카오스 시스템에 의한 DWT기반 영상의 적응적 암호화

김수민, 서영호, 김동욱
광운대학교 전자재료공학과 디지털 설계 및 테스트 연구실
전화 : 02-940-5167 / 핸드폰 : 019-613-0748

Adaptive Encryption for DWT-based Images by Chaotic system

Su-Min Kim, Young-Ho Seo, and Dong-Wook Kim
Department of Electronic Materials Eng., Kwangwoon University
E-mail : sumin@kw.ac.kr

Abstract

Security of digital images attracts much attention recently, and many image encryption methods have been proposed. This paper proposed an image encryption methodology to hide the image information. The target data of it is the result from quantization in the wavelet domain. This method encrypts only part of the image data rather than the whole data of the original image. For ciphering the quantization index we use a novel image encryption Algorithm called BRIE(Bit Recirculation Image Encryption). which was proposed by J. C. Yen and J. I. Guo in 1999. According to a chaotic binary sequence generated by BRIE, the block which is produced by quantization index is cyclically shifted in the right or left direction. Finally, simulation results are included to demonstrate its effectiveness.

I. 서론

21세기를 '정보화 시대'라 부를 만큼 현대의 생활에서 정보의 비중이 기하급수적으로 증가하고 있고, 특히 영상과 비디오 컨텐츠에 대한 선호도가 매우 급속히 증가하고 있다[1]. 그러나 영상/비디오는 그 자체의 데이터양이 매우 많아 최근의 연구방향은 주로 이들의 데이터양을 줄이는 것에 주안점을 두고 있다[2]. 영상/비디오의 데이터양을 줄이는 연구는 지금까지 두 주류를 형성하고 있다. 현재 가장 널리 사용되고 있는 분야는 JPEG 및 MPEG 분야로, 지금까지 상당부분이 국제표준으로 채택되었으며[2], 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 DCT 보다 좋은 화질을 보여[3], 최근에는 영상의 표준 변환방식 으로 채택되기도 했다[4].

본 논문에서는 현재 JPEG2000의 표준안으로 채택된 정규적인 DWT 방법과 선형양자화기를 사용하는 영상처리를 가정한다. 영상정보의 암호화는 양자화 과정을 거친 데이터를 대상으로 하며, DWT 결과의 부대역 중 일부 부대역만을 택하여 암호화를 수행 실시한다. 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 논문에서 제안하는 암호화 방식으로는 카오스 시스템(Chaotic system)을 기반으로 랜덤비트(random bit)를 생성하는 방법으로 1999년에 제안된 BRIE(Bit Recirculation Image Encryption)알고리즘[5]을 이용하였다.

II. 부대역의 선택

본 논문에서는 512×512 화소의 영상을 대상으로 하며, 그림 1에 나태낸 것과 같이 4-레벨 2차원 DWT를 수행하는 영상압축을 가정한다. 그림 1의 숫자는 선형양자화기가 양자화를 수행할 때 각 부대역에 할당된 비트수를 나타낸다. 이 양자화기에 의한 압축률은 약 20대 1이다. DWT 가 진행될수록 영상의 저주파 성분이 형성되므로 LL4가 영상의 가장 저주파성분에 해당하고 HVS(Human Visual System)에 의해서 저주파 성분이 상대적으로 더욱 중요한 정보를 담고 있다.

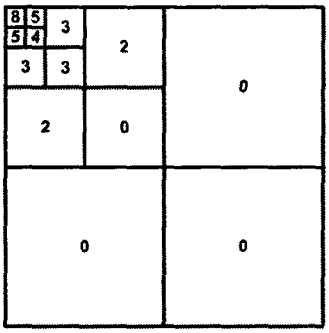


그림 1. 4-레벨 2차원 DWT 결과의 부대역

HVS 에 의해서 저주파 성분이 상대적으로 인간의 눈에 더욱 민감하므로 영상전체가 아닌 영상의 일부분을 암호화하여 영상정보를 숨기기 위해서는 저주파 성분을 암호화하는 것이 더욱 효과적이다. 따라서 그림 1의 LL4는 암호화 할 때 반드시 포함되어야 한다. 그러나 LL4만을 암호화 할 경우 고주파성분이 그대로 드러나 영상에 따라서는 어떤 종류의 영상인지를 구분할 수 있다. 따라서 본 논문에서는 다양한 실험을 통해서 다음의 4가지 종류의 부대역 조합을 선택하였다.

