밀 데이터의 내용을 숨겨 해커의 악의적인 공격을 유발하는데 반해 스테가노그라피는 비밀 데이터의 존재 유무를 숨겨 해커의 공격 자체를 유발시키지 않는데 있다. 또한 스테가노그라피에서 사용되어지는 비밀 데이터는 암호화를 사용해서 암호화된 상태로 저장될 수도 있다. 그러므로 암호화와 스테가노그라피는 독립적으로 사용되기 보다는 상호 보완적인 관계를 가진다고 할 수 있다.[9]

Ⅲ. 제안 스테가노그라피 적용 단계와 알고리즘

3.1 제안 스테가노그라피 적용 단계



(1) Account Password
(2) Group Password
(3) User Password
(4) File Lockword
(5) Terminal ID Check
(6) Database Password
(7) Data Table Read/Write
(8) Data Record(Row) Read/Write
(9) Database Lock
(10) Data Table Lock
(11) Data Record Lock
(12) Data Item Lock

〔그림 1〕 데이터베이스에서 스테가노그라피 적용 단계

컴퓨터 시스템의 데이터베이스에서 스테가노그라피 적용 단계는 그림 1과 같다.

현재의 시스템에서는 데이터베이스의 보안을 위하여 패스워드만을 사용하고 있으나, 패스워드가 노출되면 데이터베이스의 보안을 유지할 수 없기 때문에 본 논문에서는 데이터베이스에서 특별히 보호가 요구되는 데이터 아이템에 스테가노그라피를 적용한다.

그러나 데이터베이스 시스템의 스테가노그라피화는 데이터 테이블과 데이터 레코드, 데이터 아이템 단위에서 수행할 수 있으며, 각각의 단위에서 스테가노그라피화 과정 및 장단점은 다음과 같다.

3.1.1 데이터 테이블 스테가노그라피화

데이터 테이블은 데이터 레코드의 집합으로서 데이터 테이블을 스테가노그라피화하는 경우에는 데이터 레코드의 내용을 수정할 때 스테가노그라피화된 데이터 테이블을 원래대로 하고 그 중에서 데이터 레코드를 조회하여 수정 보완한 후 다시 데이터 테이블의 스테가노그라피화가 수행되어야 한다.

이 때 한 사용자가 데이터 테이블에 대한 스테가노그라피화를 수행할 때는 다른 사용자는 수행중인 데이터 테이블에 대하여 어떠한 작업도 수행할 수 없는 단점이 있다.

3.1.2 데이터 레코드 스테가노그라피화

데이터 레코드에 스테가노그라피화를 수행할 때는

현재 데이터베이스에서 데이터 레코드 단위로 입력, 삭제, 수정, 검색을 행하고 있으므로 데이터 아이템에 비하여 시간이 많이 소요된다. 데이터 레코드를 수정하고자 하면 먼저 데이터 레코드에 속한 각각의 데이터 아이템에 대하여 스테가노그라피화를 수행한 후 데이터 레코드로 합성하여 조회 후, 수정하고 다시 데이터 아이템별로 스테가노그라피화를 수행한다. 그러므로 한 데이터 레코드를 수정하기 위해서는 여러 개의 데이터 아이템을 스테가노그라피화를 수행하므로 많은 시간이 필요하다는 단점이 있다.

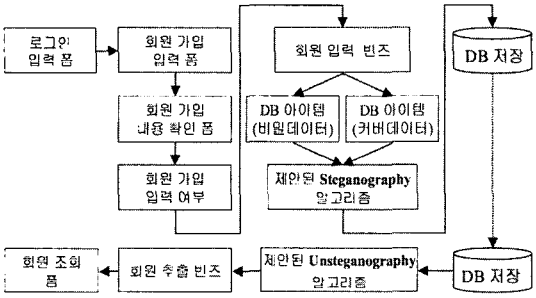
3.1.3 데이터 아이템 스테가노그라피화

데이터 아이템에 스테가노그라피화를 수행할 때는 주민번호와 같이 중요하다고 생각하는 아이템만 스테가노그라피화를 수행한 후, 데이터베이스에 저장하므로 시간이 절약되고, 데이터 테이블이나 데이터 레코드에 비하여 여러 사용자가 동시에 사용하기가 편리하다.

