디지털산업정보학회 논문지 제12권 제2호-2016년 6월
http://dx.doi.org/10.17662/ksdim.2016.12.2.041

웨이브렛 변환 계수의 특성을 이용한 생체 영상 암호화 알고리즘

신 종 홍*

Biometric Image Cryptographic Algorithm Based on the Property of Wavelet Transform Coefficient

Shin Jonghong

〈Abstract〉

Lossless encryption methods are more applicable than lossy encryption methods when marginal distortion is not tolerable. In this research, the author propose a novel lossless symmetric key encryption/decryption technique. In the proposed algorithm, the image is transformed into the frequency domain using the lifting wavelet transform, then the image sub-bands are encrypted in a such way that guarantees a secure, reliable, and an unbreakable form. The encryption involves scattering the distinguishable frequency data in the image using a reversible weighting factor amongst the rest of the frequencies. The algorithm is designed to shuffle and reverse the sign of each frequency in the transformed image before the image frequencies are transformed back to the pixel domain. The results show a total deviation in pixel values between the original and encrypted image. The decryption algorithm reverses the encryption process and restores the image to its original form. The proposed algorithm is evaluated using standard security and statistical methods; results show that the proposed work is resistant to most known attacks and more secure than other algorithms in the cryptography domain.

Key Words : Cryptography, Lossless Image Encryption, Wavelet Transform, Coefficient

Ⅰ. 서론

생체정보는 사용자 인증을 위한 강력한 도구로서 다양한 보안 시스템에 넓게 사용되고 있다. 그런데 개인의 생체정보는 영구적이기 때문에 일반적으로 변경하는 것이 불가능하다. 이런 이유 때문에 보안 시스템에서 개인의 생체정보를 담고 있는 템플릿이 도난을 당한다면, 개인 보안에 치명적인 악영향을 줄 수 있다. 결과적으로 생체정보는 보안 시스템에서 가장 유용하게 사용될 수 있지만, 그러나 잘못되었을 경우 가장 나쁜 결과를 초래할 수 있다.

일반적인 암호화 알고리즘의 개념은 저장과 전송할 수 있는 데이터를 합법화된 사용자만이 읽고 처리할 수 있는 형태로 만드는 것이다. 따라서 암호화 기술은 보안이 되지 않은 네트워크를 통해서 전송되거나 미

*숭실사이버대학교 융합정보보안학과 부교수

디어로 저장되는 데이터를 효율적으로 보호하는 것이다. 즉, 암호화의 목적은 비인가 사용자들로부터 정보를 은닉하는 것이다. 그 동안 암호화 기술은 많은 발전을 했지만, 더불어 암호화 기술을 위협하는 암호 해독 기술의 수위도 많이 높아지고 있다[1].

영상 암호화는 멀티미디어 환경에서 가장 유용하게 사용되는 디지털 영상을 암호화 하는 기술로 다양한 영역에서 많은 응용이 되고 있다. 그 동안 영상 암호화 기술은 기존의 메시지 기반의 텍스트 암호화 알고리즘을 그대로 사용하였다. 그렇지만 디지털 영상의 데이터 크기는 메시지 위주의 텍스트보다 훨씬 크다. 그리고 디지털 영상의 특성은 텍스트가 갖고 있는 특성과는 많은 차이가 있기 때문에, 전통적인 메시지 기반의 텍스트 암호화 방법들이 디지털 영상 암호화에 효과적으로 적용되기가 어렵다. 디지털 영상의 암호화 방법은 손실과 무손실의 암호화로 분류할 수 있다. 손실 암호화 방법에서는 영상의 상세부분이 다소 왜곡이 되는 것이 가능하기 때문에, 암호화된 디지털 영상이 다시 일반의 디지털 영상으로 복호화 되면 원래의 디지털 영상과는 차이가 존재할 수 있다. 그렇지만 암호화 과정에서 발생한 작은 왜곡을 포함하는 암호화된 영상은 인간의 시각적 특성이 고려되었고 그리고 응용에 따라서 무시될 수 있으므로, 일반적으로 수용할 만하다. 무손실의 암호화 방법은 의료 영상, 항공우주산업 영상, 인공위성 영상들과 같이 고품질 영상들을 필요로 하는 분야에서 왜곡이 없는 복호화 영상이 요구되는 응용에서 더 많이 적용될 수 있다[1,2].

