웨이블릿 영역에서의 선택적 부분 영상 암호화

준회원 서 영 호*, Sujit Dey**, 정회원 김 동 욱***

Selectively Partial Encryption of Images in Wavelet Domain

Young-Ho Seo* *Associate member*, Sujit Dey**
Dong-Wook Kim*** *Regular Members*

요 약

영상/비디오 컨텐츠의 사용이 급증함에 따라 유료 및 비밀유지를 필요로 하는 영상데이터에 대한 보안문제가 크게 대두되고 있다. 본 논문에서는 영상데이터를 숨기기 위한 영상 암호화 방식을 제안하였다. 이 방법은 웨이블릿 영역에서 양자화과정을 마친 영상 데이터를 대상으로 한다. 본 논문은 영상의 전체데이터가 아닌 부분데이터를 암호화하는 방식을 사용하는데, 세 가지 형태의 부분데이터 추출방식을 사용하였다. 먼저, 웨이블릿 변환이 원영상을 주파수 대역으로 재편성함을 이용하여 영상정보 중 특정 주파수를 숨김으로서 전체 영상을 인식할 수 없도록 하였다. 각 화소를 나타내는 데이터에서도 모든 데이터를 사용하지 않고 MSB만을 선택하여 암호화 대상에 포함시켰다. 마지막으로 특정 부대역의 화소들을 무작위로 선택하였으며, 이 때 선형귀환 시프트 레지스터(Linear Feedback Shift Register, LFSR)를 사용하였다. LFSR의 초기값과 출력비트의 선택에 있어서 암호화 키의 일부분을 사용함으로써 암호화 강도를 더욱 높였다.

제안한 방법을 소프트웨어로 구현하여 약 500개의 영상을 대상으로 실험한 결과 원영상 데이터의 약 1/1000의 데이터 양을 암호화함으로써 원영상을 인식할 수 없을 정도의 암호화효과를 얻을 수 있음을 알 수 있었다. 따라서 제안한 방법은 작은 양의 암호화로 효과적으로 영상을 숨기는 방법임을 확인할 수 있었다. 본 논문에서는 부대역의 선택과 LFSR 출력 중 사용비트의 양에 따른 여러 방식을 제안하였으며, 이들의 암호화 수행시간과 암호화효과 사이에 상보적인 관계가 있음을 보여, 적용분야에 따라 선택적으로 사용할 수 있음을 보였다. 또한 본 논문의 방식들은 응용계층에서 수행되는 것으로, 현재 유·무선 통합 네트워크의 중요한 문제로 대두되고 있는 끝과 끝(end-to-end)의 보안에 대한 좋은 해결방법으로 사용될 수 있으리라 기대된다.

Key Words : DWT(Discrete Wavelet Transform), Partial Encryption, Selective, LFSR, Image Ciphering

ABSTRACT

As the usage of image/video contents increase, a security problem for the payed image data or the ones requiring confidentiality is raised. This paper proposed an image encryption methodology to hide the image information. The target data of it is the result from quantization in wavelet domain. This method encrypts only part of the image data rather than the whole data of the original image, in which three types of data selection methodologies were involved. First, by using the fact that the wavelet transform decomposes the original image into frequency sub-bands, only some of the frequency sub-bands were included in encryption to make the resulting image unrecognizable. In the data to represent each pixel, only MSBs were taken for encryption. Finally, pixels to be encrypted in a specific sub-band were selected randomly by using LFSR(Linear Feedback Shift Register). Part of the key for encryption was used for the seed value of LFSR and in selecting the parallel output bits of the LFSR for random selection so that the strength of encryption algorithm increased.

The experiments have been performed with the proposed methods implemented in software for about 500 images, from which the result showed that only about 1/1000 amount of data to the original image can obtain the encryption effect not to recognize the original image. Consequently, we are sure that the proposed are efficient image encryption methods to acquire the high encryption effect with small amount of encryption. Also, in this paper, several encryption scheme according to the selection of the sub-bands and the number of bits from LFSR outputs for pixel selection have been proposed, and it has been shown that there exits a relation of trade-off between the execution time and the effect of the encryption. It means that the proposed methods can be selectively used according to the application areas. Also, because the proposed methods are performed in the application layer, they are expected to be a good solution for the end-to-end security problem, which is appearing as one of the important problems in the networks with both wired and wireless sections.

*광운대학교 전자재료공학과 디지털 설계 및 테스트 연구실(design@kw.ac.kr). **Electrical and Computer Engineering, University of California at San Diego(dey@ece.ucsd.edu). ***광운대학교 전자재료공학과 정교수(dwkim@daisy.kw.ac.kr).
논문 번호 :020478-1030, 접수일자 : 2202년 10월 30일
※본 논문은 2002년도 광운대학교 연구년에 의하여 연구되었음.

Ⅰ. 서 론

최근 20년간 컴퓨터 및 인터넷의 발달로 인해 유선 및 무선통신을 통한 정보량이 폭발적으로 늘어나고 있으며, 21세기를 '정보의 시대'라 부를 만큼 현대의 생활에서 정보의 비중이 기하급수적으로 증가하고 있다[1]. 1970년대 인터넷의 개발로부터 사용되는 정보 데이터의 종류 또한 단순한 문자정보에서부터 음성, 영상, 비디오로 그 영역이 확산되고 있다. 특히 시각적이며, 이해하기 쉽고, 또 가장 함축적인 정보를 포함하는 영상과 비디오 컨텐츠에 대한 선호도가 매우 급속히 증가하고 있다[2]. 그러나 영상/비디오는 그 자체의 데이터 양이 매우 많아 최근의 연구방향은 주로 이들의 데이터 양을 줄이는 것에 주안점을 두고 있다[3].

영상/비디오의 데이터 양을 줄이는 연구는 지금까지 두 주류를 형성하고 있다. 현재 가장 널리 사용되고 있는 분야는 JPEG 및 MPEG 분야로, 지금까지 상당부분이 국제표준으로 채택되었으며[3], 현재 대부분의 응용분야에 사용되고 있다. 이 기술은 기본적으로 DCT(Discrete Cosine Transform)을 사용하고 있는데, 변환단위를 8×8 화소블록으로 하고 있기 때문에 블록효과(block effect)라는 고유의 문제점을 안고 있다. 최근 이산 웨이블릿 변환(DWT, Discrete Wavelet Transform)을 영상변환에 사용하는 방식이 연구되고 있는데, 이 방식은 영상전체를 변환단위로 사용하기 때문에 블록효과가 없고 동일한 압축률에서 DCT보다 좋은 화질을 보여[4], 최근에는 영상의 표준변환방식으로 채택되기도 했다[5].

