通信情報保護學會誌
第3卷 第1號, 1993. 3

영상 정보의 보호에 관한 소고

이경호* · 정지원* · 원동호**

1. 서 론

고도 정보화 사회로의 진전으로 각종 정보 서비스들이 발달하고, 정보의 축적, 처리, 전송 능력이 획기적으로 증대되면서 정보가 산업사회에서의 물질이나 에너지 이상으로 그 가치를 인정받아 시장에서 유통되고 있다.

이런 무형의 정보의 가치를 유지하기 위해 전송, 처리 혹은 기억장치에 보관된 상태에서의 불법 유출, 삭제, 수정 등의 위험으로부터 적절한 정보 보호조치가 필요하다. 정보 보호를 위한 대책 중에는 설비면에서의 물리적 대책, 관리 운영면에서의 인적 자원에 대한 대책, 법과 제도면에서의 대책 등이 있으나 암호방식을 이용한 기술면에서의 대책이 가장 경제적이면서도 효율적이라고 할 수 있다[1].

종합 정보 통신망(ISDN : Integrated Services Digital Networks)의 발전과 광역성, 동보성의 위성통신을 통한 디지탈 정보 전송 시스템의 보급, 멀티미디어(multimedia)의 도입으로 음성 정보, 텍스트 정보, 영상 정보가 다양하게 사용되고 있으며 특히, 영상 정보의 비중이 높아감에 따라 영상 정보 보호에 관한 관심이 고조되고 있다[2), 3].

이런 영상 정보 보호 기술의 활용 분야로는 위성이나 유선 방송에서의 pay-TV 시스템, 기밀을 요하는 원격 회의나 영상 전화 시스템, 고부가 가치의 위성 사진의 전송, FAX를 이용한 기밀 서류의 전송, 멀티미디어 통신에서의 정보 보호 서비스 등을 들 수 있다[3), 4), 5), 6].

그러나 영상 정보는 그 정보량의 방대성 때문에 단순하게 기존의 암호방식을 이용하면 정보 보호에 문제점이 발생한다. 왜냐하면 암호방식은 충분한 암호강도를 유지하기 위해 비교적 많은 계산량을 필요로 하기 때문이다. 실제로 color TV 정도의 해상도를 갖는 한 화면을 나타내기 위해서는 약 1 Mbyte 정도의 필요하고, 또 동영상일 경우 화면이 1/30초 마다 바뀌어야 하므로 1초의 동영상에는 약 30 Mbyte 정도의 정보가 필요하다. 만약 35mm film 정도의 해상도로 영상을 나타내려면 이것의 약 열배 정도가 소요된다[7].

이처럼 엄청난 양의 영상 정보를 기존의 DES(Data Encryption Standard)나 RSA(Rivest-Shamir-Adleman) 공개키 암호방식으로 처리하려면 많은 시간이 걸려 실용화에 문제가 있다[3].

이와같은 문제점을 효과적으로 해결하기 위해 보다 빠르고 암호 구현이 간단하면서 충분한 암호강도를 갖는, 영상 정보에 맞는 암호방식에 대해 많은 연구가 진행되어 왔다. 본 논문에서는 지금까지 연구되어 온 영상 암호방식들을 살펴보고 그 특징과 문제점에

* 정회원, 성균관대학교 정보공학과
** 종신회원, 성균관대학교 정보공학과 교수

대하여 고찰한다.

2. 영상 암호방식

대표적인 영상 암호방식으로는 전치암호를 이용한 스크램블 방식을 들 수 있는데, 1982년 Tominaga, Ohtsubo, Komatsu등의 연구에서 처음 제안된 방식이다. 이 방식은 팩시밀리에서 주사선을 치환하는 방식과 주사선 내의 화소(pixel)를 치환하는 방식으로써 영상 암호의 선구적인 역할을 해왔다[6]. 또한 Maeda, Komura, Shiraishi는 이를 보다 발전시켜 가산 암호방식과 feedback 전치 암호방식을 결합시킨 복합 방식을 제안하였다[3]. 그리고 CRYPTO '87에서는 Yossi Matias와 Adi Shamir가 space filling curve라는 일종의 Hamiltonian circuit를 이용한 특이한 스크램블 방식[8]을 제안하였다. 그 외에도 영상 암호화와 통신로 부호화를 결합한 방식[9], DCT (Discret Cosine Transform)와 스크램블 방식을 결합시킨 방식[4], 위성을 통한 영상회의 시스템을 위한 암호 프로토콜에 관한 연구[5], 스크램블 방식과 벡터 양자화를 이용한 압축방식에 적용이 가능한 인덱스 치환 방식에 관한 연구[2] 등이 있다. 이상의 논문들에서 제안한 영상 암호방식들을 크게 나누어 보면, 다음과 같이 여섯가지로 나눌 수 있는데, 이를 간단히 도식화해 보면 그림 1과 같다.