3.2 제안 스테가노그라피 알고리즘

3.2.1 설계 과정

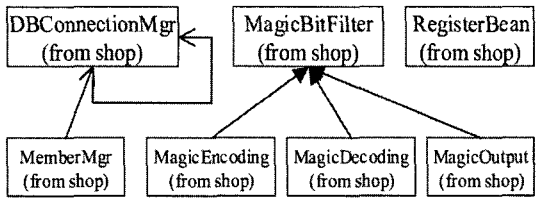
제안한 웹 상에서 스테가노그라피 기법을 이용한 안전한 데이터베이스 보안 구현은 다음과 같은 방법으로 설계되고, 실행 흐름도는 그림 2와 같다.



〔그림 2〕 제안한 알고리즘의 전체 실행 흐름도

1st. 웹 상에서 아이디와 비밀번호를 입력하여 로그인 한다.
2nd. 로그인 한 회원에 한 해서 회원 가입 여부를 체크한다.
3rd. 회원 입력시 회원 입력 빈즈가 작동한다.
4th. DB 아이템 중에서 커버 데이터로 사용할 아이템을 선택한다.
5th. DB 아이템 중에서 비밀 데이터로 사용할 아이템을 선택한다.
6th. 커버 아이템 안에 비밀 아이템을 스테가노그라피화 한다.
7th. 스테가노그라피화된 아이템을 DB에 저장한다.
8th. DB에서 비밀 데이터 추출 시 역순으로 진행한다.

여기에서 사용한 커버 데이터는 해당 레코드 중에서 한 아이템을 선택한 것이다. 외부의 파일을 선택한 것이 아니므로 파일 관리를 별도로 할 필요가 없어 관리가 용이하다. JSP 언어는 Rational Rose 지원이 안되므로 그림 3은 자바 언어로 구현된 부분만을 Rational Rose로 그린 Class Diagram이다.



〔그림 3〕 Rational Rose로 그린 Class Diagram

자바 언어로 구현한 부분에서 스테가노그라피 데이터를 생성 및 추출하여 데이터베이스에 저장하고 추출하는 부분만을 표현하면 생성 프로그램 부분은 그림 4에서, 추출 프로그램 부분은 그림 5에서 보여준다.

```
//Pseudo code
memberInsert () {
 Connect DB;
 Create cover data (address);
 Create secret data (phone);
 Create stego data (stego_address);

 Start stego work (stego_address, address,
          phone);
 Encrypt (stego_address, password);
 Finish stego work (stego_address);

 Set (db_item, stego_address);
 Insert DB (db_item);
 Disconnect DB;
 }
```

〔그림 4〕 생성 프로그램 부분

```
//Pseudo code
getmemberList () {
 Connect DB;
 Select (db_item);
 Get (stego_address, db_item);

 Create stego data (stego_address);
 Create secret data (phone);

 Start unstego work (phone,
           stego_address);
 Decrypt (stego_address, password);
 Finish unstego work (phone);

 Set (display_item, phone);
 Display (display_item);
 Disconnect DB;
 }
```

〔그림 5〕 추출 프로그램 부분

3.2.2 생성 및 추출 알고리즘

생성 및 추출 알고리즘은 텍스트 기반의 스테가노그라피이다. 텍스트 기반의 스테가노그라피는 스페이스, 탭, 뉴라인 문자를 이용한다. 비밀 메시지를 스페이스로 변환한 후, 변환된 스페이스를 라인의 끝에 추가하는 방식으로 비밀 메시지를 숨긴다. 제안한 알고리즘에서는 뉴라인 문자를 사용하지 않고 스페이스와 탭만을 사용하여 데이터 삽입량을 줄였다.

생성 알고리즘은 다음과 같다.

1st. 커버 아이템을 읽어 스테고 아이템에 쓴다.

2nd. 비밀 아이템의 내용을 ASCII 코드의 10진수로 읽어 2진수 v로 변환한다.