영상/비디오 컨텐츠의 사용량 및 분야가 확산됨에 따라 유료정보 또는 비밀 보장이 요구되는 정보의 사용이 점차 증가되고 있어서, 영상정보의 보안기술이 또 하나의 큰 연구대상이 되고 있다[6]. 기본적으로 인터넷 프로토콜은 그 자체로 보안 프로토콜을 포함하고 있으며(SSL 또는 IPsec), 통신의 시작단계에서부터 인증 및 보안을 위한 프로토콜들을 적용하도록 규정하고 있다[7]. 특히 무선통신의 경우 공격가능성이 유선의 경우에 비해 훨씬 높으나, 통신주체의 특성상 유선에 비해 훨씬 가벼운 보안 프로토콜을 적용하고 있으며[8][9], 유·무선이 같이 포함된 경우 유선구간과 무선구간의 경계에서 보안프로토콜은 변경하여야 하기 때문에 통신의 처음부터 끝까지(end-to-end)의 보안에 상당한 문제점을 안고 있는 실정이다[10][11]. 근본적으로 인터넷 또는 무선인터넷 프로토콜이 포함하고 있는 보안 프로토콜은 프로토콜 계층에 따라 수행되는 방식으로, 특정 계층의 보안알고리듬은 상위 계층으로의 진행을 위해서는 그 보안 프로토콜을 풀어야 한다. 따라서, 보다 확실한 보안을 위해서는 현존의 통신 프로토콜의 보안 프로토콜 이외에 최상위 계층, 즉 응용계층에서 보안 알고리듬을 적용하도록 권유하고 있다[11][12].

따라서 영상/비디오에 대한 보안문제도 응용계층에서 주로 다루고 있으며, 이미 MPEG계열에 대한 연구는 상당부분 진행되어 왔다[13][14]. DWT를 사용하는 영상처리 방법은 MPEG 계열의 방법과 변환단계부터 완전히 다르므로, 이들에 대한 보안 알고리듬 또한 MPEG의 것과는 다른 방법을 사용하여야 한다. 상대적으로 DWT 계열의 영상처리 방법이 최근에 발전되고 있으므로, 이 방법들에 대한 보안 알고리듬 또한 현재 초기단계에 있다고 볼 수 있다. 영상의 보안은 일반적으로 암호화 알고리듬을 적용하여 수행되는데, 암호화 알고리듬의 계산양이 많으므로 영상전체보다는 영상정보의 일부분을 암호화하는 부분암호화 방법이 연구의 주류를 이루고 있다[15]~[19]. [15]에서는 비정규적인 변환방식을 채택하고, 각 변환에 사용되는 필터의 종류를 암호화하는 방식으로 영상을 암호화하였고, [16]에서는 동일한 방식의 변환에서 부대역의 구조에 대한 정보를 암호화하여 영상정보를 숨겼다. 변환과정에서 암호화를 적용하는 방법과는 달리 [17]에서는 연산코딩 결과에 암호화를 적용하였다. 즉, 과거 비트스트림의 확률적인 모델로 그 다음 비트의 값을 결정하는 연산코딩에서 확률모델을 암호화하여 그 확률모델 자체를 숨기는 방법을 제안하였는데, 이 방법은 특정 연산코딩방법을 겨냥한 방법이다. 영상압축과정 중 특정 양자화 과정을 겨냥한 암호화 방법도 제안되었는데, [18]에서는 EZW(Embedded Zero-tree Wavelet)[20] 방법에 ATM 패킷 방법을 적용하여 암호화를 수행하였다. 또한 [19]에서는 EZW를 기반으로 하는 SPHIT[21]를 겨냥하여, 양자화된 계수값 대신에 양자화 파라메터들을 암호화하는 방법을 제안하였다. 이 두 방법은 특정 양자화 방식을 기반으로 하기 때문에 일반적인 적용은 불가능하다. 특히 EZW 기반의 양자화과정은 변환된 영상정보를 참조하는 횟수가 많아 하드웨어적인 구현에 많은 어려움이 있다.

본 논문에서는 DWT를 사용하는 영상처리방법에

서 특정 양자화 또는 특정 엔트로피 코딩방식을 겨냥하지 않는 일반적으로 적용가능한 영상의 부분 암호화 방법을 제안하고자 한다. 이 방식은 양자화 과정 다음에서 이루어지며, 이 때의 양자화 과정은 일반적으로 사용할 수 있는 어떤 양자화 방식도 가능하다. 제안하는 방식에서는 암호화 대상에 포함되는 데이터의 양을 최소화하기 위하여 각 화소 데이터의 일부분만을 택하고, DWT 결과의 부대역 중 일부 부대역만을 택하며, 특정부대역 내에서 암호화 대상 데이터의 위치를 숨기기 위해 데이터의 무작위 추출과정을 포함한다. 이 방식의 목적은 최소의 암호화 양으로 최대의 암호화 효과를 거두는 것이므로, 본 논문의 근본 취지를 만족하는 여러 선택들을 보이며, 이들을 사용함에 있어서 상보적인 관계를 밝힌다.

본 논문의 다음 장에서는 DWT를 이용한 영상 압축방법과 DWT 결과 영상 및 그 데이터 구조에 대해서 설명하고, 본 논문에서 제안하는 부분영상 암호화 방법은 III장에서 설명한다. 전체적인 암호화 및 복호화 과정은 IV장에서 상세히 언급하며, V장에서는 제안한 방법에 대한 실험 및 그 결과를 보이고, VI장에서 본 논문의 결론을 맺는다.

II. 웨이블릿 변환을 이용한 영상의 압축/복원

DWT를 이용한 영상의 압축 및 복원과정은 간단히 그림 1과 같이 나타낼 수 있다. 영상이 2차원 데이터이기 때문에 DWT 또한 2차원(2차원 DWT, 2DDWT)으로 수행되는데, 가장 대표적인 수행방식이 Mallat-tree 형식이며, 본 논문에서도 이 방식을 사용한다[4]. 2DDWT에 의해서 원 영상은 주파수 대역에 따라 3n+1(n: 2DDWT 레벨 수)개의 부대역으로 재편성되며, 레벨수가 증가할수록 주파수대역이 낮아진다. 그림에서 L은 저주파대역 통과, H는 고주파대역 통과를 각각 의미하며, XYj(X와 Y는 H 또는 L) 부대역은 j번째 레벨에서 수평방향으로 X주파대역을 통과하고 수직방향으로 Y주파수대역을 통과한 부대역을 의미한다. 그림 2 (b)에서 볼 수 있듯이, 모든 부대역은 전체영상에 대한 특정 주파수 대역의 정보를 가지게 된다. 이 중 가장 저주파 성분에 해당하는(그림 2의 경우 LL4) 부대역이 인간의 눈에 가장 민감한 성분이며, 영상에 대한 가장 함축적인 정보를 포함한다.