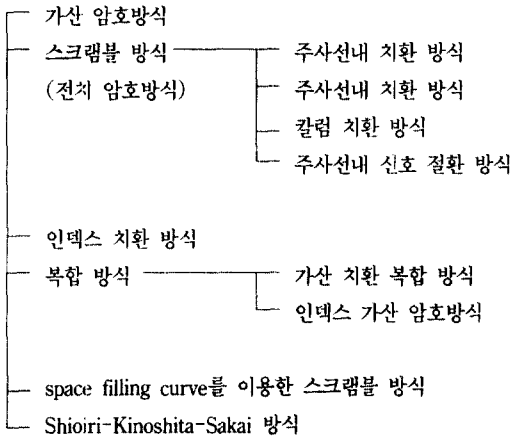


그림 1. 영상 암호방식의 종류

2.1. 가산 암호방식

가산 암호(additive cipher) 방식은 스트림 암호(stream cipher) 방식의 일종으로 암호키에 의해서 생성된 의사난수 계열을 원 정보에 가산(또는 비트의 배타적 논리합)하여 암호화를 행하는 방식이다. DES의 OFB(Output FeedBack) 모드도 일종의 가산 암호방식이며 의사난수를 생성하는 방식으로는 선형 합동법과 M계열 난수 생성법 등이 있는데, 이런 방식은 처리가 단순하고 암호화 속도가 빨라서 정보량이 방대한 디지탈 영상의 암호화에 적용이 가능하리라 사료된다[3]. 그러나 가산 암호방식은 암호 강도면에서 다음과 같은 문제점이 있다.

1) 암호문을 도청한 해독자가 원래의 정보의 일부를 알고 있을 경우 known plain-text attack 또는 probable word attack으로 가산에 사용한 의사난수 정보를 알 수 있고, 암호키를 추정할 수 있다.

2) 영상 정보는 용장도가 높아 동일 정보가 반복하여 나타나는 경우가 많으므로 난수 정보가 노출될 수 있어 해독될 우려가 있다.

3) 동일한 키로 복수의 영상을 암호화할 경우 이를 가산하면 난수 정보가 소거되어 원영상의 정보를 용이하게 판별할 수 있다. 이를 방지하기 위해서는 영상마다 키를 변화시켜야 하는데, 이렇게 하려면 키의 배분, 전송, 관리가 복잡해진다.

위의 문제점 3)은 동일한 암호키로 암호화된 두 장의 영상을 배타적으로 논리합하면 두 영상의 난수 정보가 소거되어 원영상 두 장이 겹쳐진 형태의 영상으로 나타나 원영상의 정보를 쉽게 알아낼 수 있다는 것이다. 그림 2가 그 예이다[3].

위에서 살펴본 바와 같이 이 방식은 키 관리와 암호 강도면에서의 문제점 때문에 단독으로는 사용되지 않고, 다른 암호 방식과 함께 적용되고 있다. 그 예로는 1986년 일본 전자통신학회 논문지 Maeda, Komura, Shiraishi가 제안한 가산 전치 복합방식과 ISEC-91에서 Minami, Wakasugi, Kasahara가 제안한 인덱스 가산 암호방식 등이 있다. 이 방식들은 2.4. 절에서 살펴보기로 한다.

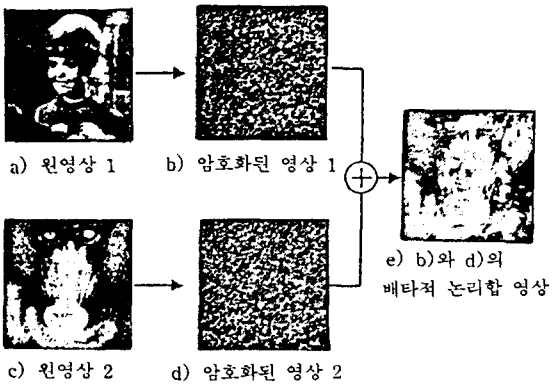


그림 2. 가산 암호를 이용한 영상 암호의 해독예

2.2. 스크램블 방식

스크램블(scramble) 방식이란 관용 암호방식의 전치 암호(transposition ciphr)를 영상 정보에 적용한 암호방식으로서, 원 정보를 작은 단위로 분할하여 각 단위의 위치를 키에 의한 순서로 치환하여 암호화하는 방식을 말한다. 특히 영상 정보는 각 화소의 계조값(gray level)과 그 화소의 위치 정보 즉, 2차원 평면상의 좌표로 나누어 생각할 수 있는데, 이 스크램블 방식이란 계조값은 변화시키지 않고 그 위치 정보만을 치환하여 원래의 영상을 알아 보지 못하게 하는 방식이다.

이 스크램블 방식에서는 치환하는 단위가 화소인지, 주사선인지, 블록인지에 따라 주사선 치환방식, 주사선내 치환 방식, 주사선내 신호 절환 방식, 칼럼 치환 방식 등으로 나누어진다. 이 방식은 속도가 빠르고 간편하여 팩시밀리나 동영상의 암호방식으로 제안되었다[2), 3)].

2.2.1. 주사선 치환 방식

주사선이란 한 화면 내에서 가로의 한 줄을 의미하는데, 주사선 치환 방식이란 한 화면내의 주사선을 랜덤하게 뒤섞어 놓는 것을 의미한다. 이 방식은 한 화면 분의, 비교적 대용량의 버퍼 메모리가 필요하다. 암호 강도의 손실은 있지만 버퍼 메모리를 줄일 수 있는 방법으로 한 화면을 몇 개의 블록으로 나누어 블록 내의 주사선만을 치환함으로써 소요 메모리를 블록 크기로 줄일 수 있는 방법이 있다.

