한국군사과학기술학회지 제14권 제3호, pp. 482~491, 2011년 6월

학술논문 정보기술 부문

군사용 비밀 영상 전송을 위한 이단계 정보은닉 기법

Two-level Information Hiding Method for the Transmission of Military Secret Images

김 인 택* 김 재 철* 이 용 균*
Intaek Kim Jaecheol Kim Yongkyun Lee

Abstract

The purpose of this study is to design and implement a 2-level secret information transmission system which can be used for information hiding of images transmitted over various IT communication media. To increase the robustness of the hiding power, we combined the steganography method which inserts secret object into cover object to hide the very fact of information hiding itself, and the preprocessing stage to encrypt the secret object before the stego-insertion stage. As a result, even when the stego-image is broken by an attacker, the secret image is protected by encryption. We implemented the 2-level image insertion and extraction algorithm by using C++ programming language. Experiment shows that the PSNR values of stego-images of ours exceed 30.00db which is the threshold of human recognition. The methodology of this study can be applied broadly to the information hiding and protection of the military secret images.

Keywords : Steganography(스태가노그래피), ARIA, PVD, Secret Image(비밀 영상), Information Hiding(정보 은닉)

1. 서 론

오늘날 통신망의 발달과 인터넷의 급격한 확산과 더불어, 비밀번호, 기밀문서 등 중요데이터의 유출에서부터 바이러스, 웜, 사이버테러 등의 의도된 침입까지 다양한 보안위협이 증가하고 있다. 최근에는 네트워크의 확장과 더불어 인터넷 뱅킹, 전자상거래 뿐만 아니라 최신 스마트폰을 통한 개인 정보의 유통과 관련하여 디지털 비밀 정보를 네트워크를 통해 전자적인 방법으로 송수신하는 비율이 급증하고 있다. 그러나 이러한 네트워크를 통한 정보전송이 비밀 정보의 전달을 위한 안전한 방법이라고는 볼 수 없다. 따라서 많은 응용분야에서 사용되고 있는 디지털 비밀 정보를 네트워크를 통해 안전하게 전달하기 위한 정보보호 기술의 필요성이 크게 대두되고 있다[1].

정보보호 기술은 사용자 인증이라는 과정을 통해서 인증된 사용자만이 디지털 매체에 접근 가능하도록 하는 접근 제어(Access Control) 기법과 데이터 암호화(Encryption) 기법을 주로 사용한다[2]. 암호화 기법은 메시지의 내용에 상관없이 메시지 그 자체를 해독 할

† 2011년 3월 22일 접수~2011년 5월 13일 게재승인
* 공군사관학교(Korea Air Force Academy)
책임저자 : 김재철(jchlkim@gmail.com)

수 없도록 비밀키를 이용하여 암호화시키는 방법이다[3,4]. 그러나 암호화된 메시지는 네트워크를 통해서 전송될 경우, 암호화된 정보라는 사실을 쉽게 알 수 있기 때문에 공격의 대상이 될 수도 있다. 따라서 비밀정보를 보낸다는 사실 자체를 어느 누구도 인지하지 못하도록 하는 방법이 요구된다. 이를 위해 최근에는 디지털 매체에 직접적으로 비밀 정보를 숨겨서 전송하여 제3자에게는 비밀 정보가 숨겨져 있다는 사실 자체를 알지 못하도록 하는 방법인 스테가노그래피(Steganography)의 연구가 활발하게 이루어지고 있다[5~8]. 스테가노그래피는 데이터 은닉을 위한 암호화 방법의 제한점과 저작권 인증을 위한 워터마킹 방법의 단점인 삽입 용량에 대한 한계를 극복할 수 있다[9]. 최근 몇 년간 많은 스테가노그래피 방법들이 제안되었으며, 대부분 이미지 데이터를 이용하여 비밀 정보를 삽입하였다[10,11].

본 연구에서는 군사용 비밀정보의 안전한 전송을 위하여, 암호화 기법과 스테가노그래피 기술을 동시에 적용함으로써, 비밀 정보의 존재자체를 숨길 뿐만 아니라, 비밀정보가 노출되더라도 그 내용은 해독할 수 없게 하여, 보다 안전한 전송을 보장하게 하였다. 특별히, 현대전에서는 많은 영상정보들이 전송되고 있는데, 이들 영상정보의 안전한 전송은 군 작전의 성패를 좌우할 만큼 매우 중요한 문제로 대두되고 있다. 아프간전에서 미군의 고고도 무인 정찰기가 전송하는 영상들이 테러단체에 거의 그대로 노출되었던 사실은 이미 언론에도 알려진 바 있다[12]. 본 연구에서 제안하는 정보은닉 기법은 학술적 가치뿐만 아니라, 군사정보의 기밀성을 유지하도록 하는데 있어서 즉시 활용 가능하다는 점에서 큰 의의가 있다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 본 연구에서 구현된 방법과 관련되는 암호화 기법과 자료은닉 방법을 살펴보고, 3장에서는 암호와 영상을 은닉하여 전송할 수 있는 알고리즘의 설계와 구현을 소개한다. 제안된 방법에 대한 실험결과를 4장에서 보이고, 5장에서는 향후과제로서, 본 연구의 결과를 군사적으로 응용할 수 있는 분야를 보이고, 마지막으로 6장에서 결론을 맺는다.

2. 관련 연구

가. 암호화 기법

전자정부 시스템 등 다양한 정보보호 환경을 대비하여 개발된 블록암호 알고리즘 ARIA는 2004년 12월에 한국 산업규격 KS 표준으로 선정되었으며, 안전성과 효율성은 미국, 유럽, 일본의 표준 블록암호 알고리즘과 비교하여 대등한 정도의 수준을 가지고 있다[13].

