한국정보전자통신기술학회논문지(jkiiect)'22-2, Vol.15 No.1
논문 22-15-01-36 http://dx.doi.org/10.17661/jkiiect.2022.15.1.36

삼중 암호화 기법을 적용한 가역 데이터 은닉기법

정수목*

Reversible data hiding technique applying triple encryption method

Soo-Mok Jung*

요약 영상의 히스토그램을 시프트 시켜 영상에 기밀 데이터를 은닉하는 가역 데이터 은닉기법들이 개발되었다. 이러한 기법들은 은닉된 기밀 데이터의 보안이 취약한 단점이 있다. 본 논문에서는 이러한 단점을 해결하기 위하여 픽셀값 정보를 사용하여 기밀 데이터를 삼중으로 암호화한 후 커버 이미지에 은닉하는 기법을 제안하였다. 제안된 기법을 사용하여 기밀 데이터를 삼중으로 암호화하여 커버 이미지에 은닉하여 스테고 이미지를 생성하면, 픽셀 정보에 기반한 암호화가 삼중으로 수행되었으므로 삼중으로 암호화되어 은닉된 기밀 데이터의 보안성이 크게 향상된다. 제안된 기법의 성능을 측정하기 위한 실험에서, 스테고 이미지로부터 삼중으로 암호화된 기밀 데이터를 추출하여도 암호화 키 없이는 원본 기밀 데이터를 추출할 수 없었다. 그리고 스테고 이미지(stego-image)의 화질이 48.39dB 이상인 매우 우수한 영상이기 때문에 스테고 이미지에 기밀 데이터가 은닉되어있는지 인지할 수 없었으며, 스테고 이미지에 30,487비트 이상의 기밀 데이터가 은닉되었다. 제안된 기법은 스테고 이미지에 은닉되어있는 삼중으로 암호화된 기밀 데이터로부터 원본 기밀 데이터를 손실 없이 추출할 수 있으며, 스테고 이미지로부터 원본 커버 이미지를 왜곡 없이 복원할 수 있다. 따라서 제안된 기법은 보안이 중요하고 원본 커버 이미지를 완벽하게 복원하는 것이 필요한 군사, 의료, 디지털 라이브러리 등의 응용 분야에 효과적으로 활용될 수 있다.

Abstract Reversible data hiding techniques have been developed to hide confidential data in the image by shifting the histogram of the image. These techniques have a weakness in which the security of hidden confidential data is weak. In this paper, to solve this drawback, we propose a technique of triple encrypting confidential data using pixel value information and hiding it in the cover image. When confidential data is triple encrypted using the proposed technique and hidden in the cover image to generate a stego-image, since encryption based on pixel information is performed three times, the security of confidential data hidden by triple encryption is greatly improved. In the experiment to measure the performance of the proposed technique, even if the triple-encrypted confidential data was extracted from the stego-image, the original confidential data could not be extracted without the encryption keys. And since the image quality of the stego-image is 48.39dB or higher, it was not possible to recognize whether confidential data was hidden in the stego-image, and more than 30,487 bits of confidential data were hidden in the stego-image. The proposed technique can extract the original confidential data from the triple-encrypted confidential data hidden in the stego-image without loss, and can restore the original cover image from the stego-image without distortion. Therefore, the proposed technique can be effectively used in applications such as military, medical, digital library, where security is important and it is necessary to completely restore the original cover image.

Key Words : Confidential data hiding, Cover image, Histogram shift, Image, Stego-image

1. 서론

데이터 은닉(data hiding)은 디지털 이미지와 같은 커버 미디어에 기밀 데이터를 삽입하는 중요한 기술이다. 데이터 은닉기법을 사용하여 커버 이미지(cover image)에 기밀 데이터를 은닉하여 스테고 이미지(stego-image)

* Division of Computer Science & Engineering, Sahmyook University
Received February 03, 2022 Revised February 08, 2022 Accepted February 16, 2022

를 생성하고, 스테고 이미지로부터 원본 기밀 데이터를 추출한다.

기밀 데이터가 스테고 이미지에 숨겨진 것을 인지할 수 없는 비인지성(imperceptibility)이 데이터 은닉기법에서 중요하다[1][2]. 비인지성을 충족하려면 스테고 이미지의 품질이 우수해야 한다. 스테고 이미지의 품질을 높게 유지하기 위한 대부분의 데이터 은닉기법들은 스테고 이미지에서 기밀 데이터를 추출한 후 복원되는 커버 이미지에 왜곡이 발생한다. 따라서 복원된 커버 이미지와 원본 커버 이미지가 일치하지 않는다[3].

복원된 커버 이미지가 원본 표지 이미지와 일치하는 가역 데이터 은닉기법은 군사, 의료 및 디지털 라이브러리 등의 응용에 중요하다[3]. 이미지의 히스토그램(histogram)을 시프트(shift) 시켜 기밀 데이터를 은닉하는 다양한 가역적 데이터 은닉기법이 제안되었다[2-8].

Ni 등은 영상의 히스토그램을 시프트 시켜 데이터를 은닉하는 NSAS 기법을 제안하였다[2]. 이 기법은 커버 이미지의 히스토그램에서 피크 포인트(peak point)와 최근접 제로 포인트(closest zero point)를 조사한 후, 그 사이에 있는 픽셀들을 이동시켜 피크 포인트에 해당하는 픽셀들에 기밀 데이터 비트를 삽입한다. 이 기법에서는 은닉할 수 있는 최대 비트 수가 커버 이미지의 히스토그램에서 피크 포인트에 해당하는 픽셀 수로 제한된다.

