Journal of Korea Multimedia Society Vol. 10, No. 11, November 2007(pp. 1417-1426)

DPSS(Discrete Prolate Spheroidal Sequence)를 이용한 영상 스크램블링 방식의 개선 및 디지털 워터마킹 응용

이혜주[†], 남제호[††]

요 약

멀티미디어 콘텐츠를 보호하기 위해 연구되고 있는 방법 중에서 선택암호화(selective encryption) 방식은 멀티미디어 콘텐츠를 부분적으로 암호화하는 방법으로 AES와 같은 전통적인 암호방식을 적용하는 방법과 비교하여 보안성은 떨어지지만 높은 보안성을 요구하지 않는 멀티미디어 콘텐츠 응용 분야에 적용될 수 있다. 본 논문에서는 DPSS(discrete prolate spheroidal sequence)를 이용하여 영상의 대역폭(bandwidth) 확장 없이 영상을 스크램블하는 Van De Ville의 방식과 이에 대한 보안성을 검증한 Shujun Li의 연구를 기초로 하여 영상을 보다 안전하게 스크램블하기 위한 개선 방법을 제안하였다. 제안 방식은 비밀행렬 구성 시에 Hadamard 행렬 대신에 랜덤행렬을 이용하고, 통계적 특성과 비밀 행렬에 대한 예측에 의한 통계적 공격이나 기지평문공격에 대해 랜덤행렬을 가산하여 영상에 대한 랜덤성을 증가시켜 공격에 대한 보안성을 높이고자 하였다. 실험 결과들로부터 기존의 방법에 비해 각 공격에 대해 MAE(mean absolute error)의 값이 각각 25, 15, 80 이상 증가되어 보안성이 증가됨을 확인하였다. 또한 제안 방식은 워터마크 응용에 적용하여 접근 제어나 복사 제어에 적용할 수 있음을 제시하였다.

Improvement of Image Scrambling Scheme Using DPSS(Discrete Prolate Spheroidal Sequence) and Digital Watermarking Application

Hyejoo Lee[†], Jeho Nam[††]

ABSTRACT

As one of schemes to protect multimedia content, it is the selective encryption scheme to encrypt partially multimedia content. Compared AES(advanced encryption standard) of traditional encryption, the selective encryption scheme provides low security but is applicable to applications of multimedia content not to require high secrecy. In this paper, we improve the image scrambling scheme proposed by Van De Ville which scrambles an image without bandwidth expansion using DPSS(discrete prolate spheroidal sequence) to make it more secure based on Shujun's research which verifies the secrecy of Van De Ville's scheme. The proposed method utilizes an orthonormalized random matrix instead of Hadamard matrix for secret matrix and to add it for providing high secrecy against statistical attack or known-plaintext attack using some statistical property or estimate of secret matrix from a scrambled image. The experimental results show that the proposed method is more secure than the existing scheme. In addition, we show that the proposed method can be applied to access control or copy control of watermarking application.

Key words: Image scrambling(영상 스크램블링), Selective Encryption(선택암호화), Digital watermarking(디지털 워터마킹)

※ 교신저자(Corresponding Author) : 이혜주, 주소 : 부산광역시 남구 대연3동 21세기센츄리빌딩 916호실(608-743), 전화 : 051)610-0654, FAX : 051)610-0655, E-mail : iamhj@paran.com

접수일 : 2007년 9월 3일, 완료일 : 2007년 10월 5일

[†] 준회원, 모빌리존

[††] 정회원, 한국전자통신연구원 전파방송연구단 방송미디어연구그룹
(E-mail : namjeho@etri.re.kr)

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 신성장동력핵심기술개발사업의 일환으로 수행하였음. [2007-S-003-01, 지상파DTV 방송프로그램 보호 기술개발]

1. 서 론

멀티미디어 콘텐츠의 사용이 증가함에 따라 콘텐츠를 보호하기 위한 여러 가지 방법들이 제안되어 왔다. 이러한 방법으로 AES(advanced encryption standard)와 같은 전통적인 암호화 기법을 적용하여 복호키를 가진 사용자들에게만 콘텐츠에 대한 접근을 허용하는 방법에서부터 저작권 정보를 멀티미디어 콘텐츠에 삽입하여 저작권을 보호하는 방법인 디지털 워터마킹 기법들을 예로 들 수 있다[1-5]. 전자와 같은 방법은 멀티미디어 콘텐츠를 가장 안전하게 보호할 수 있으나 멀티미디어 콘텐츠를 압축하고 암호화해야 하기 때문에 처리속도가 증가되는 단점이 있다. 이러한 문제를 해결하기 위해 멀티미디어 콘텐츠를 부분적으로 암호화하는 선택 암호화(selective encryption) 방식이 제안되어졌다[4-5]. 선택 암호화 방식은 부호 비트(sign bits), 헤더(header), DCT 혹은 wavelet 계수 중의 일부만을 선택적으로 암호화하는 방법으로 전통적 암호화 방법과 비교하여 보안성은 떨어지지만 상대적으로 높은 보안성을 필요로 하지 않는 멀티미디어 콘텐츠 응용 분야에 적용할 수 있어 다양한 방식의 선택 암호화가 제안되어 왔다.

