공간주파수 성분 재배치 방법을 이용한 디지털 이미지 암호화

김기종, 유기영
경북대학교 컴퓨터공학과

Digital Image Encryption using Spatial Frequency Property Rearrangement

Ki-Jong Kim, Kee-Young Yoo
Dept. of Computer Engineering, Kyungpook National University

요 약

정보전달에 있어서 멀티미디어 정보가 차지하는 비중이 점점 증대됨에 따라 멀티미디어 데이터 암호화의 필요성이 부각되고 있는 실정이다. 그러나 기존의 문자정보 암호화에 일반적으로 적용되어온 DES(Data Encription Standard)와 같은 전통적인 암호화 알고리즘은 멀티미디어 데이터를 암호화하여 실시간으로 처리하기에는 충분히 신속하지 못한 단점이 있다. 그래서 본 논문에서는 디지털 이미지 프로세싱 기법중 압축기법과 암호화 기법을 일련의 과정으로 통합하여 멀티미디어 정보의 중요부분을 차지하는 디지털 이미지의 실시간 암호화 처리기법을 연구하였다. 디지털 이미지의 저주파수 성분과 고주파수 성분을 다단계의 레벨로 분리하여 각 대역별로 성분을 집중시킨 후 임의의 배치 순서로 재배치하는 방법을 통해 DCT(Discrete Cosine Transform)과정 및 양자화과정을 거친 공간주파수 성분을 Zig-Zag순서가 아닌 임의의 배치 순서로 재배열할 때 발생되는 이미지의 크기가 상대적으로 커지는 점과 저주파수 성분이 주요 성분으로 구성된 이미지의 경우 해독이 비교적 용이하다는 점, 또한 약간의 음용으로 각 블록의 DC값만을 추출하여 이미지의 주요 내용을 파악할 수 있는 문제점을 해결하였다.

1. 서 론

쌍방간 또는 다자간의 정보전달에 있어서 멀티미디어 정보가 차지하는 비중이 커져감에 따라 멀티미디어 데이터의 암호화는 멀티미디어 데이터의 효율적인 전달 방법과 아울러 매우 중요하다. 그러나 기존의 문자정보의 암호화에 일반적으로 적용되어온 DES나 RSA(Ron Rivest, Adi Shamir, Leonard Adleman)와 같은 전통적인 암호화 알고리즘[6]은 멀티미디어 데이터를 암호화하여 실시간으로 처리하기 위해 발생되는 광범위한 처리를 위해서 충분히 신속하지 못한 단점이 있다. 그러므로 멀티미디어 정보의 중요부분을 차지하고 있는 디지털 이미지를 암호화하기 위해 디지털 이미지 프로세싱 기법중 이미지 압축 알고리즘과 암호화 기법을 통합하여 압축과 암호화를 일련의 과정으로 처리하는 연구[1]에 의해 디지털 이미지의 암호화를 실시간으로 처리할 수 있도록 하는 것은 중요한 의미를 가진다. 디지털 이미지 처리기법은 이미지의 화질을 향상시키거나 위해서 또는 시각적으로 보여지는 이미지 화질의 손상없이 효과적으로 데이터를 제거하여 압축하기 위해서 사용된다. 그리고 암호화 방법은 인증되지 않은 사용자가 비밀키 없이 원본 이미지를 얻을 수 없도록 이미지를 감추기 위해 사용된다. 이 두 기법은 서로 상반되는 효과를 가지고 있다. 기존의 연구에서는 최소한의 오버헤드로 두기법을 통합하여 한번에 처리되도록 구현하였다[1].

본 논문에서는 디지털 이미지 프로세싱과 암호화 과정을 통합할 때 발생되는 디지털 이미지 프로세싱과 암호화의 상반적인 특성이 잘 조화되도록 하여 디지털 이미지의 압축률 손상을 최소화 하고 암호화 정도를 더 높이기 위해 인접된 블록들의 주파수성분을 다단계의 레벨로 분리하고 대역별로 재배치한후 압축하도록 하여 디지털 이미지 프로세싱 기법과 암호화 기법을 일련의 과정으로 통합하는 방법에 대하여 연구하였다.