2DDWT에 의해 재구성된 영상정보는 양자화기

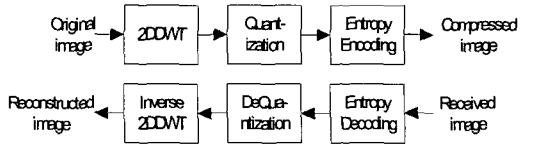
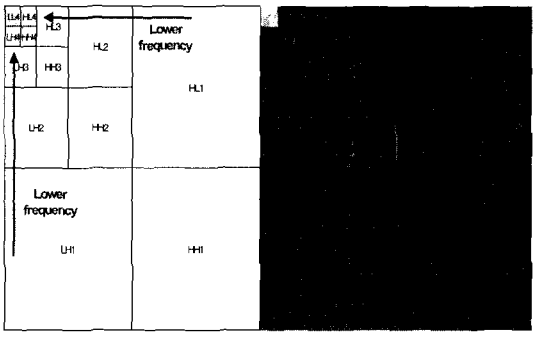


그림 1. DWT를 이용한 영상압축/복원
Fig. 1. Image compression/reconstruction using DWT



(a) (b)

그림 2. 2DDWT 결과; (a) 재편성된 부대역, (b) Lena 영상의 예
Fig. 2. The 2DDWT result; (a) Decomposed sub-bands, (b) Example of Lena image

를 거쳐 영상정보에 대한 압축이 수행된다. 양자화 과정은 특정 부대역의 특정 값을 미리 정해진 대표값으로 포화시키는 과정(손실 코딩, lossy coding)으로, 현재까지 많은 연구가 이루어졌다. 본 논문에서는 가장 간단한 형태인 선형 스칼라 양자화기를 가정하며 설명하며, 다른 형태의 양자화기를 사용하여도 무방하다. 양자화과정을 거친 영상정보는 엔트로피 코딩의 과정을 거치게 되는데, 이 과정은 양자화를 거친 값들에 대한 1:1 변환과정이므로 무손실 코딩에 해당한다. 이 과정에서 약간의 데이터 압축이 일어나며, 일반적으로 2:1을 넘지 않는 것으로 알려져 있다[4].

영상압축 코덱(codec)의 입력데이터는 일반적으로 한 화소당 8비트의 정수로 이루어져 있으므로 각 화소의 값(흑백성분 및 색성분)은 0에서 255사이의 값을 갖는다. DWT를 수행하기 위한 웨이블릿 필터는 여러 종류가 사용되나, 대부분 소수부분을 포함하기 때문에 변환이후의 값은 소수이고, 일반적으로 -256과 +255사이의 값을 갖는다. 실제의 계산에서는 부동소수점 계산보다 고정소수점 계산이 계산양이 적고 데이터양이 적으므로 주로 고정소수점의 데이터 형식을 취한다. 그러나 어느 경우에 있어서건 DWT 계산과정 중 또는 그 결과 값의 MSB는 크기의 최고값 또는 부호비트를 나타낸다.

본 논문에서는 Daubechies의 (9,7) 양직교 필터를 사용하는데, 이 경우 그림 2의 LL4의 화소는 0에서 255사이의 값을, 나머지 부대역은 -256에서 255사이의 값을 갖는다. LL4의 경우 일반적으로는 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 이 외의 영역은 양자화과정을 거치면서 대표값으로 대치되는데, 이 경우 MSB는 더 이상 부호비트나 크기의 최고비중 비트가 아니다.

Ⅲ. 영상의 부분 암호화 방법

본 장에서는 본 논문에서 제시하는 영상의 부분 암호화 방법에 대해서 설명한다. 본 논문의 영상암호화 방법은 그림 1의 영상압축/복원 과정 중 양자화와 엔트로피 코딩 사이에서 수행되며, 엔트로피 디코딩과 역양자화 과정의 사이에서 복호화가 이루어진다. 본 논문에서 제시하는 방법은 최소의 암호화 양으로 최대의 암호화 효과를 얻기 위해서 세 가지의 부분데이터 추출과정, 즉 화소 데이터의 부분선택, 부대역의 선택, 그리고 부대역 내에서의 화소선택과정을 포함한다.

1. 부분 데이터의 선택

Ⅱ장에서 설명한 바와 같이 양자화과정을 거친 결과는 특정 부대역에서 특정한 형태의 대표값들로 이루어진다. 단, LL4(최저주파수 부대역)의 경우는 양자화기를 통과하지 않기 때문에 DWT된 결과 값들을 그대로 갖는다.

본 논문에서 제안한 방법의 첫 번째 부분데이터 추출은 양자화를 거친 모든 데이터의 MSB만을 택하는 것이다. 이 경우 LL4를 제외한 부대역들에서는 양자화 과정으로 치환된 대표값의 MSB를 선택하는 것이며, LL4의 경우는 DWT 결과 계수들의 MSB들을 암호화 대상에 포함시키는 것이다. LL4의 경우 일반적으로는 부호화 비트나 계수 크기의 MSB에 해당한다. MSB가 부호비트인 경우 암호화에 의해 비트가 변화한다는 것은 반대의 부호를 갖게되는 것을 의미하며, 이 경우 단순히 크기를 조정하는 것보다 큰 효과를 얻을 수 있다. MSB가 크기의 최고비트인 경우(즉, LL4의 계수가 0에서 255사이의 값을 갖는 경우), MBS의 가중치는 나머지 비트의 가중치를 모두 더한 것보다 크다. 즉, MSB만을 암호화하는 것은 전체 계수를 암호화하는 것의 절반 이상의 효과를 거둘 수 있다. 따라서 LL4의 MSB가 어느 경우든 암호화 양에 대비한 암호화 효과는 매우 높다는 것을 알 수 있다.

그림 3에서 Lena 영상(a)에 대해 모든 데이터를 암호화 한 결과(b)와 모든 부대역의 MSB만을 암호화한 결과(c)를 비교하였다. 좌하단에 나타낸 PSNR(Peak Signal to Noise Ratio)은 전체 데이터를 암호화 경우가 훨씬 낮은 값을 보이나, MSB만을 암호화한 (c)의경우도 영상을 숨기기에는 충분하다. MSB만을 선택하여 암호화를 수행하면 암호화 양은 원 영상 데이터의 1/8에 해당한다.