Li 등은 NSAS 기법을 개선한 APD(Adjacent Pixel Difference) 기법[3]을 제안하였는데, 이 기법은 인접한 픽셀 간의 차분 시퀀스에 대한 히스토그램을 사용하여 기밀 데이터를 삽입하는 가역적 데이터 은닉기법이다. 이 기법에서는 커버 이미지에서 인접 픽셀 간의 픽셀값 차이로 구성되는 차분 시퀀스를 생성한 후, 차분 시퀀스에 대한 히스토그램을 생성한다. 인접한 픽셀은 일반적으로 서로 유사한 값을 갖기 때문에 차분 시퀀스의 요소들은 0 또는 0에 가까운 값을 갖는다. 따라서 히스토그램의 피크 포인트에서의 빈도수가 커지게 되어 커버 이미지에 은닉될 수 있는 데이터 비트 수가 증가하게 된다. APD 기법의 경우, 커버 이미지에 은닉될 수 있는 기밀 데이터의 비트 수는 인접한 픽셀 간의 차분 시퀀스에 대한 히스토그램의 피크 포인트(peak point)에서의 빈도수(frequency)로 제한된다. 그리고 이미지의 지역적 유사성과 표면 특성을 사용하는 가역 데이터 은닉기법들이 본 연구팀에 의해 제안되었다[5-8].

본 논문에서는 APD 기법의 단점인 영상에 은닉된 기밀 데이터의 보안이 취약한 문제점을 해결하기 위하여, 픽셀값 정보를 사용하여 기밀 데이터를 삼중으로 암호화하여 커버 이미지에 은닉하여 스테고 이미지를 생성하고 스테고 이미지로부터 원본 기밀 데이터를 손실 없이 추출하며 원본 커버 이미지를 왜곡 없이 복원하는 가역 데이터 은닉기법을 제안하였다. 제안된 기법은 기존의 APD 기법보다 기밀 데이터의 보안성이 크게 강화된 기법이다.

제안된 기법을 사용하면 픽셀값 정보를 사용하여 기밀 데이터가 삼중으로 암호화된 후 커버 이미지에 은닉되어 스테고 이미지가 생성된다. 따라서 스테고 이미지에 은닉된 삼중으로 암호화된 기밀 데이터의 보안성이 크게 향상된다. 또한 스테고 이미지에 저장된 삼중으로 암호화된 기밀 데이터로부터 원본 기밀 데이터를 손실 없이 추출할 수 있으며, 스테고 이미지로부터 원본 커버 이미지를 왜곡 없이 복원할 수 있다.

2. APD 기법

영상에서 인접한 픽셀들은 유사한 값을 갖는 특성이 있다. 이러한 성질을 활용하여 은닉하는 기밀 데이터를 획기적으로 증가시키는 기법이 APD 기법이다. 인접한 픽셀들이 비슷한 값을 갖는 특성을 효과적으로 활용하기 위하여, APD 기법에서는 커버 이미지를 역-S 순(inverse s-order)으로 스캔하여 커버 이미지 시퀀스(C)를 구성한다. 커버 이미지 시퀀스(C)를 식(1)에 적용하여 차분 시퀀스(D)를 생성한다. 이렇게 생성된 차분 시퀀스의 각 요소는 0과 0에 가까운 매우 작은 값들을 갖게 된다. 이는 인접 픽셀들이 대부분 비슷한 값을 갖기 때문이다. 따라서 차분 시퀀스에 대한 히스토그램을 구성하면 0과 0 주변의 값들에서의 빈도수가 매우 크게 된다. 식(1)에서 n은 (영상의 폭) x (영상의 너비)에 해당하는 값이다.

$$D_i = \begin{cases} C_i & \text{if } i = 0 \\ C_{i-1} - C_i & \text{if } 1 \le i \le n-1 \end{cases} \quad (1)$$

512x512 크기를 갖는 Lenna 영상을 사용하여 커버 이미지 시퀀스를 구성하고, 커버 이미지 시퀀스를 식(1)에 적용하여 차분 시퀀스를 생성한 다음, 차분 시

퀀스(D)에 대한 히스토그램을 생성한 결과를 그림 1에 나타내었다. 그림 1에서 보는 바와 같이 피크 포인터에서 빈도수가 매우 크게 되어 커버 이미지에 은닉 가능한 기밀 데이터의 비트 수는 48,424 비트 ($h(PP_1)+h(PP_2)$)가 된다. 이는 피크 포인터에 해당하는 영상의 픽셀들에 기밀 데이터를 비트 단위로 은닉시키기 때문이다. 따라서 APD 기법을 사용하면 NSAS 기법보다 8.5배 많은 기밀 데이터를 은닉할 수 있다.

APD 기법에서 기밀 데이터를 은닉하여 스테고 이미지를 생성하는 절차는 그림 2와 같다.

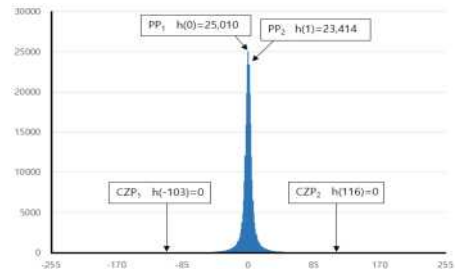

그림 1. D에 대한 히스토그램
Fig. 1. Histogram of sequence D

단계 1. 커버 이미지의 픽셀들을 역 S-순으로 스캔하여 커버 이미지 시퀀스(C)를 구성한다.

단계 2. 커버 이미지 시퀀스(C)를 식(1)에 적용하여 차분 시퀀스(D)를 생성한다.

단계 3. 차분 시퀀스(D)에 대한 히스토그램을 생성하고, PP_1, CZP_1, PP_2, CZP_2를 결정한다.