암호화 알고리즘은 임의의 기술로 쉽게 구현되는 것은 아니다. 충분한 동기와 시간을 확보하고 그리고 필요한 자원이 충분이 있다며, 최신의 발전된 디지털 암호화 기술도 개인이나 단체에 의해서 해독될 수 있기 때문이다[1,2]. 본 논문은 주파수영역에서 위치 순열, 수치변환, 그리고 시각 변환을 수행하는 무손실의 대칭키 암호화와 복호화 알고리즘을 구현하였다.

제안된 알고리즘에서 이산 웨이브렛 변환(Discrete Wavelet Transform: DWT)은 주파수 영역에서 생체 영상의 암호화를 수행할 수 있게 한다. 그래서 디지털 영상은 2레벨의 이산 웨이브렛 변환으로 분해되어 부대역 영상들로 생성된다. 이 부대역 영상들은 위치 순열, 수치변환, 그리고 시각 변환의 과정을 통해서 암호화 알고리즘이 수행된다. 제안된 암호화 과정은 제안된 복호화 알고리즘의 이외의 다른 방법으로는 결코 복호화 될 수 없는 것을 보장할 수 있도록 처리되었다. 복호화 과정은 암호화된 각 주파수의 부대역 영상들이 암호화의 반대처리 과정에 의해서 원 영상으로 복호화 된다. 결과적으로 제안된 시스템은 합법적인 수신자 이외의 다른 사용자에 의해서 도난 될 수 있거나 접속될 수 있는 민감 영상들의 위협을 감소시킨다. 또한 이 방법은 고품질 비밀 영상들의 전송을 요구하는 상황에서 유용하게 사용될 수 있다.

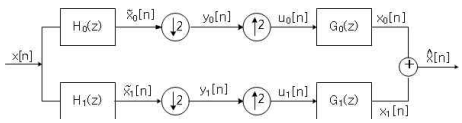
본 논문의 구성으로 2장에서는 웨이브렛 변환과 웨이브렛 계수의 특징을 설명한다. 3장에서는 제안된 알고리즘에 대한 내용을 설명한다. 그래서 암호화 과정의 수행 절차를 설명하고 이어서 복호화 과정에서 수행 절차를 설명한다. 그리고 4장에서는 제안된 알고리즘의 성능을 평가하는 실험과 그 결과를 제시하였다. 제안된 알고리즘을 우수성을 위해서 이전 기술과 비교 우위 실험이 수행되었다. 마지막으로 5장에서는 본 연구에 대한 결론과 향후 연구방향을 제시하였다.

Ⅱ. 웨이브렛 변환과 계수의 특징

웨이브렛 변환은 다해상도(multi resolution) 신호처리를 가능하게 하는 기술로서, 웨이브렛 기저함수가 확장(dilation) 및 축소(contraction)와 전이

(translation)를 통해서 입력 신호를 부대역 신호들로 분해한다. 그래서 웨이브렛 변환은 각 주파수 영역에 따라 변화하는 다양한 기저 함수를 생성할 수 있기 때문에, 시간과 주파수 정보를 동시에 파악할 수 있는 시간-주파수에 국부적인 성질을 갖는다[3].

웨이브렛 변환은 2채널 필터 뱅크(filter bank)의 연속적인 동작에 의해서 실행된다. 필터 뱅크는 저주파 통과 필터와 고주파 통과 필터들로 구성되며, 이 필터들은 특수하게 설계되어서 직교 특성, 선형 특성을 만족한다. 또한 이 필터들은 고대역 부분과 저대역 부분을 정확하게 분할하는 반대역(half band)필터의 특징을 갖는다. <그림 1>은 완전재생(perfect reconstruction)을 만족하는 2채널 필터 뱅크의 관계를 나타낸 것이다[3-4].



<그림 1> 2채널 웨이브렛 필터 뱅크

완전재생을 만족하기 위해서는 식(1)을 만족한다.