① LL4
② LL4와 HH4
③ Level 4의 네 부대역
④ Level 4의 네 부대역과 HH3

III. 암호화/복호화 알고리즘

3.1 카오스 시스템

카오스이론은 결정론적 비선형 동역학 시스템에서 나타나는 불규칙하고 예측 불가능한 양상을 정성적으로 연구하는 학문이다. 카오스란 말은 원래 무질서 또는 복잡함을 뜻하는 고대 그리스어로부터 유래 하였지만, 공학에서는 결정론적 비선형 동역학 시스템으로부터 생성되는 복잡하고 잡음과 같은 현상을 말한다[6].

카오스 시스템이 가지는 특징으로 두 가지를 들 수 있는데 위상공간상에 유한한 영역내에서 주기성이 없이 그려지는 이상한 끌개(Strange Attractor)와 초기조건의 민감성을 들 수 있다. 식(1)은 카오스함수를 나타내는데 여기서 x_0는 초기값을 나타내고 파라메타, r이 3.5의 이상인 범위에서는 수렴값을 알 수 없는 특성을 가진다. 즉, 그림 2에서 보는 것 같이 r값이 1에서는 하나의 수렴값을 가지다가 분기가 일어나면서 3.5이상의 어느 영역에서는 수렴값을 알아 볼 수 없게 됨을 알 수 있다[7].

$$x_{n+1} = r x_n (1 - x_n) \qquad (1)$$

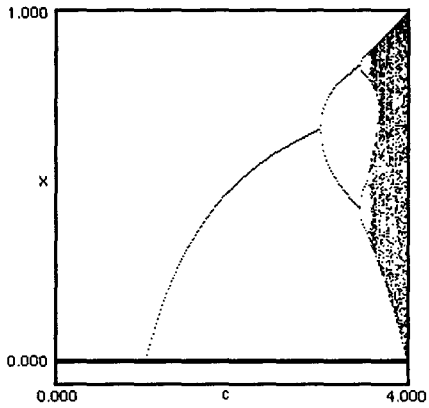


그림 2. $f_a(x) = rx(1-x)$ 함수에 대한 분기도형

3.2 BRIE 알고리즘

본 논문에서 제시한 BRIE 알고리즘의 전체적인 암호화 과정을 살펴보면 원 영상을 4-레벨 DWT 를 수행하면 13개의 부대역으로 나눠지게 된다. 원 영상이 M×N 크기의 영상일 때 식 (1)에 의해서 $\{x(i)\}^{[MN/8]}$의 값을 얻게 되고 식 (2)에 의해 $\{b(i)\}^{MN}$을 얻을 수 있다.

$$x(i) = 0.b(8i+0)b(8i+1)\cdots b(8i+7) \qquad (2)$$

알고리즘에서 p, q값에 의해 암호화 정도가 결정된다. 즉, p=0일 때 왼쪽 쉬프트를 하고 p=1일 때는 오른쪽 쉬프트를 하게 된다. 여기서 p값은 식 (2)에 의해 얻어지고, q값은 쉬프트하는 횟수로써 미리 정해진 키 값인 α, β에 의해 얻어지게 된다.

$$f(x,y)\,(0 \leq x \leq M-1, 0 \leq y \leq N-1)$$
$$f'(x,y) = ROLP_p^q(f(x,y)),$$
$$p = b(N\times x+y),\ q = \alpha + \beta \times b(N\times x+y+1)$$
$$ROLP_p^q(x = b_7 b_6 \cdots b_0) = \begin{cases} \sum_{i=1}^{7} b_i \times 2^{(i-q+8) \bmod 8}, & p = 0 \\ \sum_{i=1}^{7} b_i \times 2^{(i+q) \bmod 8}, & p = 1 \end{cases}$$
$$f(x,y) = ROLP_{1-p}^{8-q}(f'(x,y)) = ROLP_p^{8-q}(f'(x,y))$$

그림 3. BRIE 알고리즘의 유사코드

본 논문에서 제안하는 방법은 1)암호화를 수행할 때 일정한 블록의 크기(8bits, 16bits, 32bits)로 나누어서 암호화하는 것과 2)q값을 정해진 키 값이 아닌 카오스 시스템을 이용한 랜덤한 수를 생성하여 q값을 조절하여 암호화하는 것이다.