2. 부대역의 선택

그림 2에서 나타낸 것과 같이 DWT 결과의 부대역들은 서로 원영상에 대한 다른 주파수 성분들을 포함하고 있다. DWT 레벨이 증가할수록 저주파 성분이 강하며, 따라서 인간의 눈에 대한 중요도가

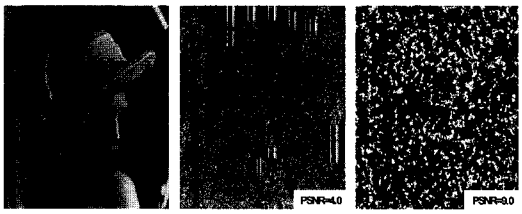


그림 3. 부분 데이터 암호화; (a) 원영상, (b) 모든 데이터를 암호화한 결과, (c) MSB만 암호화한 결과
Fig. 3. Partial data encryption; (a) Original image, (b) result from encrypting all the data, (c) result from encrypting only MSBs

증가한다. LL4를 양자화과정에서 제외하는 만큼 이 영역의 계수들은 원 영상의 매우 중요한 성분들을 포함하고 있다.

앞에서 설명한 바와 같이 그림 2의 DWT결과는 DCT의 경우와는 달리 각 부대역은 서로 다른 주파수 성분일 뿐 전체 영상에 대한 정보를 포함하고 있다. 따라서 각 부대역은 복원 시 전체영상에 영향을 준다. 영상정보를 숨기는 작업은 영상정보가 전송되는 동안 하락되지 않은 사람이 영상정보를 포획하여 그 영상의 내용을 파악하거나 그 영상을 다시 사용하지 못하게 하는 것이 목적이다. 따라서 암호화 결과 영상을 인식하지 못하거나 영상을 다시 사용하지 못할 정도로 영상이 왜곡된다면 반드시 전체영상을 암호화할 필요는 없다. 더구나 암호화 알고리듬이 복잡한 과정을 거쳐 수행되므로 암호화를 위한 처리시간 때문에 전체 영상처리시간에 큰 영향을 줄 수

있으며, 특히 무선통신의 경우 암호화 및 복호화 과정으로 인한 지연시간(latency time)과 전력소모는 큰 장애요소가 되고 있다[8][9]. 따라서 가능하면 암호화 양을 최소로 하는 것이 바람직하다.

앞에서 언급한 바와 같이 인간의 눈에 가장 큰 영향을 주고 가장 많은 영상정보를 담고 있는 부대역이 최저주파 부대역, 즉 LL4이다. 따라서 부대역을 선택하는데 있어서 가장 우선이 되어야 하는 부대역은 LL4이다. 그림 4 (a) LL4만을 선택하여 MSB만을 암호화한 결과 영상을 보여주고 있다. 그림에 나타낸 것과 같이 PSNR값이 전체영상을 암호화한 경우(그림 3 (c))와 큰 차이를 보이지 않는다. 그러나 그림에서 볼 수 있듯이 이 영상을 다른 목적으로 사용할 수 없을 정도로 영상이 왜곡되었다 하더라도 원 영상의 고주파 성분이 상당부분 남아있음을 알 수 있다. 이 고주파성분의 잔존은 대부분의 응용분야에서는 수용 가능하지만 특정 응용분야(예를 들어 군사적인 목적 등)에서는 수용할 수 없는 경우가 있다. 따라서 이 고주파 성분을 더욱 왜곡시킬 필요가 있을 수 있다.

그림 4 (a)의 고주파 성분을 더욱 왜곡시키기 위해서는 LL4보다 고주파 부대역에 대한 암호화를 수행하여야 한다. 그러나 암호화 양의 증가를 고려할 때 가장 적절한 선택은 HH4이다. 그림 4 (b)에 LL4와 HH4의 MSB만을 암호화한 결과 영상을 나타내었다. 그림 4 (a)와 비교할 때 PSNR은 큰 차이를 보이지 않지만 가시적인 암호화 효과는 (a)에 비해 훨씬 높음을 알 수 있다(암호화 결과에 있어서 PSNR이 절대적인 암호화 효과를 나타낸다고는 볼 수 없음). 즉, LL4와 HH4의 MSB만을 암호화한 결과는 원 영상을 거의 인식할 수 없을 정도의 충분한 효과를 얻을 수 있다.

그림 4 (c)에서 보인 바와 같이 레벨 4의 네 부대역을 모두 암호화대상에 포함시키면 그림 4 (b)보다 더 고주파 성분을 정밀하게 왜곡시킴을 알 수 있다. 영상에 따라 다소의 차이가 있으나, 레벨-4의 네 부대역을 모두 포함하는 (c)의 경우가 일반적으로는 (b)의 경우에 비해 더욱 암호화효과가 두드러지는 것을 실험적으로 확인할 수 있다. 그림 4의 (b)나 (c)의 경우보다 더 고주파 성분을 왜곡시키고자 한다면, 그림 4 (d)에 보인 것과 같이 LL4와 HH3을 암호화대상에 포함시킬 수 있다. 또는 더욱 영상을 왜곡시킬 필요가 있는 경우는 레벨-4의 모든 부대역과 HH3을 암호화할 수 있다. 많은 부대역을 포함할수록 암호화효과는 증가하겠으나, 상대적으로 암호화에 소요되는 시간과 비용은 기하급수적으로 늘어난다.

n 레벨 2DDWT를 수행하는 경우 레벨-k의 한 부대역(LLk, HLk, LHk, 또는 HHk)의 크기 Zk는,

$$Z_k = \frac{1}{2^{2k}} Z_0, \quad 1 \le k \le n \qquad (1)$$

이며, 이 때 Z0은 원영상의 크기를 나타낸다. 따라서 4-레벨의 2DDWT를 수행한 경우 레벨 4의 각 부대역은 원영상의 1/28=1/256의 크기에 해당하며, 원영상에서 한 화소를 나타내는데 8 비트를 사용한다고 가정하면 그림 4의 네 방법의 원영상의 데이터양에 대비한 암호화양은, 1/2048, 1/1024, 1/512, 1/409.6에 해당한다.