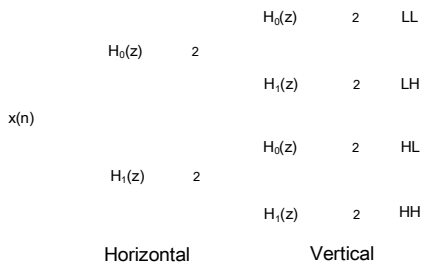
$$x(n) = \hat{x}(n) \tag{1}$$

<그림 2>는 연속적인 필터뱅크 적용을 통한 이산 웨이브렛 변환을 나타낸 것이다. 이 과정에서 입력 신호는 웨이브렛 변환을 통해 다해상도 신호로 분해된다. 그리고 웨이브렛 역변환을 통해서 다해상도 신호는 다시 원래의 영상으로 합성된다. 합성된 신호는 입력신호와 완벽하게 동일하여 완전 재생이 만족된다. 웨이브렛 함수는 저주파 필터 $H_0(z)$의 필터링과 다운 샘플링(down sampling)을 무한 반복하면 얻어진다[3].

이산 웨이브렛 변환을 2차원의 디지털 영상에 적용하려면, 디지털 영상을 수평 방향으로 필터 뱅크에 입력한 후, 그 출력이 연속해서 수직 방향으로 필터 뱅크에 입력되어 처리되는 분리 가능(separable)의 2차원 이산 웨이브렛 변환이 사용된다.

<그림 2> 필터뱅크를 이용한 웨이브렛 변환과 역변환 실행

<그림 3>은 2차원 웨이브렛 변환의 수행 방법을 나타낸 것으로 4개의 부대역 영상이 생성된다. *LL*은 가장 낮은 저주파 부대역 영상을 나타내며, 순차적으로 *LH*, *HL*, *HH*순으로 높은 주파수 부대역 영상을 생성하게 된다. 그래서 *HH*는 고주파 부대역 영상이 된다.



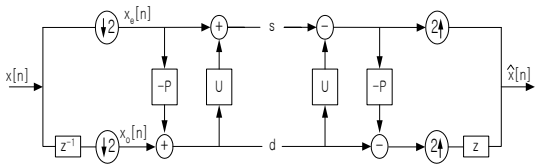
<그림 3> 2차원 이산 웨이브렛 변환의 실행

공간 주파수상의 차이는 시각적인 정보의 차이를 나타낸다. 그래서 고주파 성분은 영상에서 테두리와 경계와 같이 갑작스런 변화가 존재하는 부분을 나타낸다. 저주파 성분은 일반적인 방향성과 비율들과 같은 형태에 대한 전제적인 정보를 표현한다. *LL*성분은 수평과 수직 방향에서의 저주파수들로 구성된다. 이 주파수들은 영상을 다시 복원할 수 있는 필수요소이

다. *HL*은 수직 방향에서의 고주파 성분으로 잔여의 수직 주파수를 담고 있다. *LH* 수직 방향에서 고주파 성분들로 잔여 수직 주파수 성분들이다. *HH*는 수평과 수직 방향에서의 고주파 성분들이다. 따라서 4개의 부대역 영상들이 함께하며 원영상의 모든 주파수 정보를 구성하는 것이다. 최저주파수 *LL* 계수 값의 특징은 디지털 영상의 가장 중요한 부분이 포함되어 있어, 가장 큰 에너지 값을 갖는다. 따라서 나머지 부대역 영상 *LH*, *HL*, *HH*의 계수 값들과는 구별이 충분히 가능하다. 그렇지만 *LH*, *HL*, *HH* 부대역 영상의 계수 값들은 서로 구별이 잘 되지 않는다.

Ⅲ. 제안 알고리즘

생체 영상에 대한 암호화를 수행하기 위해서 본 논문에서는 리프팅 웨이브렛 변환을 사용하였다. 리프팅(lifting) 이론은 웨이브렛 변환의 다위상(polyphase) 표현에서 다위상 행렬들을 Euclidean 알고리즘을 사용하여 인수분해를 통해 predict와 update단계로 나누어 실행하는 방법이다. 그래서 리프팅 웨이브렛 변환은 <그림 4>와 같이 곱셈과 과정 없이, 덧셈과 지연 연산만으로 간단하게 실행될 수 있다[5].