ARIA 알고리즘은 암호화와 복호화를 수행하는 라운드 함수와 키 확장으로 구성되어 있다. ARIA 라운드 함수의 기본 구조는 Involution SPN 구조이다. 입, 출력의 크기는 128비트이고 키의 크기는 128비트, 192비트 그리고 256비트를 선택할 수 있다. 키의 크기에 따라 12, 14 또는 16번 라운드 함수를 반복 수행한다.

1) ARIA 구조

Fig. 1과 같이 ARIA의 라운드 함수는 확산계층 대신 라운드 키 덧셈을 수행하는 마지막 라운드를 제외하고는 라운드 키 덧셈(AddRoundKey), 치환 계층(SubstLayer) 그리고 확산 계층 (DiffLayer) 등의 세 부분으로 구성되어 있다.

라운드 키 덧셈은 128비트 라운드 키를 라운드 입력 128비트와 비트별 XOR한다. 암호화 과정과 복호화 과정은 Fig. 1과 같이 주어지며 암호화 과정과 복호화 과정은 라운드 키를 제외하고는 일치한다.

치환 계층은 두 가지의 S-boxes S_1, S_2 을 사용한 두 가지 유형의 치환계층 (LS, LS, LS, LS), $(LS^{-1}, LS^{-1}, LS^{-1}, LS^{-1})$ 을 갖는다. 단, LS는 $(S_1, S_2, S_1^{-1}, S_2^{-1})$ 이다. 홀수 라운드(F_o)의 치환 계층은 (LS, LS, LS, LS) 이고, 짝수 라운드(F_e)의 치환 계층은 $(LS^{-1}, LS^{-1}, LS^{-1}, LS^{-1})$ 이다. 라운드 함수는 Fig. 2와 같다.

확산 계층은 ARIA와 다른 블록 암호를 구별 짓는 주요 부분으로 16×16 involution 이진 행렬을 사용한다. 확산 함수는 입력 16-바이트에 대하여 바이트 단위의 행렬 곱을 수행한 결과의 16-바이트를 출력으로 한다. ARIA의 확산 함수 A : $GF(2^8)^{16} \rightarrow GF(2^8)^{16}$는 입력을 $(x_0, x_1, \ldots, x_{15})$ 라 하고 출력을 $(y_0, y_1, \ldots, y_{15})$ 라 하면, 행렬 (1)의 곱으로 표현된다.