3rd. 변환된 v의 자릿수를 확인하여, 비트가 있으면 1, 없으면 0을 나타낸다.

4th. 변환된 v를 시프트 연산자를 이용하여 아래와 같이 연산한다.

v = v 〈〈 1, v = 0~7

5th. 3rd와 4th를 OR 연산을 한다.

6th. 첫 번째 OR 연산한 값 v를 두 번째 값으로 사용하고, 두 번째 OR 연산한 값 v를 세 번째 값으로 사용한다.

7th. 세 번째 OR 연산한 값 v를 아래와 같이 스페이스의 수 spc로 변환한다.

spc = ((v & 1) 〈〈 2) | (v & 2) | ((v & 4) 〉〉 2)

8th. 비밀 아이템을 추가한다는 내용을 알리기 위해 탭을 추가한다.

9th. 스페이스의 수 spc 만큼 스페이스를 스테고 아이템에 추가한다.

10th. 스페이스의 블록(스페이스의 수)을 구분하기 위해 탭을 하나씩 추가한다.

추출 알고리즘은 다음과 같다

1st. 스테고 아이템에서 커버 아이템을 추출한다.

2nd. 이어서 스페이스의 수를 탭이 나타날 때까지 읽어 가산된 스페이스 v로 변환한다.

3rd. 변환된 v의 자릿수를 확인하여, 비트가 있으면 1, 없으면 0을 나타낸다.

4th. 변환된 v를 시프트 연산자를 이용하여 아래와 같이 연산한다.

v = v 〈〈 1, v = 0~127

5th. 3rd와 4th를 OR 연산을 한다.

6th. 첫 번째 OR 연산한 값 v를 두 번째 값으로 사용하고, 두 번째 OR 연산한 값 v를 세 번째 값으로 사용하는 방식으로 여덟 번 반복한다.

7th. 여덟 번 반복한 값 v가 ASCII 코드 값이다.

8th. ASCII 코드 값을 텍스트로 출력하면 비밀 아이템의 내용이 나타난다.

3.2.3 비밀 아이템의 내용과 삽입량

데이터베이스 안에서 감추고자 하는 비밀 아이템의 내용을 표 2에서는 한글로 된 커버 아이템에 숫자로 된 비밀 아이템을 사용하여 스테가노그라피 작업을 하였지만, 한글 커버 아이템에 한글 비밀 아이템을 스테가노그라피 작업을 하고, 숫자 커버 아이템에 숫자 비밀 아이템을 스테가노그라피 작업을 하면 비밀 아이템의 존재를 파악하기가 훨씬 어려울 것이다.

〔표 2〕 비밀 아이템의 내용과 삽입량

cover item			secret item			stego item		
item name	content	byte	item name	content	byte	item name	content	byte
address	경기 용인시 수지읍	19	아이템 없음	016-364-3333 (휴대전화번호)	12	address	경기 용인시 수지읍	149
address	경기 용인시 수지읍	19	아이템 없음	2167917 (주민번호뒷자리)	7	address	경기 용인시 수지읍	95

제안한 시스템에서는 비밀 아이템이 화면상에만 존재하기 때문에 데이터베이스를 생성 시 비밀 아이템을 만들지 않아 표 2에서 아이템 이름을 "아이템 없음" 으로 기술하였다.

3.2.4 제안 방식의 장단점

웹 상에서 스테가노그라피 기법을 이용하여 데이터베이스 보안을 구현하는 제안 방식의 장단점은 표 3과 같다.

〔표 3〕 제안방식의 장단점

장 점	단 점
-. 웹상에서 구현 -. 외부의 커버 데이터가 필요 없음 -. 여러 개의 아이템을 동시에 구현할 수 있음 -. 연산 속도가 빠름	-. 텍스트 형식에만 적용 -. 데이터베이스 용량의 증가

위의 단점을 고려해 볼 때, 첫 번째 단점으로 기술한 텍스트 형식에만 적용은 앞으로 기술 개발을 통하여 이미지나 오디오 파일로의 확대가 가능하다. 둘째로 기술한 데이터베이스 용량의 증가는 무어의 법칙에 근거하여 하드웨어의 용량이 증가함에 따라 크게 걱정할 문제는 아니라고 생각된다.

