영상 보안통신을 위한 적응적인 데이터 은닉 기술

정회원 서 영 호*, 김 수 민*, 종신회원 김 동 욱*

Adaptive Data Hiding Techniques for Secure Communication of Images

Young-Ho Seo*, Su-Min Kim* *Regular Members*, Dong-Wook Kim* *A Life Member*

요 약

본 논문에서는 대용량의 대역폭을 이용한 무선 데이터통신 장치들이 널리 보급됨에 따라 사용자들은 영상과 비디오 같은 풍부한 대중매체를 다양한 환경에서 더욱 많이 사용하게 되었다. 최근 컨텐츠들은 유료화 형태로 서비스되고 있고 컨텐츠 자체가 개인의 정보를 담고 있어 통신의 보안성을 유지할 필요성이 있다. 그러나 많은 계산양과 연산능력을 요구하는 기존의 보호 방식은 사용자원에 제약을 받는 이동통신 환경의 무선통신이나 내장형 기기들에는 적합하지 않다.

본 논문에서는 영상 데이터를 부분적으로 암호화하여 자원이 제한된 무선 통신에서 양방향으로 영상 데이터의 안전하고 효율적인 통신을 가능하게 하는 기술을 제안하고자 한다. 암호화 기법은 양자화를 통해 암호화 정보의 소실이 없으면서 영상의 압축비를 유지하기 위해서 양자화와 엔트로피 코딩 사이에서 수행되고 부대역의 선택, 데이터의 비트 선택, 그리고 데이터 비트 무작위 선택 등의 3가지 데이터 선택 방법을 제안하여 사용한다. 제안된 방법으로 안전한 통신을 위해서 다수의 영상에 적용하였고 추가적으로 제안된 방법이 무선 환경에서 사용되었을 경우에 대한 효율성 여부와 암호화하는 데이터양과 계산양의 상보적인 관계를 나타내었다.

영상에 대한 실험은 500가지 다양한 영상을 대상으로 수행하였는데 제안된 방법을 통한 암호화 율은 원 영상의 0.0244%에서 0.39%에 해당하고 암호화된 영상의 PSNR(peak signal to noise ratios)은 7.5dB에서 9.5dB 범위를 보였다. 또한, 시각적인 테스트를 통해서 적은 계산양으로 높은 암호화 효율을 얻을 수 있음을 확인하였다.

ABSTRACT

Widespread popularity of wireless data communication devices, coupled with the availability of higher bandwidths, has led to an increased user demand for content-rich media such as images and videos. Since such content often tends to be private, sensitive, or paid for, there exists a requirement for securing such communication. However, solutions that rely only on traditional compute-intensive security mechanisms are unsuitable for resource-constrained wireless and embedded devices.

In this paper, we propose a selective partial image encryption scheme for image data hiding , which enables highly efficient secure communication of image data to and from resource constrained wireless devices. The encryption scheme is invoked during the image compression process, with the encryption being performed between the quantizer and the entropy coder stages. Three data selection schemes are proposed: subband selection, data bit selection and random selection. We show that these schemes make secure communication of images feasible for constrained embed-ded devices. In addition we demonstrate how these schemes can be dynamically configured to trade-off the amount of ded devices. In addition we demonstrate how these schemes can be dynamically configured to trade-off the amount of data hiding achieved with the computation requirements imposed on the wireless devices.

Experiments conducted on over 500 test images reveal that, by using our techniques, the fraction of data to be encrypted with our scheme varies between 0.0244% and 0.39% of the original image size. The peak signal to noise ratios (PSNR) of the encrypted image were observed to vary between about 9.5dB to 7.5dB. In addition, visual test indicate that our schemes are capable of providing a high degree of data hiding with much lower computational costs.

*광운대학교 전자재료공학과 Digital Design & Test Lab.(ddntlab.kw.ac.kr, design@kw.ac.kr)

논문번호 : 030331-0801, 접수일자 : 1998년 6월 8일

※본 논문은 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신기초연구지원사업의 연구결과(과제번호 : 03-기초-0025)입니다.

Ⅰ. 서 론

무선 통신기술의 발전은 무선 환경에서 다양한 멀티미디어 데이터의 전송을 가능하게 하였다. 핸드폰, PDA 등의 일반적인 무선 통신기기와 함께 무선 감지기, 감시시스템, 의료시스템 등 무선기기들의 발전에 따라서 영상, 비디오, 그리고 오디오 데이터의 효율적인 처리와 전달을 위한 무선기술이 요구되고 있다. 이러한 무선 환경을 통한 데이터 통신이 이루어질 때에 특히나 중요시 되는 부분이 개인정보의 보호이다. 개인정보는 무선 채널을 통한 악의적인 도청 혹은 해킹을 통해서 유출될 수 있고 디지털 기술 기반의 멀티미디어 자체의 특성으로 인해서 다양한 경로를 통해서 유출될 수 있다. 그러나 무선 데이터통신 장비들이 가지는 이동성으로 인해서 장비 및 기기들은 경량화되어 있어 제한된 계산 능력과 배터리 용량을 가진다. 따라서 과거의 암호화 방법을 통해서 개인정보를 보호하기 위해 암호 알고리즘을 사용하는 것은 계산양이 너무 많아 무선 장치에 적당하지 않다. 또한 무선 네트워크들에서 사용되는 장치들은 자원의 상황에 따라(예를 들면, 남아있는 전력량, 무선 채널 상태) 암호화 하고자 하는 데이터를 처리하는 시간에 영향을 받게 된다. 이 특징들은 직/간접적으로 무선 환경에서 큰 영향을 받게 되고 멀티미디어 내용의 안전한 전송을 위해 계산 능률과 통신의 보안 사이의 상보적인 관계에 의한 기기와 암호화 기술의 개발이 중요하는 것으로 귀결된다.