a) 주사선 치환 방식 b) 원영상 c) 암호화된 영상

그림 3. 주사선 치환 방식의 적용예

2.2.2. 주사선내 치환 방식

주사선내 치환 방식은 한 주사선 안에 있는 화소들의 위치를 랜덤하게 치환하고 각 주사선 마다 다른 치환을 적용하는 방식이다. 이 방식은 화소 단위로 치환을 해야 하기 때문에 주사선 수 만큼의 랜덤하게 생성된 치환이 필요하며 주사선 치환 방식 보다 오버헤드가 크나 암호강도는 훨씬 강하다. 화소 단위로 치환함으로써 생기는 오버헤드를 줄이기 위해 몇개의 화소를 하나의 블록으로 잡아 블록을 치환하는 방식도 있다.

a) 주사선내 치환 방식 b) 원영상 c) 암호화된 영상

그림 4. 주사선내 치환 방식의 적용예

2.2.3. 칼럼 치환 방식

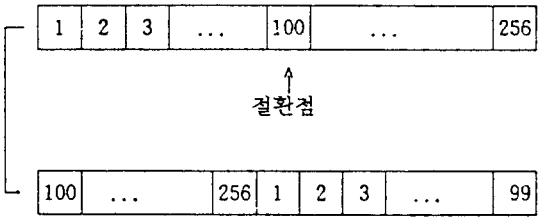
칼럼 치환 방식은 한 화면에서 세로의 한 줄을 의미하는 칼럼들을 랜덤하게 치환하는 방식이다. 이 방식은 주사선내 치환 방식을 주사선 마다 같은 치환을 적용하는 방식이기 때문에 한 주사선 분의 버퍼 메모리가 필요하다. 이 방식도 치환의 오버헤드를 줄이기 위해 주사선을 동일 화소수의 세그먼트로 나누어 세그먼트를 치환하는 방법도 있다.

a) 칼럼 치환 방식 b) 원영상 c) 암호화된 영상

그림 5. 칼럼 치환 방식의 적용예

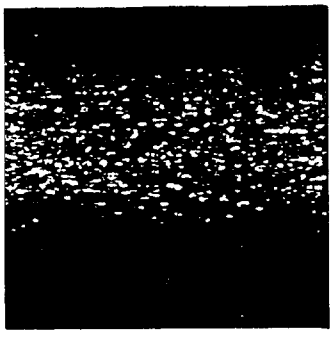
2.2.4. 주사선내 신호 절환 방식

주사선내 신호 절환 방식은 line rotation 방식으로도 불리우는데, 그림 6의 a)와 같이 한 주사선을 의사난수 발생기(pseudo-random number generator)에서 발생시킨 주사선 내의 화소의 주소만큼 시프트시키는 방식이다. 이 때 의사난수 발생기에서 발생시킨 주사선 내의 화소의 주소를 절환점(cutting point)이라한다. 이 방식은 한 주사선 분의 버퍼가 필요하며, 난수 발생기로부터 발생시킨 난수를 주사선당 화소수로 modulo 연산시킴으로서 쉽게 절환점을 구할 수 있기 때문에 구현이 간편하고 속도가 빠르다. 이러한 장점으로 인해 위성이나 유선 방송의 pay-TV 시스템에 적용이 고려되고 있다.



a) 주사선내 신호 절환 방식

b) 원영상



c) 암호화된 영상

그림 6. 주사선내 신호 절환 방식의 적용예

그러나 이 스크램블 방식을 다치 계조 영상에 적용할 경우 다음과 같은 문제점이 발생할 수 있다.

1) 단순한 전치 암호는 원영상의 히스토그램 정보를 그대로 갖고 있기 때문에, 암호화된 영상의 히스토그램 정보로 원영상의 종류를 추정할 수 있다. 따라서 충분한 주의가 필요하다.

2) 블록의 크기가 어느 정도 클 경우, 영상 정보간의 용장도를 이용하여 블록간의 상관 관계를 계산하여 해독할 수 있다.

3) 키의 수와 전치 주기의 자유도가 작으면 암호화된 정보를 많이 확보하면 할수록 키의 추정이 용이해진다. 전치 암호의 키를 선택하는 방법으로는 전치 함수를 이용하는 방법과 M계열의 합동식을 이용하는 방법 등이 알려져 있는데, 이런 이유로 인해 블록의 크기는 충분히 작게 하고 전치 주기는 될수록 길게 하여야 한다.

문제점 2)는 한 블록이 한 주사선일 경우에 다음과 같은 상관계수 H를 계산하여 쉽게 해독 가능하다.

$$H=\sum_{m=1}^{M}(X_{im}-X_{jm})^2 \qquad (2.1)$$

단, X_{im}은 좌표(i, m)의 계조값이다.

즉, H가 0에 가까우면 상관도가 커짐을 의미하고, 반대로 H가 커지면 상관도가 작아짐을 의미한다.

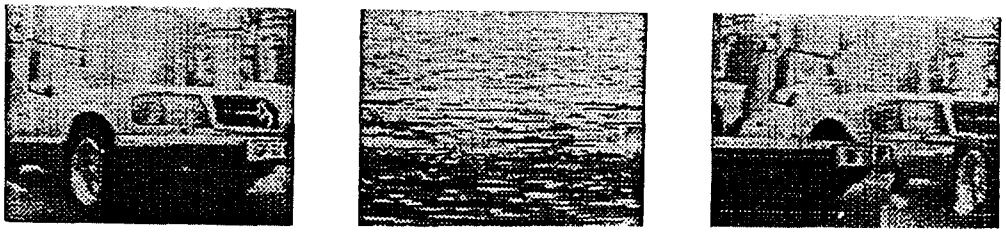
주사선 치환 방식으로 암호화한 경우 이 상관계수 H를 사용하여 해독하는 방법은 다음과 같다. 암호화된 영상 중 임의의 한 주사선에 대한 전체 주사선의 상관도를 계산하여, 가장 상관도가 큰 주사선을 선택하여 바로 그 다음 주사선의 위치에 놓고, 그 주사선과 가장 상관도가 큰 주사선을 계산하여 선택하는 방식으로 해독이 가능하다. 다음의 그림 7은 이 방법으로 해독한 예이다[3].