Ⅳ. 구현과 결과 분석

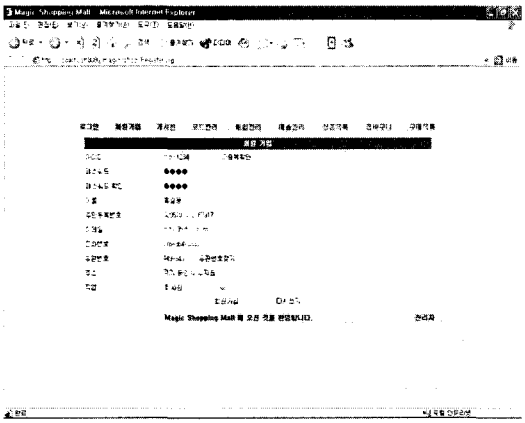
4.1 데이터 아이템의 스테가노그라피 구현

스테가노그라피를 적용할 수 있는 아이템들은 웹 상의 쇼핑몰 시스템에서 상품관리, 회원관리, 구매관리, 판매관리, 물류관리 등 다양하게 존재하는데 여기에서는 회원관리에 적용하였다. 회원관리 부분을 더 세분화하면 회원의 입력, 삭제, 수정, 조회가 있는데 제안한 스테가노그라피의 구현은 입력, 수정 및 조회 부분에 적용하였다.

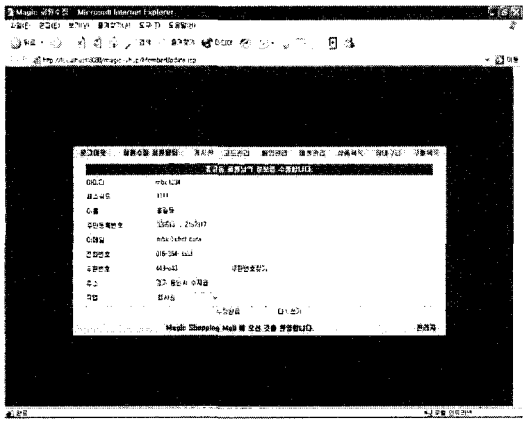
그림 6은 스테가노그라피 설계를 적용하여 구현한 입력 프로그램의 예이다. 여기에서는 스테가노그라피를 적용할 아이템으로 전화번호를 선택하였다. 해당 아이템을 입력한 후, 회원가입 버튼을 누르면 된다. 입력화면에는 전화번호 아이템이 존재하지만 데이터베이스 테이블에는 전화번호에 대한 아이템이 존재하지 않는다. 전화번호의 내용은 주소 아이템을 커버 아이템으로 이용하여 스테가노그라피를 적용하여 삽입되었기 때문이다. 그림 7은 스테가노그라피를 적용한 아이템을 수정하기 위한 화면이다. 전화번호 아이템에 보이는 전화번호는 스테가노그라피를 풀어서 보여주는 내용이다. 수정하고자 하는 전화번호를 입력 후 수정완료 버튼을 누르면, 전화번호는 입력과 같은 방법으로 스테가노그라피 작업을 거쳐 데이터베이스 안에 저장된다.

그림 8은 스테가노그라피를 적용하여 구현한 입력 아이템의 예이다. 이처럼 데이터베이스의 아이템을 보면 어디에 전화번호가 숨겨져 있는지를 알 수 없다. 왜냐하면 전화번호에 대한 아이템이 없기 때문이다.