지금까지 정보보안 분야의 응용은 대부분 인증(authentication)이나 전자서명(digital signture)과 관련되어 왔다. 요즈음 사용하고 있는 각 기업체의 전자서명 방식, 인터넷 뱅킹에서 인증절차, 신용카드 결제 절차 등이 모두 이들의 응용분야에 속한다. 정보보호 분야 또한 불법복제 방지 등을 위한 조치에 국한되어 사용되어 왔다. 인터넷의 발달, 네트워크의 다양화 및 관련 서비스의 증대 등으로 영상/비디오 컨텐츠의 사용은 이제 이러한 특별한 분야에 국한되지 못하고 있다. 즉, 이제는 우리가 상상할 수 있는 모든 영상/비디오 응용이 가능하고 또 상상 가능한 불법적인 행위들이 모두 가능한 상황에 이르렀다고 할 수 있다. 금전적인 배경을 가진 컨텐츠 뿐 아니라 흔히 사용하는 컨텐츠들(의료영상, 개인적 비디오, 감시시스템의 영상/비디오 등)이 대중화되고 상품화됨에 따라서 이들이 지니고 있는 개인적이고 기밀성을 요하는 정보들이 무방비로 누출되는 경우가 허다하며, 이것은 컨텐츠의 사용자 뿐 아니라 공급자에게도 매우 바람직하지 못한 일이다. 따라서 최근 정보보호 및 보안의 연구 및 업계의 동향은 보다 다양한 보안/보호 체제를 구비하는 방향으로 나아가고 있다[1]. 이러한 추세는 영상/비디오의 준비과정과 보안/보호 장치과정이 분리되던 과거와는 달리 이 과정들이 통합되어 수행되는 방법으로 추구하고 있으며, 영상/비디오를 캡쳐(capture)함과 동시에 전송되는 응용분야 등을 고려하여 이 통합동작이 실시간으로 이루어지는 것이 바람직하다는 것에 동의하고 있다. 영상/비디오 시장의 크기를 감안할 때 이들을 대상으로 하는 보호/보안 관련 시장의 규모는 이에 버금간다고 할 수 있으므로 이 분야와 관련된 업계의 움직임은 매우 활발하고 경쟁적이다. 특히 최근 정보가전 분야가 또 하나의 뜨거운 감자로 부상됨에 따라 무선통신에 대한 보호/보안은 그 연구개발이 현재 최고조에 달하고 있다.

이산 웨이블릿에 기반을 둔 JPEG2000/MJPEG2000의 사용 확대에 따라 자연히 보안/보호 연구도 이들을 기반으로 하는 시스템을 겨냥하는 경우가 늘어나고 있고, 향후 이들 기술의 확대에 따라 이러한 경우는 더욱 늘어날 전망이다[2][3]. 아직 영상/비디오 처리기술과 보안 및 보호 기술을 하나의 시스템으로 구현하는 연구는 세계적으로 이루어지지 않고 있으나, 각각의 솔루션들이 활발히 연구되고 있는 현재의 추세로 보면 조만간 토압 솔루션의 연구개발이 이루어질 것이며, 영상/비디오 처리 및 정보보안/보호의 통합 솔루션은 영상/비디오 응용분야의 기반 핵심부품의 선점이라는 의미에서 세계 굴지의 업체에서 이 분야에 대한 경쟁이 곧 시작될 것이라 전망할 수 있다.

최근에 무선 환경에서의 안전한 멀티미디어 통신 기술을 위한 응용 계층에서의 방법이 제안되고 있으며 이미 MPEG-4 [4]~[6]기반에 대한 연구는 상당부분 진행되어 왔다. 상대적으로 웨이블릿 기반의 영상처리 방법이 더욱 최근에 발전되고 있으므로 이 방법들에[7]~[12] 대한 보안 알고리즘 또한 초기 단계의 연구가 이루어지고 있다. [7]에서는 다른 2가지 방법으로 부분 암호화 방식을 제안하였고, [14]에서는 쿼드트리(quad-tree)를 기반으로 하는 SPHIT를 겨냥하여 암호화는 방법을 제안하였다. [8]과 [9]에서는 웨이블릿 변환 방식인 NSMRA (non-stationary multi-resolution analysis) 방법으로 각각 필터[8]와 트리구조 변환[9]을 통해 암호화를

수행하였는데 이러한 방법은 엔트로피 코딩의 하나인 산술 코딩을 목표로 하였다. [10]에서는 확률적인 암호화방법을 제안하고 [13]에서 그 방법을 개선시켰다. [11]에서는 EZW 방법을 제안하였는데 ATM 패킷 방법을 적용하여 암호화를 수행하였다. [12]에서는 데이터를 변형하지 않고 데이타 그 자체를 암호화하였다. 대신에 그것은 영상의 중요한 비트 평면을 암호화하여 원 영상에서 1/8에 해당하는 적은 양의 데이터를 암호화였다.

실제로 JPEG2000의 경우 Part 8에서 워터마킹과 영상암호화와 같은 기술을 적용한 JESEC(Secure JPEG2000)에 대한 표준화 과정이 현재 논의되어 2005년에 국제표준으로 제정한다는 계획을 가지고 있고 DRM(Digital right management)이나 MPEG-21등에서도 역시 다양한 방식으로 적용되고 있어 본 연구와 같이 프로토콜 레벨(Protocol level)이 아닌 어플리케이션 레벨(Application level)에서의 컨텐츠 보호 방식은 표준화에 대한 기여뿐만 아니라 다양한 분야에서 좋은 솔루션으로 제공될 수 있다.