본 논문에서는 오디오에 적용한 Wyner의 방식[6]을 2D 영상에 확장 적용한 Van De Ville의 방식인 DPSS(discrete prolate spheroidal sequence)를 이용한 영상 스크램블링 방법(이하 DPSS 방식)[7]과 이에 대한 보안성(secrecy)을 검증한 Shujun Li의 논문[8]을 기초로 하여 DPSS 방식의 개선과 디지털 워터마킹에 응용한 영상 보호 방법을 제안한다. 먼저 2장에서는 Van De Ville의 DPSS 방식과 보안성에 대한 Shujun Li방식을 간략하게 기술한다. 그리고, 3장에서는 본 논문에서 제안하는 방식에 대해 기술하고, 4장에서는 제안방식의 실험 및 결과를 보이고자 한다. 마지막으로 5장에서는 제안 방식에 대한 문제점 및 향후 과제에 대해 논의한다.

2. DPSS를 이용한 영상 스크램블링 방식

Van De Ville가 제안한 DPSS를 이용한 영상 스크램블링 방식은 Slepian에 의해 알려진 주어진 주파수 밴드(frequency band) $[-W,W]$, $0 \le W \le \frac{1}{2}$에 대해 행렬

$$\mathbf{V} = \left[\frac{\sin(2\pi W(m-n))}{\pi(m-n)} \right]_{0 \le m,n \le N-1} \quad (1)$$

의 고유벡터(eigenvector) $\{\phi_j\}_{j=0}^{N-1}$, $\phi_j = \lfloor \phi_j(0), \cdots \phi_j(N-1) \rfloor$인 정규직교 기저(orthonormal basis)를 생성하는 DPSS(discrete prolate spheroidal sequence)를 이용하여 다음과 같이 영상을 스크램블링하는 방식이다. 즉, DPSS를 $S=[\phi_0 \cdots \phi_{N-1}]^T$ 라고 하면 영상신호 a와의 행렬곱(matrix multiplication)인 α에 대해 비밀 행렬(secret matrix) M을 이용하여

$$a' = S^T M a = S^T M S a, \text{ 단 } a = Sa \quad (2)$$

와 같이 영상을 스크램블링하게 된다. 이때 비밀 행렬 M은 스크램블링을 위한 비밀키가 된다. Van De Ville의 DPSS 방식은 $k \times k$ Hadamard 행렬 H에 대해 비밀행렬을

$$\mathbf{M} = \frac{1}{\sqrt{k}} \mathbf{P}_r \mathbf{H} \mathbf{P}_c, \quad (3)$$

와 같이 정의하고 있다. 이 때 P_r과 P_c는 M의 보안성을 높이기 위한 Hadamard 행렬 H의 행과 열을 치환(permutation)하기 위해 이용된다. 복호화 과정은 스크램블링된 신호 a′에 대해 S와 M의 역변환(inverse transform)을 이용하여 간단하게 복호할 수 있다. 이 과정을 레벨 L=256을 갖는 평문 영상(plain-image)의 $N_1 \times N_2$ 블록 I에 적용하면 스크램블링된 블록 I'는

$$I' = \text{round}\left(\frac{M(I - L/2)}{\gamma} + L/2 \right), \text{ 단 } M = S^T M S \quad (4)$$

와 같이 처리하여 얻을 수 있다. 이때 $\gamma = \max_n \left(\sum_{j=0}^{N_1 N_2 - 1} |M_{n,j}| \right)$으로 설정하여 스크램블된 블록 값의 영역(range)을 조정한다. 복호화 과정은 식(4)로부터

$$\hat{I} = \text{round}(M^T(\gamma (I' - L/2)) + L/2) \quad (5)$$

와 같이 수행하여 복호화된 영상 $\hat{I}$를 얻을 수 있다.

Shujun Li 등은 DPSS 방식의 보안성(secrecy)을 검증하기 위해 4가지의 암호 해독(cryptanalysis) 방법을 수행하여 표 1과 같은 결과를 제시하였다[8].

표 1에 나타난 바와 같이 블록마다 키를 변경하는 경우(change_key=1)에 대해 암호문 공격을 제외한 모든 공격에 충분한 보안성을 제공해 주지 않음을 검증하였다. 특히, 비밀행렬로 Hadamard 행렬 H의

표 1. DPSS 방식의 보안성 결과[8]

분류		change_key=0	change_key=1
암호문공격 (ciphertext-only attack)	Error-concealment based attack	insecure	insecure
	랜덤 치환 해독	insecure	secure
	Hadamard key 비보안성	insecure	secure
기지평문공격		insecure	insecure
선택평문공격		insecure	insecure
선택암호문공격		insecure	insecure

행과 열의 치환 행렬 P_r과 P_c를 이용하는 경우 Shunjun Li는 행렬 H의 행과 열의 교환(swapping) 등 간단한 방법으로도 인식 가능할 정도의 복호 영상을 얻을 수 있음을 실험적으로 제시함에 따라 Hadamard 행렬의 행과 열의 치환만으로는 충분한 보안성을 제공할 수 없음을 검증하였다. 또한 기지평문 공격, 선택평문공격, 선택암호문 공격은 비밀정보 M에 대해 예측 오류(estimation error) $\Delta_M = \tilde{M}-M$을 최소화할 수 있는 파라메터 값을 예측하였다. 가령, 선택 평문 공격은 $I-L/2=sI$(I는 단위행렬)이라고 가정하여

$$|\Delta_{\mathbf{M}}(i,j)| = \left|\frac{\gamma\Delta_{\mathbf{I}}(i,j)}{s}\right| \le \frac{\gamma}{2|s|} \tag{6}$$

을 유도하였는데, 식(6)으로부터 $|s|$의 값이 최대인 경우, 즉 $s=-L/2$일 때 예측오류가 최소가 되어 효과적인 암호해독이 가능함을 제시하였다, 또한 선택암호문 공격에서는 $I'-L/2=sI$이라고 가정하고 효과적인 영상 해독이 가능한 경우를

$$|\Delta_{\mathbf{M}^T}| = \left|\frac{\gamma\Delta_{\mathbf{I}}}{s}\right| \le \frac{1}{2|s|\gamma} \tag{7}$$

와 같이 유도하여 s값의 변화에 따른 공격에 의해 $|s|=47$인 경우 가장 효과적인 공격이 가능함을 제시하였다.

