GF(2^m) 역산을 이용한 컬러 영상 복호화 알고리즘

이광옥* · 배상현**

*조선대학교

Color image Decryption Algorithm using GF(2^m) inverse

Kwang-ok Lee* · Sang-hyun Bae**

*Chosun University

E-mail : csskwang@empal.com, shbae@chosun.ac.kr

요 약

최근 인터넷의 확산과 시스템 성능 향상으로 멀티미디어 데이터 전송을 위한 정보보호의 관점이 대두됨에 따라 안정적인 디지털 암호화에 따른 복호화 방법론이 절실하게 요구되고 있다. 본 논문에서는 컬러 영상 데이터 전송시 기존의 복호화 방법에 영상 데이터의 각 프레임에 대한 복호화 기법을 제안한다. 또한 보다 빠른 복호화 방법으로 각 프레임에 대한 유한체 GF(2^m) 역산의 4bit 이진화를 통한 컬러 영상의 복호화 방법을 제안한다.

ABSTRACT

Nowadays, the rapid increase of the available amount of internet and system performance has revealed urgent need a method of decryption about digital encryption for stabilization of multimedia data transmission. In this paper, we propose a method of decryption of each frame about video data. Also for advanced decryption, we propose color image decryption method through 4-bit binary of GF(2^m) inverse about an each frame.

키워드

GF(2^m)역산. 멀티미디어 데이터, 복호화, 이진화

Ⅰ. 서 론

인터넷의 확산과 시스템 성능 향상으로 환경이 급변함에 따라 디지털 형태의 멀티미디어 데이터 전송이 증가하고 있다. 기존의 암호와 방법을 통해 멀티미디어 데이터에 대한 저작권을 보호하고, 전송시 해킹차단을 위한 다양한 연구가 진행되고 있다.[1][2]

픽셀 단위의 암호화 방법은 옆 픽셀과의 값 차이가 발생할 수 있기 때문에 암호화 작업 후 짧은 시간에 암호화가 적용된 픽셀의 위치 파악이 가능하다. 하지만 컬러 이미지 전체의 암호화 작업은 전체 픽셀에 같은 값이 적용되기 때문에 미세한 변경은 변형 값을 파악하기에 다소 시간이 걸릴 수 있다.

유한체 GF(2^m)은 암호이론과 에러정정코드와 같은 어플리케이션에서 많이 사용되며, GF(2^m)상에서 정의된 덧셈, 뺄셈, 곱셈 및 곱셈 역원 연산을 고속으로 계산하는 것이 중요하다.[3][4][5]

Ⅱ. 블록암호와 컬러 영상

1. 블록암호

1) 본 연구는 문화관광부 및 한국문화콘텐츠진흥원의 문화콘텐츠기술연구소(CT)육성사업의 연구결과로 수행되었음.

암호 해독자가 이용할 수 있는 연산능력이 무한할 지라도 암호해독에 이용할 수 있는 정보의 양이 불충분하여 암호해독이 불가능할 경우와 암호 해독자가 이용할 수 있는 정보의 양이 충분하여 언젠가는 암호를 풀 수 있지만, 해독과정이 복잡하고 시간과 경비가 많이 요구되어 경제적으로 불합리한 경우가 있으며, 현재의 대부분 암호 알고리즘은 후자에 속한다.

암호 알고리즘은 비공개키 방식과 공개키 암호 방식으로 나눌 수 있으며, 대표적으로 비공개키 방식에는 DES(Data Encryption Standard)가 있으며, 공개키 방식에는 RSA 방식이 있다.

데이터를 어떤 형태로 암호화시킬 것인가에 따라 크게 스트림 암호와 블록암호로 나뉜다. 스트림 암호는 문자단위 혹은 비트단위로 암호화 하는 방식으로, Vegenere 암호와 Vernam 암호가 분류된다. 블록암호는 평문을 일정 길이의 블록으로 잘라 이를 암호알고리즘에 따라 암호화하는 방식으로 DES의 운영모드 가운데 ECB(Electronic Code Book), CBC(Cipher Block Chaining)로 나눌 수 있다.

그리고, 대부분의 공개키 기반 암호 시스템에서는 큰 수의 m을 갖는 GF(2^m)상에서 구축되며, 암호화 및 복호화의 수행 시간은 주로 곱셈 및 곱셈 역원 연산에 좌우된다.[6]

2. 컬러 영상

컬러영상은 이미지를 인지하는 기초적인 시각 특징이다. 컬러 유사도를 이용하는 이미지 검색을 위해서는 컬러를 표현하는 공간 모델이 필요하다. 가장 일반적으로 사용되는 하드웨어 중심 공간은 컬러 모니터와 컬러 비디오 카메라를 위한 RGB(Red, Green, Blue) 공간, 조명 기기를 위한 XYZ 공간, 컬러 프린터를 위한CMY(Cyan, Magenta, Yellow) 공간과 CMYK(Cyan, Magenta, Yellow, Black) 공간, 컬러 텔레비전 방송을 위한 YIQ(Luminace, Inphase, Qu adrature) 공간 등이 있으며 컬러를 재현하는 장치의 특성에 따라 정의된다.