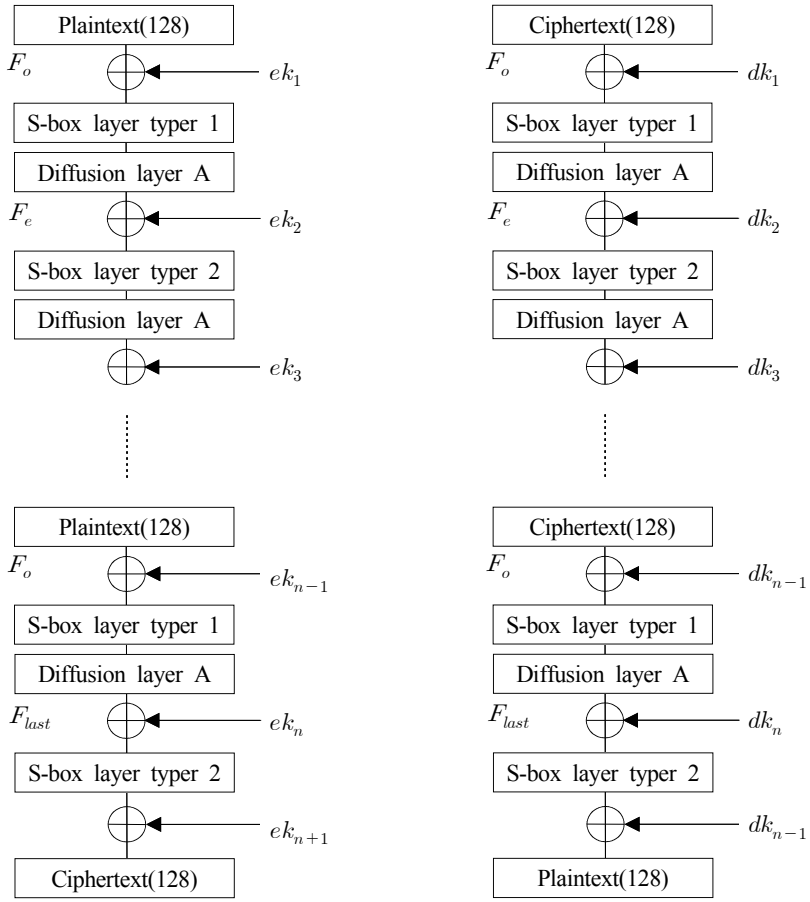


Fig. 1. 암호화, 복호화 과정

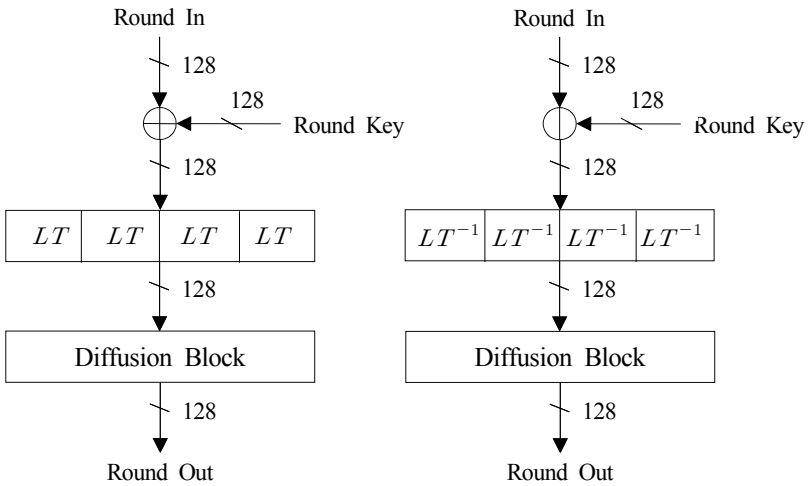


Fig. 2. 라운드 함수

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \end{pmatrix} = \begin{pmatrix} 0001101011000110 \\ 0010010111001001 \\ 0100101000111001 \\ 1000010100110110 \\ 1010010010010011 \\ 0101100001100011 \\ 1010000101101100 \\ 0101001010011100 \\ 0011100100100101 \\ 0011011000011010 \\ 1100011010000101 \\ 1100100101001010 \\ 0110001101011000 \\ 1001001110100100 \\ 1001110001010010 \\ 0110110010100001 \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{pmatrix} \quad (1)$$

2) 키 확장(Key Scheduling)

키 확장은 초기화 과정과 라운드 키 생성과정으로 나뉠 수 있다. 초기화 과정에서는 암·복호화 한 라운드를 F 함수로 하는 256비트 입·출력 3라운드 Feistel 암호를 이용하여, 암호키 MK로부터 4개의 128비트 값 W_0, W_1, W_2, W_3을 생성한다. 암호키 MK의 길이는 128, 192 또는 256이므로 위 Feistel 암호의 입력에 필요한 256비트 (KL, KR)를 다음과 같이 구성한다.

- 128비트 KL은 MK의 상위 128비트를 취한다.
- MK의 남은 비트를 이용하여 KR의 상위 비트를 채우고 나머지는 0으로 채운다.

$$KL \| KR = MK \| 0 \cdots 0$$

F_o와 F_e을 각각 홀수, 짝수 라운드 함수라고 할 때, 다음과 같이 W_0, W_1, W_2, W_3을 생성한다.

$$\begin{aligned} W_0 &= KL, \\ W_1 &= F_o(W_0, CK_1) \oplus KR \\ W_2 &= F_e(W_1, CK_2) \oplus W_0 \\ W_3 &= F_o(W_2, CK_3) \oplus W_1 \end{aligned}$$

라운드 키 생성 과정에서는 4개의 128비트 W_0, W_1, W_2, W_3을 조합하여 암호화 라운드 키 ek_i와 복호화 라운드 키 dk_i을 생성한다. 라운드 수는 암호키의 크기가 128, 192, 256비트인 경우 각각 12, 14, 16 라운드이고 마지막 라운드에는 키 덧셈계층이 두 번 있으므로 각각 13, 15, 17개의 라운드 키를 생성해야 한다.

복호화 라운드 키는 암호화 라운드 키로부터 유도된다. 먼저 키의 순서가 바뀌고 처음과 마지막 라운드 키를 제외하고 암호키를 입력으로 하는 확산 함수 A의 출력이 복호화 라운드 키가 된다. 라운드 수가 n일 때. 복호화 라운드 키는 다음과 같다.

$$\begin{aligned} dk_1 &= ek_{n+1}, \\ dk_2 &= A(ek_n), \\ dk_3 &= A(ek_{n-1}), \\ &\cdots, \\ dk_n &= A(ek_2), \\ dk_{n+1} &= ek_1 \end{aligned}$$

나. 자료은닉 방법

스테가노그래피(Steganography)는 커버 객체(Cover-object)에 비밀 객체(Secret-object)를 숨기는 방법을 통해, 생성된 스테고 객체(Stego-object)에 비밀 정보가 숨겨져 있다는 사실 자체를 공격자로부터 숨기는 기법을 의미한다. 즉, 제 3자의 눈에는 커버 객체만 보이게 되기 때문에, 비밀 객체가 내부에 숨겨져 있다는 사실 자체를 인지할 수 없게 하는 것이다. 여기에서 객체는 텍스트, 이미지, 오디오, 비디오 등을 포함한다.

스테가노그래피를 구현하는 기법은 매우 다양하게 발전해 왔는데, 그 중에서 최근에 가장 널리 사용되고 있는 PVD(Pixel-Value Differencing) 방법은 픽셀값 차이를 이용한 두 연속된 픽셀값의 차이에 따라서 숨길 수 있는 비트수를 결정하는 기법이다[10]. 주어진 커버 이미지에서 차이값 d_i는 중복되지 않는 연속된 두 픽셀을 기준으로 계산된다. 먼저 두 픽셀값을 각각 p_i, p_{i+1}라고 하면, 차이값 $d_i = |p_i - p_{i+1}|$로 계산되며, $0 \le d_i \le 255$조건을 만족한다. 하나의 서브-블록 B와 인덱스값을 i라고 정의하면 숨길 수 있는 비트수 $n = \log_2(u_i - l_i + 1)$로 계산된다. 여기서 u_i와 l_i는 범위 테이블 $R_{i+1}(i = 1, 2, \cdots, w)$에서의 상계(Upper Bound)와 하계(Lower Bound)값을 나타낸다. 다음으로 비밀자료 S에서 n개의 비트값을 가져와서 새로운 차이값 $d'_i = |l_i + b|$이 계산되며, 여기서 b는 선택된

비밀자료의 비트값에 대한 정수값을 나타낸다. d'_i 값이 계산된 이후 스테고 이미지에 해당되는 새로운 두 픽셀값 p'_i, p'_{i+1}이 만들어지게 된다. 새로운 두 픽셀값은 d_i와 $m = d'_i - d_i$에 따라 다음 식 (2)와 같이 얻어진다.