또한 주사선내 신호 절환 방식으로 암호화된 경우는 다음의 알고리즘을 이용하면 쉽게 해독할 수 있다.

순서 1. 암호화된 영상 정보의 첫 번째 주사선을 버퍼 1에, 그 다음 주사선을 버퍼 2에 입력한다.

a) 원영상 b) 암호화된 영상 c) 해독 영상

그림 7. 주사선 치환 방식의 암호해독 예



a) 원영상 b) 암호화된 영상 c) 해독 영상

그림 8. 주사선내 신호 절환 방식의 암호해독 예

순서 2. 버퍼 1과 버퍼 2의 같은 주소의 화소끼리의 상관 계수 H를 구하여 저장한다.

순서 3. 버퍼 2를 한 화소씩 시프트하여 H를 구한 뒤 이전의 H 값보다 작으면 새로운 H값을 저장하고 그 때의 절환점 주소 P값을 저장, 아니면 통과한다.

순서 4. 순서 2, 3을 M회 반복한다.

순서 5. 순서 2, 3, 4에서 얻어진 최종 H값을 복호 알고리즘의 순서 3의 절환점 P로 사용하여 복호화한다.

순서 6. 순서 1, 2, 3, 4, 5를 그 다음 주사선에 적용시켜 N-1회 반복한다.

그림 8은 위 방법으로 해독한 예이다. 이런 해독방식은 치환하는 블록의 크기가 클수록 해독이 용이하다.

2.3. 인덱스 치환 방식

이 방식은 최근 들어 영상 정보의 압축 방식으로 관심의 대상이 되고 있는 벡터 양자화 방식으로 부호화하는 경우에 적용 가능한 암호 방식으로, 코드북의 인덱스를 치환하여 부호화함으로써 원영상을 감추는 방식이다. 이 방식은 벡터 양자와 부호화 방식으로 영상을 전송할 경우 코드북은 공개하고 인덱스와 코드북의 치환표를 비밀키로 배포하여 간단하게 실현 가능하다. 또한 이 방식은 G3 FAX의 MH(Modified Huffmann) 부호화 방식과 같은 코드북 부호화 방식에 적용 가능하리라 사료된다. 그러나 이 방식은 인덱스가 치환되기는 하지만, 용장도가 큰 영상 정보에서는 같은 값을 갖는 정보가 많아서 인덱스를 차례로 바꾸어 적용시키면, 정보의 일부가 해독되는 단점이 있다. 그림 9는 인덱스 치환 방식의 예이다[2].

a) 원영상(일기예보)

b) 암호화된 영상

그림 9. 인덱스 치환 방식

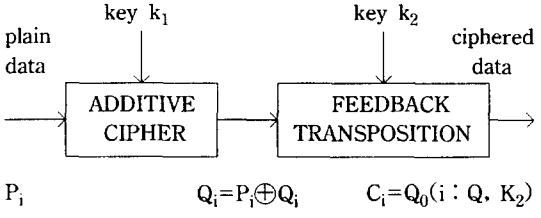
2.4. 복합 방식

위에서 설명한 방식들의 장단점을 고려하여, 효율과 암호 강도를 높히기 위해, 위 방식들의 복합 방식을 쓰기도 한다. 예를 들면 가산 전치 복합 방식, 인덱스 가산 암호방식 등이 있다.

2.4.1. 가산 전치 복합 방식

디지탈 영상 정보는 정보량이 대용량이기 때문에 영상 암호방식은 고속이어야 한다. 그렇기 때문에 속도가 비교적 빠른 관용 암호방식의 가산 암호나 전치 암호가 고려될 수 있으나 용장도가 높은 영상 정보에 이런 방식을 적용하는 데에는 2.1.절과 2.2.절에서 살펴본 바와 같은 암호강도 면에서의 문제점이 발생한다. 따라서 고속성을 유지하면서 암호강도면에서의 문제점을 해결하기 위해서 가산 전치 복합 방식이 1986년 Maeda, Komura, Shiraishi에 의해 제안되었다[3].

이 방식은 가산 암호화 feedback 전치 암호를 혼합한 방식으로 먼저 평문정보 P_i를 key k_1으로 가산 암호를 취하고 이를 다시 key k_2를 사용하여 feedback 전치 암호를 취하여 암호정보를 얻는다. 이를 도식화한 것이 그림 10이다. 여기서 feedback 전치 암호 부분을 보면, 효율이 좋다고 널리 알려진 Knuth의 random shuffing algorithm을 이용하여 N개의 요소로 나누어지는 평문 $P_0, P_1, \cdots, P_{N-1}$의 순서를 바꾼다. 이 feedback 전치 암호를 도식화 해보면 그림 11과 같고 random shuffling algorithm은 다음과 같다.