DPSS 방식의 보안성은 비밀 행렬의 구성에 의존한다. 그러나, 비밀 행렬을 구성하는 Hadamard 행렬의 상관성과 식(4)의 처리과정에서 이용하는 고정 값 $L/2$에 의해 비밀 행렬을 예측 가능하게 만든다는 문제가 존재한다. 따라서 본 논문에서는 Hadamard 행렬의 상관성을 제거하고 고정값 대신에 랜덤 행렬(random matrix) R_M 을 이용하여 보안성을 향상시키는 방법을 제안한다.

3. 제안 방식

3.1 스크램블 처리

앞에서 기술한 바와 같이 랜덤성은 보안성과 밀접하다. 즉, 평문과 암호문간의 랜덤성이 높게 되면 암호 해독의 가능성이 낮아지므로 높은 랜덤성을 제공하는 것이 보안성 측면에서 바람직하다. 제안방식은 DPSS 방식에 랜덤성을 추가하기 위한 비밀행렬 M을 구성하기 위해 Hadamard 행렬 대신에 랜덤 행렬 R_M을 이용한다. 즉, 영상에 R_M을 가산하여 영상을 스크램블링함으로써 공격에 대한 보안성을 향상시키고자 한다.

원 영상 a에 대한 스크램블 시 랜덤 행렬 R_M을 이용하는 경우, 랜덤 행렬 R_M의 정규직교화 행렬 $\hat{\mathbf{M}}$을 비밀행렬로 하여 스크램블하게 된다. 따라서 원영상 a에 랜덤행렬 R_M을 가산하고 DPSS S와의 행렬곱 $\hat{a}=S(a+R_M)$에 대해서

$$\begin{aligned}\mathbf{a}' &= \mathbf{S}^T\hat{\mathbf{M}}\hat{\alpha} = \mathbf{S}^T\hat{\mathbf{M}}\mathbf{S}(\mathbf{a}+\mathbf{R}_M)\\ &= \mathbf{S}^T\hat{\mathbf{M}}\mathbf{S}\mathbf{a}+\mathbf{S}^T\hat{\mathbf{M}}\mathbf{S}\mathbf{R}_M\end{aligned} \tag{8}$$

와 같이 스크램블된다. 이때 랜덤 행렬은 PRNG (pseudo random number generator)에 의해 행렬 원소(element)가 범위 $[-r, r]$에서 무작위의 값을 갖는 행렬이 된다. 스크램블된 영상을 복호하기 위해서는 랜덤행렬의 복잡한 역행렬 계산이 필요하다. 따라서 주어진 랜덤행렬을 정규직교화하여 스크램블하는 것이 복호 시에 역행렬 계산 과정이 없앨 수 있다. 결과적으로 식(8)에 의하면 최종 스크램블된 영상 a′은 스크램블된 원 영상과 스크램블된 랜덤 행렬 R_M을 결합한 결과와 동일하다. 복호 영상 $\hat{\mathbf{a}}$는 S와 $\hat{\mathbf{M}}$의 역변환을 이용하여

$$\begin{aligned}\hat{\mathbf{a}} &= \mathbf{S}^T\hat{\mathbf{M}}^{-1}\mathbf{S}\mathbf{a}' = \mathbf{S}^T\hat{\mathbf{M}}^{-1}\mathbf{S}\left(\mathbf{S}^T\hat{\mathbf{M}}\mathbf{S}(\mathbf{a}+\mathbf{R}_M)\right)\\ &= \mathbf{S}^T\hat{\mathbf{M}}^{-1}\mathbf{S}\left(\mathbf{S}^T\mathbf{M}\mathbf{S}\right)\mathbf{a}+\mathbf{S}^T\hat{\mathbf{M}}^{-1}\mathbf{S}\left(\mathbf{S}^T\hat{\mathbf{M}}\mathbf{S}\right)\mathbf{R}_M\\ &= \mathbf{a}+\mathbf{R}_M\end{aligned} \tag{9}$$

와 같이 수행하여 구하여진다. 결국 식(9)로부터 원 영상 a를 얻기 위해서는 정확한 랜덤 행렬 R_M을 알고 있어야만 복호화가 가능함을 알 수 있다.

3.2 워터마킹 응용

랜덤 행렬 R_M을 영상에 대한 접근을 제어하거나 복사방지를 위한 워터마크 응용에 이용 가능하다. 일반적으로 워터마크 검출 과정은 그림 1과 같이 워터마크를 삽입한 후 암호화를 수행하고, 워터마크 검출은 복호화를 수행한 후에 이루어지게 된다.

그러나, DPSS 방식은 다음과 같이 워터마크를 삽입한 후 암호화를 수행하고, 복호화를 수행하지 않고 바로 워터마크를 검출할 수 있는 구조를 가질 수 있다.