Fig. 3은 두 픽셀값 (60, 95)에 대하여 자료은닉과정을 설명한다. 두 픽셀값의 차이값 $d = |95 - 60| = 35$으로 구해지고, 숨길 수 있는 비트수 $n = 5$로 결정된다. 이때 비밀자료를 10111_2라고 주어진다면 이 값에 해당되는 정수값은 23로 계산된다. 다음으로 새로운 차이값 $d' = 47$이 계산되고, 최종적으로 새로운 픽셀값 (54, 101)을 얻게 된다.

3. 제안 알고리즘: 2단계 정보은닉 기법

Fig. 4는 일반적인 스테가노그래피 시스템의 삽입 및 추출 알고리즘의 동작방식을 개념적으로 나타내고 있다. 삽입 알고리즘은 비밀 영상을 일정한 규칙에 의해서 비트스트림 형태로 변형하여 선택된 커버 영상의 특정 비트들에 삽입한다.

커버 영상과 비밀 영상을 혼합하여 스테고 영상을 만든다. 추출알고리즘은 스테고 영상으로부터 삽입된 비밀 정보를 추출한다.

Fig. 5는 본 논문에서 제안하는 2단계 정보은닉 기법의 동작 개념도이다. 본 논문에서 제안하는 2단계

$$(p'_i, p'_{i+1}) = \begin{cases} \left(p_i - \dfrac{m+1}{2}, p_{i+1} + \dfrac{m-1}{2}\right) & d_i : \text{홀수}, m : \text{홀수 일때} \\ \left(p_i - \dfrac{m-1}{2}, p_{i+1} + \dfrac{m+1}{2}\right) & d_i : \text{짝수}, m : \text{홀수 일때} \\ \left(p_i - \dfrac{m}{2}, p_{i+1} + \dfrac{m}{2}\right) & m : \text{짝수 일때} \end{cases} \quad (2)$$