Ⅳ. 암호화 과정

영상을 암호화하는 위치는 앞에서 언급한 바와 같이 양자화와 엔트로피 코딩 사이에서 일어나며, 그 과정은 그림 4에 나타낸 것과 같다. 양자화 계수를 대상으로 먼저 암호화될 부대역을 결정하고 양자화 계수를 일정한 블록(8bits, 16bits, 32bits)에 넣은 후에 BRIE 알고리즘에 의해 암호화를 수행하게 된다.

일반적인 암호화 알고리즘이 그렇듯이 본 논문에서도 암호화/복호화를 위한 암호화 키는 통신대상 양측에서 이미 보유하고 있다고 가정한다.

Ⅴ. 구현 및 실험결과

2장, 3장, 4장에서 설명한 영상의 선택적 부분 암호화 방법은 C언어로 구현하였으며, 실험환경은 Pentium IV 1.5Mhz의 PC이었다. 본 논문의 영상암호화 알고리즘은 본 연구실에서 연구한 DWT-기반 영상압축기 중 양자화기와 엔트로피인코더 사이에 삽입하는 형태로 구현하였다. 사용된 암호화 키는 α=6, β=12, x_0=0.75, r=0.75 이다.

먼저 2장에서 선택한 각 부대역의 조합에 각각에 블록에 맞게 암호화를 수행하였다. 암호화 할 때 암호화

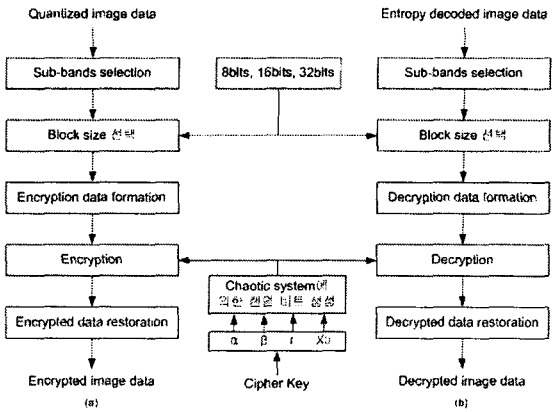
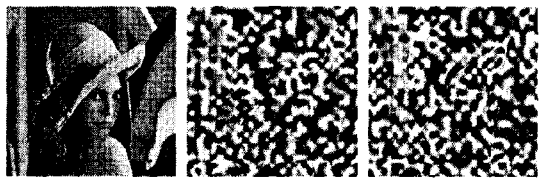
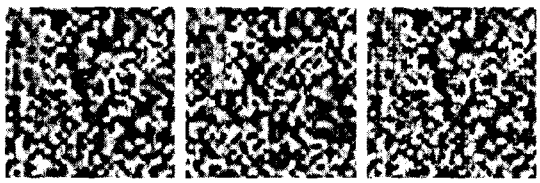


그림 4. 선택적 부분 영상 암호화/복호화 과정
(a) 암호화 (b) 복호화

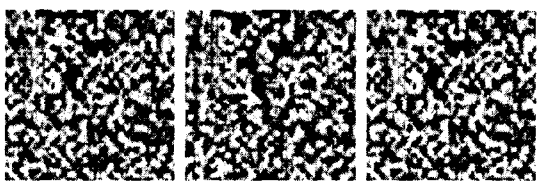
블록에 따른 Lena영상을 적용한 결과를 그림 5에 나타



(a)원영상 (b)LL4 : 8 (c)LL4 : 32



(d)LL4-HH4 : 8 (e)LL4-HH4 : 32 (f)Level 4 :8



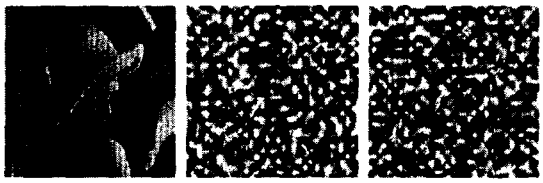
(g)Level4 : 32 (h)Level4-HH3:8 (i)Level4-HH3:32

그림 5. 암호화방법을 적용한 영상

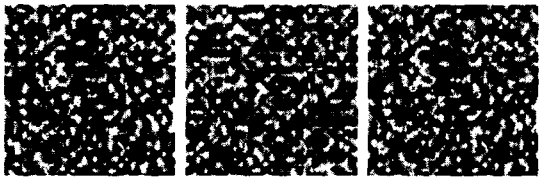
내었다. 각 조합에서 8, 16, 32는 블록의 크기를 나타낸다. 그리고 q값을 랜덤하게 조절하여 암호화한 결과가 그림 6에 나타내었다. LL4만을 암호화한 경우 예상했던 것과 같이 영상의 고주파성분이 인식할 수 있을 정도로 나타났으나, 원 영상을 모르는 상태에서는 영상을 구분할 수 없을 정도이다. 그 외의 경우는 영상을 구분할 수 없을 정도로 암호화 효과가 충분한 것을 볼 수 있으며, 따라서 통신매체 또는 통신 단말기의 상태에 따라 적응적으로 암호화 방법을 선택할 수 있다.