즉, 그림 2와 같이 복호화 없이 워터마크 검출이 가능하고, 정확한 워터마크 검출이 이루어지지 않으면 영상의 복호화를 수행할 수 없게 한다. 따라서 워터마크의 정확한 검출 없이 복호된 영상으로의 접근을 허용하는 기존의 방법과 비교하여 콘텐츠 보호를 위한 이중의 장치를 제공할 수 있다. 이러한 과정이 가능한 이유는 다음과 같다. 식(8)의 구조를 살펴보면 스크램블된 영상 a′은 스크램블된 영상과 스크램블된 램덤행렬의 합으로 구성된다. 이러한 구조는 워터마킹 방식 중에서 영상에 워터마크를 가산하는 가산적 워터마킹(additive watermarking) 기법과 유사한 구조이다. 따라서, 제안 방식에 의한 워터마크 검출은 그림 3과 같이 그림 3과 같이 랜덤 행렬 R_M을 DPSS 방식으로 스크램블링하고 스크램블된 영상 a′과 R'_M을 워터마크 검출기(watermark detector)의 입력으로 하여 상관값 c 를 계산하여 워터마크를 검출한다.

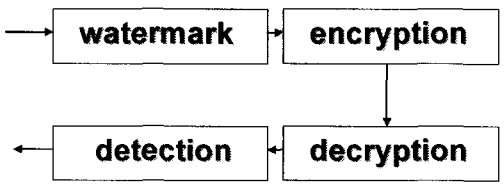


그림 1. 일반적인 워터마크 검출 순서

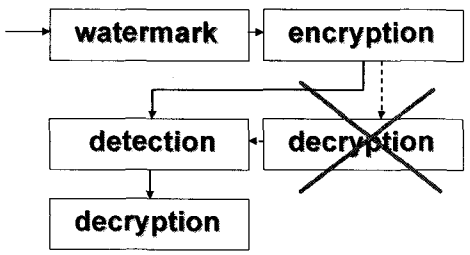


그림 2. 제안방식에서의 워터마크 검출 순서

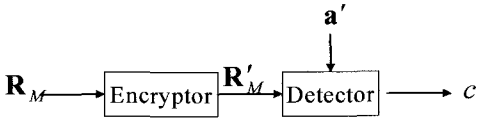


그림 3. 랜덤행렬을 이용한 워터마크 검출

따라서 그림 3의 과정처럼 워터마크 검출을 위한 상관값 c를 검증하여 워터마크가 존재하면 식(9)를 이용하여 영상의 복호과정을 수행하게 된다.

4. 실험 및 결과

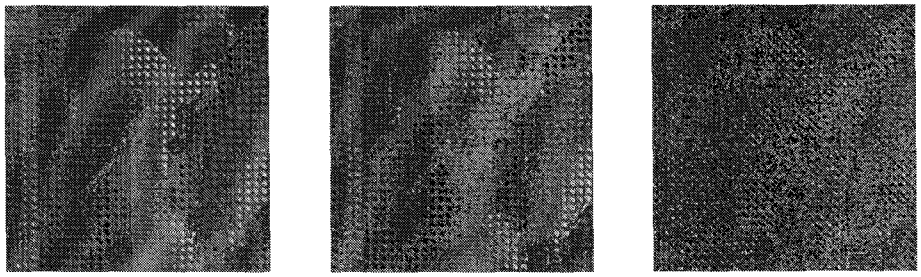
그림 4와 같은 2개의 영상 'Lena'와 'Cameraman' (256×256, 256레벨)을 실험영상으로 제안방식을 검증하였다.

파라메터의 값은 각각 L=256, γ=3으로 설정하고, 3가지 방식에 대해 실험하였다. 방식Ⅰ은 기존 DPSS 방식인 비밀행렬 구성에 Hadmard 행렬을 이용하고 $L/2$을 이용하는 경우이며, 방식Ⅱ는 비밀 행렬 구성시 Hadamard 행렬을 이용하고, 랜덤 행렬 R_M을 $L/2$ 대신에 이용하는 경우, 방식Ⅲ은 랜덤 행렬 R_M을 비밀행렬 구성과 $L/2$ 대신에 이용하는 경우의 각각에 대해 실험하였다. 이때 랜덤행렬은 평균이 0이고 분산이 1인 실수로 실험적으로 [-15,15]의 범위 내의 값으로 구성한다. 실험에서는 영상의 스크램블과 복호 및 공격의 효과를 측정하기 위한 척도로 원 영상과 결과 영상들 간의 MAE(mean absolute error)를 이용한다. 랜덤행렬 R_M을 이용하여 스크램블링 및 복호화 과정을 영상 I에 대해 식(4)와 식(5)의 형태로 나타내면

스크램블링 과정:

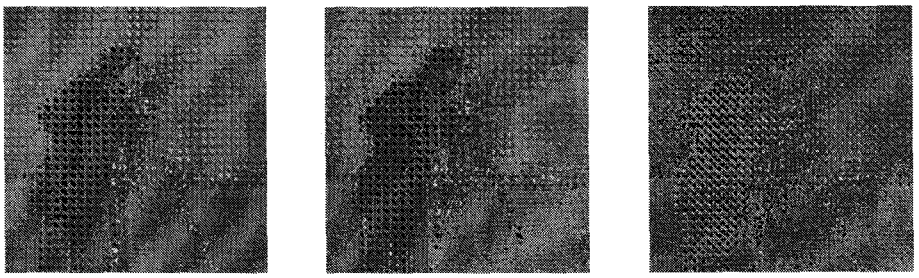
$$I' = \text{round}\left(\frac{\hat{M}(I - L/2 - R_M)}{\gamma} + L/2 + R_M\right) \tag{10}$$

그림 4. 원영상 Lena 및 Cameraman



(a) 방식 I (b) 방식 II (c) 방식 III

그림 5. 스크램블 영상(Lena)



(a) 방식 I (b) 방식 II (c) 방식 III

그림 6. 스크램블 영상(Cameraman)

복호화 과정:

$$\hat{I} = \text{round}\left(\hat{M}^T\left(\gamma\left(I' - \tfrac{1}{2} - R_M\right)\right) + \tfrac{L}{2} + R_M\right) \quad (11)$$

와 같이 표현할 수 있다. 단, $\hat{M} = \mathbf{S}^T\hat{\mathbf{M}}\mathbf{S}$ 이다.