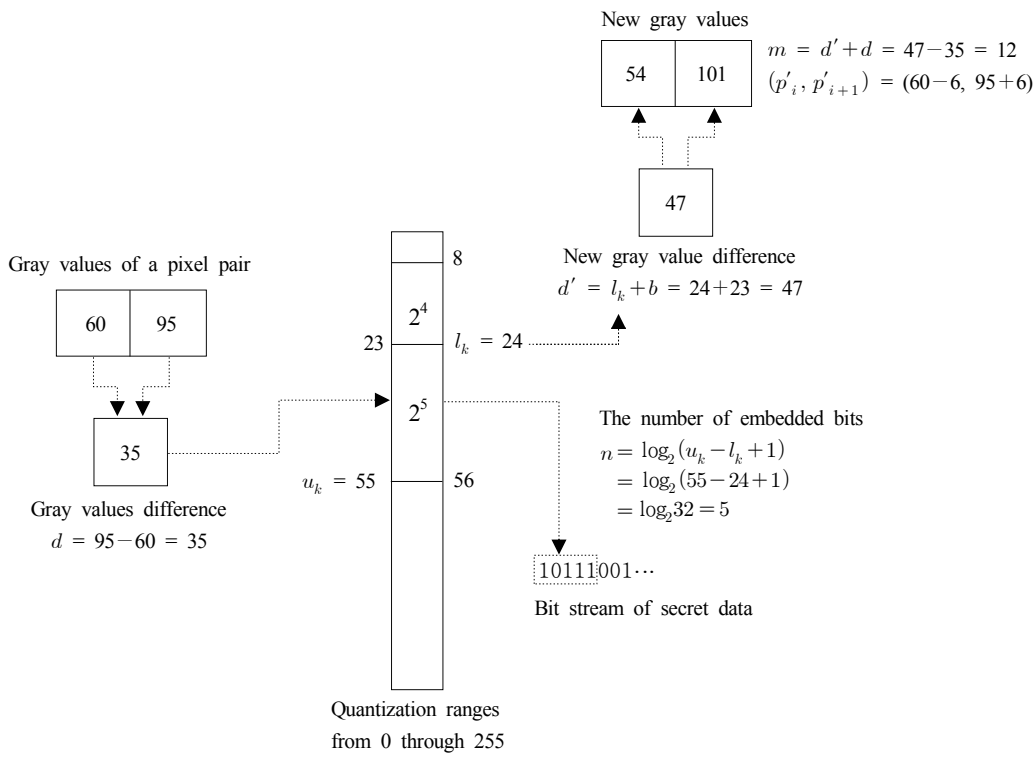


Fig. 3. PVD를 이용한 자료은닉 예

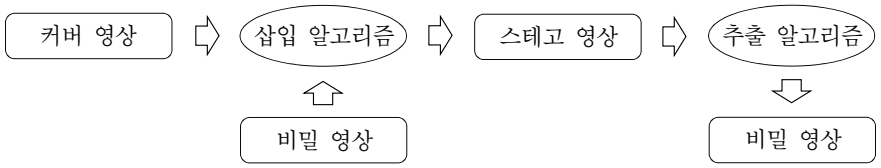


Fig. 4. 스테가노그래피의 기본 동작과정

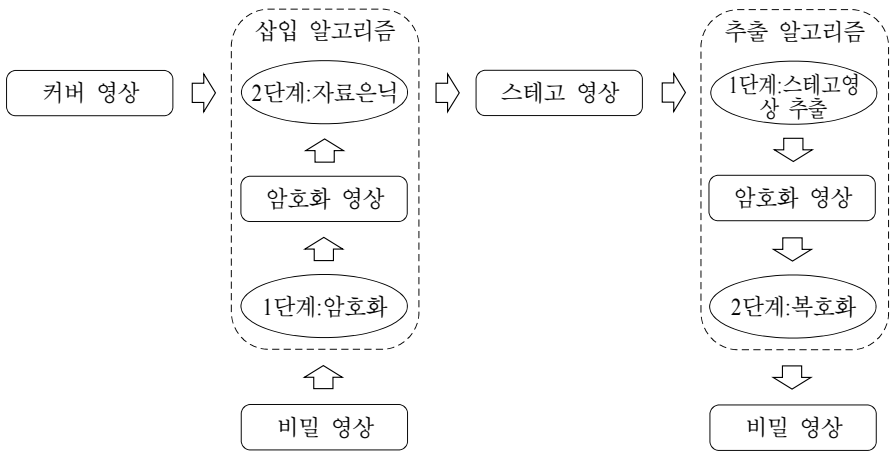


Fig. 5. 제안된 2단계 정보은닉 기법의 동작과정

정보은닉 기법은 블록암호 알고리즘(ARIA)을 적용하여 비밀 영상을 생성하는 암호화 영상 단계(1단계)와, 자료은닉 기법(PVD)을 이용하여 스테고 영상을 완성하는 단계(2단계)로 나뉜다. 추출 알고리즘 또한 스테고 영상에서 삽입된 암호화 영상을 추출하는 과정과, 이를 복호화하여 비밀 영상의 원본을 복원하는 2단계 구조로 동작한다. 따라서 주어진 비밀 영상을 암호화 시킴으로써 1차적인 정보보호를 할 수 있으며, 커버 영상을 이용한 자료은닉을 통하여 2차적인 정보은닉이 완성된다. 이를 다시 추출하고 복호화하는 과정을 통하여 전체 프로세스가 구현된다.

가. 삽입 알고리즘

우선 전송하고자 하는 비밀영상을 2장 가.절에서 소개한 블록암호 알고리즘(ARIA)을 이용하여 암호화 영상으로 만든다. 암호화 영상이 만들어지면 2장 나.절에서 소개한 자료은닉 방법인 PVD를 이용하여 자료를 은닉한다. 삽입 알고리즘의 동작 과정은 다음과 같다. 앞 절에서 제시한 바와 같이 암호화 단계(1단계)와 스테고 영상화 단계(2단계)를 모두 포함하고 있는 알고리즘이다.

알고리즘 1. 삽입 알고리즘

입력 : $cw \times ch$ 크기의 커버 영상과 숨기려는 비밀 영상

출력 : $sw \times sh$ 크기의 스테고 영상

1단계 : 숨기려는 비밀 영상의 픽셀값을 16배수화 한다.

2단계 : 블록암호 알고리즘을 이용하여 영상을 암호화 한다.

3단계 : 암호화 영상을 비트스트림으로 변환한다.

4단계 : 커버영상에서의 주어진 서브-블록과 차이값 (d_i)을 이용하여 숨길 수 있는 비트수 (n_i)를 계산한다.

5단계 : 비트스트림 암호화 영상으로부터 n_i 비트 크기 만큼 읽어들여 이 값을 정수값 b_i 로 바꾸고, 새로운 차이값 d'_i 를 계산한다.

6단계 : 주어진 두 픽셀값에 대해서 새로운 두 픽셀값을 식 (1)을 이용하여 계산한다.

나. 추출 알고리즘

스테고 영상으로부터 숨겨진 비밀 영상을 추출하는 과정도 역시 2단계의 과정을 거친다. 영상의 삽입 알고리즘과는 역함수의 성격을 가진다. 추출과정에는 커버 영상에 대한 정보가 필요하지 않으며, 스테고 영상으로부터 직접 암호화 영상을 추출하고, 그 다음 이 영상을 복호화하여 최초의 원본 영상을 추출할 수 있다.

아래에 알고리즘을 7단계로 세분하여 제시하였는데, 크게는 두 단계로 구분하여 이해할 수 있다. 1단계에서 5단계까지는 스테고 영상에서 암호화된 영상을 추출해 내는 과정이며, 6단계와 7단계는 이 암호화된 영상으로부터 원본 영상(비밀영상)을 복호화시켜 복원하는 과정이다.

알고리즘 2. 추출 알고리즘

입력 : $sw \times sh$ 크기의 스테고영상과 범위테이블
출력 : 숨겨진 비밀 영상

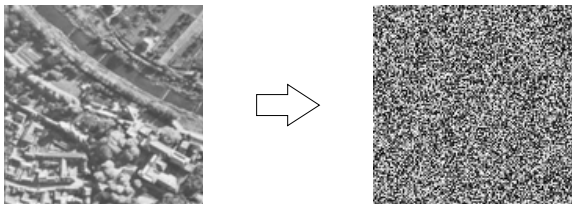
1단계 : 중복되지 않게 서브-블록으로 나눈다.
2단계 : 서브-블록에서의 픽셀 차이값 d'_i를 계산한다.
3단계 : 범위 테이블을 이용하여 범위의 하계 값(l_i)을 계산한다.
4단계 : 숨겨진 비트스트림에 대한 정수값(s_i)를 추출한다.
여기서 $s_i = |d'_i - l_i|$에 의해서 구해진다.
5단계 : 추출된 비트를 순서대로 연결하여 숨겨진 암호화 영상의 비트스트림을 완성한다.
6단계 : 블록암호 알고리즘을 이용하여 복호화 한다.
7단계 : 복호화된 자료를 이용하여 비밀 영상을 생성 한다.