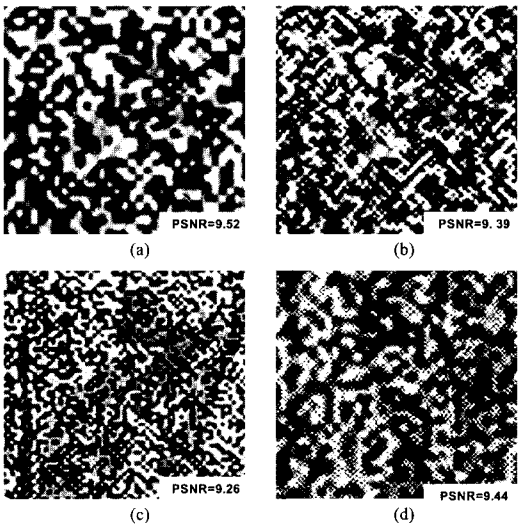


그림 4. 부대역 선택; (a) LL4만 선택, (b) LL4와 HH4 선택, (c) 레벨4의 네 부대역 선택, (d) LL4와 HH3 선택.
Fig. 4. Selection of sub-bands; (a) LL4 only, (b) LL4 and HH4, (c) All four sub-bands in level 4, (d) LL4 and HH3

3. 부대역 내의 화소 선택

그림 3과 그림 4의 암호화 방식은 특정 부대역 또는 부대역들의 모든 화소들을 포함한다. 그러나, 암호화과정이 영상정보를 숨기는 것을 목적으로 하고 공격자가 원래의 영상정보를 쉽게 구하지 못하게 하는 것이 목적이므로[7] 특정 부대역의 화소들을 모두 포함하는 것보다 그 중 일부분을 선택하고, 그 선택 방법을 숨기는 것이 공격에 대한 강인성을 더욱 높이는 방법이다.

특정 부대역에서 암호화 대상 화소들을 선택하는 방법으로 본 논문에서는 무작위(더욱 엄밀히 말하면 의사무작위) 패턴을 사용한다. 무작위 패턴을 생성

하는 방법은 여러 가지가 있으나, 여기서는 선형귀환 쉬프트 레지스터(LFSR, Linear Feedback Shift Register)를 사용한다. 그림 5에 LFSR을 나타내었는데, 이 LFSR의 동작순서는 다음과 같다. 먼저, Initial Value Control 신호를 '1'로 하여 LFSR의 초기치(S1~Sn)를 입력한다. 그 후 LFSR 함수를 수행할 때마다 병렬출력(R1~Rn)에 주어진 비트수의 무작위 수가 생성된다. n 비트 LFSR의 경우 한 사이클의 최고 길이는 2n-1(모든 비트가 0이 되는 경우를 제외)이다. LFSR의 초기값은 영상정보를 암호화할 때 사용되는 암호화 키의 일부분 또는 전체 키를 특정함수를 통해 축소하여 사용한다. LFSR의 성격상 초기값이 다르면 출력되는 패턴이 달라진다. 따라서 초기값, 즉 암호화 키를 모르면 출력 시퀀스를 알 수 없고, 만약 출력시퀀스에 따라 암호화 대상화소를 결정한다면 공격자가 쉽게 암호화 대상화소를 찾을 수 없다.

그림 5의 LFSR 출력은 귀환되는 값에 따라 특성을 달리한다. 암호화와 관련하여 병렬출력을 사용한다면 반복되는 주기를 최대로 하는 것이 바람직하다. 이것은 귀환 특성 방정식이 primitive 다항식이 되도록 구성하여 얻을 수 있으며, 본 논문에서는 32 비트 LFSR을 구성하여 다음의 특성다항식을 구현하여 사용한다.

$$P(x) = x^{32} + x^{22} + x^2 + x + 1 \qquad (2)$$

이러한 LFSR은 다음의 특성을 갖는다. 출력 시퀀스의 길이가 충분히 길다고 가정하면, 특정 비트(i)에서 특정 시간(j)에 '0'과 '1'이 나올 확률은 거의 같다. 즉,

$$\Pr(b_{ij} = 0) = \Pr(b_{ij} = 1) = \frac{1}{2} \qquad (3)$$

가 된다. 또한 n 비트 중 k 비트를 선택하는 경우 k 비트가 구성하는 조합은 2k(0, 1, · · ·, 2k-1)이며 각 조합의 발생확률 또한 거의 같다. 따라서 k 비트를 선택하는 경우 k 비트의 평균값은,

$$AVG_k = \frac{2^k - 1}{2} \qquad (4)$$

이다. k 비트를 화소선택에 사용하는 경우, 본 논문에서는 k 비트의 값을 현재의 암호화 대상 화소에서 다음 암호화 대상 화소까지 지나쳐야 하는 화소의 개수로 사용한다. 이 경우 k 비트에 의한 평균 화소 선택률 SRk는,

$$SR_k = \frac{2}{2^k + 1} \qquad (5)$$

이 된다. 즉, SR1=2/3, SR2=2/5, SR3=2/9, SR4=2/17,··· 가 된다.

그림 6에 그림 4 (b)의 LL4-HH4 경우에 대해 그림 5의 출력비트 중 사용한 비트수에 따른 암호화 결과를 보였다. 그림에서 보는 바와 같이 사용 비트 수가 증가함에 따라 영상의 암호화 효과는 급격히 감소하는 것을 볼 수 있으며, (a)와 (b)는 영상자체를 숨기는 용도로 사용할 수 있으나, (c)와 (d)의 경우는 영상을 재사용하지 못하도록 하는 용도 정도로 밖에 사용할 수 없음을 알 수 있다. 많은 영상으로 실험한 결과 LFSR의 세 비트 이상을 사용하는 경우는 원 영상을 인식할 수 있었으며, 한 비트 또는 두 비트를 사용하는 경우 원 영상 자체를 모르는 상태에서는 그 영상을 인식하기 어려웠다.

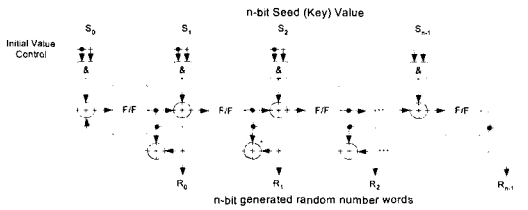


그림 5. 무작위 패턴 생성을 위한 LFSR
Fig. 5. LFSR to generate random patterns

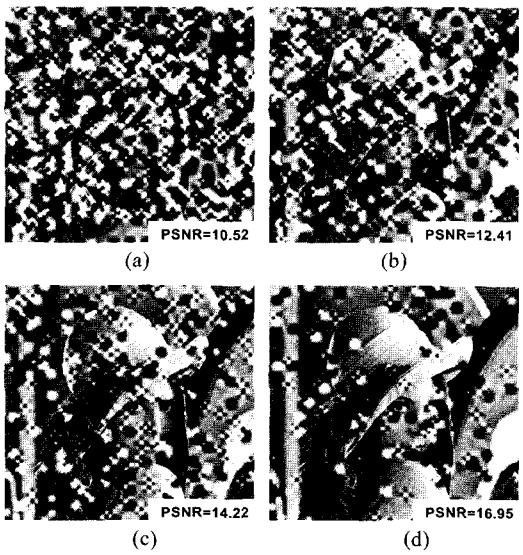


그림 6. 무작위 선택 후 암호화 결과; (a) 1 비트 사용, (b) 2 비트 사용, (c) 3 비트 사용, (d) 4 비트 사용.
Fig. 6. Result from encryption after random selection; (a) using 1 bit, (b) using 2 bits, (c) using 3 bits, (d) using 4 bits