실험결과 영상에서 보는 바와 같이 블록의 크기에 의한 암호화 정도의 차이는 블록의 크기가 커질수록 암호화 효과가 커지는 것을 알 수 있었다. 또한 블록의 크기를 슌김으로써 하나의 암호화 키 기능을 할 수 있다는 것을 알 수 있다.

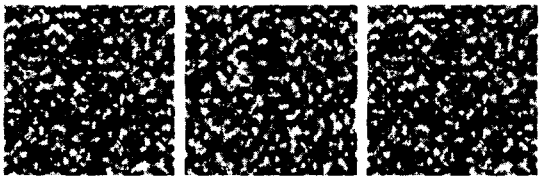
400개의 영상에 대한 실험결과의 통계치를 표 1에 나타내었다. 표 1에서 네 번째와 다섯 번째 행은 암호화를 수행할 때 식 (2)에서 얻어진 랜덤비트의 수이고 여섯 번째와 일곱 번째 행은 암호화를 수행한 결과 영상의 화질을 PSNR(Peak Signal to Noise Ratio)을 각각 나타낸다.



(a)원영상 (b)LL4 : 8 (c)LL4 : 32



(d)LL4-HH4 : 8 (e)LL4-HH4 : 32 (f)Level 4 :8



(g)Level4 : 32 (h)Level4-HH3:8 (i)Level4-HH3:32

그림 6. 랜덤한 q값을 적용한 영상

VI. 결론

본 논문에서는 DWT 를 기반으로 하는 영상압축을 가정하고 암호화 알고리즘이 아닌 계산양이 상대적으로 적으면서 실시간 동작이 가능한 Chaotic 시스템을 사용하여 랜덤비트를 발생시켜 암호화하여 영상데이터를 감추는 방법을 제시하였다. 또한 원 영상에 암호화비율, 암호화효과, 그리고 암호화에 사용되는 랜덤비트 수에 따라 전송매체나 통신단말기의 상태에 따라 적응적으로 영상암호화를 실시할 수 있는 방안을 제시하였다.

본 논문의 방법은 통신프로토콜의 응용수준에서 이루어지므로 유/무선 복합 통신매체를 사용하는 경우의 유선과 무선구간 사이에서의 복호화를 필요로 하지 않아 통신의 끝과 끝(end-to-end) 보안을 위해서도 상용가능하리라 전망된다.

표 1. 암호화에 대한 실험 결과

	전체영상에대한암호화비율	블록크기	사용 되는 랜덤비트 수		PSNR	
			고정된 q값	변화되는 q값	고정된 q값	변화되는 q값
LL4	1:256	8	2048	4096	8.25064	8.62216
		16	1024	2560	8.24340	8.52223
		32	768	1536	8.21396	8.52931
LL4 HH4	1:128	8	3072	6144	8.16422	8.51702
		16	1536	3840	8.16017	8.42870
		32	768	2304	8.13931	8.44502
Level 4	1:64	8	5632	11264	8.09216	8.39009
		16	2816	7040	8.08778	8.30383
		32	1408	4224	8.07143	8.31834
Level 4 HH3	1:32	8	8704	17408	8.08604	8.37878
		16	4352	10880	8.08243	8.29403
		32	2176	6528	8.06753	8.30742

Acknowledgment

본 연구는 2003년도 중소기업청 산학연 공동기술개발 컨소시엄 사업에 의해 지원되었음.

참고문헌

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

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

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

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

[5] Jui-Cheng Yen and Jiun-In Guo, "A new imag encryption and its VLSI architecture," in Proc. IEEE Workshop Signal Processing Systems, 1999, pp. 430-437.

[6] 박배식, 카오스란 무엇인가, 범양사, 1995.

[7] Kathleen T. Alligood, Tim D. Sauer and James A. York, "CHAOS AN INTRODUCTION TO DYNAMICAL SYSTEMS", Springer, pp.17-22, 2000.