단계 4. 식(2), (3)을 차분 시퀀스(D)에 적용하여 시프트된 차분 시퀀스(DS)를 생성한다.

$$DS_i = \begin{cases} D_i & \text{if } i=0 \text{ or } D_i \notin [PP_j + sd_j, CZP_j] \\ D_i + sd_j & \text{if } D_i \in [PP_j + sd_j, CZP_j] \end{cases} \quad (2)$$

$$sd_j = \begin{cases} 1 & \text{if } PP_j < CZP_j \\ -1 & \text{if } CZP_j < PP_j \end{cases} \quad \text{where } j \in \{1,2\} \quad (3)$$

단계 5. 시프트된 차분 시퀀스(DS)에 식(4)를 적용하여 기밀 데이터가 삽입(embedding)된 은닉 시퀀스(DE)를 생성한다.

$$DE_i = \begin{cases} DS_i & \text{if } i=0 \text{ or } DS_i \neq PP_j \text{ or } data=0 \\ DS_i + sd_j & \text{if } DS_i = PP_j \text{ and } data=1 \end{cases} \quad (4)$$

단계 6. 식(5)를 사용하여 스테고 이미지 시퀀스(S)를 생성한다. n의 값은 (영상의 폭) x (영상의 높이) 이다.

$$S_i = \begin{cases} DE_i & \text{if } i=0 \\ C_{i-1} - DE_i & \text{if } 1 \le i \le n-1 \end{cases} \quad (5)$$

단계 7. 스테고 이미지 시퀀스(S)를 역 S-순으로 구성하여 스테고 이미지를 생성한다.

그림 2. APD 기법에서 기밀 데이터 은닉 절차
Fig. 2. Confidential data hiding procedure in APD technique

스테고 이미지로부터 기밀 데이터를 추출하고 원본 커버 이미지를 복원하는 절차가 그림 3에 나타나 있다. 그림 3에 나타난 바와 같이 스테고 이미지로부터 기밀 데이터를 손실 없이 추출할 수 있고, 스테고 이미지로부터 원본 커버 이미지를 왜곡 없이 복원할 수 있다. APD 기법의 절차를 따라 커버 이미지에 기밀 데이터를 은닉하여 스테고 이미지를 생성하면, NSAS 기법보다 8.5배 많은 기밀 데이터를 은닉할 수 있다. 따라서 APD 기법은 매우 효과적인 기밀 데이터 은닉기법이지만, 은닉된 기밀 데이터의 보안이 취약한 단점이 있다.

단계 8. 스테고 이미지를 역 S-순으로 스캔하여 스테고 이미지 시퀀스(S)를 구성한다.

단계 9. i 값을 증가시키면서 단계 9.1~단계 9.2를 반복적으로 수행하여 커버 이미지 시퀀스(C)와 은닉 시퀀스(DE)를 복원한다.

단계 9.1. 식(6)을 만족하는 은닉 시퀀스(DE)를 복원한다.

$$DE_i = \begin{cases} C_i & \text{if } i = 0 \\ C_{i-1} - S_i & \text{otherwise} \end{cases} \quad (6)$$

단계 9.2. 식(7)을 사용하여 커버 이미지 시퀀스(C)를 복원한다.

$$C_i = \begin{cases} S_i & \text{if } i = 0 \\ S_i + sd_j & \text{else if } 1 \le i \le n-1 \text{ and} \\ & \quad C_{i-1} - S_i \in [PP_j + sd_j, CZP_j] \\ S_i & \text{otherwise} \end{cases} \quad (7)$$

단계 10. 식(8)을 은닉 시퀀스(DE)의 각 요소에 적용하여 기밀 데이터를 추출한다.

$$\text{Extraction bit} = \begin{cases} 0 & \text{if } DE_i = PP_j \\ 1 & \text{else if } DE_i = PP_j + sd_j \end{cases} \quad (8)$$

단계 11. 커버 이미지 시퀀스(C)를 역 S-순으로 원본 커버 이미지를 구성한다.

그림 3. APD 기법에서 기밀 데이터 추출 및 원본 커버 이미지 복원 절차

Fig. 3. Confidential data extraction and original cover image restoration procedure in APD technique

3. 제안 기법

APD 기법의 문제점인 취약한 기밀 데이터(CD, confidential data)의 보안을 강화하기 위하여, 제안 기법에서는 영상의 픽셀 정보를 사용하여 기밀 데이터를 삼중으로 암호화한 후, 삼중으로 암호화된 기밀 데이터(TECD, triple encrypted confidential data)를 커버 이미지에 은닉하여 스테고 이미지를 생성한다. 따라서 제안 기법으로 기밀 데이터를 커버 이미지에 은닉하여 스테고 이미지를 생성하면, 스테고 이미지에 은닉된 기밀 데이터의 보안이 매우 강력하게 된다.

제안 기법에서 영상의 픽셀 정보를 사용하여 기밀 데이터를 삼중으로 암호화한 후 커버 이미지에 은닉하여 스테고 이미지를 생성하는 절차는 그림 4와 같다. 그림 4에서 보는 바와 같이, APD 기법의 단계 5가 제안 기법에서는 단계 5.1~5.4로 변경되었다. 그리고 나머지 단계(단계 1~4, 단계 6~7)는 APD 기법의 해당 단계와 같다.