4.1 스크램블 결과

그림 5는 영상 'Lena'에 대해 각 3가지 방식을 적용한 경우의 스크램블 영상을 순서대로 나타내고 있다.

그림 5에 나타난 바와 같이 DPSS방식에서의 고정값 $L/2$의 가산과 비밀행렬 구성시 Hadamard 행렬을 이용한 경우보다 랜덤행렬을 이용한 스크램블 영상이 시각적으로 효과있게 스크램블되었음을 확인할 수 있다. 이러한 결과는 'Cameraman'에 대해서도 그림 6에 나타난 바와 같이 유사한 결과를 확인할 수 있다.

그림 7은 방식III에 의해 얻어진 그림 5(c), 그림 6(c)를 복호하여 얻어진 복호 영상으로 각각의 MAE는 각각 0.6880, 0.7247로 측정되었다. 그림 7의 복호 영상은 방식 I 과 방식III의 복호 영상에 비해 MAE는 저하되나 시각적으로 많은 차이가 나타나지 않는다.

표 2는 각 실험에 대한 스크램블 영상 및 복호 영상의 MAE를 측정하여 나타낸 표로써 랜덤행렬 이용 시 높은 MAE를 제공함에 따라 스크램블 효과가 있음을 알 수 있다.

(a) 'Lena'의 복호 영상 (b) 'Cameraman'의 복호 영상

그림 7. 제안방식에 의한 복호영상

표 2. 스크램블 영상 및 복호 영상의 MAE

		스크램블영상	복호 영상
Lena	방식III	39.2561	0.6880
	방식II	33.8636	0.6873
	방식 I	32.5593	0.6881
Camera-man	방식III	49.4329	0.7247
	방식II	42.5811	0.6915
	방식 I	41.5796	0.6902

방식Ⅲ에 의해 스크램블된 영상은 원래의 랜덤행렬이 아닌 다른 랜덤 행렬을 이용하여 영상을 복호할 수 없어야 한다. 즉, 정확한 행렬의 역변환이 수행되지 않기 때문이다. 따라서, 그림 5(c)를 다른 랜덤행렬로 복호 하였을 때 그림 8과 같이 영상의 복호가 이루어지지 않는다.

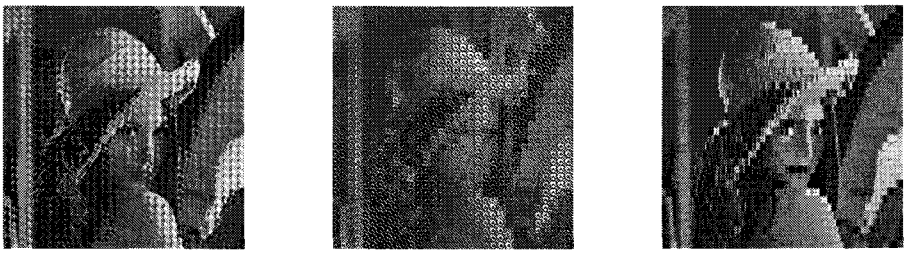
4.2 JPEG 압축Z

일반적으로 영상은 JPEG과 같은 손실 압축 과정에 의해 압축된다. 제안방식에 의해 스크램블된 영상을 JPEG 압축을 수행하고 복호하였을 경우 그림 9와 같이 화질 저하가 발생되었다

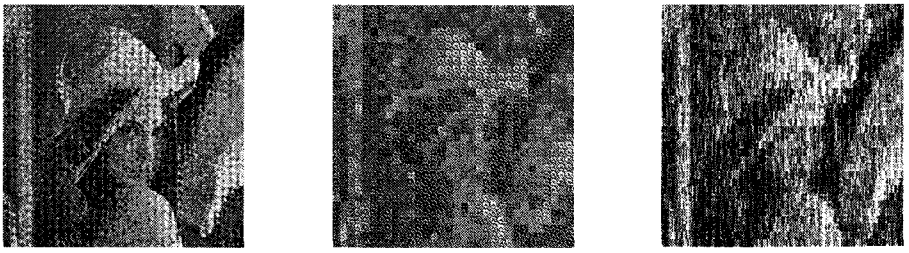
JPEG 압축 후 복호 영상의 화질 저하는 JPEG 압축의 양자화 과정에 의해 발생된다. 이로 인해 JPEG 압축된 스크램블 영상을 복호(decryption)하는 경우 정확한 랜덤행렬로 복호 처리를 수행하였다 하더라도 복호 영상의 화질은 떨어지게 된다. 특히 표 3의 결과에 의하면 제안 방식은 랜덤행렬의 가산에 의해