⊕ : 비트의 배타적 논리합
N_i : k_i로부터 생성된 난수 계열

그림 10. 가산 전치 복합 방식

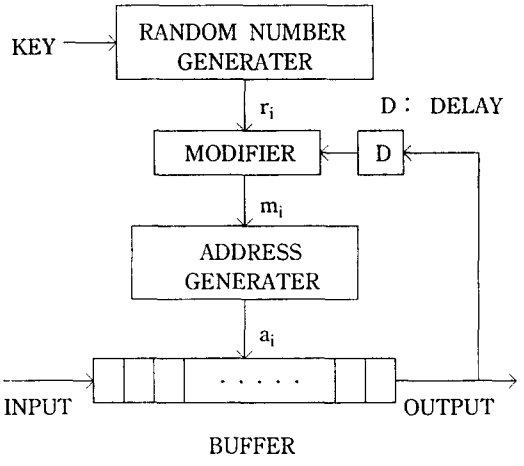


그림 11. feedback 전치 암호

순서 1. j를 N으로 초기화한다.

순서 2. 난수 r을 생성한다. $(0.0 \le r \le 1.0)$

순서 3. int(r, j)를 계산하여 k로 한다. $(0 \le k \le j-1)$
단, int는 소수점 이하를 잘라 정수화하는 함수이다.

순서 4. P_k와 P_j를 교환한다.

순서 5. $j>1$일때 까지 $j \leftarrow j-1$로 한다. 순서 2로

이 random shuffling algorithm으로 치환된 출력되기 직전의 암호 정보를 다시 다음의 랜덤 주소를 생성하는데 사용한다.

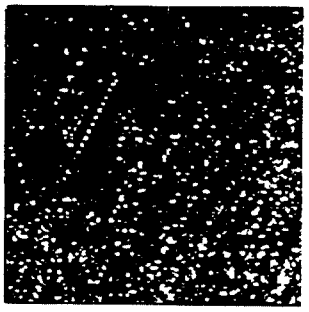
이 복합 방식의 장점은 2.1.절에서 본 가산 암호의 암호강도 면에서의 문제점 1~3과 2.2.절 전치 암호의 문제점 1~3이 모두 해결되어 암호강도가 향상되었다는 점이다.

2.4.2. 인덱스 가산 암호방식

인덱스 치환 방식은 한 화면 내에서 같은 패턴의 블록은 같은 인덱스로 나타나기 때문에, 그림 9의 b)에서 볼 수 있듯이 윤곽이 들어나므로 암호강도 면에서의 문제점을 갖고 있다. 인덱스 가산 암호방식은 이런 문제점을 해결하기 위해 인덱스에 m차 원시다항식으로부터 생성한 M계열의 난수를 modulo-2로 가산하여 스크램블하는 방식이다. 예를 들어 8차 원시 다항식 $x^8+x^4+x^3+x^2+1$을 사용하면 255개의 난수를 얻을 수 있는데, 이 난수를 인덱스에

비트 단위로 더하고 modulo-2를 하여, 같은 패턴의 블록도 난수에 의해 다른 인덱스로 치환하는 방식이다. 주의할 점으로는 난수의 주기를 충분히 길게 하여 한 화면에 난수의 주기가 나타나지 않게 해야 안전하다. 만약 난수의 주기가 반 화면 즉 한 필드(field)에 해당할 경우, 한 화면 내의 두 필드를 배타적으로 논리합하면 2.1. 절의 문제점 3)과 같이 원 정보가 드러난다. 그림 13은 이 방식의 적용예이다[2].

a) 원영상



b) 암호화된 영상

그림 12. 인덱스 가산 암호방식

2.5. space filling curve를 이용한 스크램블 방식

이 방식은 Yossi Matias와 Adi Shamir가 CRYPTO'87에서 제안한 방식으로서, 그림 13과 같이 랜덤하게 발생된 일종의 Hamiltonian circuit인 space filling curve의 순서에 의해 계조값들을 재배열함으로써 위치 정보를 뒤섞어 암호화하는 일종의 스크

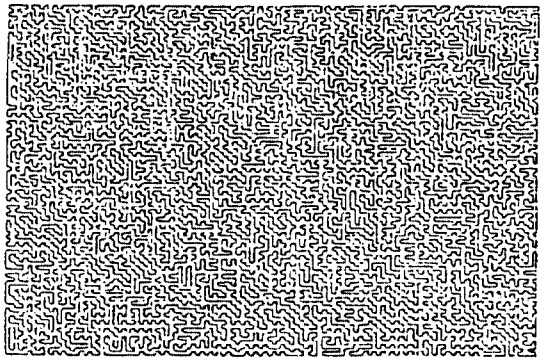
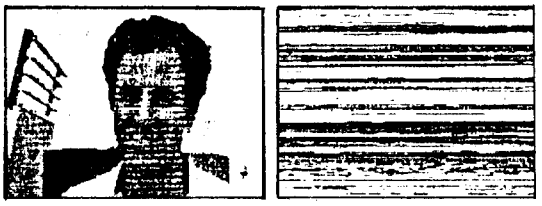


그림 13. space filling curve의 예

램블 방식(이하, SFC 방식)이다. 이 방식은 아날로그 영상 정보의 암호화에는 기존의 암호방식이 부적당하다는 세가지 이유를 전제하고 있다. 첫째, 전송 신호가 아날로그 신호이다. 둘째, 전송율이 매우 높다. 셋째, 영상 정보는 상관 관계가 높다. 즉 현재 주로 사용되고 있는 영상의 전송방식은 아날로그 방식인데, 앞에서 살펴본 여러 영상 암호방식으로 암호화를 할 경우, 화소 간의 상관관계가 깨어져 고주파 성분이 많이 발생하여 전송 대역폭의 증가를 초래한다는 문제점을 지적한 것이다. 이런 문제점을 해결하기 위해, 이 SFC 방식은 디지탈 영상 전송이 아니라 아날로그 영상 전송에 알맞게 제안된 방식이다[8].