제안 기법에서 픽셀 정보를 사용하여 기밀 데이터를 삼중으로 암호화하는 과정은 다음과 같이 진행된다. 단계 5.1에서 보는 바와 같이, 식(9)를 사용하여 기밀 데이터(CD)를 1회 암호화한다. 식(9)에 사용된 SECD는 1회 암호화된 기밀 데이터(SECD, single encrypted confidential data)를 나타낸다. CD_i는 i번째 피크 포인트에 은닉될 i번째 기밀 데이터 비트를 나타낸다. DS_{i-b}는 i번째 기밀 데이터가 은닉될 픽셀 위치로부터 b번째 앞의 위치에 있는 시프트된 차분 시퀀스(DS)의 값을 나타낸다. mod k는 k로 나눈 나머지를 구하는 연산을 나타낸다. 차분 시퀀스(DS)의 성분은 양의 값, 0, 음의 값을 가질 수 있으므로 절대치를 취한 값이 사용된다. $(\sim)_{LSB}$는 괄호 안 값(~)의 LSB (least significant bit)를 나타낸다. 식(9)에 사용된 기호(⊙)는 exclusive NOR 연산기호이다.

1회 암호화된 기밀 데이터(SECD)는 단계 5.2와 같이 식(10)을 사용하여 이중으로 암호화된다. 식(10)에서 DECD(double encrypted confidential data)는 2중으로 암호화된 기밀 데이터를 나타낸다. DS_{i+n}은 i번째 기밀 데이터가 은닉될 픽셀 위치로부터 n번째 뒤의 위치에 있는 시프트된 차분 시퀀스(DS)의 값을 나타낸다. 식(10)에서 사용된 SECD는 식(9)에서 구해진 1회 암호화된 기밀 데이터를 나타낸다. 식(9), (10) 에서 i-b, i+n에 해당하는 위치가 시프트된 차분 시퀀스(DS)에 없는 경우에는 i번째 기밀 데이터가 은닉될 픽셀 위치로부터 가장 멀리 떨어져 있는 위치의 시프트된 차분 시퀀스(DS)의 값을 사용한다.

단계 5.3의 식(11)을 사용하여 삼중으로 암호화된 기밀 데이터(TECD)를 생성한다. 식(11)에서 보는 바와 같이, 이중으로 암호화된 기밀 데이터($DECD_i$)와 p번째 앞에 있는 암호화된 기밀 데이터($DECD_{i-p}$)가 exclusive OR 되어 삼중으로 암호화된 기밀 데이터가 생성된다. 식(11)의 $DECD_{i-p}$에서 p는 1 이상인 값을 갖고, i-p가 0보다 적으면 $DECD_{i-p}$는 0의 값을 갖다. 식(11)에서 사용된 기호(⊕)는 exclusive OR를 나타내는 연산기호이다.

식(9)~(11) 을 사용하여 삼중으로 암호화된 기밀 데이터(TECD)가 APD 기법에서와 같은 방법으로 커버 이미지에 은닉되어 스테고 이미지를 생성한다. 따라서 제안 기법으로 기밀 데이터를 삼중으로 암호화하여 커

버 이미지에 은닉하여 스테고 이지를 생성하면, 스테고 이미지에 은닉되는 기밀 데이터의 보안이 크게 강화된다. 기밀 데이터를 삼중으로 암호화하는데 사용되는 암호화 키는 k, b, n, p이다.

제안된 기법에서 기밀 데이터(CD)룰 세 번 암호화하여 삼중으로 암호화된 기밀 데이터(TECD)를 생성하는 간단한 예는 다음과 같다. 3x3 크기의 영상에 대하여 역-s 스캔한 커버 이미지 시퀀스(C)는 260, 258, 259, 255, 256, 258, 258, 258, 255라고 가정하고, 기밀 데이터(CD) 비트는 1001이라고 가정한다. 식(9)~(11)에 사용된 암호화 키는 각각 k=3, b=1, n=1, p=1이라고 가정한다. 이 경우, 식(1)을 적용하여 단계 2에서 생성되는 차분 시퀀스(D)는 260, 2, -1, 4, -1, -2, 0, 0, 3이 된다. 단계 3과 같이 차분 시퀀스(D)에 대한 히스토그램을 생성하면 PP_1=-1, PP_2=0, CZP_1=-3, CZP_2=1이 된다. 단계 4와 같이, 차분 시퀀스(D)와 피크 포인트(PP_1, PP_2)와 최근접 제로 포인트(CZP_1, CZP_2)를 식(2)에 적용하여 쉬프트된 차분 시퀀스(DS)를 구하면 260, 2, -1, 4, -1, -3, 0, 0, 3이 된다. 쉬프트된 차분 시퀀스(DS)의 성분이 피크 포인트(PP1=-1, PP2=0) 값을 갖는 위치에 기밀 데이터 비트가 차례대로 은닉된다. 따라서 차분 시퀀스(DS)의 성분이 -1, -1, 0, 0인 위치에 기밀 데이터 비트들이 차례대로 은닉된다. 그러므로 이러한 영상에는 4비트의 기밀 데이터가 은닉될 수 있다. 이 위치들에 은닉될 기밀 데이터를 1회 암호화한 기밀 데이터(SECD)는 0010이다. 이 값은 단계 5.1에서 다음과 같이 구해진다. $SECD_0$= $(|DS_{0-1}| \bmod 3)_{LSB}$⊙$CD_0$=$(2 \bmod 3)_{LSB}$⊙1= $(2)_{LSB}$⊙1=0⊙1=0, $SECD_1$=$(|DS_{1-1}| \bmod 3)_{LSB}$⊙$CD_1$=$(4 \bmod 3)_{LSB}$⊙0=$(1)_{LSB}$⊙0=1⊙0=0, $SECD_2$=$(|DS_{2-1}| \bmod 3)_{LSB}$⊙$CD_2$=$(3 \bmod 3)_{LSB}$⊙0=$(0)_{LSB}$⊙0=0⊙0=1, $SECD_3$=$(|DS_{3-1}| \bmod 3)_{LSB}$⊙$CD_3$=$(0 \bmod 3)_{LSB}$⊙1=$(0)_{LSB}$⊙1 =0⊙1=0.