<그림 4> predict와 update의 리프팅 단계 블록도

그리고 암호화의 강도를 높이기 위해서 2레벨의 웨이브렛을 수행하는 과정에서 각 레벨마다 다른 탭 길이를 갖는 분석필터들을 사용하였다. 따라서 복호화 과정에서도 완전재생을 위해서 각 레벨에서 해당 탭 길이를 갖는 합성필터들이 사용된다.

3.1 암호화 알고리즘

제안된 알고리즘에서 필터 길이 1의 분석 필터를 사용하여 웨이브렛 변환의 첫 레벨의 분해 단계를 수행하여서 입력 영상을 최저 주파수의 부대역 영상 LL_1과 상세 계수의 부대역 영상들 LH_1과 HL_1 그리고 HH_1을 생성한다. 암호화 처리의 첫 번째 단계에서는 생성된 부대역 영상들 중에서 LL_1의 부대역 영상의 계수 값들을 수정한다. LL_1의 부대역 영상의 계수 값들은 가장 큰 에너지를 포함하고 있어, 나머지 부대역 영상의 계수 값들과는 구별이 가능하다. 그래서 다른 나머지 부대역 영상의 계수 값들과 구별이 되지 않도록 LL_1의 부대역 영상의 계수 값들을 설정하는 것이 중요하다. 이것은 가중치 인자를 사용하여 가능하며, 이 과정이 제안한 알고리즘에서 암호화 키로 사용이 될 수 있다. 즉, LL_1의 부대역 영상의 계수 값을 $(m_1 \times n_1)$으로 나누는 것이다. 여기서, m_1과 n_1은 LL_1 행렬의 차원으로 행의 웨이브렛 계수의 갯수와 열의 웨이브렛 계수의 갯수를 나타낸다. 따라서 LL_1는 다음으로 변경된다.

$$LL_1(i,j) \Rightarrow \frac{LL_1(i,j)}{(m_1 \times n_1)} \tag{2}$$

두 번째 단계에서는 LL_1를 제외한 나머지 부대역 영상의 계수 값들의 부호를 반전 시키는 것이다. 그래서 LH_1, HL_1, HH_1의 부대역 영상들의 계수 값들에 (-1)을 곱한다. 부호의 반전 연산을 실행하는 이유는 영상에서 가장 어두운 값과 가장 밝은 값의 차이인 대비(contrast)값을 반전시키기 위한 것이다. 그래서 대비값 반전은 밝은 값이 어두운 값이고 어두운 값이

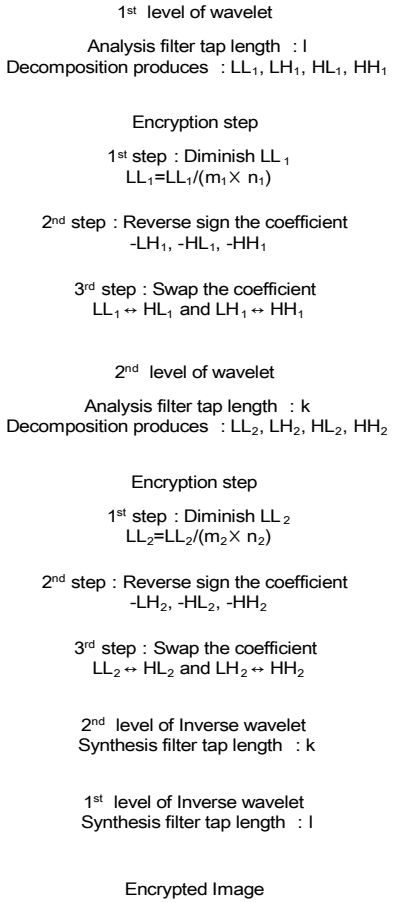
밝은 값이 되는 것이다. 결국 암호화되는 영상에서는 원본 영상과 밝기 차이가 달라져서 원본 영상을 파악할 수 없다.

세 번째 단계는 두 번째 단계와 같이 원본 영상을 추측할 수 없도록 하는 과정으로 LH_1와 HH_1를 서로 바꾸고 LL_1와 HL_1를 서로 바꾸는 과정이다. 즉, 4개의 부대역들 간의 교환은 역 웨이브렛 변환이 적용되기 전에 저주파와 고주파의 위치를 변경하는 것이다.