컬러를 표현하는 공간 모델 중에서 사용자 중심 공간은 HSV(Hue, Saturation, Value) 공간, HSI(Hue, Saturation, Intensity) 공간, HSB(Hue, Saturation, Brightness) 공간, L*u*v* 공간, L*a*b* 공간 등으로 분류할 수 있다. 사용자 중심 공간은 인간의 컬러 인식을 기초로 정의되며 인간이 느끼는 컬러간의 거리를 3차원 컬러 공간으로 표현한다. 하나의 컬러 공간에서 다른 컬러 공간으로 컬러 데이터를 변환할 때 컬러 공간의 기하학적인 모양이 처리 과정에 영향을 미친다.

이러한 컬러 영상들에 대한 픽셀 단위의 암호화 작업은 주변 픽셀과의 변동차이의 파악함에 정보의 유출 가능성이 있다.

3. 확장 유클리드 알고리즘

확장 유클리드 알고리즘은 역수 연산이 스칼라 곱셈 연산의 대부분의 시간을 차지하며, 암호학에서 역수 관련 연상을 하기 위한 알고리즘은 [그림 1]과 같다.[7]

```
GCD(a,b) = GCD(b, a mod b)

unsigned int gcd(unsigned int a, unsigned int n)
{
        unsigned int c
        while(b>0)
        {
                c = a;
                a = b;
                b = c;
        }
        return a;
}
```

[그림 1] 역수 연산 알고리즘

III. 유한체 GF(2^m)의 블록화

컬러 영상의 복호화 작업을 위하여 유한체 GF(2^m)를 사용한다.

유한체 GF(2^m)의 임의의 원소 β는 GF(2) 상에서 정규기저(Normal Basis), a^{2^0}, a^{2^1}, · · · , $a^{2^{m-1}}$($a \in GF(2^m)$)를 사용해서 다음과 같이 나타낼 수 있다.[8]

$$\beta = \beta_0 a^{2^0} + \beta_1 a^{2^1} + \cdot \cdot + \beta_{k-1} a^{2^{k-1}}, \ \beta_i \in GF(2) \quad (1)$$

또한, β는 벡터 (β_0, β_1, · ·, β_{m-1})으로도 표현할 수 있으며, 다음과 같이 변형될 수 있다.

$$e = e_0 2^0 + e_1 2^1 + \cdot \cdot + e_{m-1} 2^{m-1}, \ e_j \in GF(2) \quad (2)$$

e_j는 0과 1로 표현된다.

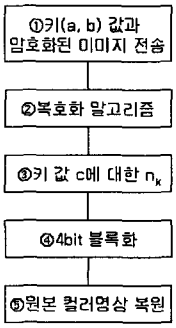
각 지수승 자리의 0과 1로 표현된 값은 4bit의 블록화가 가능하며, 전체 블록의 크기는 $m/4$이며, 다음과 같이 표현이 가능하다.

$$n_k = m_j/4 \quad (3)$$

Ⅳ. 복호화 알고리즘

1. 컬러 영상 복호화

다음 [그림 2]는 컬러 영상을 4bit 단위의 블록화 된 키를 가지고 복호화 시키는 과정을 나타낸다.



[그림 2] 복호화 과정

다음은 ① 키(a, b)값과 암호화된 이미지 전송에 대한 ② 복호화 알고리즘을 이용해 값을 계산한 후 ③ 키 값 c에 대해 ④ 4bit 단위로 키 값을 블록화 한 후 ⑤ 원본 컬러 영상을 나타낸다.

2. 변형된 e에 대한 블록화와 알고리즘

복호화 알고리즘을 이용한 키 값에 대한 유한체 GF(2^m) 변형된 e 에 대한 블록화는 [그림 3]과 같다.

$$e_{m-1}e_{m-2}e_{m-3}e_{m-4} \cdots e_3\ e_2\ e_1\ e_0$$
$$\underbrace{\qquad\qquad}_{n_k} \qquad\qquad \underbrace{\qquad\qquad}_{n_0}$$

[그림 3] e에 대한 4bit 블록화

다음 [그림 4]은 키 값이 gcd(60, 37)이라고 가정하고, 암호키 값을 계산한 식이다.

```
gcd(60, 37) = gcd(37, 23) = gcd(23, 14)
= gcd(14,9) = gcd(9, 5) = gcd(5,4) = 1
.
1 = 5-4*1 = 5-(9-5*1)*1
.
.
1 = 37*13 + 60*(-8)
⇒ 37*13 + 60*(-8) = 1 mod 60
```

[그림 5]와 [그림 6]은 키 값 c 에 대한 $e_0 \cdot e_1 \cdot e_2 \cdot \cdot \cdot e_{m-1}$ 알고리즘과 복호화 과정에 대한 알고리즘을 나타내고 있다.

```
Binary(val, binary);
                    .
                    .
                    .
void Binary(int val, int *binary)
{
int i;
for(i = 7; i > 0; i--)
{
binary[i] = val;
val = val/2;
}
binary[0] = val;
}
                    .
                    .
                    .
for(i = 1; i >= 0; i--)
{
l = 1;
for(k = 1; k <= 4; k++)
{
if(j >= 0)
{
hex[i] += bin[j--]*l;
l = l*2;
}
else
break;
}
}
```