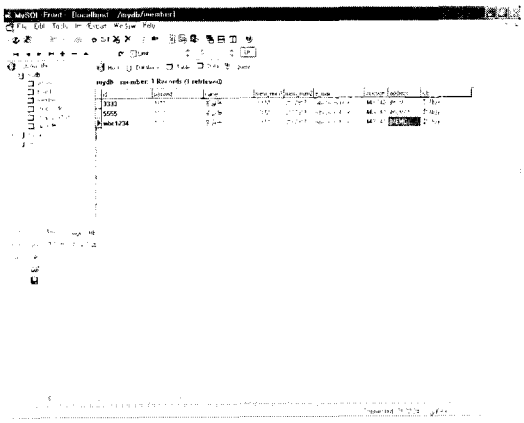
스테가노그라피를 확인하기 위하여 해당되는 스테고 아이템을 클릭하면 Text 탭에 스테가노그라피가 생성된 내용이 나타난다. 이 내용은 육안으로는 구분할 수 없다. 또한 그림 9처럼 HEX 탭을 클릭하면 스테가노그라피가 적용된 부분이 HEX 값으로 나타



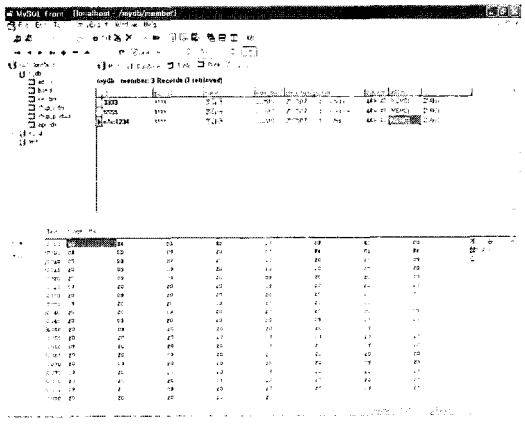
〔그림 6〕 스테가노그라피를 적용한 입력 프로그램



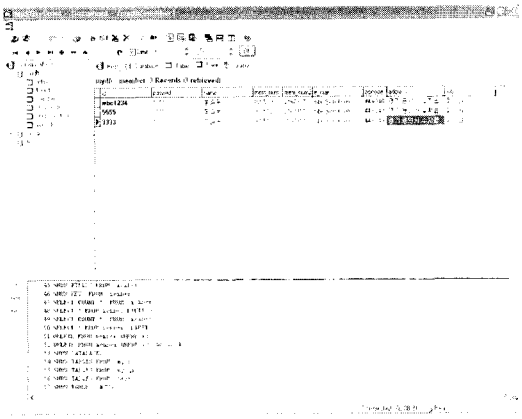
〔그림 7〕 스테가노그라피를 적용한 수정 프로그램



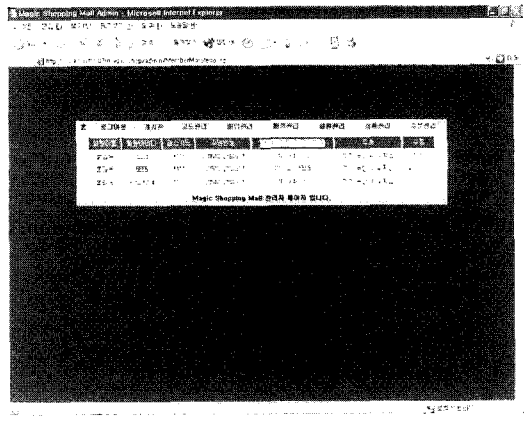
〔그림 8〕 데이터베이스 아이템의 Text 내용



〔그림 9〕 데이터베이스 아이템의 Hex 내용



〔그림 10〕 Type을 VARCHAR로 적용한 내용



〔그림 11〕 스테가노그라피를 적용한 조회 프로그램

나 스페이스와 탭을 육안으로 볼 수 있다. 스테고 아이템으로 사용된 주소 아이템에 저장된 용량은 비밀 메시지를 포함하여 149 바이트이다.

그림 8과 그림 9의 내용은 아이템의 Type을 TEXT로 했을 때 나타나는 화면이다. 스테가노그라피의 구현이 잘 되었는지 확인하기 위해 TEXT로 하였지만, 실제 현업에서 사용할 때는 그림 10과 같이 아이템의 Type을 VARCHAR로 한다. 그러면 MEMO라고 나오지도 않고 실제 데이터만 보이므로 주소 아이템에 비밀 내용이 들어가 있는 지를 확인할 수 없다.