웨이브렛의 두 번째 레벨 분해 단계에서는 첫 단계에서 생성된 최저주파수 부영상 LL_1을 길이 k의 분석 필터를 사용하여 다시 분해해서 LL_2와 그리고 LH_2, HL_2, HH_2의 부대역 영상들을 생성한다. 암호화 처리의 과정은 웨이브렛 첫 번째 분해 레벨에서와 동일하다. 그래서 첫 단계에서는 부대역 영상들 중에서 LL_2의 부대역 영상의 계수 값들을 다른 나머지 부대역 영상의 계수 값들과 구별이 되지 않도록 LL_2의 부대역 영상의 계수 값들을 설정한다. 그래서 LL_2 의 부대역 영상의 계수 값을 $(m_2 \times n_2)$으로 나누는 것이다. 여기서, m_2과 n_2은 LL_2 행렬의 차원으로 행의 웨이브렛 계수의 갯수와 열의 웨이브렛 계수의 갯수를 나타낸다. 따라서 LL_2는 다음으로 변경된다.

$$LL_2(i,j) \Rightarrow \frac{LL_2(i,j)}{(m_2 \times n_2)} \quad (3)$$

두 번째 단계에서는 LL_2를 제외한 LH_2, HL_2, HH_2의 부대역 영상들의 계수 값들에 (-1)을 곱한다. 마찬가지로 영상에서 가장 어두운 값과 가장 밝은 값의 차이인 대비(contrast)값을 반전시키기 위한 것이다. 세 번째 단계는 LH_2와 HH_2를 서로 바꾸고 LL_2와 HL_2를 서로 바꾸는 과정이다. 마지막으로 영상의 2레벨과 1레벨의 역 웨이브렛 변환을 수행한다. 이때, 2레벨에서 사용되는 합성 필터 댑의 길이는 k가 되고 1레벨에서 사용되는 합성 필터 댑 길이는 l이다. 이 과정은 영상의 주파수들이 변경된 화소 값과 영상의 자세한 부분이 숨겨진 상태의 화소 영역으로 다시 변환되는 것이다. 제안된 암호화 알고리즘은 임의의 보안 공격과 통계적 공격에 강인한 암호화된 영상을 생성하기 위해서 두 단계의 웨이브렛 분해만이 사용되었다. 더불어 두 단계의 웨이브렛 분해는 알고리즘의 복잡도를 낮게 유지시킨다. 즉, 적은 수의 계산량이 사용된다. <그림 5>는 제안된 영상의 암호화 알고리즘 처리 과정을 나타낸 것이다.



<그림 5> 제안된 영상 암호화 알고리즘의 처리 과정

3.2 복호화 알고리즘

암호화된 영상에 대한 복호화 알고리즘은 영상 원본이 갖고 있는 상세 부분을 드러나게 하는 것이다. 이 목적을 위해서 제안된 알고리즘은 길이 l의 분석 필터를 이용하여 1레벨 웨이브렛 변환을 수행한다. 이 때 암호화 과정과 마찬가지로 최저 주파수의 부대역 영상 LL_1과 상세 계수의 부대역 영상들 LH_1과 HL_1 그리고 HH_1을 생성한다. 그리고 LL_1에 대해서 길이 k의 분석필터를 이용하여 2레벨 웨이브렛 분해를 수행하여 LL_2와 그리고 LH_2, HL_2, HH_2의 부대역 영상들을 생성한다. 웨이브렛 계수에 대한 복호화 과정은 암호화 과정의 반대로 진행된다. 첫 번째 단계에서 LH_2와 HH_2를 서로 교환하고 LL_2와 HL_2를 서로 교환한다. 두 번째 단계에서는 LH_2, HL_2, HH_2의 부대역 영상의 계수 값들의 부호를 반전 시키는 것이다. 그래서 계수 값들에 (-1)을 곱한다. 마지막 단계에서는 암호화 단계에서 사용한 동일한 가중치 인자를 다음과 같이 LL_2에 곱하여 준다.