Ⅳ. 선택적 부분 암호화/복호화 과정

앞장에서 설명한 본 논문의 영상암호화 및 복호화 진행과정을 그림 7에 나타내었다. 암호화 과정(그림 7 (a))은 양자화기를 지난 결과의 영상데이터를 입력으로 받아 먼저 암호화할 부대역을 선택한다. 암호화를 위한 키 중 일부를 LFSR의 초기값으로 사용하여 LFSR 동작을 수행하며, 출력 중 일부 비트들을 선택하여 특정 부대역 중 암호화 대상에 포함할 회소값들을 결정한다. 선택된 값 화소값들 중 MSB만을 골라 암호화 블록을 형성하여 암호화를 수행하고, 그 결과를 다시 원래의 위치로 되돌려 놓는다. 복원과정(그림 7 (b))은 영상복원 과정 중 엔트로피 디코딩을 거친 결과를 대상으로 암호화와 같은 과정을 반복하는데, 이 때 암호화 대신 복호화를 수행한다. 암호화 및 복호화 과정에서 암호화 알고리듬으로 본 논문에서는 128-비트 국내표준 블록 암호화 알고리듬인 SEED[23]를 사용하였다. 그러나 암호화 알고리듬으로는 본 논문에서 제시한 방법의 다른 부분에 영향을 주지 않고 다른 암호화 알고리듬을 사용할 수 있다.

암호화 알고리듬에 사용되는 암호화 키는 LFSR의 초기값과 LFSR의 출력비트들을 선택하는 데도 사용된다고 하였는데, 그 방법을 그림 8에 나타내었다. 암호화 키의 128 비트(다른 암호화 알고리듬의 경우는 그 암호화 알고리듬에 해당하는 키의 비트수)중 가장 처음 '1'을 만나서부터 37 비트를 선택하여 사용한다. 이 중 32 비트는 LFSR의 초기값으로 사용되는데, 처음 '1'을 만났을 때부터 32 비트를 선택하는 이유는 초기값으로 모든 비트가 '0'인 값이 입력되면 LFSR의 출력은 모든 비트가 '0'인 조합만을 출력하기 때문이다. 37 비트 중 나머지 5 비트는 32 비트 LFSR 출력 중 특정 출력을 지정한다. 그 출력부터 사용될 출력비트수 만큼의 출력을 선택하게 되는데, 5 비트의 값이 P이고 b 비트를 사용하는 경우 출력비트의 선택은,

$$\begin{aligned} P &\bmod 32 \\ (P+1) &\bmod 32 \\ (P+2) &\bmod 32 \\ &\cdots \\ (P+b-1) &\bmod 32 \end{aligned}$$

의 b 비트를 선택한다. 출력비트의 위치를 결정하는데 있어서 암호화 키의 일부분을 사용하는 것은 영상 암호화 방법의 강인성을 높이기 위해서이다.

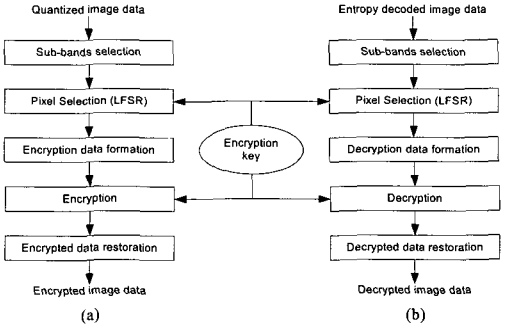


그림 7. 선택적 부분 영상 암호화/복호화 과정; (a) 암호화, (b) 복호화.
Fig. 7. Selectively partial image encryption/decryption procedures; (a) Encryption, (b) Decryption

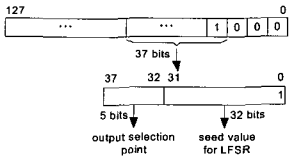


그림 8. LFSR seed 값 및 출력비트 선택
Fig. 8. LFSR seed value and selection of the output bits

Ⅴ. 실험 및 결과

본 장에서는 Ⅲ장과 Ⅳ장에서 설명한 본 논문에서 제시한 영상암호화 방법에 대한 실험데이터를 소개한다. 본 논문에서는 앞에서 설명한 영상암호화 방법을 C-언어로 구현하였고, 최적화 과정은 거치지 않았으며, 약 500개의 영상을 대상으로 실험을 수행하였다. C 프로그램을 수행시킨 환경은 Pentium Ⅳ 1.7GHz 환경이었으며, CPU 시간은 C 프로그램의 유틸리티를 사용하였다. 영상의 화질은 편의상 평균 PSNR로 나타내었으나, 이 값이 절대적으로 영상의 화질을 대표할 수 있다고는 할 수 없음을 다시 한 번 강조한다. Ⅲ장의 설명을 진행하면서 이미 영상의 예를 보였기 때문에 여기서는 500여 개 영상에 대한 평균치로만 설명하도록 한다.

표 1에 앞에서 언급한 네 가지 부대역 선택방법과 LFSR 비트의 선택방법에 대한 평균 PSNR과 평균 CPU 시간을 나타내었으며, 그림 9에 이를 그래프로 나타내었다. 표에서 제일 좌측의 'bits'는 화소를 선택하는데 사용된 LFSR 비트수를 나타내며, 여기서 '0'은 LFSR의 비트를 사용하지 않은 경우,

즉 모든 화소를 암호화대상에 포함시킨 경우를 뜻한다. 표 1과 그림 9에서 보는 바와 같이 LFSR의 특정 비트수를 사용하는 경우 네 가지의 부대역 선택방법들에 대한 PSNR은 큰 차이를 보이지 않으나 수행시간에 있어서는 약 3배에서 7배까지의 차이를 보이고 있다. 실제 암호화된 영상을 보면 네 방법의 화질에서 뚜렷한 차이를 볼 수 있으며, 따라서 PSNR이 이 경우에는 좋은 비교항목이 되지 못함을 알 수 있다. LFSR 사용비트 수가 증가함에 따라 PSNR의 증가가 확연함을 알 수 있고(실제의 결과영상에서도 뚜렷이 나타남), 반면에 CPU 시간은 급격히 감소한다. 따라서 영상화질(암호화 효과)과 CPU 시간은 상보적인 관계임을 알 수 있고, 응용분야에 따라서 적절한 암호화 알고리듬을 선택할 수 있다.