본 논문에서는 무선 환경에서의 사용을 위해 계산량을 줄이면서 데이터를 효율적으로 은닉할 수 있는 영상 암호화 방법에 목표를 두었다. 본 논문에서 사용되는 암호화 방법은 DWT를 기반에서의 영상 압축 방법을 사용하였는데 이 방법은 암호화하는 데이터의 양과 계산양의 서로 상보적인 관계가 있고 안전한 영상 전송을 하기 위해 암호화하는 데이터의 양을 적응적으로 조절하여 다양한 환경에서 적용하는 것이 가능하다. 다음 장에서는 DWT를 이용한 영상압축방법과 DWT 결과 영상 및 그 데이터 구조에 대해서 설명하고, 본 논문에서 제안하는 부분영상 암호화를 위한 데이터 선택 방법과 선택된 데이터를 암호화하는 방법을 3장에서 설명한다. 4장에서는 제한한 방법에 대한 실험 결과를 보이고 마지막으로 5장에서는 본 논문의 결론을 맺는다.

Ⅱ. 이산 웨이블릿 변환과 웨이블릿 계수의 특성

DWT를 이용한 영상의 압축 및 복원과정은 간단히 그림 1과 같이 나타낼 수 있다. 영상이 2차원 데이터이기 때문에 DWT 또한 2차원(2차원 DWT, 2D DWT)으로 수행되는데, 가장 대표적인 수행방식인 Mallat-tree 방식을 사용한다[2]. 또한 Daubechies의 (9,7) 쌍직교 필터를 사용하는데, 이 경우 그림 2는 2D DWT후의 부대역들에 대한 결과를 나타내는데 LL4의 화소는 0에서 255사이의 값을, 나머지 부대역은 -256에서 255사이의 값을 갖는다. LL4의 경우 일반적으로는 정수부분은 양자화 대상에서 제외되는데 그 이유는 이 부대역의 정보는 매우 중요하고 많은 정보를 포함하고 있기 때문에 양자화과정에서 약간의 정보손실이 복원한 영상의 화질에 큰 영향을 미치기 때문이다. LL4 부대역 이 외의 영역은 일반적인 선형양자화 방식을 따라 양자화 과정을 거친다. 양자화 과정을 거친 데이터들은 데이터들이 가지는 계수분포가 흐트러지지 않는 방식으로 암호화되고 엔트로피 코딩을 거쳐서 압축과정을 마친다. 또한 복원과정은 그 역과정을 수행한다.

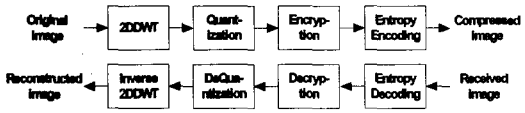


그림 6. DWT를 이용한 영상압축/복원

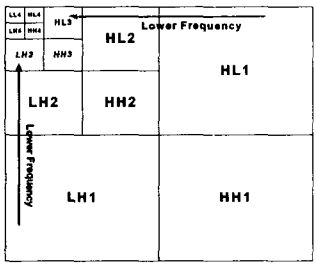


그림 7. 2D DWT 결과의 부대역

Ⅲ. 영상의 부분 암호화

본 장에서는 부분 암호화를 위한 데이터 선택과 암호화 방식에 대해서 설명한다.

Ⅲ-1. 부대역 조합의 선택

첫 번째 데이터 선택 방법은 부대역을 선택하는 것으로 LL4 부대역은 인간의 눈에 가장 큰 영향을 주는 중요한 에너지 성분을 포함하고 있으므로 부대역을 선택하는데 있어서 가장 우선이 되어야 하는 부대역은 LL4이다. 그러나 LL4 부대역의 암호화를 통해 영상을 다른 목적으로 사용할 수 없을 정도로 왜곡시킨다 하더라도 원 영상의 고주파 성분은 상당부분 남는다. 이러한 실험 결과를 기초로 본 논문에서는 부대역 선택에 있어 아래와 같이 4가지 방법을 제시한다.

① LL4 : only LL4
② LL4-HH4 : LL4 and HH4
③ Level 4 : all four subbands in level 4
④ Level 4-HH3 : all subbands in level 4 and HH3

그림 3에서 4가지 선택 방법에 대한 영상을 보여주고 있다. 그림 3의 (e)는 가장 좋은 암호화 효과를 보이고 있다. LL4만을 암호화한 영상(①의 경우, 그림 3의 (b))을 보면 고주파 성분이 남아 있음을 알 수 있다. LL4-HH4를 암호화한 영상(②의 경우, 그림 3의 (c))에서는 최저 저주파 성분과 동일 레벨의 최대 고주파 성분을 암호화했는데 암호화로 적당히 영상이 은닉되었다는 것을 볼 수 있다. 그림 3의 (b), (c), (d)(③의 경우의 경우), 그리고 (e)(④의 경우)에서의 원 영상에 대한 암호화 비율(암호화 대상 영상에서 전체 화소수 혹은 계수에 대해 암호화화에 이용되는 화소수/계수의 비율)은 각각 1:256, 1:128, 1:64, 그리고 1:32 이고 그에 따른 암호화 효과도 증가함을 알 수 있는데 순서대로 9.32dB, 9.22dB, 9.13dB, 9.27dB, 그리고 4.0dB의 PSNR(Peak Signal-to-Noise Ratios)을 가진다.