그림 11은 스테가노그라피를 적용한 후, 조회 화면이다. 입력 시 회원의 전화번호 아이템을 스테가노그라피화 하여 데이터베이스의 주소 아이템에 저장하였다가 관리자가 조회할 때는 데이터베이스의 스테고 아이템인 주소 아이템에서 비밀 메시지인 전화번호만을 추출해 조회할 수 있어 사용자가 입력한 내용의 올바름을 확인할 수 있다.

4.2 결과 분석

제안 시스템은 일반적으로 사용하고 있는 DBMS를 사용하면서 스테가노그라피 기법을 결합시킨 것으로 제안 시스템의 접근을 위해서는 먼저 로그인 아이디와 패스워드를 알아야 한다. 사용자 인증 절차에서 아이디와 패스워드를 입력하면 서버 컴퓨터 인증파일에 등록되어 있는 아이디와 패스워드를 확인 후 인증여부를 통보한다. 또한 데이터 아이템의 내용이 스테가노그라피화되어 저장되어 있으므로 허가받지 않은 자가 접근하였을 때 전혀 알아볼 수 없는 평범한 문자로 되어 있으므로 귀중한 정보를 보호할 수 있다.

여기에서 사용한 커버 데이터는 해당 레코드 중에서 한 아이템을 선택하여 구현한 것이나, 하나의 레

코드 안에서 보안을 필요로 하는 여러 개의 아이템을 동시에 스테가노그라피화 할 수 있다. 또한 외부의 파일을 선택한 것이 아니므로 파일 관리를 별도로 할 필요가 없어 관리가 용이하다.

V. 결 론

인터넷 시대에 각종 데이터의 보호가 점차 요구됨에 따라서 웹 서버 시스템에 보관하고 있는 데이터베이스에 대하여 인가 받지 않은 자로부터 자료의 변경이나 파괴, 도용 등이 있기 때문에 데이터의 보호는 필수적이다. 각 분야의 정보를 효율적으로 구성하여 여러 사용자가 이용하고 있는 것이 데이터베이스 시스템인데, 이렇게 정보를 공유함에 있어서 고객에 대한 비밀 데이터와 같은 특정 부분의 데이터는 사용자를 제한할 필요가 있으며 인가 받지 못한 자로부터 비밀 데이터는 보호되어야 한다.

본 논문에서는 웹 서버 데이터베이스 사용자에게 데이터베이스 내에 보호해야 할 비밀 아이템에 대하여 기존의 DBMS를 사용하면서 비밀 데이터의 보호를 실현할 수 있는 시스템을 제안하였다. 만약에 해독자가 데이터베이스의 데이터를 입수하더라도 형태를 몰라 원문으로 변환할 수 없어 보안성이 유지되며, 또한 데이터를 알고 있더라도 키를 몰라서 원문을 취득할 수 없다.

데이터베이스 안의 데이터가 점차 멀티미디어화가 되어감에 따라 멀티미디어 데이터 안에 비밀 데이터를 삽입하는 방법을 개선하고, 제한된 커버 아이템 안에 많은 양의 비밀 데이터를 넣고자 하는 방법이 향후과제이다.

참 고 문 헌

[1] Jeffrey D. Ullman, *Principles of Database and Knowledge-Base Systems*, Computer Science Press, 1988.

[2] Charles Pfleeger, Shari Lawrence Pfleeger, *Security in Computing*, Prentice-Hall, 3rd Edition, 2002.

[3] Y. C. Hong, Stanley Y. W. Su, "Associative hardware and software techniques for integrity control," *ACM Transactions on Database Systems*, Vol.6, No.3, pp.416-440, 1981.

[4] Neil F. Johnson, Zoran Duric, Sushil Jajodia, "*Information Hiding : Steganography and Watermarking - Attacks and Countermeasures*," Kluwer Academic Publishers, pp.18-44, 2001.

[5] Neil F. Johnson, Sushil Jajodia, "Steganalysis of images created using current steganography software," *Proceedings of Information Hiding Workshop*, LNCS, No.1525, pp.273-289, 1998.