표 2에는 원영상의 데이터양에 대해 본 논문에서 제시하는 암호화 방법들의 암호화 데이터 양을 나타내었다. 앞에서 언급한 것과 같이 LFSR의 출력 비트 중 세 비트 이상을 사용하는 경우를 제외하고, 또 암호화 효과가 조금 떨어지는 LL4만을 암호화하는 경우를 제외하더라도, 가장 많은 양을 암호화하여야 하는 LL4-HH3 조합의 LFSR 비트를 사용

표 1. 영상 암호화의 평균화질 및 CPU 시간
Table 1. Average image quality and CPU time for image encryption

item / bits	Average PSNR (dB)				Average CPU time (ms)			
	LL4	LL4 HH4	level 4	LL4 HH3	LL4	LL4 HH4	level 4	LL4 HH3
0	7.966	7.760	7.699	7.830	22.118	40.185	74.805	96.248
1	9.244	8.573	7.933	8.561	15.420	35.033	74.190	94.908
2	10.651	9.725	8.579	9.602	9.765	22.710	47.073	59.938
3	11.961	10.888	9.470	10.872	6.730	15.533	32.388	36.893
4	14.598	13.232	11.372	13.043	3.360	8.480	19.475	21.675

하지 않는 경우 1:409.6이며, 가장 적은 양인 LL4-HH4 조합의 LFSR 한 비트를 사용하는 경우는 1:1,536이다. 이 양은 전체영상을 숨기기 위한 암호화 양으로서는 매우 적은 양이라고 할 수 있으며, 따라서 본 논문에서 제시한 방법이 작은 양의 암호화로 큰 암호화 효과를 얻을 수 있음을 나타내준다.

영상의 암호화에 대한 암호화 효과는 일부 주관적일 수 있다. [19], [20], 그리고 [21]의 논문에서도 본 논문과 마찬가지로 암호화 효과에 대해서는 일부 주관적인 판단을 내리고 있는데 이는 영상에 대해서 원래의 영상과의 왜곡 정도를 PSNR로 판단하는 것이 보통이지만 PSNR이 15dB이하일 경우에 영상과 PSNR간의 상관도가 거의 없어지는 것이 보통이기 때문이다. 영상암호화의 경우 PSNR을 10dB이하로 유지해야 하기 때문에 그 이하에서는 암호화 효과에 대해서 주관적인 시각적 인지도를 따를 수 밖에 없다.

기존의 연구들에서 살펴보면 암호화 율과 영상의 질(dB 혹은 MSE) 그리고 연산 시간들의 상호관계

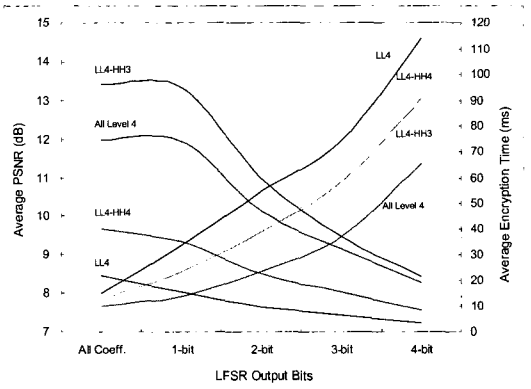


그림 9. 암호화 결과영상의 화질 및 암호화 수행시간
Fig. 9. Image quality of the encrypted images and execution time

표 2. 원영상 데이터에 대한 암호화 양
Table 2. Amount of encryption to the original image data

bits	LL4	LL4-HH4	Level 4	LL4-HH3
0	1:2,048	1:1,024	1:512	1:409.6
1	1:3,072	1:1,536	1:768	1:614.4
2	1:5,120	1:2,560	1:1,280	1:1,024
3	1:9,216	1:4,608	1:2,304	1:1,843.2
4	1:17,408	1:8,704	1:4,352	1:3,481.6

를 명확히 나타내지 못하고 있다. 이는 앞서 언급한 것과 같이 영상암호화 결과가 일부 주관적인 판단에 근거를 하기 때문이다. 현재 JPEG2000을 위한 영상 보안 및 보호 기술로써 웨이블릿 기반의 영상암호화에 대한 연구는 초기 단계이고 수치적인 비교를 할 적당한 보편적인 객관적 결과가 나와 있지는 않다. [18]에서는 암호화 율을 언급하였는데 실제적인 수치적인 해석은 나타나있지 않고 [15], [16], [20], [21] 등의 논문에서 사용하고 있는 암호화 방식들은 웨이블릿의 제로트리 기반의 암호화 방식인데 제로 트리 기반의 영상압축 방식이 가지는 코딩 패스의 반복수, 즉 압축율에 따른 암호화율을 따져야 본 논문의 결과와 비교가 가능하다. 그러나 논문들에서 이러한 결과들에 대한 수치적, 혹은 그래프적인 결과 및 경향성 제시를 하지 않고

있기 때문에 비교가 어렵다. 하지만 제로트리 기반의 양자화 방식에 의해 일반적인 30dB의 영상 화질을 가질 수 있는 압축율이라면 20:1에서 30:1의 암호화 율을 보이므로 본 논문에서 제시한 알고리즘이 우수하다는 것을 알 수 있다. 또한 [21]과 [24]에서 각각의 방식이 각각 2%와 13%~27%의 데이터를 암호화하면서 유사한 암호화 효과를 보이므로 본 논문에서 제시한 알고리즘이 효율면에서 상당히 개선되었음을 볼 수 있다.

Ⅵ. 결 론

본 논문에서는 웨이블릿 영역에서 암호화를 통해 영상정보를 숨기는 방법을 제시하였다. 이 방법은 웨이블릿 변환 및 양자화 과정을 거친 영상데이터를 대상으로 하며, 웨이블릿 변환 결과의 주파수 대역에 따라 암호화 대상을 선택한다. 각 화소가 갖는 데이터 중 MSB만을 암호화 대상에 포함시키며, 특정 부대역에서 암호화 대상이 되는 화소들의 위치를 숨기기 위해 무작위로 화소를 선택하는 방법을 취하였다. 무작위 선택을 위해서는 LFSR을 사용하였으며, LFSR의 병렬출력 비트들 중 일부분으로 화소를 선택하도록 구성하였다. 암호화 키는 선택된 영상 데이터를 암호화하기 위해서 뿐만 아니라 LFSR의 초기치와 병렬출력 비트를 선택하는 데에도 사용하여 암호화 강도를 높였다. 부대역의 선택 및 LFSR의 출력 중 사용비트 수를 변화하여 가능한 여러 방법을 제시하였다.