III-2. 데이터 비트의 선택

데이터 선택의 두 번째 방법은 선택된 부대역에서 계수의 일부 비트만을 암호화 대상으로 삼는 것이다. 양자화 후 LL4의 계수는 8비트 그리고 다른 부대역의 계수는 부대역별로 할당된 양자화 비트로 구성된다. 선택된 부대역에서 정보를 나타내는 데이터들의 모든 비트에 대해 암호화를 수행하면 암호화를 수행하는 처리 시간이 길어지게 되므로 부대역당 어느 일정한 비트수를 선택하여 암호화 량을 감소시킬 수 있다. LL4 부대역의 계수값을 Qx_i^{LLA} (WC_i^{LLA})=$a_{m-1}a_{m-2}a_{m-3}\cdots a_1a_0$ (a_{m-1}는 MSB, a_0 는 LSB)와 같이 나타낼 수 있다.

$$QX_i^{LL4} = a_{m-1}\cdot 2^{m-1} + a_{m-2}\cdot 2^{m-2} + \cdots + a_1\cdot 2^1 + a_0\cdot 2^0 \quad (1)$$

여기서 비트의 가중치 ($W(a_i)$)을 나타내면,

$$W(a_i) > W(a_{i-1}) + W(a_{i-2}) + \cdots + W(a_1) + W(a_0) \quad (2)$$

LL4 부대역의 경우 일반적으로 MSB의 가중치는 나머지 비트의 가중치를 모두 더한 것보다 크다. 즉, MSB만을 암호화하는 것은 전체 계수를 암호화하는 것의 절반 이상의 효과를 거둘 수 있고 이러한 정보는 암호화양을 줄이데 사용될 수 있다. 그림 4의 실험결과는 LL4 부대역에서 비트를 선택하여 암호화한 것으로 그림 4의 (a), (b), (c), 그리고 (d)의 PSNR은 원래 영상에 대해서 9.32dB, 9.33dB, 9.30dB, 그리고 9.28dB의 값을 가진다.

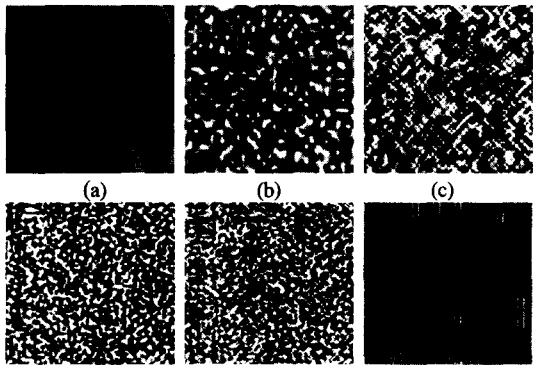


그림 3. 부대역 선택에 의한 암호화 효과 (a) Original image (b) LL4 (c) LL4-HH4 (d) Level 4 (e) Level 4-HH3 (e) All

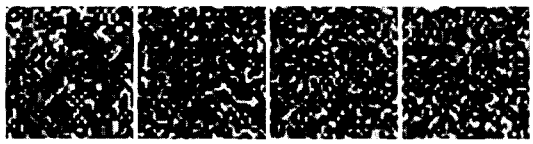


그림 4. 부대역 LL4만을 비트 선택하여 암호화 한 영상

그러나 다른 부대역에서의 양자화 값은 계수값에 대한 가중치가 성립하지 않는다. 본 논문에서 2가지 방법으로 양자화된 비트를 재배열하는 방법을 제시한다. 그림 5의 (a)에서 보이는 top-bottom 방법과 그림 5의 (b)에 나타낸 reflected code 방법으로 재배열하는 방법이 그것이다.

양자화 계수에 대해 암호화를 수행할 경우 암호화된 데이터의 분포를 고려해야 되는데 이는 압축율이 양자화 인덱스를 입력으로 하는 엔트로피 코딩에 의해 변화하기 때문이다. 만약 데이터가 가지는 특성과 통계적인 분포에 관계없이 무작위적으로 데이터를 암호화하면 암호화 후에 데이터가 가지고 있던 분포가 흐트러져서 원래의 분포에 최적화되어있던 엔트로피 코딩과정에 영향을 미치게 되고 결과적으로 압축률이 낮아지는 결과를 보인다. 그러나 암호화 과정에서 암호화 전/후에 대한 데이터의 분포를 고려한다면 데이터의 분포도가 넓어지는 것을 방지

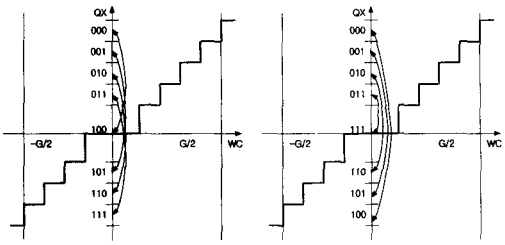
할 수 있다. 그림 5에 이러한 방법을 나타냈다. 그림 5의 (a)에 나타난 것은 top-bottom 방식으로 양자화 계수의 MSB만를 암호화 대상에 포함시키기 때문에 각 양자화 계수에 대해 최대 변위를 발생시킨다. 그리고 그림 5의 (b)에 나타난 방식은 reflection code 방식으로 암호화 결과를 동일한 확률의 양자화 영역으로 한정시키게 되어 (a)에 비해 암호화 효과는 나쁘지만 거의 압축률을 변화시키지 않는다. 그림 6의 (b)와 (c)는 그림 5의 (a)와 (b)방법을 이용해서 MSB만을 암호화한 것이다. 암호화하기 전의 그림 6의 (a)에 나타난 분포도는 일반적인 DWT 후 부대역의 계수들이 가지는 가우시안(gaussian) 분포인데 여기서 그림 6의 (b)는 그림 6 (c)에 비해 그 분포가 더욱 흐트러진 것을 볼 수 있고 압축률도 역시 4%와 0.7%로 차이를 보인다. 암호화된 결과에 최적으로 허프만 코드를 재 생성하여 엔트로피 코딩을 수행한 뒤 압축률을 재 측정하면 압축률이 2.1%와 0.3% 정도 감소되는 결과를 얻을 수 있고 암호화를 통해 낮아진 압축율을 일정부분 보상할 수 있다.