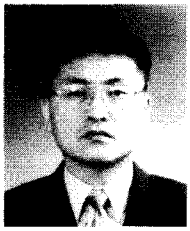
[6] E. Fanz, A. Jerichow, S. Moller, A. Pfitzmann, I. Stierand, "Computer-based steganography : How it works and why therefore any restrictions on cryptography are nonsense, at best," *Proceedings of Information Hiding Workshop*, LNCS, No.1174, pp.7-21, 1996.

[7] 주낙근, 이재현, 김동서, "웨이블릿 계수 교환을 이용한 워터마킹 기법", *한국정보보호학회논문지*, 제13권 제5호, pp.49-56, 2003.

[8] 최순영, 서영호, 유지상, 김대경, 김동욱, "DWT 기반 영상 압축기의 다해상도의 통계적 특성을 이용한 실시간 워터마킹 알고리즘", *한국정보보호학회논문지*, 제13권 제6호, pp.33-43, 2003.

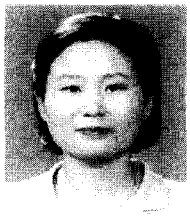
[9] Fabian A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn, "Information Hiding - A survey," *Proceedings of the IEEE*, Vol.87, No.7, pp.1062-1078, 1999.

〈著者紹介〉



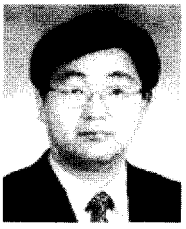
문 봉 근 (Bong-Keun Moon) 정회원
1988년 2월: 수원대학교 전자계산학과 학사
1993년 8월: 광운대학교 전자계산학과 석사
2001년 3월~현재: 숭실대학교 대학원 컴퓨터학과 박사과정
1988년 11월~1993년 3월: 한신공영(주) 전산실
1993년 6월~1998년 3월: 한라정보시스템(주) 마이스터 IS팀
〈관심분야〉 네트워크, 침입탐지시스템, 정보보안
e-mail: mbk2000@chol.com

유 두 규 (Do-Gyu Ryoo) 정회원
1984년 2월: 숭실대학교 전기공학과 학사
2001년 2월: 숭실대학교 컴퓨터교육학과 석사
2005년 2월: 숭실대학교 대학원 컴퓨터학과 박사
1984년 3월~현재: 세명컴퓨터고등학교 인터넷영상 부장
〈관심분야〉 네트워크 보안, 정보보안, DB보안, DRM, 암호학
e-mail: bima@dreamwiz.com



고 명 선 (Myung-Sun Ko) 정회원
1981년 2월: 덕성여자대학교 영양학과 학사
1991년 8월: 서울대학교 보건대학원 환경보건학과 석사
2000년 8월: 숭실대학교 정보통신학과 석사
2001년 9월~현재: 숭실대학교 대학원 컴퓨터학과 박사과정
2005년 3월~현재: 신목고등학교 정보사회와 컴퓨터교과 교사로 재직 중
〈관심분야〉 네트워크 보안, 정보보안, 암호학
e-mail: iamkms@chol.com

엄 기 원 (Ki-Won Eom) 정회원
1981년 2월: 덕성여자대학교 경영학과 학사
2000년 8월: 숭실대학교 컴퓨터교육학과 석사
2001년 9월~현재: 숭실대학교 대학원 컴퓨터학과 박사과정
2005년 3월~현재: 부명정보산업고등학교 교사로 재직 중
〈관심분야〉 컴퓨터보안, 보안, 암호 이론, 침입탐지
e-mail: durii46@naver.com



전 문 석 (Moon-Seog Jun) 정회원
1980년 2월: 숭실대학교 전자계산학과 학사
1986년 2월: University of Maryland 전산과 석사
1989년 2월: University of Maryland 전산과 박사
1989년: Morgen State University 전산수학과 조교수
1989년~1991년: New Mexico State University 부설 Physical Science Lab. 책임연구원
1991년~현재: 숭실대학교 정보과학대학 정교수
〈관심분야〉 네트워크보안, 컴퓨터 알고리즘, 암호학
e-mail: mjun@computing.ssu.ac.kr