$$LL_2(i,j) \Rightarrow LL_2(i,j)(m_2 \times n_2) \quad (4)$$

그리고 필터 길이 k의 합성 필터를 이용하여 역 웨이브렛 변환을 수행하여 LL_1을 복원한다. 여기서의 복호화 과정도 암호화 과정의 반대로 진행된다. 첫 번째 단계에서 LH_1와 HH_1를 서로 교환하고 LL_1와 HL_1를 서로 교환한다. 두 번째 단계에서는 LH_1, HL_1, HH_1의 부대역 영상의 계수 값들의 부호를 반전 시키는 것이다. 그래서 계수 값들에 (-1)을 곱한다. 마지막 단계에서는 암호화 단계에서 사용한 동일한 가중치 인자를 다음과 같이 LL_1에 곱하여 준다.

$$LL_1(i,j) \Rightarrow LL_1(i,j)(m_1 \times n_1) \quad (5)$$

Encrypted Image

1st level of wavelet

Analysis filter tap length : l
Decomposition produces : LL_1, LH_1, HL_1, HH_1

2nd level of wavelet

Analysis filter tap length : k
Decomposition produces : LL_2, LH_2, HL_2, HH_2

Decryption step

1st step : Swap the coefficient
$LL_2 \leftrightarrow HL_2$ and $LH_2 \leftrightarrow HH_2$

2nd step : Reverse sign the coefficient
$-LH_2$, $-HL_2$, $-HH_2$

3rd step : Grow LL_2 Coefficient
$LL_2=LL_2 \times (m_2 \times n_2)$

2nd level of Inverse wavelet

Synthesis filter tap length : k
Reproduces : LL_1

Decryption step

1st step : Swap the coefficient
$LL_1 \leftrightarrow HL_1$ and $LH_1 \leftrightarrow HH_1$

2nd step : Reverse sign the coefficient
$-LH_1$, $-HL_1$, $-HH_1$

3rd step : Grow LL_1 Coefficient
$LL_1=LL_1 \times (m_1 \times n_1)$

1st level of Inverse wavelet
Synthesis filter tap length : l

Decrypted Image

<그림 6> 제안된 복호화 알고리즘의 처리 과정

마지막으로 길이 1의 합성 필터를 이용하여 역 웨이브렛 변환을 수행하여 복호화된 영상을 생성한다. 제안된 암호화 알고리즘은 무손실 암호화 기법이므로 복호화된 영상의 화소들은 원래의 영상과 동일한 값을 갖는다. <그림 6>은 제안된 복호화 알고리즘 처리 과정을 나타낸 것이다.

Ⅳ. 성능 실험 결과

본 논문에서는 제안된 방법의 성능을 분석하기 위해서 이전에 제안되었던 알고리즘[6]과 비교하면서 객관적인 실험을 수행하였다. 실험 디지털 영상은 8비트 그레이 영상으로 이 디지털 영상들의 크기는 256×256이다. <그림 7>은 실험 영상을 나타낸 것이다.

그리고 실험 성능을 정량적으로 평가하기 위해 식(6)로 정의되는 첨두 신호대 잡음비(Peak Signal to Noise Ratio)를 사용하였다.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (6)$$

MSE(mean square error)는 평균 제곱 오차로 식(7)과 같다.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \| I(i,j) - k(i,j) \|^2 \quad (7)$$

여기서, $I(i,j)$는 원 영상, $k(i,j)$는 복원 영상을 나타낸다.

<그림 8>은 기존 방법과 본 논문에서 제안된 방법으로 암호화된 영상을 비교한 것이다. (a), (c), (e), (g)는 기존 방법으로 암호화된 영상이고 (b), (d), (f), (h)는 본 논문에서 제안한 방법으로 암호화된 영상이다. 두 방법 모두 시각적으로 원 영상을 유추하는데 어려움이 존재한다. 그렇지만 원영상과 비교해서 유추해 보면 기존의 방법[6]보다 제안된 방법의 암호화된 영상이 원 영상의 내용을 확인하는 것이 더 어렵다.

<그림 9>는 제안된 방법으로 암호화된 영상을 복호화해서 재생한 영상이다. 시각적으로 원본 영상과 동일하게 복호화된 것을 확인할 수 있다.