3-1과 3-2 장에서 제안된 방식으로 암호화를 수행할 경우 3-1장에서 보인 4가지 부대역 선택방법에 대해서 암호화되는 데이터량이 각각 1:2048, 1:1024, 1:512, 그리고 1:256으로 감소되는 것을 알 수 있다.

III-3. 계수 비트의 무작위 선택

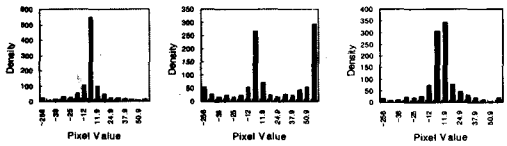
마지막 데이터 선택 방법은 계수의 비트를 무작위적으로 선택하는 것으로 이는 암호화하는 비트를 줄이면서 데이터 선택 자체를 암호화하는 것을 목적으로 한다. 암호화 대상 비트는 암호화키에 따라서 선택되는데 무작위수 발생을 위해서 그림 3에 나타난 선형귀환 쉬프트 레지스터(LFSR, linear feedback shift register)을 사용하였고 LFSR은 아래와 같은 5가지 특징을 가진다[15].

(1) LFSR은 귀한 특징을 가지며 병렬 및 직렬 출력을 가진다.
(2) LFSR의 초기값(seed 값)에 의해서 병렬 및 직렬 출력이 결정된다.
(3) 먼저, Initial Value Control 신호를 '1'로 하여 LFSR의 초기치(S_1~S_n)를 입력한다. 그 후 LFSR 함수를 수행할 때마다 병렬출력(R_1~R_n)에 무작위수가 발생한다.
(4) n비트 LFSR의 경우 한 사이클의 최고길이는 2^n-1(모든 비트가 0이 되는 경우 제외)이다.
(5) 출력 시퀀스의 길이가 충분히 길다고 가정하면, 특정 비트(i)에서 특정 시간(j)에 '0'과 '1' 이 나올 확률은 거의 같다.



(a) (b)

그림 5. 양자화 과정에서 두 가지 양자화 인덱스 할당방식 (a) top-bottom 방식 (b) reflection code 방식



(a) (b) (c)

그림. 6. 그림 1의 방식에 의한 양자화 계수의 암호화 후 계수 분포 (a) 암호화 전 (b) top-bottom 방식 (c) reflection code 방식

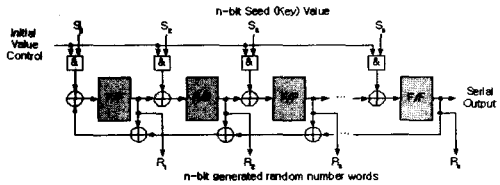


그림 7. 무작위 패턴 생성을 위한 LFSR

III-4. 암호화 절차

지금까지 아래의 3가지 데이터 선택 방법에 대해서 논의를 했었고 본 장에서는 이를 바탕으로 암호화와 복호화 절차를 설명하고자 한다.

(1) 부대역 조합의 선택: 3-1에 제시한 4가지 방법
(2) 데이터의 비트 선택: MSB 선택과 양자화 인덱스에 대한 reflection code 방법
(3) 계수의 무작위 선택: LFSR의 직렬 출력 사용

위와 같은 모든 방법은 암호화되는 데이터의 양을 줄이고자 하는 것으로 (1)과 (2)의 과정을 통해서 충분히 원하는 결과를 얻을 수 있다. 여기에 (3)번의 과정을 부가시킴으로써 더욱 암호화되는 데이터의 양을 줄이면서 데이터를 선택하는 과정에 보

안성을 부여할 수 있지만 영상의 인지와 암호화 양 사이에 상보성(trade-off)이 크기 때문에 암호화가 사용되는 목적 및 적용 분야에 따라서 세심한 고려가 요구된다.

그림 8에서 본 논문의 영상 암호화 및 영상 복호화 과정을 나타내었는데 왼쪽은 암호화과정이고 오른쪽은 복호화 과정을 나타낸다. 본 논문에서는 데이터의 암호화를 위해서 128 비트의 블록 단위로 암호화를 수행하는 SEED[16]를 사용하였다. 앞서 설명한 데이터 선택 방법에 의해 선택된 비트들을 메모리에 있는 계수들로부터 추출하여(Data extraction) 128 비트 크기의 블록을 생성하고 이를 암호화 알고리즘을 이용하여 암호화(Encryption)한다. 이때 무작위로 데이터를 선택할 경우에는 암호화키(Encryption key)로 LFSR을 이용하여 무작위수를 발생(Random number Generation)시킨다. 암호화가 수행된 데이터 블록은 비트로 나눈 후 원래의 데이터 위치에 재배열(Data restore)하고 데이터들을 재생성하여 암호화 과정을 마친다. 그리고 최종적으로 엔트로피 인코딩(Entropy coding)을 통해서 암호화과정을 거친 압축된 영상(Encrypted compressed image)을 얻는다. 또한 복원과정은 영상복원 과정 중 엔트로피 디코딩(Entropy decoding)을 거친 결과를 대상으로 암호화와 동일한 과정을 반복하는데, 이 때 암호화 대신 복호화 과정(Decryption)을 수행한다.