단계 5.2의 식(10)을 적용하여 2중으로 암호화된 기밀 데이터(DECD)를 구하면 0101이 된다. 이 값은 단계 5.2에서 다음과 같이 구해진다. $DECD_0$=$((|DS_{0+1}| \bmod 3)_{LSB}$⊙$SECD_0$=$(4 \bmod 3)_{LSB}$⊙0=$(1)_{LSB}$⊙0=1⊙0=0, $DECD_1$= $((|DS_{1+1}| \bmod 3)_{LSB}$⊙$SECD_1$=$(3 \bmod 3)_{LSB}$⊙0=$(0)_{LSB}$⊙0=0⊙0=1, $DECD_2$=$((|DS_{2+1}| \bmod 3)_{LSB}$⊙$SECD_2$=$(0 \bmod 3)_{LSB}$⊙1=$(0)_{LSB}$⊙1=0⊙1=0, $DECD_3$=$((|DS_{3+1}| \bmod 3)_{LSB}$⊙$SECD_3$=
$(3 \bmod 3)_{LSB}$⊙0=$(0)_{LSB}$⊙0=0⊙0=1.

단계 5.3의 식(11)을 적용하여 삼중으로 암호화된 기밀 데이터(TECD)를 구하면 0111이 된다. 이 값은 단계 5.3에서 다음과 같이 구해진다. $TECD_0$=$DECD_0$⊕$DECD_{0-1}$=0⊕0=0, $TECD_1$=$DECD_1$⊕$DECD_{1-1}$=1⊕0=1, $TECD_2$=$DECD_2$⊕$DECD_{2-1}$=0⊕1=1, $TECD_3$=$DECD_3$⊕$DECD_{3-1}$=1⊕0=1.

제안 기법에서 스테고 이미지로부터 원본 기밀 데이터를 추출하고, 원본 커버 이미지를 복원하는 절차는 그림 5와 같다. 그림 5에서 보는 바와 같이, APD 기법의 단계 10이 제안 기법에서는 단계 10.1~10.6으로 변경되었다. 그리고 나머지 단계(단계 1~9, 단계 11)는 APD 기법의 해당 단계와 같다. 제안된 기법에서 스테고 이미지로부터 삼중으로 암호화된 기밀 데이터(TECD)를 추출하고, 삼중으로 암호화된 기밀 데이터로부터 원본 기밀 데이터를 추출하는 절차는 그림 5의 단계 10.1~10.6에 나타나 있다. APD 기법에서 식(8)을 사용하여 추출하는 것은 스테고 이미지에 은닉되어있는 원본 기밀 데이터이다. 그러나 제안 기법에서는 삼중으로 암호화된 기밀 데이터(TECD)를 은닉하였기 때문에 단계 10.1에서 보는 바와 같이, 식(13)을 은닉 시퀀스(DE)의 각 요소에 적용하여 삼중으로 암호화된 기밀 데이터(TECD)를 추출한다. 이때 사용된 은닉 시퀀스(DE)는 제안 기법의 단계 9(단계 9.1~9.2)에서 복원된 것이다.

단계 10.1에서 추출된 삼중으로 암호화된 기밀 데이터(TECD)가 단계 10.2~10.6에 따라 원본 기밀 데이터(CD)로 변환되는 과정은 다음과 같다. 단계 10.2에서 보는 바와 같이 식(14)를 사용하여 삼중으로 암호화된 기밀 데이터(TECD)로부터 이중으로 암호화된 기밀 데이터(DECD)를 추출한다. 식(14)에서 i-p가 0보다 적은 경우는 $DECD_{i-p}$=는 0으로 둔다. 따라서 $DECD_0$=$TECD_0$가 된다. i=1이고 p=1인 경우, $DECD_1$=$TECD_1$⊕$DECD_0$가 된다.

단계 10.3에서 보는 바와 같이, 커버 이미지 시퀀스(C)를 식(1)에 적용하여 차분 시퀀스(D)를 생성한다.

이때 사용되는 커버 이미지 시퀀스(C)는 제안 기법의 단계 9(단계 9.1~9.2)에서 복원된 것이다. 단계 10.4와 같이 식(2)~(3)을 차분 시퀀스(D)에 적용하여 시프트된 차분 시퀀스(DS)를 생성한다. 단계 10.4에서 생성된 차분 시퀀스(DS)와 단계 10.2에서 추출된 이중으로 암호화된 기밀 데이터(DECD)를 식(15)에 적용하여 1회 암호화된 기밀 데이터(SECD)를 추출하는 과정이 단계 10.5에 나타나 있다.

단계 10.5에서 추출된 1회 암호화된 기밀 데이터(SECD)를 식(16)에 적용하여 원본 기밀 데이터(CD)를 추출하는 단계가 단계 10.6이다.

제안된 기법에서 삼중으로 암호화된 기밀 데이터(TECD) 0111로부터 원본 기밀 데이터(CD) 1001을 추출하는 예는 다음과 같다. 이 경우, 삼중으로 암호화된 기밀 데이터(TECD) 0111을 생성하는 전술한 예에서와 같은 조건이 적용되는 것으로 가정한다. 단계 8, 9(9.1, 9.2)에서 복원된 커버 이미지 시퀀스(C)는 260, 258, 259, 255, 256, 258, 258, 258, 255이고, 은닉 시퀀스(DE)는 260, 2, -2, 4, -2, -3, 1, 1, 3이 된다. 단계 10.1에서 은닉 시퀀스(DE)로부터 추출되는 삼중으로 암호화된 기밀 데이터(TECD)는 0111이 된다.