그림 8. 다른 비밀행렬에 의해 복호된 영상

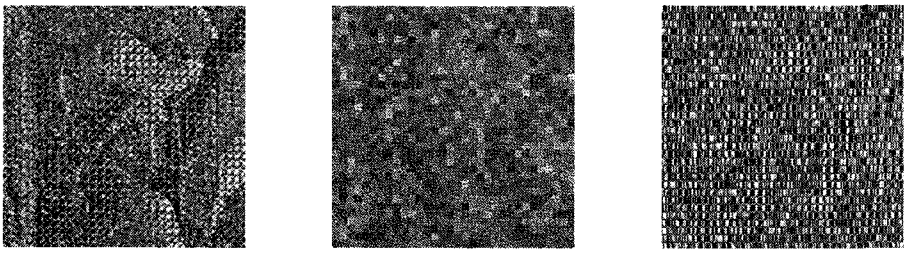
그림 9. JPEG 압축 후의 복호영상 (품질계수: 75%, MAE:17.7320)



(a) 방식Ⅰ 에 대한 스크램블 영상의 공격영상 : 치환공격(좌), 통계적 공격(중), 기지평문공격(우)



(b) 방식Ⅱ 에 대한 스크램블 영상의 공격영상 : 치환공격(좌), 통계적 공격(중), 기지평문공격(우)



(c) 방식Ⅲ 에 대한 스크램블 영상의 공격영상 : 치환공격(좌), 통계적 공격(중), 기지평문공격(우)

그림 10. 공격 영상(Lena)

표 3. JPEG 압축 후 측정된 MAE

	방식Ⅲ	방식Ⅱ	방식Ⅰ
Lena	17.7320(6.6465)	17.6945	6.0384
Cameraman	17.0763(7.6151)	17.0629	7.1412

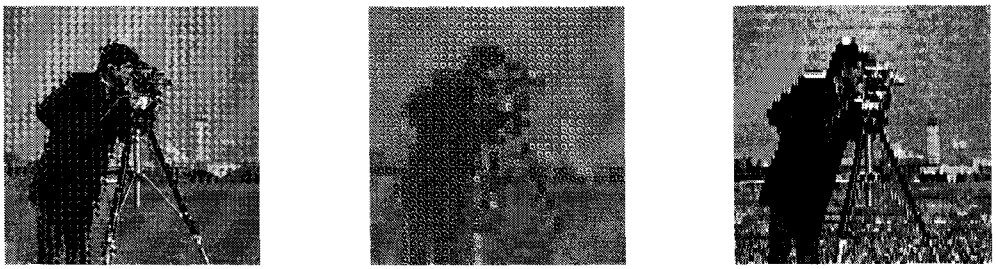
오차가 더욱 커지기 때문에 DPSS 방식에 비해 화질 저하가 많이 발생된다(표 3의 방식Ⅲ에서의 괄호는 랜덤행렬을 가산하지 않은 경우의 MAE 값이다).

따라서 랜덤성의 제공하는 랜덤행렬을 이용하기 위해 JPEG 압축에 대한 영향을 감소하기 위한 방법이 요구된다.

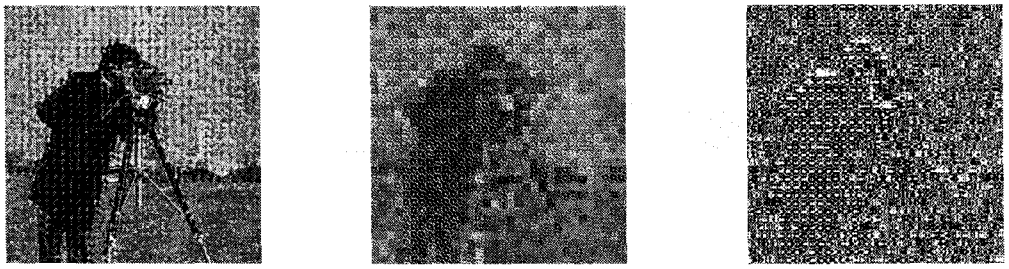
4.3 공격

스크램블된 영상에 대한 공격은 (1) 비밀 행렬의 1행과 8행의 위치를 바꾸어 복호한 경우(치환공격), (2) Shunjun에 의해 제안된 통계적 공격법으로 스크램블된 블록 계수 중 $\alpha_0 = 2.8\alpha_8$ $\alpha_4 = \alpha_5 = 1.68\alpha_8$, $\alpha_1 = \alpha_3 = \alpha_6 = \alpha_7 = 0$ 로 설정하여 비밀행렬 없이 복호한 경우(통계적 공격), (3) 기지평문공격(known-plainttext attack)의 방법을 이용하였다. 그림 10의 'Lena'에 대한 공격에서도 Hadamard 행렬을 이용한 경우에 비해 정규직교화와 랜덤행렬을 함께 이용한 경우가 공격에 대한 보안성을 제공함을 알 수 있다.

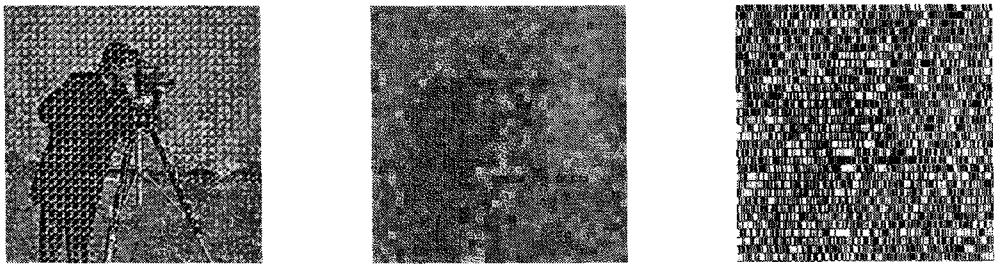
그림 11은 실험영상 'Cameraman'에 대한 공격영상들을 나타내고 있다. 실험결과에서 'Lena'보다 'Cameraman'의 경우가 스크램블 성능과 공격에 대한 보안성이 떨어짐을 확인할 수 있는데, 그 이유는 영상의 특성상 'Cameraman'의 복잡도가 'Lena'에 비해 높지 않기 때문이다. 따라서, 영상의 특징에 따라 스크램블 방식을 적용할 필요가 있다.