2. JPEG의 압축절차

JPEG(Joint Photographic Experts Group)는 컬러와 그레이 스케일 정지화상을 엔코딩, 디코딩하는 표준안으로 대표적인 이미지 압축 표준기법이다. 그리고 이러한 기법은 멀티미디어 응용에 광범위하게 구현되어 지고 있다. JPEG의 기본적인 압축절차는 그림 1에서 보여준다. 상세한 JPEG 표준에 대한 것은 [2]에서 참조할 수 있다.

기본적인 압축절차는 다음과 같이 요약할 수 있다. RGB로 구성된 원본 이미지를 YCrCb로 구성된 적절한 색상영역으로 전이한후 각 8x8 블록을 DCT를 통하여 DC 및 AC계수로 구성된 주파수성분을 가진 새로운 8x8 블록으로 구성한다.

Forward DCT의 정의는 다음과 같다

$$S_{vu} = \frac{1}{4} C_u C_v \sum_{x=0}^{7} \sum_{y=0}^{7} S_{xy} \cos\frac{(2x+1)u\pi}{16} \cos\frac{(2y+1)v\pi}{16}$$

Inverse DCT의 정의는 다음과 같다

$$S_{xy} = \frac{1}{4} \sum_{u=0}^{7} \sum_{v=0}^{7} S_{vu} \cos\frac{(2x+1)u\pi}{16} \cos\frac{(2y+1)v\pi}{16}$$

$u, v = 0$ 일때 $C_u, C_v = 1/\sqrt{2}$, 그외 $C_u, C_v = 1$

DCT과정을 거친후에 구성된 8x8 블록내의 몇몇 계수 특히 DC계수에 원본 이미지 8x8 샘플 블록의 신호에너지 대부분이 집중된다. 그리고 가시적으로 중요치 않은 정보를 제거하기 위해 64개의 DCT 계수 각각은 엔코더에 입력하기 위한 응용프로그램 또는 사용자에 의해 미리 규정되어진 64개 요소의 양자화 테이블에 의해 비균등하게

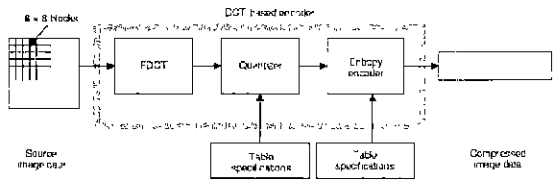

그림 1 JPEG의 기본적인 압축절차

양자화된다. 양자화는 다대일 관계로 근본적인 손실을 가져온다. 양자화된 DC계수는 엔코딩 순서상의 전블록의 DC요소와의 차이를 DPCM(Differential Pulse Code Modulation)방법으로 엔코딩되고 AC계수들은 Zig-Zag 순서에 의해 RLE(Run Length Encode)방법으로 엔코딩된다. 그리고 Huffman coding 또는 arithmetic coding 방법으로 DCT계수들의 통계정보를 기준으로 추가적인 무손실 압축을 구현한다[9]

3. 임의 배치 순서에 의한 암호화 방법

디지털 이미지의 암호화를 압축과정의 일련과정으로 구현하려는 시도는 다음과 같은 과정에 의해서 구현되었다 원본이미지를 8x8 단위로 샘플링 한 블록을 DCT 및 양자화과정을 거쳐 DC 및 AC값으로 구성된 8x8 계수블록으로 변환하고 $d_7d_6d_5d_4d_3d_2d_1d_0$의 8비트로 구성된 DC값을 $d_7d_6d_5d_4$와 $d_3d_2d_1d_0$의 0~15 범위의 값을 가지는 두 개의 값으로 분리한 후 DC값은 $d_4d_2d_1d_0$으로 AC계수의 마지막 값으로는 $d_7d_6d_5d_4$를 설정한다. 그리고 기존의 Zig-Zag 순서대신에 이미 계산된 64개의 계수를 대상으로 하는 Random Permutation 알고리즘으로 만들어진 임의의 배치 순서에 의하여 한 블록내의 DC 및 AC 계수를 임의의 위치로 재배열 한다. 재 배열된 계수값을 다음 절차인 엔코딩 과정으로 넘겨줌으로 인하여 디지털 이미지의 암호화를 압축과정과 일련의 과정으로 구현하였다

양자화된 각 8x8 블록의 64개 계수 순서를 기존의 Zig-Zag순서 대신 임의의 배치 순서에 의하여 재배치했을 때 원본 이미지와는 전혀 다른 알 수 없는 이미지로 암호화 된다. 그리고 임의의 배치 순서를 모르는 상태에서 원본 이미지를 추출하기 위한 이론적인 시도 횟수는 다음과 같다.