[그림 5] 키 값 c 에 대한 $e_0 \cdot e_1 \cdot e_2 \cdot \cdot \cdot e_{m-1}$ 알고리즘

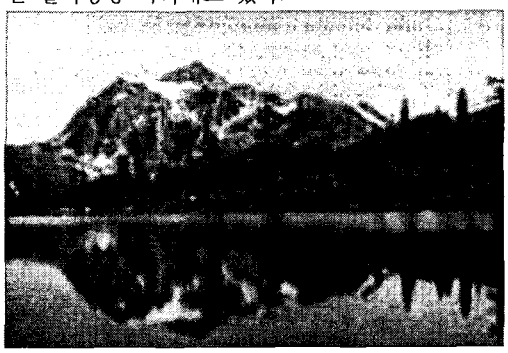
```
step1 : 키 값에 대한 역수 연산과 4bit 블록화
step2 : 첫 번째 컬러 영상 이미지 인식
step3 : 4bit화된 m-1번째 키 값 적용
step4 : k > 0 때까지 step1 반복
```

[그림 6] 복호화 과정

3. 컬러영상의 이진화와 복호화

컬러 영상에 대한 암호화 작업을 위해서 원본 컬러영상에 픽셀단위 2진화 작업이 필요하다.

다음 [그림 7]은 4bit 블록 복호화를 위한 전송된 컬러영상 나타내고 있다.



[그림 7] 전송된 컬러영상

위 그림은 원본 컬러영상을 복호화 시키기 위해 180*120*256 을 이용하여 256컬러값을 적용하여 2진화 작업을 하였다.

그리고 [그림 8]은 gcd(a, b)을 이용해 복호화된 값에 대해 4bit 단위의 첫 번째 키 값에 대한 복호화를 적용한 복원된 원본 컬러영상을 나타내고 있다.

[그림 8] 복원된 원본 컬러영상

V. 결 론

텍스트 단위의 메시지를 통해 전송되는 암호화와 복호화 방법에 대한 연구가 활발히 연구되어지고 있다. 하지만, 최근에는 웹상에서 메시지 전송이 아닌 멀티미디어 데이터 전송이 활성화되고 있다.

이에 멀티미디어 데이터 전송에 따른 정보의 유출 가능성이 높아지고 있다.

따라서 본 논문에서는 컬러 영상에 대해 변형된 GF(2^m)통한 키 값을 gcd(a, b) = 1 역산 작업을 통해 얻어진 키 값을 계산한 후 4bit 블록화를 통한 컬러 영상의 복호화에 대해 제안하였다.

컬러 영상에 대한 블록단위의 복호화 작업은 각 픽셀 단위의 암호화에 있어 픽셀 변동값이 심한 경우의 정보의 유출 가능성을 차단할 수 있다.

역산 값 계산 후 변형된 GF(2^m)통한 키 값을 이진화 시킨 후 4bit 블록화에 따른 복호화 방법은 모든 픽셀에 적용되므로, 컬러영상의 변동값을 감지하기가 어렵다.

따라서, 본 논문에서 제안한 GF(2^m) 역산을 이용한 컬러 영상 복호화 알고리즘은 멀티미디어 데이터 전송시 정보의 유출에 대한 가능성을 줄이고, 또한 수치 데이터의 안전한 전송도 가능하다.

참고문헌

[1] 이용효, 황대준, "에이전트 기반의 동적 디지털 저작 권 관리시스템 설계 및 구현", 정보처리학회 논문지 D, 제8-D권 제 5호, pp.613-622, 2001.

[2] 김정재, 박재표, 전문석, "동영상 데이터 보호를 위한 공유키 풀 기반의 DRM시스템", 정보처리학회 논문지 C, 제12-C권 제 2호, pp.183-190, 2005.

[3] T. Itch and S. Tsujii, "A Fast Algorithm for Compu ting Multiplicative Inverses in GF(2^m) Using Norma l Basis", Information and Computing, vol. 78, pp. 1 71-177.

[4] T. Chang, E. Lu, Y. Leu and H. Shyu, "Two Algori thms for Computing Multiplicative Inverses in GF(2^m) Using Normal Basis" accepted by information Processing Letters.

[5] N. Takagi, J. Yoshiki, and K. Takagi, "A Fast Algorithm for Multiplicative Inversion in GF(2^m) Using Normal Basis", Proceeding IEEE Trans. on Computers, vol. 50, pp.394-398, May 2001.

[6] L. Gao and G. E. Sobelman, "Improved VLSI Designs for Multiplication and Inversion in GF(2^m) over Normal Basis", Proceeding of ASIC/SOC Conference 2000, pp. 97-101.

[7] http://math88.com.ne.kr/crypto.htm

[8] 장용희, 권용진, "GF(2^m)에서 정규기저를 이용한 고속 곱셈 역원 연산 방법", 정보보호학회논문지, 제1권 제 1호, pp. 127-131. 2003.