단계 10.2에서, 삼중으로 암호화된 기밀 데이터(TECD) 0111이 이중으로 암호화된 기밀 데이터(DECD) 0101로 변환된다. 이 변환과정은 단계 10.2에서 다음과 같이 이루어진다. $DECD_0=TECD_0 \oplus DECD_{0-1}=0 \oplus 0=0$, $DECD_1=TECD_1 \oplus DECD_{1-1}=1 \oplus 0=1$, $DECD_2=TECD_2 \oplus DECD_{2-1}=1 \oplus 1=0$, $DECD_3=TECD_3 \oplus DECD_{3-1}=1 \oplus 0=1$.

단계 10.3에 따라 차분 시퀀스(D)를 생성하면 260, 2, -1, 4, -1, -2, 0, 0, 3이 되고, 단계 10.4에 따라 쉬프트된 차분 시퀀스(DS)를 생성하면 260, 2, -1, 4, -1, -3, 0, 0, 3이 된다.

단계 10.5에서 이중으로 암호화된 기밀 데이터(DECD) 0101이 1회 암호화된 기밀 데이터(SECD) 0010으로 변환된다. 이 변환과정은 단계 10.5에서 다음과 같이 이루어진다. $SECD_0=((|DS_{0+1}| \bmod 3)_{LSB}) \odot DECD_0=(4 \bmod 3)_{LSB} \odot 0=(1)_{LSB} \odot 0=1 \odot 0=0$, $SECD_1=((|DS_{1+1}| \bmod 3)_{LSB}) \odot DECD_1=(3 \bmod 3)_{LSB} \odot 1=(0)_{LSB} \odot 1=0 \odot 1=0$, $SECD_2=((|DS_{2+1}| \bmod 3)_{LSB}) \odot DECD_2=(0 \bmod 3)_{LSB} \odot 0=(0)_{LSB} \odot 0=0 \odot 0=1$, $SECD_3=((|DS_{3+1}| \bmod 3)_{LSB}) \odot DECD_3=(3 \bmod 3)_{LSB} \odot 1=(0)_{LSB} \odot 1=0 \odot 1=0$.

단계10.6에서 1회 암호화된 기밀 데이터(SECD) 0010이 원본 기밀 데이터(CD) 1001로 변환된다. 이 변환과정은 단계 10.6에서 다음과 같이 이루어진다. $CD_0=(|DS_{0-1}| \bmod 3)_{LSB} \odot SECD_0=(2 \bmod 3)_{LSB} \odot 0=(2)_{LSB} \odot 0=0 \odot 0=1$, $CD_1=(|DS_{1-1}| \bmod 3)_{LSB} \odot SECD_1=(4 \bmod 3)_{LSB} \odot 0=(1)_{LSB} \odot 0=1 \odot 0=0$, $CD_2=(|DS_{2-1}| \bmod 3)_{LSB} \odot SECD_2=(3 \bmod 3)_{LSB} \odot 1=(0)_{LSB} \odot 1=0 \odot 1=0$, $CD_3=(|DS_{3-b}| \bmod 3)_{LSB} \odot SECD_3=(0 \bmod 3)_{LSB} \odot 0=(0)_{LSB} \odot 0=0 \odot 0=1$.

제안된 단계 10.1~10.6과 같이, 스테고 이미지로부터 삼중으로 암호화된 기밀 데이터(TECD)를 추출하고, 삼중으로 암호화된 기밀 데이터로부터 원본 기밀 데이터(CD)를 손실 없이 추출할 수 있다. 그리고 단계 9(단계 9.1~9.2)에 따라 스테고 이미지로부터 원본 커버 이미지를 왜곡 없이 복원할 수 있다.

⋮

단계 5.1 식(9)를 사용하여 1회 암호화된 기밀 데이터(SECD)를 생성한다.

$$SECD_i=(|DS_{i-b}| \bmod k)_{LSB} \odot CD_i \quad (9)$$

단계 5.2 식(10)을 사용하여 이중으로 암호화된 기밀 데이터(DECD)를 생성한다.

$$DECD_i=((|DS_{i+n}| \bmod k)_{LSB}) \odot SECD_i \quad (10)$$

단계 5.3 식(11)을 사용하여 삼중으로 암호화된 기밀 데이터(TECD)를 생성한다.

$$TECD_i=DECD_i \oplus DECD_{i-p} \quad (11)$$

단계 5.4 식(12)를 시프트된 차분 시퀀스(DS)에 적용하여 삼중으로 암호화된 기밀 데이터(TECD)가 은닉된(embedding) 은닉 시퀀스(DE)를 생성한다.

$$DE_i=\begin{cases} DS_i & \text{if } i=0 \text{ or } DS_i \neq PP_j \text{ or } TECD_i=0 \\ DS_i+sd_j & \text{if } DS_i=PP_j \text{ and } TECD_i=1 \end{cases} \quad (12)$$

⋮

그림 4. 제안 기법에서 기밀 데이터 은닉 절차
Fig. 4. Confidential data hiding procedure in the proposed technique

⋮

단계 10.1 식(13)을 은닉 시퀀스(DE)의 각 요소에 적용하여 삼중으로 암호화된 기밀 데이터(TECD)를 추출한다.

$$TECD_i = \begin{cases} 0 & \text{if} \quad DE_i = PP_j \\ 1 & \text{else if} \quad DE_i = PP_j + sd_j \end{cases} \quad (13)$$

단계 10.2 단계 10.3에서 추출된 삼중으로 암호화된 기밀 데이터(TECD)를 식(14)에 적용하여 이중으로 암호화된 기밀 데이터(DECD)를 추출한다.

$$DECD_i = TECD_i \oplus DECD_{i-p} \quad (14)$$

단계 10.3 단계 9에서 복원된 커버 이미지 시퀀스(C)를 식(1)에 적용하여 차분 시퀀스(D)를 생성한다.