이 SFC 방식의 특징은 위치 정보가 인접 화소로만 바뀌기 때문에 상관관계가 깨어지는 것이 아니라 비월 주사 방식(raster scan) 보다도 더 상관관계가 향상되어, 전송시 비월 주사 방식 보다 더 적은 대역폭으로 좋은 화질을 유지할 수 있다. 이런 특성으로 인해 DCT 기반의 압축방식을 사용할 때 좋은 압축 효과를 나타내리라 사료된다. 하지만 이는 SFC 스크램블을 취하는 대상 영상이 비교적 클 경우(즉 256×256, 512×512)에만 압축 효과를 기대할 수 있다[8].

이 방식에서의 연구 과제로는 키로 사용될 SFC를 어떤 방법으로 랜덤하게 빨리 만들어 내는가 하는 문제가 있다. 몇가지 랜덤 SFC 생성 알고리즘이 제시되어 있으나 키공간이 크고 속도가 빠르면서 암호강도가 큰 알고리즘이 필요하다.



a) 원영상 b) 암호화된 영상

그림 14. Sapce Filling Curve 방식

2.6. Shioiri-Kinoshita-Sakai 방식

이 방식은 Shioiri, Kinoshita, Sakai가 일본 전자통신학회 논문지 ISEC-90에서 제안한 방식으로 위성을 통한 영상 통신 회의 프로토콜에서의 정보 보호를 다룬 방식(이하, SKS방식)이다. 그 중 영상 암호화 부분에서는 JPEG과 같이 DCT 기반의 압축을 행하는 정보원 부호화 방식에 적합한 암호 방식을 제안하였다. 이 방식은 DCT의 특성 중 정보의 대부분이 포함되어 있는 저주파 성분이 한쪽으로 집중된다는 점을 이용해 그 부분만을 암호화하는 방식으로서 DCT가 취해진 주파수 성분 정보 중에서 저주파 쪽 일부만을 암호화해도 IDCT(Inverse DCT)를 취하면 전체 영상에서 높은 암호 효과를 얻을 수 있다[5].

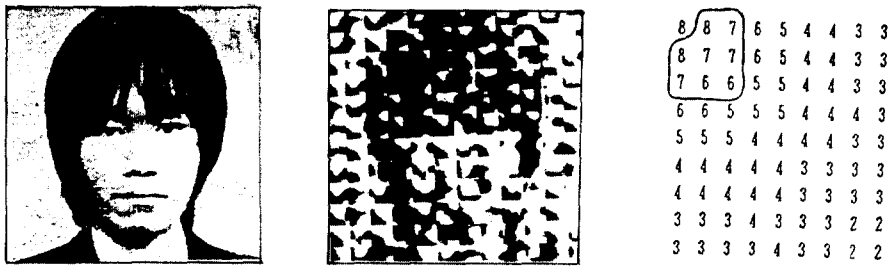
또한 이 SKS 방식은 원격 영상 회의의 서비스 목적상 회의 참가자의 신원을 확인하고, 회의 내용에 대한 높은 보안성을 위하여 디지탈 서명과 사용자나 메시지 인증이 가능한 RSA 공개키 암호 방식을 사용하였다[10), 11]. 이 RSA 공개키 암호 방식은 1978년 Rivest와 Shamir, Adleman에 의해 제안된 방식으로 여러 장점들을 갖고 있지만 200자리 이상의 큰 수의 누승 등 계산량이 많아 이로 인해 처리 속도가 느리다는 단점이 있다[12), 13]. 특히 동영상 처리가 요구되는 영상 회의 시스템에서는, 엄청난 양의 영상 정보를 처리 속도가 느린 RSA 공개키 암호 방식을 이용해 실시간으로 암호화한다는 것은 불가능하다. 이를 해결하기 위해서 이 SKS 방식은 영상 정보를 DCT를 이용하여 주파수 공간으로 변환시킨 뒤 정보의 대부분을 포함하고 있는 저주파 부분을 RSA 공개키 암호방식에 대한 현재 기술수준의 처리 한계에 맞게 선별하여 암호화한다.

이 방식에 대해 구체적으로 살펴보면 16×16 블록 단위로 DCT를 취하며 압축은 아래의 표 1과 같이 FDCT(Forward DCT)후 계수값 중 저주파 성분에는 많은 비트를 고주파 성분에는 적은 비트를 할당하여 줌으로써 실현하였다.