4. 실험 결과

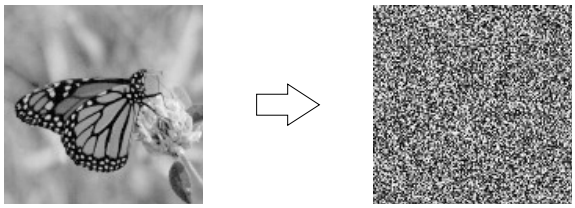
3장에서 제안한 알고리즘을 기반으로, 본 논문의 실험에서는 1단계 암호화 과정은 블록암호화 알고리즘인 ARIA를 사용하였고, 2단계 자료은닉방법은 스테가노그래피 기법인 PVD를 사용하였다. 사용된 영상은 Lena(512×512)와 Baboon(512×512) 영상을 커버 영상으로 사용하였으며 비밀 영상은 Aerial(128×128)과 Butterfly(128×128)영상을 사용하였다.

실험을 위하여, ARIA알고리즘과 PVD기법은 윈도우즈 운영체제하에서 C++ 프로그래밍 언어를 사용하여 구현하였다.

Fig. 6은 ARIA 알고리즘을 이용하여 비밀 영상을 암호화시킨 영상을 보여준다. (a)는 Aerial 영상을, (b)는 Butterfly 영상을 암호화시킨 결과를 보여주고 있는데, 암호화과정을 거치면서 사람의 시각으로는 인지하기 어려운 잡음형태의 도트패턴을 가지는 영상을 가지고 있음을 알 수 있다. 따라서, 혹시 공격자가 스테고 영상의 스테가노그래피 적용을 인지하였다 할지라도 추출한 영상은 Fig. 6에서 보이는 암호화 영상이므로, 원본 영상을 식별하는 것은 불가능하다. 이것이 비밀영상을 1차적으로 ARIA 암호화 기법을 이용하여 보호한 이유이다.



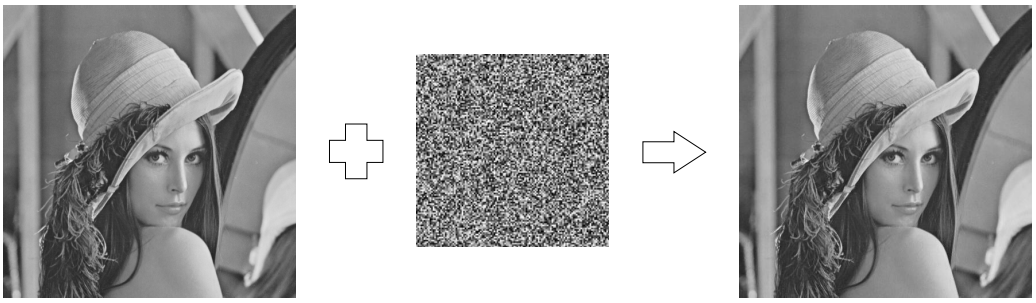
(a) Aerial 영상의 암호화 영상



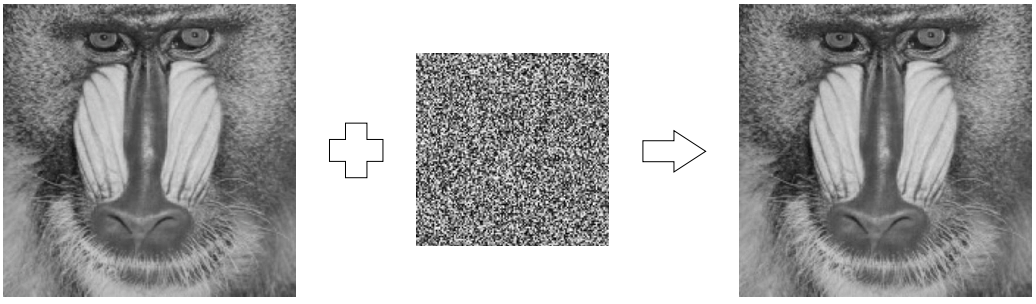
(b) Butterfly 영상의 암호화 영상

Fig. 6. 비밀 영상의 암호화

Fig. 7은 스테가노그래피의 자료은닉 방법인 PVD를 이용하는 과정과 결과를 보여주고 있다. 왼쪽의 Lenna 영상과 Baboon 영상은 커버 영상이고, 가운데 영상은 Fig. 6에서 암호화시킨 영상들로서, Lenna 영상에는 Aerial 영상을 암호화한 영상을, Baboon 영상에는 Butterfly 영상을 암호화한 영상을 삽입한다. 오른쪽 영상은 각각의 암호화 영상이 숨겨진 결과를 나타내는 스테고 영상을 보여주고 있다.