단계 10.4 식(2), (3)을 차분 시퀀스(D)에 적용하여 시프트된 차분 시퀀스(DS)를 생성한다.

단계 10.5 이중으로 암호화된 기밀 데이터(DECD)를 식(15)에 적용하여 1회 암호화된 기밀 데이터(SECD)를 추출한다.

$$SECD_i = ((|DS_{i+n}| \bmod k)_{LSB}) \odot DECD_i \quad (15)$$

단계 10.6 1회 암호화된 기밀 데이터(SECD)를 식(16)에 적용하여 원본 기밀 데이터(CD)를 추출한다.

$$CD_i = (|DS_{i-b}| \bmod k)_{LSB} \odot SECD_i \quad (16)$$

⋮

그림 5. 제안 기법에서 기밀 데이터 추출 및 원본 커버 이미지 복원 절차
Fig. 5. Confidential data extraction and original cover image restoration procedure in the proposed technique

4. 실험 결과

제안 기법의 성능을 확인하기 위하여 512x512 크기를 갖는 그레이 스케일 영상인 Lenna, man, Elaine, goldhill을 사용하여 실험을 수행하였다. 본 논문의 영문 초록을 기밀 데이터로 사용하였고, 식(9)~(11)을 사용하여 기밀 데이터를 삼중으로 암호화한 후, 삼중으로 암호화된 기밀 데이터(TECD)를 커버 이미지에 은닉하여 스테고 이미지를 생성하였다. 식(9)~(11)에서 사용된 암호화 키는 k=3, b=1, n=1, p=1로 하여 실험을 수행하였다.

그림 6은 제안 기법으로 기밀 데이터를 삼중으로 암호화한 후, 삼중으로 암호화된 기밀 데이터(TECD)를 커버 이미지에 은닉하여 생성된 스테고 이미지들이다. 그림 6에서 보는 바와 같이 기밀 데이터가 삼중으로 암호화된 후, 삼중으로 암호화된 기밀 데이터가 커버 이미지에 은닉된 결과 영상인 스테고 이미지의 화질이 매우 우수하여 스테고 이미지와 원본 커버 이미지 사이의 구별이 불가능하고, 스테고 이미지에 삼중으로 암호화된 기밀 데이터가 은닉되어있어 스테고 이미지에 은닉된 기밀 데이터의 보안이 매우 우수하게 된다.

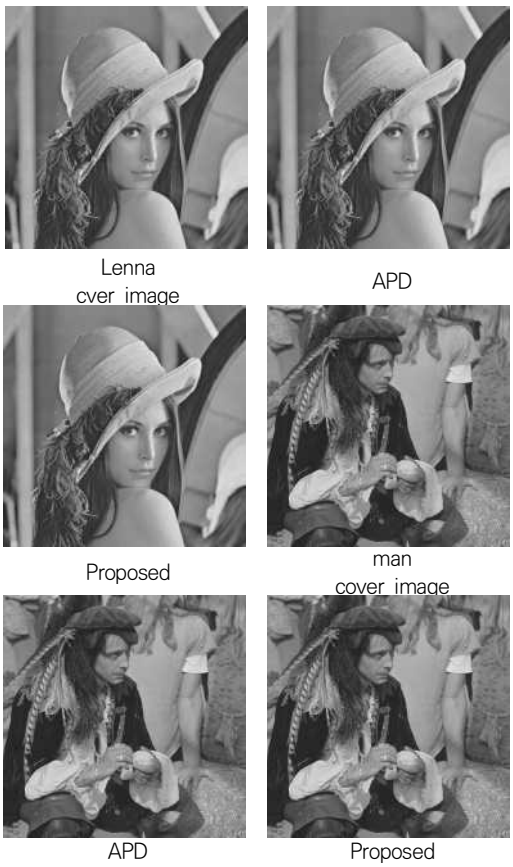

그림 6. 커버 이미지, 스테고 이미지
Fig. 6. Cover image, stego-image

표 1은 실험 결과 데이터를 나타낸다. 제안 기법을 사용하여 기밀 데이터를 은닉하여 생성된 스테고 이미지의 화질은 48.39dB 이상이다. 따라서 스테고 이미지와 커버 이미지를 구분할 수 없을 정도로 스테고 이미지의 화질이 우수하다. 일반적으로 화질이 40dB 이상이면 인간의 시각으로 차이를 구별할 수 없다.

표 1에서 보는 바와 같이 제안된 기법을 사용하는 경우, 은닉되는 기밀 데이터의 비트 수는 각 커버 이미지의 차분 시퀀스(D)에 대한 히스토그램의 피크 포인트에서의 빈도수($h(PP_1)+ h(PP_2)$)에 해당하는 비트 수만큼을 은닉할 수 있다. Lnna, man, Elaine, goldhill 영상의 경우 각각 48,424, 47,408, 30,487, 35,868 비트의 기밀 데이터를 은닉할 수 있다. 이러한 은닉되는 기밀 데이터는 APD 기법을 적용하여 기밀 데이터를 은닉하는 경우의 기밀 데이터의 크기와 같다. 이는 제안 기법은 APD 기법의 보안을 강화하기 위하여 기밀 데이터를 은닉할 때 그림 4의 단계 5.1~5.3에서 식(9)~(11)을 사용하여 원본 기밀 데이터를 삼중으로 암호화한 다음 APD 기법과 같은 방법으로 은닉하기 때문이다. 따라서 APD 기법의 단점인 기밀 데이터의 보안 취약성이 제안 기법에서는 크게 개선되지만, 은닉되는 기밀 데이터의 비트 수는 APD 기법과 같게 된다. 제안 기법으로 기밀 데이터를 커버 이미지에 은닉하여 스테고 이미지를 생성하면, 스테고 이미지로부터 원본 기밀 데이터를 손실 없이 추출할 수 있고 또한 스테고 이미지로부터 원본 커버 이미지를 왜곡 없이 복원할 수 있다.