동일값 그룹이 k개, 각 그룹이 $n_1,n_2..,n_k$ 라고 할때

$$\frac{(\sum_{i=1}^{k} n_i)!}{\prod_{i=1}^{k}(n_i!)}$$

이고 8x8 계수 블록의 하삼각 부분 32개 계수에 0값을 집중할 때

$$\frac{(64-32)!}{\prod_{i=1}^{k}(n_i!)}$$

과 같다 위 수식 에서도 살펴볼 수 있듯이 원본 이미지의 대부분이 저주파수 성분만을 가지고 있어서 AC계수의 대부분이 0값으로 양자화되는 특성을 갖는 특정 이미지의 경우에는 해독하기 위한 시도횟수가 줄어들게 되고 원본 이미지로 해독될 가능성도 생각해 볼 수 있다. 그리고 전체 64개의 계수중 4비트씩 분리된 2개값의 조합만으로 DC값을 생성하는 것이 가능하다

$$_{64}P_2 = \frac{64!}{(64-2)!} = 4032$$

이와같이 약간의 응용만으로 원본 이미지의 DC값을 추출하여 그림 2의 원본 이미지에 근접하는 그림 3과 같은 이미지를 추출할 수 있게 된다. 또한 Zig-Zag순서가 아닌 임의의 순서로 DC 및 AC계수를 배치하게 되면서 8x8계수 블록의 하삼각 부분에 집중됐던 0값이 임의의 자리로 분산됨으로 해서 기존의 압축 알고리즘인 RLE의 적용에 압축률 감소요인으로 작용하게 되어 원본 이미지와 비교하여 상당한 압축률의 감소를 초래하게 된다[3,5,8]

그림 2 원본 이미지

그림 3 DC값만 있는 이미지

4. 공간주파수 성분 재배치에 의한 암호화 방법

디지털 이미지를 위한 암호화는 암호화된 이미지가 원본 이미지와 비교하여 화질은 낮지만 원본 이미지의 내용을 보여주는 불분명한 이미지(obscured image)와 내용을 알아볼 수 없는 알 수 없는 이미지(incomprehensible image)의 두 부류로 나눌 수 있다. 그리고 디지털 이미지 암호화 알고리즘을 위해 요구되는 몇가지 사항으로는 디지털 이미지 데이터의 많은 정보량에 의한 암호화 또는 복호화 절차에 부가되는 계산적인 오버헤드가 가능한한 적어야 하고 기존의 압축률을 감소시키지 않아야 한다 그리고 암호화 알고리즘은 이미지 enhencement, 이미지 restoration 같은 일반적인 이미지 프로세싱 방법에 대하여 견고해야 한다 또한 디지털 이미지의 암호화, 복호화는 원본 이미지의 화질에 영향을 주지 않아야 한다[1].

DCT과정과 양자화과정을 거친 각 8x8블록의 64개 계수의 순서를 Zig-Zag순서 대신 임의의 배치 순서에 의해 재배치하여 압축했을 때 발생될 수 있는 압축률 감소, 저주파수 성분만을 가지고 있는 특정 이미지의 해독 가능성, DC값 추출로 인한 원본 이미지에의 접근등의 문제점을 해결하기 위한 방안으로서 인접블록의 계수를 각 블록에 재분산하는 방법[7]을 응용하여 인접블록(예: 4개 블록)들의 저주파수 성분과 고주파수 성분을 다단계의 레벨(예: 4개 레벨)로 분리하여 각 대역별 성분을 집중시킨 후 암호화 하는 개선된 방법을 그림 4에 나타내고 다음과 같은 기법을 제안한다