(a) 방식Ⅰ 에 대한 스크램블 영상의 공격영상 : 치환공격(좌), 통계적 공격(중), 기지평문공격(우)



(b) 방식Ⅱ 에 대한 스크램블 영상의 공격영상 : 치환공격(좌), 통계적 공격(중), 기지평문공격(우)



(c) 방식Ⅲ 에 대한 스크램블 영상의 공격영상 : 치환공격(좌), 통계적 공격(중), 기지평문공격(우)

그림 11. 공격 영상(Cameraman)

표 4. 공격영상에 대한 측정 MAE

		치환공격	통계적 공격	기지평문 공격
Lena	방식Ⅲ	41.5668	51.7796	101.0905
	방식Ⅱ	31.4902	46.9749	98.3720
	방식Ⅰ	15.9478	36.7116	19.3226
Camera-man	방식Ⅲ	45.5008	58.2751	117.0111
	방식Ⅱ	31.4370	51.6316	96.1045
	방식Ⅰ	17.4108	43.1096	26.1031

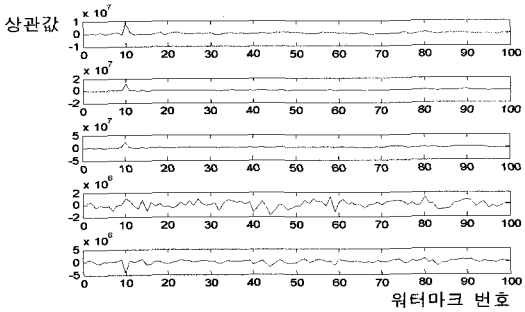
표 4는 각 결과 영상들에 대해 공격에 대한 보안성을 확인하기 위해 측정한 MAE(mean absolute error) 들을 나타내고 있다.

표 4에 나타난 바와 같이 방식Ⅲ을 이용하는 경우가 스크램블 결과나 공격에 대한 보안성이 방식Ⅰ이나 방식Ⅱ보다 더 효과적임을 알 수 있다.

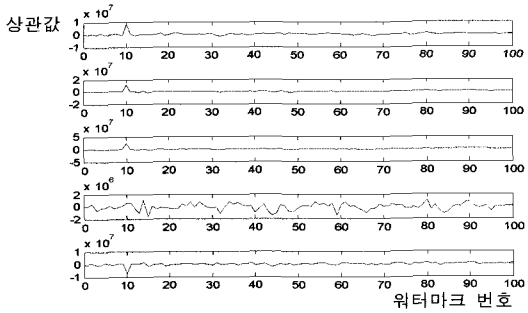
4.4 워터마크 검출

제안 방식의 워터마크 응용은 앞에서 기술한 바와 같이 스크램블 영상에서 워터마크 검출을 수행하여 워터마크가 검출된 경우에만 복호 수행하도록 하는 접근 제어에의 응용할 수 있다. 즉, 스크램블 영상과 JEPG 압축된 영상에서 워터마크가 검출되면 복호 과정을 수행한다. 본 실험에서는 간단하게 비밀행렬 구성에 이용한 랜덤행렬을 워터마크로 이용하여 실험하였다. 워터마크 검출은 워터마킹 기법의 하나인 대역확산(spread-spectrum) 기법을 적용하여 스크램블된 영상과 랜덤 행렬간의 상관(correlation)을 계산하여 워터마크를 검출한다. 그림 12는 방식Ⅲ으로 스크램블된 그림 5(c), 그림 6(c)와 그림 10, 그림 11의 공격영상들에 워터마크 검출을 수행한 결과로 100개의 서로 다른 워터마크(랜덤행렬)과 스크램블시 이용된 워터마크(10번째 랜덤행렬)과의 상관값을 나타내고 있다.

그래프는 위에서부터 스크램블 영상, JPEG 압축된 영상, 그리고 치환공격, 통계적 공격, 기지평문공격에 의한 공격영상들에 대한 워터마크 검출 결과로, 스크램블 영상, JPEG 압축된 영상, 치환 공격 영상에서 삽입된 워터마크(10번째)가 검출됨을 알 수 있다. 그림 12의 결과에서 치환 공격 영상에서 워터마크 검출이 가능함으로써 치환 공격이 강한 공격임을 의미하는데, 방식Ⅲ의 경우 정확한 랜덤행렬을 모를 경우에 그림 13과 같은 치환 공격 영상을 얻게 된다(MAE=50.5621). 따라서, 제안 방식에 대해서는 성공적인 치환 공격이 가능하지 않음을 알 수 있다.