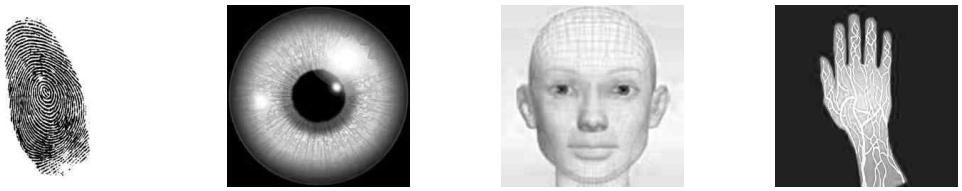
<표 1>은 암호화 되었다가 복호화 된 영상과 원 영상과의 차이점을 비교한 것이다. 일반적으로 PSNR 30dB이상이면 시각적으로 차이를 구별하기 어렵다. 기존의 방법[6]은 Fingerprint 영상을 제외한 190dB이상으로 계산과정에서 발생할 수 있는 오차를 제외하고 원래의 영상과 거의 동일하게 복호화된 것을 확인할 수 있다. 제안된 방법은 전부 230dB 이상으로 기존 방법보다 우수하다. 따라서 제안한 영상의 암호화 알고리즘이 가역적이면서 성능적으로 더 우수하다는 것을 확인할 수 있다.

<표 1> 복호화 영상의 PSNR값

image	**Fingerprint**	Eye	Face	Vein
previous	181.5460	198.9536	195.0574	195.7982
proposed	246.2982	263.9142	235.1525	259.4050

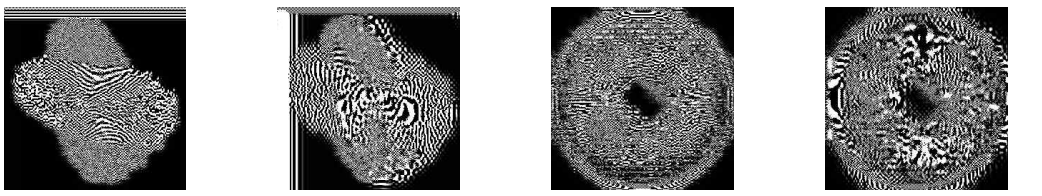
Ⅴ. 결론

그 동안 많은 암호화 알고리즘들이 개발되었지만 대부분이 메시지 데이터에 대한 암호화 기법들 이었다. 최근에는 생체인식 기술에 관심이 증가하고 있어 생체 영상정보에 대한 암호화의 필요성 요구가 높아지고 있다. 그렇지만 기존의 메시지 기반의 암호화 알고리즘들을 생체 영상 암호화에 적용하는데 있어

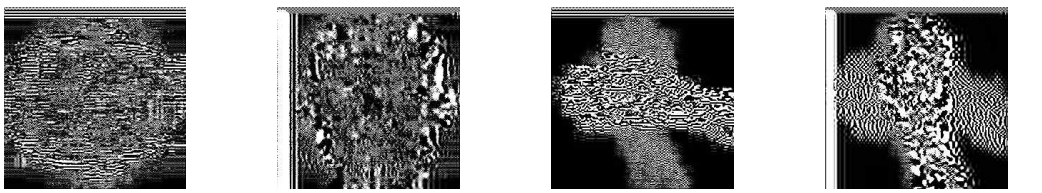


(a) Fingerprint (b) Eye (c) Face (d) Vein

<그림 7> 실험 영상

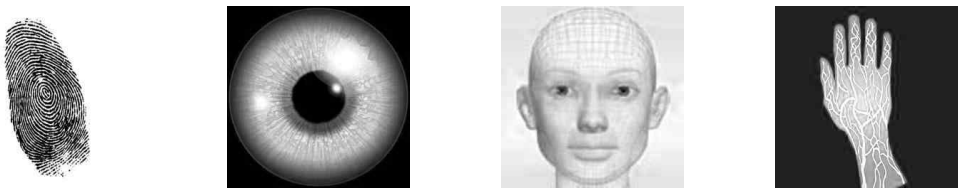


(a) 기존 방법의 Fingerprint 암호 영상 (b) 제안된 방법의 Fingerprint 암호 영상 (c) 기존 방법의 Eye 암호 영상 (d) 제안된 방법의 Eye 암호 영상



(e) 기존 방법의 Face 암호 영상 (f) 제안된 방법의 Face 암호 영상 (g) 기존 방법의 Vein 암호 영상 (h) 제안된 방법의 Vein 암호 영상