그런데 앞에서 언급한 바와 같이 RSA 공개키 암호

표 1. 비트 할당

8	8	7	6	5	4	4	3	3	2	2	2	0	0	0	0
8	7	7	6	5	4	4	3	3	2	2	2	0	0	0	0
7	6	6	5	5	4	4	3	3	2	2	2	0	0	0	0
6	6	5	5	5	4	4	4	3	3	2	2	2	0	0	0
5	5	5	4	4	4	4	3	3	3	2	2	2	0	0	0
4	4	4	4	4	3	3	3	3	3	2	2	2	2	0	0
4	4	4	4	4	3	3	3	3	2	2	2	2	2	0	0
3	3	3	4	3	3	3	2	2	2	2	2	2	0	0	0
3	3	3	3	4	3	3	2	2	2	2	2	2	2	0	0
3	3	3	3	3	3	2	2	2	2	2	2	2	0	0	0
2	2	2	2	2	2	2	2	2	2	2	0	0	0	0	0
2	2	2	2	2	2	2	2	2	2	2	0	0	0	0	0
2	2	2	2	2	2	2	2	2	2	2	0	0	0	0	0
2	2	2	2	2	2	2	2	2	2	0	0	0	0	0	0
2	2	2	2	2	2	2	2	2	2	0	0	0	0	0	0
2	2	2	2	2	2	2	2	2	2	0	0	0	0	0	0
2	2	2	2	2	2	2	2	2	2	0	0	0	0	0	0



a) 원영상 b) 암호화된 영상 c) 암호화 적용 부분

그림 15. Shioiri-Kinoshita-Sakai 방식

방식는 처리 속도의 한계가 있기 때문에 동영상 처리가 요구되는 영상 회의 시스템에 적용하기 위해서는 블록당 암호화 처리 가능 비트 수가 한정된다.

이 방식에서는 RSA 공개키 암호 방식을 이미 일부 업체에서 구현한 하드웨어의 처리 속도가 약 500 Kbps임을 전제로 하여 계산하면 블록당 약 16 비트 정도를 암호화 처리할 수 있다.

$$500\ \text{Kbps} \div 30\ \text{frame/sec} \div 1024\ \text{block/frame} \fallingdotseq 16\ \text{bit/block} \qquad (2.2)$$

이런 암호화 처리 비트 수의 한계에 맞추고 암호화 효과를 극대화하기 위해, 한 블록을 FDCT한 후의 계수값들 중에서 저주파 쪽의 계수값들을 선별하고, 그 계수값들의 MBS쪽 몇 비트만을 암호화한다. 다음의 그림들이 이 SKS 방식으로 암호화한 영상과 암호화한 부분을 나타낸다.

3. 결 론

최근 심각히 대두되고 있는 정보 보호의 문제를, 앞으로 다가올 ISDN이나 멀티미디어 시대에서 주요 관심 사항이 될 영상 정보에 적용시킬 수 있는 여러 영상 암호방식에 대해 개괄적으로 살펴보았다.

영상 정보의 특성으로는 정보량의 방대성과 높은 용장도를 들 수 있다. 영상 정보는 그 양이 방대해서 많은 계산량을 필요로 하는 암호방식 적용에 난점으로 작용한다. 특히 동영상 암호화의 경우 1초에 30장이라는 엄청난 양의 영상 정보를 암호화할 수 있는 빠른 암호방식이 필수적이다. 또한 영상 정보는 용장도가 높아서 2.2. 절에서 본 바와 같이 상관관계를 이용한 암호해독에 약한 단점을 갖고 있다[3), 14)]. 그렇기 때문에 영상 암호방식에서는 암호 강도면에 특히 주의를 기울여야 한다. 또한 영상 정보는 윤곽선 정보만으로도 전체 영상을 쉽게 파악할 수 있으므로 작은 양의 해독이 이외로 많은 정보의 누출을 가져올 수 있기 때문에 이런 면에서도 주의를 요한다.

이런 영상 정보의 특성으로 인해, 주로 텍스트나 음성 정보에만 적용하던 기존의 암호방식들은 적용에 문제점이 많다. 그렇기 때문에 앞에서 살펴본 것과 같은 여러 영상 암호방식들이 제안되었다.

초기에는 영상 정보 압축을 고려하지 않은 단순 전치나 가산 암호를 이용한 방식들이 제안되었으나 암호강도 면에서의 문제점으로 인해 이후에는 복합 방식들이 제안되었다. 그러나 영상 정보의 방대성으로 인해 저장, 전송에 지장을 초래하면서부터 연구된 영상 압축방식이 보급되면서부터 압축을 고려한 영상 암호방식이 제안되었다. 그 예로는 벡터 양자화 부호화 방식에 적용 가능한 인덱스 치환 방식과 DCT 기반의 압축방식에 적용 가능한 SKS 방식을 들 수 있다. 그리고 암호 서비스 측면에서도 인증이나 디지탈 서명과 같은 높은 수준의 서비스가 가능한 암호방식이 제안되는 추세이다.

앞으로도 영상 정보의 보호에 관한 연구는 멀티미디어 개념의 확산에 따라 지속되리라 사료되는데, 연구 과제로는 영상 암호화에서의 암호강도 분석 기법에 관한 연구, 동영상에 적용 가능한 보다 효율적이고 암호강도가 강한 영상 암호방식에 관한 연구와 암호화의 오버헤드를 줄이기 위한 암호화와

부호화의 동시 처리에 관한 연구, 암호화 서비스 수준의 향상, 암호화 프로토콜의 구현 등이 있다[15), 16)].

참 고 문 헌

1. 원동호, "암호방식과 키 분배", 통신정보보호학회지, 제 1 권, 제 1 호, 1991.

2. 南憲明, 若杉耕一郎, 笠原正雄, "畫像情報のセキュリテイ確保に關する考察", 信學技報, Vol. 90, No. 31, ISEC91-8, 1991.