(a) 영상 'Lena'에 대한 워터마크 검출



(b) 영상 'Cameraman'에 대한 워터마크 검출

그림 12. 워터마크 검출 성능

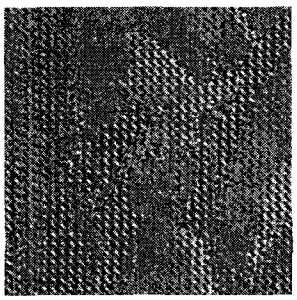


그림 13. 다른 비밀행렬을 이용한 경우의 치환공격

위와 같이 워터마크 검출이 성공적으로 이루어진 후에 영상에 대한 접근을 허용함으로써 영상에 대한 접근을 제어할 수 있으며, 이는 영상의 복사 제어에도 응용할 수 있다. 즉, 정확한 비밀행렬로 복호된 영상은 워터마크 검출이 되지 않기 때문에 복사 방지 시스템이 있는 장치에서는 워터마크 검출이 되지 않으면 복사를 허용하지 않도록 하여 복호된 영상의 유출을 방지할 수 있다.

5. 결 론

멀티미디어 콘텐츠를 보호하기 위해 AES와 같은 전통적 방법을 이용하여 암호화를 수행하는 것이 가장 보안성이 높은 방법이기는 하지만 많은 비용이 요구되기 때문에 콘텐츠를 부분적으로 선택하여 암호화하는 방법이 다양한 분야에서 이용되는 콘텐츠를 보호하는데 더 적합할 수 있다. 이것이 선택 암호화(혹은 스크램블) 방법들이 계속 연구되고 있는 이유라고 할 수 있다.

본 논문에서는 DPSS를 이용하여 대역폭의 확장없이 영상을 스크램블하는 Van De Ville의 방식과 이에 대한 보안성을 검증한 Shujun의 연구를 기초로 하여 영상을 보다 안전하게 스크램블하기 위한 개선 방법을 제안하였다. 제안 방식은 비밀행렬 구성시에 Hadamard 행렬 대신에 랜덤행렬을 이용하고 이를 정규화하여 단순한 행과 열의 치환 공격에 대한 보안성을 향상시켰으며, 통계적 특성과 비밀 행렬에 대한 예측에 의한 통계적 공격이나 기지평문공격에 대해 랜덤행렬을 가산하여 영상에 대한 랜덤성을 증가시켜 공격에 대한 보안성을 높이고자 하였다. 이에 기존의 방법보다 공격에 대한 보안성이 증가됨을 실험적으로 확인하였다. 또한 워터마크 응용에 적용하여 접근 제어나 복사 재어에 적용할 수 있음을 제시하였다. 향후의 연구 과제로 제안 방식에서는 단순히 랜덤행렬을 워터마크로 이용하였으나 JPEG 압축에 대한 강인성을 제공하고 랜덤성을 제공하기 위해 새로운 워터마크를 생성하는 방법을 고려하여야 할 것이다.

참 고 논 문

[1] W. Zeng, H. Yu, and C-Y Lin, *Multimedia Security Technologies for Digital Rights Management*, ACADEMIC PRESS, 2006.

[2] H. T. Sencar, M. Ramkumar, and A. N. Akansu, *Data Hiding Fundamentals and Applications: Content Security in Digital Multimedia*, Elsevier, 2004.

[3] I. Cox, M. Miller, and Jeffrey Bloom, *Digital Watermarking: Principles & Practice*, MOGAN KAUFMANN PRESS, 2001.

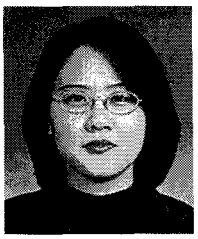
[4] A. Uhl and A. Pommer, *Image and Video Encryption From Digital Rights Management to Secured Personal Communication*, Springer, 2005.

[5] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," *IEEE Trans. on Multimedia*, Vol.5, pp. 118-129, Mar. 2003.

[6] A. D. Wyner, "An analog scrambling scheme which does not expand bandwidth, Part I: Discrete time," *IEEE Trans. on Information Theory*, Vol. IT-25, pp. 261-274, May 1979.

[7] D. Van De Ville, W. Philips, R. Van De Walle, and I. Lemahieu, "Image Scrambling Without Bandwidth Expansion," *IEEE Trans. on Circuits and Systems for video technology*, Vol. 14, No. 6, pp. 892-897, June 2004.

[8] S. Li, C. Li, K. Lo, and G. Ghen, "Cryptanalysis of an Image Scrambling Scheme without Bandwidth Expansion," http://eprint.iacr.org/2006/215.pdf, 2006.



이 혜 주

1994년 부경대학교 전자계산학과(이학사) 졸업
1997년 부경대학교 대학원 전자계산학과(이학석사) 졸업
2000년 부경대학교 대학원 전자계산학과(이학박사) 졸업
2000년~2001년 한국정보통신대학교 박사후 연구과정생
2001년~2005년 한국전자통신연구원 디지털방송연구단 선임연구원
2005년~2006년 경성대학교 멀티미디어대학 컴퓨터정보학부 초빙교수
2006년~현재 모빌리존 개발팀장
2007년~현재 한국전자통신연구원 전파방송연구단 방송미디어연구그룹 방통융합콘텐츠보호연구팀 초빙연구원
관심분야 : 디지털 콘텐츠 보호 및 관리, DRM, 디지털 워터마킹, 멀티미디어 처리 기술

남 제 호

1994년 홍익대학교 전기제어공학과(학사)

1997년 University of Minnesota, Dept. of Electrical Eng. (석사)

2000년 University of Minnesota, Dept. of Electrical Eng. (박사)

2001년~현재 한국전자통신연구원(ETRI) 방송미디어 연구그룹 선임연구원, 방통융합콘텐츠보호연구팀장

2007년~현재 과학기술연합대학원대학교(UST) 이동통신 및 디지털방송공학 겸임 부교수

관심분야 : 멀티미디어 신호처리, 디지털방송기술, MPEG, 콘텐츠 보호관리