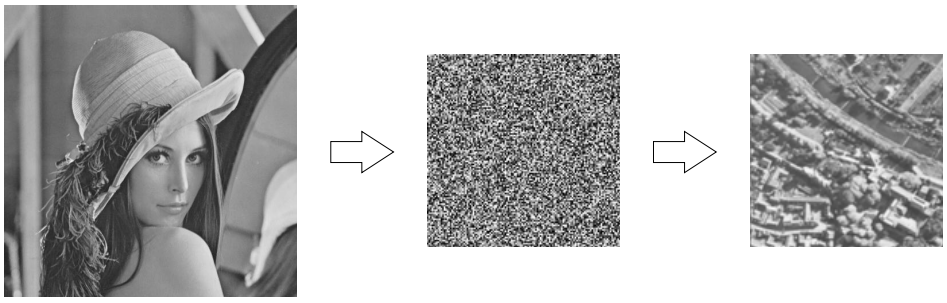


커버 영상(Lenna) 암호화 영상(Aerial) 스테고 영상(PSNR=45.94dB)

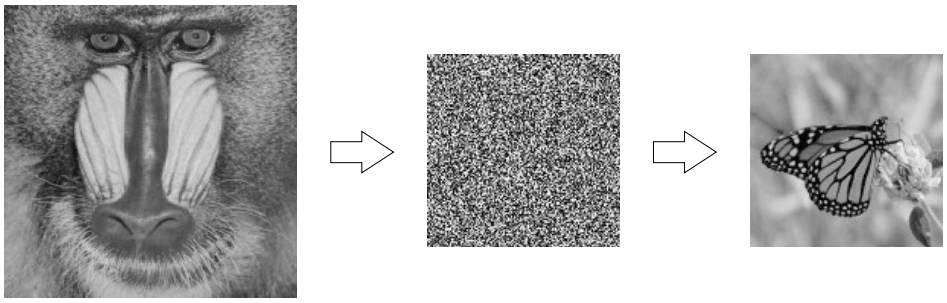


커버 영상(Baboon) 암호화 영상(Butterfly) 스테고 영상(PSNR=48.03dB)

Fig. 7. 암호화 영상 은닉 결과



스테고 영상(Lenna Stego) 암호화 영상(Aerial) 비밀 영상(Aerial)



스테고 영상(Baboon Stego) 암호화 영상(Butterfly) 비밀 영상(Butterfly)

Fig. 8. 추출 알고리즘 결과

스테고 영상에는 사람의 시각 인지 정도를 측정하기 위하여 PSNR(Peak Signal-to-Noise Ratio)값을 측정하여 명기하였다. PSNR 값이 30.00dB 이상이면 사람의 시각으로는 원본 영상과의 차이를 구별할 수가 없게 된다[14]. 실험결과에서 PSNR 값이 Lenna 스테고 영상의 경우 45.94dB, Baboon 스테고 영상의 경우는 48.03dB 이므로 사람의 육안으로는 그림의 변경 유무를 구별하기가 힘들게 된다.

Fig. 8은 스테고 영상에 추출 알고리즘을 적용하여 얻어진 비밀영상을 보여주고 있다. 첫 번째 그림은 Lenna 스테고 영상에서 먼저 Aerial 암호화 영상이 추출되고 복호화 과정을 거쳐 Fig. 6(a)의 Aerial 비밀 영상이 만들어지는 과정을 보여준다. 두 번째 그림에서도 Baboon 스테고 영상에서 암호화 영상이 추출되고 복호화 과정을 거쳐 Fig. 6(b)의 Butterfly 비밀영상이 성공적으로 추출되었음을 보여주고 있다. 추출과정 자체는 삽입과정의 역함수이므로 당연한 결과를 얻었다고 할 수 있지만, 본 논문에서 제안하는 2단계 알고리즘의 효용성을 잘 보여주고 있다. 즉, 스테가노그래피의 정보은닉 여부가 공격자에게 노출되었다 하더라도, 추출한 이미지 자체가 암호화되어 있어서, 암호화 여부를 모르는 경우에는 전송하는 비밀영상의 식별이 불가능하며, 암호화 여부를 알았다 하더라도 라운드 함수와 키값을 모르는 상태에서 암호를 깨뜨리고 비밀영상을 추출하는 것은 현실적으로 매우 어렵다.

5. 군사 응용 분야

서론에서도 언급한 바와 같이 아프간 전쟁에서 미군의 고고도 무인 정찰기가 촬영하여 전송한 영상정보가 고스란히 반군에게 손쉽게 노출되었던 사실은 군사적 비밀 영상의 전송에서 정보은닉 기법의 필요성과 중요성을 잘 대변해 준다[12]. 본 논문에서 제안한 2단계 정보은닉 기법은 다음과 같은 분야에서 활발하게 이용될 수 있다. 실험에서는 영상정보만을 대상으로 하였지만, 전송대상은 영상 뿐만 아니라 다양한 정보에 폭넓게 활용될 수 있다.

첫번째로, 군용 데이터통신 분야이다. 전술데이터통신의 경우에도 기본적인 암호화는 사용되고 있으나, 2단계 정보은닉 기법을 통하여 적에게 정보의 존재 자체를 숨김으로써 강인성(Robustness)를 강화할 수 있다.

두번째 응용분야는 군사 정찰 영상정보의 전송이다. 정찰위성의 촬영 영상, 국내 도입예정인 중고고도 무인정찰기의 촬영 영상의 디지털 실시간 전송시에 본 논문에서 제안한 2단계 정보은닉 기법은 바로 활용될 수 있다.

세번째 분야는 스마트폰용 에플리케이션화를 통한 개별 전투요원간의 정보전송시에 정보은닉 기법으로 활용하는 것이다. 본 연구에서 구현된 2단계 정보은닉 기법은 일부수정을 통하여 활발하게 보급되고 있는 스마트폰용 엡으로 재개발할 수 있다. 스마트폰, 혹은 군사용으로 재개발 납품된 스마트폰 유사기기가 개별 전투요원을 위한 전술 단말기로 사용되는 상황은 쉽게 예측해 볼 수 있다. 이 경우, 개별 전투요원은 전장상황을 스마트폰으로 촬영하여 상호간 혹은 통제실로 전송할 수 있는데, 본논문에서 제안한 2단계 정보은닉 기법을 구현한 엡을 활용하여 안전하게 전송할 수 있게 된다. 향후 과제로서 엡개발은 진행될 예정이다.