3. 前田章, 古村文伸, 白石高義, "デイジタル畫像に適したデータ暗號化の一方法", 電子通信學會論文誌, Vol. J69-B, No. 11, 1986.

4. Noboru Katta, Seiji Nakamura, Hiroki Murakami, Hatsukazu Tanaka, "A New Approach to Digital Scrambling of Image Signals", 信學誌報, ISEC90-33, 1990.

5. Norio Shioiri, Hirotsugu Kinoshita, Yoshinori Sakai, "A Study on the Satellite Teleconferencing Protocol for Security", 信學技報, Vol. 90, No. 31, ISEC 90-34, 1990.

6. Hideyoshi Tominaga, Yasuo Ohtsubo, Naohisa Komatsu, "On a Confidential Message Handling Facility for Facsimile Communications", 電子通信學論文誌, Vol. J65-B, No. 11, 1982.

7. Magid Rabbani, Paul W. Jones, "Digital Image Compression Techniques", SPIE Optical Engineering Press, pp.3-10, 1991.

8. Yossi Matias, Adi Shamir, "A Video Scrambling Technique Based On Space Filling Curve", CRYPTO'87, 1987.

9. Kazuhito Tanaka, Masao Kasahara, "A Combinding Error-Control and Encryption for Image Signal and Its Evaluation", 信學技報, ISEC89-39, 1989.

10. Jennifer Seberry, Josef Pieprzyk, "Cryptography, An Introduction to Computer Security", Prentice Hall, pp.88-111, 1989.

11. Charles P. Pfleeger, "Security in Computing", Prentice Hall, pp.100-104, 1989.

12. 辻井重男, 笠原井雄, "暗號と情報セキコリテイ", 昭晃堂, pp.57-81, 1990.

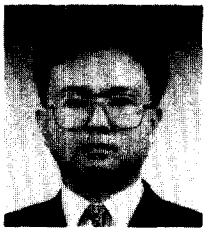
13. 한국전자통신연구소, "현대 암호학", 한국전자통신연구소, pp.125-132, 1991.

14. Michael Bertilsson, F. Brickell, "Cryptanalysis of Encryption Based on Space-Filling Curves", EUROCRYPT'89, 1989.

15. Mineo Shigemitsu, Toshikazu Miyasaki, Kenichi Matsumodo, "Encryption System for Facsimile Transmissions", 信學技報, ISEC89-41, 1989.

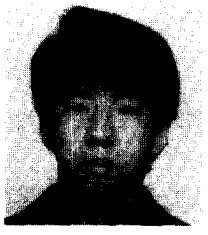
16. Seiichi Namba, "Information Security in Broadcasting", 信學技報, ISEC89-35, 1989.

□ 著者紹介



이 경 호(정 회 원)

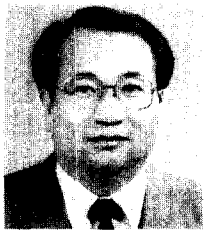
1991년 성균관대학교 정보공학과 졸업(공학사)
1993년 성균관대학교 대학원 정보공학과 졸업(공학석사)
1993년~현재 : 성균관대학교 대학원 정보공학과 박사과정



정 지 원(정 회 원)

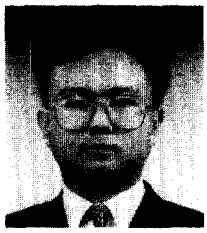
1989년 성균관대학교 전자공학과 졸업(공학사)
1990년 성균관대학교 대학원 전자공학과 졸업(공학석사)
1990년 11월~1992년 1월 : 금성정보통신연구소 연구원
1992년~현재 : 성균관대학교 대학원 정보공학과 박사과정

원 동 호(종신회원)



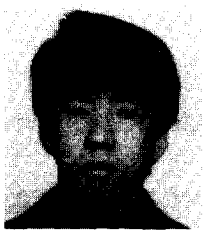
1976년 성균관대학교 전자공학과 졸업
1978년 성균관대학교 대학원 졸업
1978년~1980년 한국전자통신연구소 연구원
1985년~1986년 일본 동경공대 객원연구원
1988년 성균관대학교 공학박사
1982년~현재 : 성균관대학교 정보공학과 조교수, 부교수, 교수

□ 著者紹介



이 경 호(정 회 원)

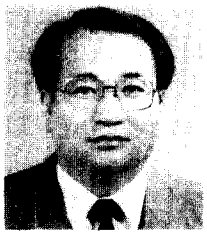
1991년 성균관대학교 정보공학과 졸업(공학사)
1993년 성균관대학교 대학원 정보공학과 졸업(공학석사)
1993년~현재 : 성균관대학교 대학원 정보공학과 박사과정



정 지 원(정 회 원)

1989년 성균관대학교 전자공학과 졸업(공학사)
1990년 성균관대학교 대학원 전자공학과 졸업(공학석사)
1990년 11월~1992년 1월 : 금성정보통신연구소 연구원
1992년~현재 : 성균관대학교 대학원 정보공학과 박사과정

원 동 호(종신회원)



1976년 성균관대학교 전자공학과 졸업
1978년 성균관대학교 대학원 졸업
1978년~1980년 한국전자통신연구소 연구원
1985년~1986년 일본 동경공대 객원연구원
1988년 성균관대학교 공학박사
1982년~현재 : 성균관대학교 정보공학과 조교수, 부교수, 교수