<그림 8> 암호화 실험 결과 영상



(a) Fingerprint (b) Eye (c) Face (d) Vein

<그림 9> 복호화 실험 영상

비효율적인 면들이 많이 존재한다. 본 논문에서는 주파수 영역에서 생체 영상을 암호화 방법을 제안하였다. 그리고 이 방법은 위치순열, 수치변환, 그리고 시각 변환을 기본으로 하는 무손실의 대칭키 암호화와 복호화 알고리즘으로 구현하였다. 따라서 제안된 알고리즘에서는 이산 웨이브렛 변환을 사용하여 영상을 변환하고, 생성된 부대역 영상의 주파수 영역에서 암호화 처리를 수행하는 하는 것으로, 부대역 영상의 고주파와 저주파 성분들은 비밀성을 보장하면서 처리된다. 생체 영상의 복호화 알고리즘은 주파수 영역에서 암호화 과정을 반대로 처리하는 것이다. 이 때, 고주파와 저주파의 부대역 영상들은 원래의 정보를 얻을 수 있도록 처리된다. 제안된 암호화 방법이 생체인식에서 응용되기 위해서, 여러 상세부분을 갖는 다양한 생체영상들에 대한 실험을 수행하였고 기존의 방법보다 효율적이라는 것을 확인하였다. 그래서

제안된 시스템은 합법적인 수신자 이외의 다른 사용자에 의해서 도난 될 수 있거나 접속될 수 있는 생체 영상등의 민감 영상들에 대한 위협을 감소시킨다. 또한 고품질 비밀 영상들의 전송을 요구하는 상황에서 유용하게 사용될 수 있다.

수정 가능한(cancelable) 생체정보의 개념은 모든 응용에서 사용되고 있는 패스워드처럼 수정이 가능하고 쉽게 삭제될 수 있는 생체정보 템플릿을 만드는 것이다. 수정 가능 생체정보는 생체정보 템플릿의 왜곡된 버전의 저장을 요구한다. 생체정보의 템플릿은 동일 생체정보 데이터와 연관되는 여러 종류의 템플릿들 생성이 가능해서 높은 개인비밀 수준을 제공할 수 있다. 이것은 다양한 데이터베이스에 저장되는 사용자 생체정보의 불연결 가능성을 촉진하는데 도움을 준다. 향후적으로 제안된 방법은 수정 가능한 생체정보 기술에서 효율적으로 적용될 수 있을 것이라고 예상된다.

참고문헌

[1] Sara Tedmori, Nijad Al-Najdawi, “Image Cryptographic Algorithm Based on the Haar Wavelet Transform,” Information Sciences, Vol. 269, 2014, pp. 21-34.

[2] Y. Chen “Cheating Prevention in Visual Cryptography,” IEEE Trans. Image Process., Vol 21, No 7, 2012, pp. 3319-3323.

[3] Daubechies, I., W. Sweldens, Factoring Wavelet transforms into lifting steps, Asilomar Conference on Signals, Systems, and Computers, 1997.

[4] Shin Jonghong, “Digital Image Processing Using Tunable Q-factor Discrete Wavelet Transformation”, Jonghong Shin, The Korea Society of Digital Industry & Information Management, Vol. 10, No. 3, Sep. 2014, pp. 237-247

[5] P. P. Vaidynathan, Multirate digital filters, filter banks, polyphase network and applications: A Tutorial, Proceedings of the IEEE. Vol. 78, No. 1, 1990

[6] Park Byeonghoon, Lim Joonghee, Shin Jonghong, “Imaged Cryptographic Algorithm Based on the Lifting Wavelet Transform”, 2015 The Korea Society of Digital Industry & Information Management Falling Proceeding, 21th Nov. 2015, pp. 47-51

■ 저자소개 ■

신 종 홍
Shin Jonghong

2003년 3월~현재 숭실사이버대학교 융합정보보안학과 교수
2002년 8월 홍익대학교 전자전기공학과 (공학박사)
1999년 2월 홍익대학교 전자전기공학과 (공학석사)
1997년 2월 홍익대학교 전자전기공학과 (공학사)

관심분야 : 멀티미디어 신호처리, 보안영상처리
E-mail : sigs@mail.kcu.ac

논문접수일: 2016년 5월 24일
수 정 일: 2016년 6월 2일
게재확정일: 2016년 6월 6일