이 외에도 군사 비밀 정보의 전송시 정보은닉이 필요한 모든 분야에 본 연구에서 제안한 기법은 손쉽게 적용될 수 있다.

6. 결 론

인터넷과 네트워크의 사용이 점점 더 확대되고 용이해짐에 따라 많은 정보들이 공개된 네트워크를 통해 전송되고 있다. 그에 따라 자신의 정보가 의도된 수신자 외에게는 노출되지 않도록 하는 정보은닉기법의 중요성이 더욱 대두되고 있다. 특별히, 현대전에서 군사정보의 상당량이 이미지 정보임을 감안할 때, 이들 이미지의 정보보호는 매우 중요하다고 할 수 있다.

본 논문에서는 비밀 정보의 보다 안전한 전송을 위해, 암호화 기술을 통하여 생성된 암호문을 일반 영상에 숨겨서 전송할 수 있는 2단계 정보은닉 알고리즘의 구현에 대하여 논의하였다. 비밀 영상을 암호화하기 위해서는 블록암호 알고리즘인 ARIA가 사용되었으며, 암호화된 영상을 은닉하기 위해서 PVD 알고리즘이 적용되었다. 본 논문에서는 암호화된 영상을 숨겨서 전송할 수 있는 스테가노그래피 시스템을 설계하고 구현하였으며, 이에 대한 실험결과를 제시하였다.

실험결과에 따르면, ARIA 알고리즘을 통하여 사람

의 시각으로는 비밀정보인지의 여부를 인지하기 어려운 1단계 정보은닉이 이뤄진 암호화 영상을 얻었으며, 2단계로 PVD 알고리즘을 구현한 결과 PSNR 값이 사람의 눈으로 인지하기 어려운 30.00dB 이상인 스테고 영상을 만들었다. 또한, 삽입 알고리즘의 역순으로 진행된 추출 알고리즘의 적용을 통해 비밀 영상을 성공적으로 추출하였다. 이는 제3자에게 드러나는 암호화의 취약성을 스테가노그래피 기법을 통하여 강화할 수 있으며, 암호화 된 비밀 정보를 영상에 삽입하여 전송함으로써 기존 스테가노그래피 기법보다 안전하게 정보를 은닉하여 전송할 수 있는 하나의 프로세스를 구현한 것이라 할 수 있다.

향후, 본 논문에서 구현된 기법을 기반으로, 명함도 영상이외에도 컬러영상과 3D 영상의 은닉에 대한 연구와 더불어 최신 스마트폰의 애플리케이션 및 군사용 영상전송에 응용할 수 있는 다양한 방법에 대한 연구가 필요하다.

후 기

본 논문은 2011년도 공군사관학교 국고연구비의 지원으로 수행된 것임(KAFA11-01).

References

[1] 이신주, 정성환, “멀티미디어에 적용된 스테가노그라피 기술”, 한국컴퓨터범죄연구학회 추계학술대회 논문집, 1(2), pp. 27～31, 2001.

[2] 한국전산원, “지적재산권 보호를 위한 정보은닉 기술 및 표준화 연구”, NCA IV=RER-0010, 2000.

[3] 이준, “국방망 보안 채널 구현에 관한 연구”, 한국군사과학기술학회지, 제11권 제3호, pp. 106～114, 2008.

[4] 이준, 김인택, 박종범, “해쉬함수를 이용한 그룹키 합의에 관한 연구”, 한국군사과학기술학회지, 제13권 제4호, pp. 627～634, 2010.

[5] F. A. Petitcolas, R. J. Anderson & M. G. Kuhn, “Information Hiding - A Survey”, In Proceedings of the IEEE, 87(7), pp. 1062～1078, 1999.

[6] D. Kahn, “The History of Steganography”, Proceedings of the First Workshop on Information Hiding, Lecture Note in Computer Science, 1174, pp. 1～5, 1996.

[7] 정기현, “가변 길이 자료 은닉이 가능한 이미지 스테가노그래픽 방법 연구”, 한국군사과학기술학회지, 제11권 제3호, pp. 115～122, 2008.

[8] 정기현, 김인택, 김재철, “세 방향 자료 은닉이 가능한 이미지 스테가노그래픽기법 연구”, 한국군사과학기술학회지, 제13권 제2호, pp. 268～274, 2010.

[9] 이종관, 최현주, “군 통신상에서 워터마킹 기술을 이용한 피아식별 방법”, 한국군사과학기술학회지, 제9권 제4호, pp. 81～89, 2006.

[10] D. C. Wu, W. H. Tsai, “A Steganographic Method for Images by Pixel-value Differencing”, Pattern Recognition Letters, 24, pp. 1613～1626, 2003.

[11] C. C. Chang, H. W. Tseng, “A Steganographic Method for Digital Images using Side Match”, Pattern Recognition Letters, 25, pp. 1431～1437, 2004.

[12] S. Gorman, Y. J. Dreazen & A. Cole, “Insurgents Hack U.S. Drones”, The Wall Street Journal, p. A1, December 17, 2009.

[13] 국가보안기술연구소, ARIA 알고리즘 명세서(ARIA Ver. 1.0). 2004.

[14] N. I. Wu, and M. S. Hwang, “Data Hinding : Current Status and Key Issues”, International Journal of Network Security, 4(1), pp. 1～9, 2007.