Ⅳ. 실험결과 및 고찰

본 장에서는 제안한 암호화 방법에 대한 실험 결과를 그림으로 나타내고 암호화 비용과 암호화 효

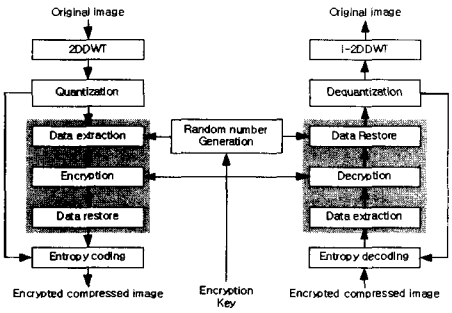


그림 8. 암호화 및 복호화 절차

과사이의 상보적인관계를 나타냈다. 암호화 알고리즘으로는 SEED[16]를 사용하였고 제안한 알고리즘은 C/C++로 구현하여 500개의 흑백 영상을 대상으로 실험하여 평균값으로 나타냈다.

그림 9는 3장에서 제시한 방법을 통해 Lena 영상을 암호화한 결과 영상들로 각각의 그림에 선택된 부대역과 PSNR 결과를 나타냈다. 그림 9의 (a)는 LL4 부대역만을 선택하고 무작위 선택 방법(RS)으로 암호화를 수행하여 결과 영상이 9.39dB의 PSNR을 보였다는 것을나타내고 그림 9의 (f)는 모든 Level 4영역을 대상으로 암호화를 수행하여 그 결과 영상의 PSNR이 11.18dB임을 나타낸다. 그림 9의 (a), (b)와 같이 LL4만 암호화한 영상을 보면 경계성분(고주파)이 보인다는 것을 알 수 있다. 그러나 그림 9의 (c), (d)와 같이 LL4와 HH4를 암호화한 영상은 거의 원 영상을 인식할 수 없다. 동일 부대역에 대해서 무작위 선택을 한 것과 안한 영상을 비교하면 암호화한 양은 1/2로 큰 차이를 보이지만 PSNR은 크게 변하지 않는다. 즉, 본 논문에서

표 1. 각 암호화 방식에 따른 영상의 결과

Item case	Encry-ption ratio	Encry-ption # of blocks	CPU (ms)	PSNR (dB)	Huffman code adjustment							
					Symbol assignment (a)				Symbol assignment (b)			
					Before		After		Before		After	
					Comp	%	Comp	%	Comp	%	Comp	%
LL4 : RS	1:4096	4	10.76	9.244	24.23	100	24.23	100	24.23	100	24.23	100
LL4	1:2048	8	21.79	7.996	24.23	100	24.23	100	24.23	100	24.23	100
LL4-HH4 : RS	1:2048	8	22.45	8.673	23.75	98.02	24.01	99.09	24.15	99.67	24.22	99.96
LL4-HH4	1:1024	16	44.59	7.760	23.32	96.24	23.79	98.18	24.07	99.34	24.20	99.88
Level 4 : RS	1:1024	16	45.09	7.933	23.02	95.01	23.51	97.03	24.00	99.05	24.18	99.79
Level 4	1:512	40	93.64	7.669	22.03	90.92	23.19	95.71	23.78	98.14	24.14	99.63
Level 4-HH3 : RS	1:512	40	105.21	7.785	21.34	88.07	23.09	95.30	23.55	97.19	24.11	99.50
Level 4-HH3	1:256	64	201.43	7.624	19.32	82.29	22.24	91.79	22.94	94.68	24.05	99.26

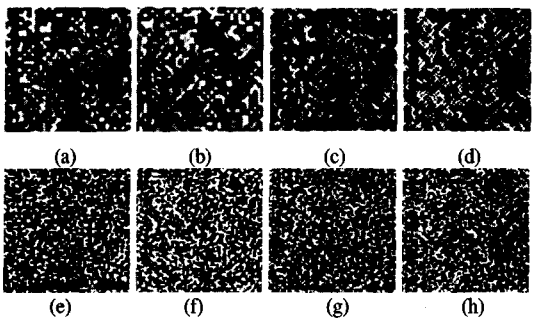


그림 9. 제안한 방법에 따른 Lena 영상의 암호화(dB) (a) LL4:RS(9.39) (b)LL4(9.52) (c)LL4-HH4:RS(9.18) (d) LL4-HH4(9.26dB) (e) Level4:RS(10.52) (f) Level4(11.18) (g) Level4-HH3:RS(9.53) (h) Level4-HH3(9.67)

암호화 효율을 위해 사용된 PSNR은 암호화 정도를 측정하는 기준으로 부족하다는 것을 알 수 있고 단지 영상의 질에 대한 대략적인 척도로서 사용한다.

표 1에 500개의 영상을 양자화한 후 제안된 알고리즘을 적용하여 암호화를 수행한 결과를 나타냈다. 여기서 원 영상의 각 계수는 8비트로 구성되었다고 가정한다. 첫 번째 행은 암호화에 사용된 부대역과 방법을 나타내고 두 번째 행은 원 영상에 대한 암호화된 영상의 데이터양을 비율로 나타내며 암호화에 사용되는 블록의 크기를 세 번째 행에 나타냈다. 표 1에서 암호화 율이 0.024%(LL4에서 무작위로 선택한 경우 : 1/4,096)에서 0.4%(Level 4-HH3에서 무작위로 선택하지 않은 경우 : 1/256)까지로 나타나는데 이 비율은 이전의 암호화 방법에 비해 상당히 적은 양을 암호화한다는 것을 나타낸다. 다섯 번째 행은 암호화된 영상의 평균 PSNR을 보여주는 것으로 PSNR 값은 암호화 양이 많아질수록 적어지는 것을 알 수 있다. 또한 더욱 LL4를 무작위로 암호화했을 경우 PSNR이 더 작아지는 것을 볼 수 있다.