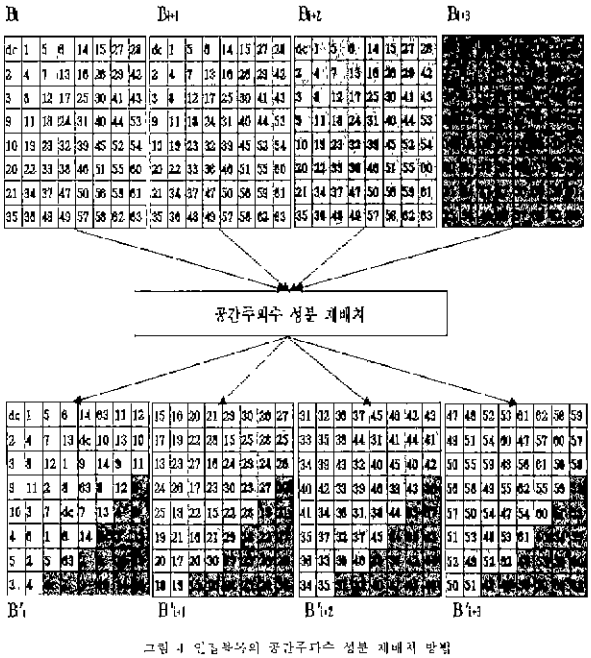

그림 4 인접블록의 공간주파수 성분 재배치 방법

공간주파수 성분 재배치에 의한 암호화 기법

Step 1. $B_i \sim B_{i+3}$ 블록의 DC값을 비트 분리하여 AC_{63}에 $d_7d_6d_5d_4$ 값을 설정하고, DC에 $d_3d_2d_1d_0$값을 설정한다.

Step 2. 0가 아닌값을 모으기 위하여 $B_i \sim B_{i+3}$ 블록의 AC_{63}값을 AC_{15}자리로 이동하고, $AC_{15} \sim AC_{62}$값을 $AC_{16} \sim AC_{63}$으로 이동한다.

Step 3. 세구성된 $B_i \sim B_{i+3}$ 블록 각각의 DC 및 $AC_1 \sim AC_{15}$까지의 값을 B'_i 블록에, $AC_{16} \sim AC_{31}$값을 B'_{i+1} 블록에, $AC_{32} \sim AC_{47}$값을 B'_{i+2} 블록에, $AC_{48} \sim AC_{63}$값을 B'_{i+3} 블록으로 재배치한다.

Step 4. $B_i \sim B_{i+3}$ 블록의 DC 및 AC 값을 재배치한 $B'_i \sim B'_{i+3}$ 블록 각각을 대상으로 이미 계산된 임의의 배치 순서에 의하여 값을 분산한다.

Step 5. 각 블록의 재배열된 계수값을 다음 절차인 엔코딩 과정으로 넘겨준다.

제안된 기법의 1~4번 Step에 의해 B'_{i+2} , B'_{i+3}블록에는 $B_i \sim B_{i+3}$ 블록의 고주파수 성분이 집중 되면서 RLE 적용에 압축률 상승요인으로 작용하게 된다 그리고 DC값을 4비트로 분리한 $B_i \sim B_{i+3}$ 블록 각각의 DC 값과 $AC_1 \sim AC_{14}$ 값, AC_{63} 값이 이동된 AC_{15} 값이 B'_i에 집중되기 때문에 원본 이미지를 추출하기 위하여 시도해야 하는 횟수와 원본 이미지의 불분명한 이미지를 추출하기 위하여 DC값 조합을 시도해야 하는 횟수는 다음과 같다

$$\frac{64!}{\prod_{i=1}^{k}(n_i!)}$$

$$_{64}P_8 = \frac{64!}{(64-8)!} = 1.78462876378e+14$$

이와같이 임의로 생성된 계수값 배치순서를 모르고서는 원본 이미지에 접근하지 못하게 된다 그리고 임의로 생성된 계수값 배치순서를 DES 또는 RSA와 같은 암호화 방법을 이용하여 서비스 한다면 자격이 있는 사용자에게만 이미지 서비스를 제공하게 된다