제안한 암호화 방법은 C-언어로 구현하여 실험을 수행하였으며, 실험은 약 500개의 영상을 대상으로 하였다. 평균 PSNR 및 영상의 암호화 정도를 비교할 때 합리적인 암호화 효과는 원 영상 데이터의 약 1/1,000의 데이터 양을 암호화하여 얻을 수 있었으며, 영상에 따라서는 1/2,000 이하의 양을 암호화하여서도 영상을 숨기는 효과를 충분히 발휘할 수 있는 것으로 나타났다. 본 논문에서 제시한 여러 선택 가능한 방법이 암호화 효과와 암호화 수행시간 간에 상보적인 관계가 있음을 보였으며, 이것은 응용분야에 또는 영상을 전송하는 네트워크의 상태에 따라 암호화 방식을 적응적으로(adaptively) 선택할 수 있음을 시사하는 것이다.

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 웨이블릿 변환 및 양자화과정 등이 소프트웨어의 경우 완전히 직렬로 수행되어야 하나, 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.

본 논문에서 제안한 방식은 암호화 효과와 암호화 수행시간의 상보적인 관계를 이용하여 적응 암호화 알고리듬으로 구현할 수 있다. 특히 무선통신의 경우 네트워크의 상태와 무선단말기의 전력소모, 그리고 영상의 중요도에 따라서 암호화 방식을 선택할 수 있도록 하여 적응성을 부여할 수 있다. 또한 본 논문에서 제안한 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] Want, R and Borriello, G, "Survey on Information Appliances", *IEEE Compute Graphics and Applications*, Vol. 20 Issue 3, pp. 24-31, May-June 2000

[2] Chisalita, I. and Shahmehri, N, "Issues in image utilization within mobile e-services" *Proceedings of WET ICE 2001*. Proceedings. pp. 62-67, 2001

[3] J. D. Gibson, et al., *Digital Compression for Multimedia, Principles and Standards*, Morgan Kaufmann Pub., San Francisco CA, 1998.

[4] R. M. Rao, and A, S. Bopardikar, *Wavelet Transforms, Introduction to Theory and Applications*, Addison-Wesley, Readings MA, 1998.

[5] Martin Boliek, et al., *JPEG 2000 Part I Final Draft International Standard*, ISO/IEC JTC1/SC29 WG1, 24 Aug. 2000.

[6] Stajano, F. and Isozaki, H. "Security issues for Internet appliances", *Proceedings of Applications and the Internet (SAINT) Workshops*, pp. 18-24, 2002

[7] William Stallings, *Cryptography and Network Security, Principles and Practice, 2nd Ed.*, Prentice Hall Inc., Upper Saddle River,

NJ., 1999.

[8] Sandra K. Miller, "Facing the Challenge of Wireless Security", *IEEE Computer Magazine,* pp. 16-18, July 2001.

[9] S. R. Ravi, et al., "Securing Wireless Data: System Architecture Challenges", *ISSS'02*, pp. -, Oct. 2002.

[10] *Wireless Application Protocol, WAP 2.0*, www.wapforum.org, Jan. 2002.

[11] *WAP Transport Layer ENd-to-end Security*, www.wapforum.org, WAP-187-TransportE3ESec-20010628-a, June 28 2001.

[12] Certicom whiter paper, "Introduction to Information Security", www.certicom.com /resources/w_papers/w_papers.html.

[13] C. Shi and B. Bhargava, "A Fast MPEG video Encryption Algorithm", *Proceeding of ACM Multimedia,* pp. 81-88, 1998.

[14] L. Qioa, and K. Nahrstedt, "Comparison of MPEG Encryption Algorithms", *Int'l J. on Computers and Graphics*, Vol. 22, No. 3, pp. 437-444, March 1998.

[15] Andeas Pommer and Andeas Uhl, "Wavelet Packet Methods for Multimedia Compression and Encryption", *IEEE Pacific Rim Conf. on Communications, Computers and Signal Processing*, pp. 1-4, Aug. 2001.

[16] Andeas Pommer, "Selective Encryption of Wavelet-Coded Image Data", http://www.ganesh.org/, May 22 2002.

[17] Xiaolin Wu and Peter W. Moo, "Joint Image/Video Compression and Encryption via High-Order Conditional Entropy Coding of Wavelet Coefficients", *IEEE Int'l Conf. on Multimedia Computing and Systems*, pp. 908-912, 1999.

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

[19] Haward Cheng and Xiaobo Li, "Partial Encryption of Compression Images and Videos", *IEEE Trans. on Signal Processing*, Vol. 48, No. 8, pp.2439-2451, Aug. 2000.

[20] J. M. Shapiro,"Embedded Image Coding using Zerotrees of Wavelet Coefficients", *IEEE Trans. on Signal Processing*, Vol. 41, No. 12, pp. 3445-3462, Dec. 1993.

[21] Amir Said, et al., "A New Fast and Efficient Image Codec based on Set Partitioning in Hierarchical Trees", *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 6, No. 3, pp. 243-250, June 1996.

[22] Solomon W. Golomb, *Shift Register Sequences*, Aegean Park Press, 1982

[23] KISA, *128-Bit Symmetric Block Cipher (SEED), TTAS.KO-12.0004*, 28, Sep. 1999.

[24] 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.

서 영 호(Young-Ho Seo) 준회원

e-mail : design@kw.ac.kr
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

<주관심분야> Image Processing/Compression, 워터마킹, 암호학, FPGA/ASIC 설계

Sujit Dey (S'90~M'91) received the Ph.D. degree in computer science from Duke University, Durham, NC, in 1991. He is a professor in Department of Electrical and Computer Engineering, University of California at San Diego (UCSD), La Jolla. His research group at UCSD is developing configurable platforms, consisting of adaptive wireless protocols and algorithms, and deep submicron adaptive system-on-chips, for next-generation wireless appliances as well as network infrastructure devices.

김 동 욱(Dong-Wook Kim) 정회원

1983년 2월 : 한양대학교 전자공학과 졸업(공학사).
1985년 2월 : 한양대학교 대학원 졸업(공학석사).
1991년 9월 : Georgia 공과대학 전기공학과 졸업(공학박사).
1992년 3월~현재 : 광운대학교 전자재료공학과 정교수. 광운대학교 신기술 연구소 연구원.
1997년 12월~현재 : 광운대학교 IDEC 운영위원.
2000년 3월~현재 : 인티스닷컴(주) 연구원.

<주관심분야> 디지털 VLSI Testability, VLSI CAD, DSP 설계, Wireless Communication
e-mail : dwkim@daisy.kw.ac.kr