암호화로 인해 데이터의 압축률은 낮아지게 되는데 여덟 번째 행은 허프만 압축 비율을 보여주고 있고 그림 10에서도 그래프로 나타내었다. 여기서 (a), (b)는 3장에서 설명한 그림 5의 (a), (b)에 나타낸 암호화 방법에 의한 것으로 여기서 종전의 허프만 코드를 사용한 압축비와 수정된 허프만 코드를 적용한 후의 압축비를 보여준다. 표 1과 그림 10에서 보는 것과 같이 (b)의 방법이 (a)의 방법에 비해 압축비가 더 좋다는 것을 알 수 있다. 예를 들면 Level 4-HH3 경우 허프만 코드 수정 후 압축비를 살펴보면 (a)의 경우는 92%이지만 (b)의 경우는 원 영상과 거의 같은 압축비를 보이는 것을 확인할 수 있다.

표 1에서 네 번째 행은 암호화를 수행 할 때의 CPU 수행시간을 나타내고 있다. 표에 나타난 시간은 암호화하는 시간과 LFSR를 수행하는 시간, 데이터를 암호화 블록에 넣는 시간 그리고 암호화된 블록에서 비트를 분리하고 데이터를 재구성하는 시간이 포함되어있다. 암호화하는 양이 증가할수록 암호화하는 시간이 증가한다. 실험에 사용된 C 코드가 각 암호화 방식에 대해 최적화된 코드가 아니라 다양한 실험을 위한 범용적인 코드이므로 절대적인 수행시간을 비교하는 것은 무리가 있고 각 방식들 간의 비교를 위해서만 참조해야한다.

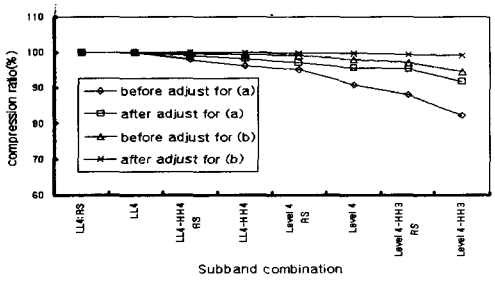


그림 10. 허프만 코드 조정에 의한 압축율 복원

암호화과정에서 각 단계별로 수행되는 시간을 그림 11에 나타냈다. 암호화를 수행하는데 가장 크게 소요되는 시간은 암호화한 데이터를 원래의 영상에 재배열시키는 것으로 데이터를 블록으로 넣고 다시 암호화된 비트들을 다시 재배열시키는 시간이 암호화하는데 걸린 시간보다 3배 이상 크다는 것을 알 수 있다. 그래서 전체적으로 소요된 시간은 암호화시키는 시간의 5배 이상이 소요된다. 그러나 이러한 수행 시간은 각 방식별로 최적화된 코드를 통해 측정된 것이 아니므로 절대적인 값으로 참조해서는 안되고 각 방식간의 비교를 위해서만 참조해야한다.

그림 12에서 암호화되는 데이터의 양, 암호화 효율, 그리고 암호화하는 시간의 관계는 서로 상보적임을 볼 수 있다. 그림에서 보이는 것과 같이 암호화하는 양이 증가하면 그에 따른 수행 시간(CPU Time)과 암호화 정도(PSNR)가 증가하게 된다. 무선 환경에서 안전하게 영상을 전송하려면 채널의 밴드폭과 무선 장치의 상태(연산능력의 제약, 전력의 제약)에 따른 제약조건이 존재하고 사용자가 영상정보를 전송하려면 현재상태(현재의 대역폭, 배터

리의 수명)에 따라서 제약조건을 가지게 되는데 본 논문에서 보인 방식과 결과에 대한 정보를 바탕으로 사용자들은 사용자의 환경에 따른 적합한 암호화를 선택할 수 있다.

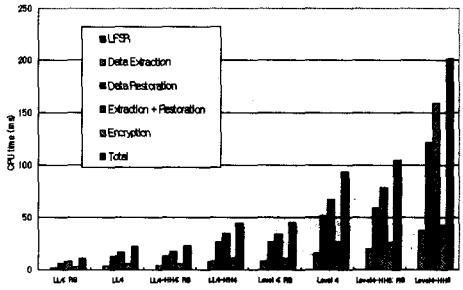


그림 11. 암호화 과정에서 단계별 시간소모

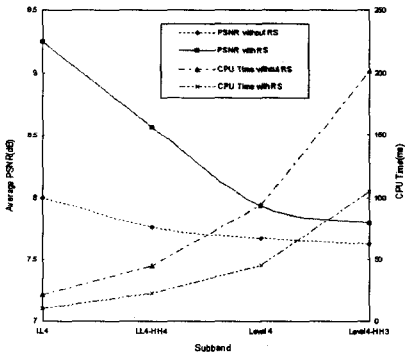


그림 12. 암호화양, 처리시간, 암호화효과에 대한 관계

V. 결 론

본 논문에서는 웨이블릿 영역에서 암호화를 통해 영상정보를 효율적으로 은닉하는 방법을 제시하였다. 이 방법은 웨이블릿 변환 및 양자화 과정을 거친 영상데이터를 대상으로 하며 웨이블릿 변환 결과의 주파수 대역에 따라 암호화 대상을 선택한다. 3가지 데이터 선택 방법으로 선택적 부분 암호화를 하였다. 실험 결과는 부대역 Level4-HH3을 암호화를 수행했을 경우 암호화 비용이 압축비용의 2%인 것을 알 수 있고 원 영상에 대한 암호화 비율은 최대 1/4,096에서 최소 1/256이다. 이 비율은 유선 환경을 비롯하여 무선환경에서 사용되기에 적합한 수치이므로 적은 비용으로 암호화가 가능하고 휴대용 기기에 적용하는 것도 가능하다.