5. 검토 및 평가

위에 제안한 기법을 구현하기 위해 IJG JPEG library[4]를 목적에 맞도록 수정하여 Windows95 운영체제의 PentiumII 233 CPU IBM호환 PC에서 실험하였다. 그리고 제안한 알고리즘을 실험하기 위한 대상 이미지로 'lena' 파일을 사용하였고, DC 값을 제외한 나머지 AC값을 0로 치환하여 그림 3에 나타내고, DC 값을 비트분리하여 AC_{63}과 DC위치로 값을 분할한 후 표 1의 방법 1에 모든 계수를 임의의 배치 순서에 의해 재배열한 결과와 방법 2에 DC 값을 분리하고 4개블록의 계수값을 주파수 성분별로 각 블록에 재배치 한후 임의의 배치 순서에 의해 재배열한 결과를 여러번 실험하여 평균값을 표시하여 비교하였다. 그리고 암호화된 이미지에 임의의 배치순서를 역으로 적용하는 방법으로 복호화하여 원 이미지와 동일한 이미지인 그림 7과 그림 8을 얻을 수 있었다.

표 1 원본 이미지와 암호화 이미지의 파일 크기 비교

구분	파일크기(byte)	비고
원본 이미지	46,536	그림1
방법1	81,530	그림5
방법2	63,631	그림6

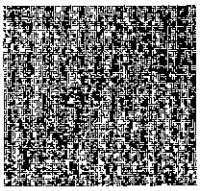

그림 5 암호화한 이미지(방법1)

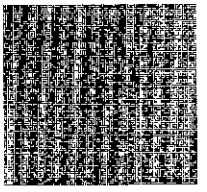

그림 6 암호화한 이미지(방법2)

그림 7 복호한 이미지(방법1)

그림 8 복호한 이미지(방법2)

6. 결론

본 논문에서는 디지털 이미지의 실시간 암호화를 위해 압축과 암호화를 일련의 과정으로 처리하기 위한 방법으로 DCT과정과 양자화 과정 후에 디지털 이미지의 저주파수 성분이 DC값과 Zig-Zag순서상의 선두에 있는 일부 AC값에 집중되는 특성을 이용하여 인접된 블록들의 저주파수 성분과 고주파수 성분을 다단계 레벨로 분리하고 각 대역별로 성분을 집중시킨 후 임의의 배치 순서로 재배열하여 암호화하는 방법을 제안하였다 그리하여 디지털 이미지 프로세싱과 암호화의 상반적인 특성이 잘 조화시켜서 디지털 이미지의 압축률 손상을 최소화하고 암호화정도를 더 높일 수 있었다. 그리고 JPEG표준에 근거하여 실험과 계산에 의한 정험적인 결과를 살펴 보았다 암호화의 레벨을 좀 더 높이기 위해서는 DC값을 비트분리하는 절차전에 DC값을 DES와 같은 암호화 알고리즘을 적용하여 변환하는 절차를 포함시키면 될 것이다. 추후 DC값에 DES 또는 RSA를 적용하여 암호화했을때와 임의 배치 순서만에 의한 암호화를 비교 실험할 필요성이 있는 것으로 사료된다

참고문헌

[1] Lei Tang, "Methods for Encrypting and Decrypting MPEG Video Data Efficiently," *Proceeding of ACM Multimedia '96*, Nov. 1996

[2] CCITT, *Information technology digital compression and coding of continuous-tone still images requirements and guidelines*. Sep. 1992

[3] Gregory A. Baxes, *Digital image processing principles and applications*, John Wiley & Sons, 1994

[4] Thomas G Lane, IJG JPEG library and apllication, Release 6a, Feb. 1996

[5] Mark Nelson, *The Data Compression Book*, M&T books, 1992

[6] Douglas R. Stinson, *Cryptography theory and practice*, CRC Press, 1995

[7] Prashant J. Shenoy, Harrick M. Vin, "Failure Recovery Algorithms for Multimedia Servers," *Technical Report 96-06, Dept. of Computer Sciences, Univ Texas*, Apr 1996

[8] Ralf steinmetz, Klara nahrstedt, *Multimedia- Computing, Communications & Applications*, Prentice Hall

[9] 기술인협회, BRR(Bit Rate Reduction) Tecnology, http://www.kjmbc.co.kr/beta/digital/title.html