따라서 제안 기법은 보안이 중요하고 원본 커버 이미지를 완벽하게 복원하는 것이 필요한 의료, 군사, 디지털 라이브러리 등의 응용 분야에 효과적으로 적용될 수 있는 우수한 가역 기밀 데이터 은닉기법이다.

표 1. 실험 결과
Table 1. Experimental results

Image	technique	PSNR (dB)	embedded confidential data bits
Lenna	APD	48.59	48,424
	Proposed	48.55	48,424
man	APD	48.58	47,408
	Proposed	48.56	47,408
Elaine	APD	48.41	30,487
	Proposed	48.39	30,487
goldhill	APD	48.47	35,868
	Proposed	48.44	35,868

5. 결론

본 논문에서는 APD 기법에서의 문제점인 기밀 데이터의 보안성을 크게 강화하는 기법을 제안하였다. 제안된 기법에서는 암호화 키 k, b, n, p와 픽셀 정보를 사용하여 기밀 데이터를 삼중으로 암호화한 후, 삼중으로 암호화된 기밀 데이터를 커버 이미지에 은닉하여 스테고 이미지를 생성하기 때문에 스테고 이미지에 은닉된 기밀 데이터의 보안성이 매우 크게 향상된다. 제안 기법으로 기밀 데이터를 커버 이미지에 은닉하여 스테고 이

미지를 생성하면, 스테고 이미지의 화질은 표 1에서 보는 바와 같이 48.39dB 이상이기 때문에 스테고 이미지와 원본 커버 이미지를 구분할 수 없다. 그리고 스테고 이미지에 30,487비트 이상의 기밀 데이터가 은닉되었다.

3장에서 설명한 바와 같이, 제안 기법을 사용하면 스테고 이미지로부터 삼중으로 암호화된 기밀 데이터를 추출한 후, 삼중으로 암호화된 기밀 데이터로부터 원본 기밀 데이터를 손실 없이 추출할 수 있다. 또한 스테고 이미지로부터 원본 커버 이미지를 왜곡 없이 복원할 수 있다. 따라서 제안된 기법은 보안이 매우 중요하고 원본 커버 이미지를 완벽하게 복원하는 것이 필요한 의료, 군사, 디지털 라이브러리 등의 응용 분야에 효과적으로 적용될 수 있는 우수한 가역 기밀 데이터 은닉기법이다.

REFERENCES

[1] H. C. Huang, C. M. Chu, and J. S. Pan, "The optimized copyright protection system with genetic watermarking," Soft Computing, Vol. 13, No. 4, pp. 333-343, Feb. 2009.

[2] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. on Circuits and Systems for Video Technology, Vol. 16, No. 3, pp. 354-362, March 2006.

[3] Y. C. Li, C. M. Yeh, and C. C. Chang, "Data hiding based on the similarity between neighboring pixels with reversibility," Digital Signal Processing, Vol. 20, No. 4, pp. 1116-1128, July 2010.

[4] X. Li, J. Li, B. Li, B. Yang, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion," Signal Processing, Vol. 93, Issue 1, pp. 198-205, 2013.

[5] S. M. Jung, "Reversible Data Embedding Algorithm using the Locality of Image and the Adjacent Pixel Difference Sequence," The Journal of Korea Institute of Information, Electronics, and Communication Technology, Vol. 9, No. 6, pp.573-577, Dec. 2016.

[6] Sahmyook University Industry-Academic Cooperation(S. M. Jung), "A METHOD FOR DATA HIDING BASED ON PIXEL VALUE PREDICTION, A METHOD FOR DATA WATERMARKING USING IT, AND AN APPARATUS FOR DATA HIDING," http://www.kipris.or.kr, Korea Patent, 1017645300000, July 2017.

[7] Sahmyook University Industry-Academic Cooperation (S. M. Jung, B. W. On), "A METHOD FOR REVERSIBLE DATA HIDING BASED ON PIXEL VALUE PREDICTION ACCORDING TO SPATIAL LOCALITY AND SURFACE CHARACTERISTICS, A METHOD FOR REVERSIBLE WATERMARKING USING IT, AND AN APPARATUS FOR REVERSIBLE DATA HIDING, REVERSIBLE WATER MARKING," http://www.kipris.or.kr, Korea Patent, 1018754010000, March 2018.

[8] S. M. Jung, B. W. On, "An advanced reversible data hiding algorithm using the local similarity, the curved surface characteristics, and the edge characteristics in image," Applied Sciences, Vol. 10, No. 3, pp. 836(1)-836(27), Feb. 2020.

저자약력

정 수 목(Soo-Mok Jung) **[종신회원]**

- 1984: 경북대학교 전자공학 공학사
- 1986: 경북대학교 대학원 전자공학 공학석사
- 2002: 고려대학교 대학원 컴퓨터학 이학박사
- 현 재: 삼육대학교 컴퓨터공학부 교수

〈관심분야〉 영상처리, 컴퓨터 아키텍쳐