처리시간에 대한 실험 결과에서 암호화하는 시간보다 암호화를 수행하기 위해 데이터를 추출하고 암호화를 수행한 후 그 데이터를 다시 재배열하는데 더 많은 시간이 소요되었는데 이러한 시간의 감소를 통해서 더욱 효과적인 암호화를 수행할 수 있다. 제안한 방법의 구현에 있어서 현재는 소프트웨어로만 구현되었으나 하드웨어로 구현할 경우 더욱 효과적인 영상 암호화 방법이 될 수 있다. 즉, LFSR의 동작이나 LFSR에 의한 화소의 선택, 그리고 2D DWT 및 양자화 과정 등이 소프트웨어의 경우 완전히 직렬로 수행되어야 하지만 하드웨어의 경우 이들이 병렬로 처리될 수 있으므로 암호화 과정을 훨씬 빠른 시간에 수행할 수 있다. 따라서 본 논문의 다음 단계 연구는 본 논문에서 제안한 암호화 방식을 하드웨어로 구현하는 것이다.

마지막으로 제안된 방법은 응용계층에서의 암호화 방식이므로 현재 유/무선 통합 네트워크 환경에서 큰 문제가 되고 있는 끝과 끝(end-to-end) 보안의 영상에 대한 좋은 해결방안이 될 수 있을 것이라 기대한다.

참 고 문 헌

[1] W. Staliings, *Cryptography and Network Security, Principles and Practice*, Prentice-Hall, Upper Saddle River, NJ, 1999.

[2] R. M. Rao and A. S. Bopardikar, *Wavelet Transforms, Introduction to Theory and Application*, Addison-Wesley, Reading, 1998.

[3] Edited by Martin Boliek, *JPEG 2000 Final Draft International Standard*, ISO/IEC JTC 1/SC 29/WG 1, 2000.

[4] L. Qiao and K. Nahrstedt, "Comparison of MPEG Encryption Algorithms", International Journal on Computer and Graphics(Special Issue on Data Security in Image Communication and Networks), Vol. 22, No. 3, pp. 437-444, 1998.

[5] A. M. Alattar, et al., "Improved Selective Encryption Techniques for Secure Transmission of MPEG Video Bit-streams", ICIP'99, pp. --, 1999.

[6] C. Shi and B. Bhargava, "A Fast MPEG Video Encryption Algorithm", Proc. Of ACM Multimedia 1998, pp. 81-88, 1998.

[7] H. Chaeng and X. Li, "Partial Encryption of Compressed Images and Videos", IEEE Trans, on

Signal Processing, Vol. 48, No. 8, pp. 2439-2451, Aug. 2000.

[8] A. Pommer and A. uhl, "Wavelet Packet Methods for Multimedia Compression and Encryption", *IEEE Pacific Rim Conf. On Communications, Computers, and Signal Processing*, pp. 1-4, 2001.

[9] A. Pommer and A. Uhl, "Selective Encryption of Wavelet Packet Subband Structures for Obscured Transmission of Visual Data", IEEE Benerux Signal Processing Symposium, pp. 25-28, 2002.

[10] X. Wu and P. W. Moo, "Joint Image/Video Compression and Encryption via High-Order Conditional Entropy Coding of Wavelet Coefficients", Int'l Conference on Multimedia Computing and Systems, pp. 908-912, 1999.

[11] P. P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications", IEEE Trans. on Consumer Electronics, Vol. 46, No. 3, pp. 395-403, Aug. 2000.

[12] M. Podesser, H. P. Schmidt, and A. Uhl, "Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments", Proc. 5th Nordic Signal Processing Symposium, pp. --, 2002.

[13] T. Uehara and R. Safavi-Naini, "Attacking and Mending Arithmetic Coding Entropy Schemes", Proc. Of Australian Science Conference, pp. 408-419, Jan. 1999.

[14] G. J. Sullivan and R. L. Baker, "Efficient Quadtree coding of images and videos", IEEE Trans. on Signal Processing, Vol. 3, pp. 327-331, May 1994.

[15] S. W. Golomb. *Shift Register Sequences*, Algean park Press, Laguna Hills, CA, 1982.

[16] 한국정보보호센터, *128비트 블록 암호알고리즘 (SEED) 개발 및 분석 보고서*, 12. 1998.

서 영 호(Young-Ho Seo) 정회원

1999년 2월 : 광운대학교 전자재료공학과 졸업(공학사).
2001년 2월 : 광운대학교 대학원졸업(공학석사).
2000년 3월~2001년 12월 : 인티스닷컴(주) 연구원.
2001년 3월~현재 : 광운대학교 전자재료공학과 박사과정.
2003년 6월~현재 : 한국전기연구원 연구원
<관심분야> Image Processing/Compression, 워터마킹, 암호학, FPGA/ASIC 설계
e-mail : design@kw.ac.kr

김 수 민 (Su-Min Kim) 학생회원

2002년 8월 : 전주대학교 전기전자공학과 졸업(공학사).
2003년 3월 ~ 현재 : 광운대학교 전자재료공학과 석사과정.
<관심분야> : Image Processing, 암호학, FPGA/ASIC 설계
e-mail : sumin@kw.ac.kr

김 동 욱(Dong-Wook Kim) 종신회원

1983년 2월 : 한양대학교 전자공학과 졸업(공학사).
1985년 2월 : 한양대학교 대학원 졸업(공학석사).
1991년 9월 : Georgia공과대학 전기공학과 졸업(공학박사).
1992년 3월~현재 : 광운대학교 전자재료공학과 정교수.
광운대학교 신기술 연구소 연구원.
2000년 3월~2001년 12월 : 인티스닷컴(주) 연구원.
<관심분야> 디지털 VLSI Testability, VLSI CAD, DSP 설계, Wireless Communication
e-mail : dwkim@daisy.gwu.ac.kr