Journal of Digital Contents Society Vol. 13 No. 4 Dec. 2012(pp. 531-538)
http://dx.doi.org/10.9728/dcs.2012.13.4.531

커버영상을 이용한 개선된 시각암호

장시환*, 최용수**, 김형중***

요 약

시각암호는 복잡한 암호학적 연산 없이 분산된 영상을 중첩함으로써, 인간의 시각에 의해 비밀영상을 직접 복원할 수 있는 방법이다. 최근까지 시각암호 분야는 크게 복호화 된 영상의 해상도를 향상시키기 위한 비밀 분산법, 분산된 영상의 크기가 변하지 않는 비밀 분산법 그리고 크기조절에 강인한 비밀 분산법 등에 관하여 연구되고 있다. 시각암호 그 자체는 단순히 분산된 영상만 이용하기 때문에 공격받기 쉽다. 따라서 비밀영상을 안전하게 공유할 수 있는 시각암호 구조가 필요하기 때문에 본 논문에서는 실제 사용될 수 있는 기본적인 시각암호 구조에서 커버영상을 이용해 개선된 시각암호 구조를 제안한다. 제안된 방법은 커버영상의 변조를 줄임으로써 steganalysis를 어렵게 하여 확률적으로 높은 안전성을 제공한다. 또한 잡음을 생성하지 않고, 비밀영상을 온전히 복원할 수도 있음을 보였다.

키워드 : 시각암호, 비밀분산, 스테가노그래피

Improved Visual Cryptography Using Cover Images

Si-Hwan Jang*, Yong Soo Choi**, Hyoung Joong Kim***

Abstract

Visual cryptography is a scheme that recovers secret image through human vision by overlapping distributed share images without cryptographic operations. Distribution methods are still being developed for improving quality of shared images keeping size of images invariant and enhancing robustness against resize of images. Since visual cryptography only uses shared images, this fact is exploited to attack. From this fact, a scheme safe for sharing distributed images is needed. In this paper, a new visual cryptographic scheme using cover image is proposed. This scheme reduces the chance of detection against steganalysis and increases security. In addition, this paper shows that the proposed scheme can completely decrypt secret image without creating noise.

Keywords : Visual Cryptography, Secret Sharing, Steganography

※ 교신저자(Corresponding Author): Hyoung Joong Kim
접수일:2012년 10월 24일, 수정일:2012년 11월 24일
완료일:2012년 12월 17일
* 고려대학교 정보보호대학원
** 고려대학교 정보보호대학원
*** 고려대학교 정보보호대학원
Tel: +82-2-3290-4895, Fax: +82-2-928-9109
email: khj-@korea.ac.kr
▣ 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. (2012R1A2A2A01015587)
▣ 본 연구는 문화체육관광부 및 한국콘텐츠진흥원의 2012년도 콘텐츠산업기술지원사업의 연구결과로 수행되었음.(R2012050022)

1. 서 론

시각암호는 복잡한 암호학적 연산 없이 분산된 영상을 중첩함으로써, 인간의 시각에 의해 비밀영상을 직접 복원할 수 있는 방법으로 Naor와 Shamir에 의해 제안되었다[1]. 일반적인 (k,n) 시각암호 VCS(Visual Cryptography Scheme)는 비밀영상을 n개의 share로 비밀을 분산할 경우, k장 이상의 서로 다른 share를 중첩하면 비밀영상을 복원할 수 있지만 $k-1$개 이하의 share를 중첩하는 경우에는 비밀영상을 복원할 수 없도록 하는 방법이다.

최근까지 시각암호 연구 분야는 크게 복호화된 영상의 해상도를 향상시키기 위한 비밀 분산법, 분산된 영상의 크기가 변하지 않게 하는 비밀 분산법, 그리고 크기조절에 강인한 비밀 분산법 등에 관하여 연구되고 있다[2-6].

분산된 영상은 비밀 분산법에 의해 흑백화소 2비트로 무작위하게 구성되므로, 분산된 영상만 사용하여 비밀영상을 공유하고자 했을 때, 변조된 영상임을 분명하게 인지시켜 공격의 대상이 될 가능성이 높아진다. 따라서 단순히 분산 영상만으로는 실효성을 가질 수 없기 때문에 비밀영상을 안전하게 공유할 수 있는 시각암호 구조가 필요하다[7-11].

본 논문에서는 시각암호 방식으로 생성된 분산 영상의 정보를 커버영상에 은닉하여 사용될 수 있는 기본적인 시각암호 응용 구조를 보이고, 나아가 커버영상을 이용해 steganography 방법을 접목시킨 시각암호 응용 구조를 제안한다. 또한 기존의 시각암호 구조에서 복원된 영상은 확률적으로 잡음을 생성했지만, 제안된 방법은 비밀영상을 온전히 복원할 수 있음을 보였다.

2. 시각암호

2.1 Naor와 Shamir의 기본 모델

시각암호에 의한 비밀 분산 기본 형태는 흑백화소로 구성된 이진영상을 사용하는 것이다. 비밀영상의 각 화소는 n개의 share에 각각 m개의 부화소(subpixel)로 분산된다.

이 구조는 비밀영상의 각 화소가 $n\times m$ 부울 행렬 $S=[s_{ij}]$로 표현될 수 있으며, 이때 s_{ij}의 값은 i번째 share 중 j번째 부화소가 흑인 경우 1, 백인 경우 0이 된다. 분산된 share들을 중첩했을 때 흑백 레벨은 OR 연산을 거친 m차 벡터 V의 해밍가중치(Hamming weight) $H(V)$에 비례한다. 식 (1)과 같이 이 흑백 레벨은 임계값 $(1\le d\le m)$ 과 상대적인 차이 $\alpha>0$에 대하여 $H(V)\ge d$ 이면 흑으로, 그렇지 않을 경우 $H(V)\le d-\alpha m$ 이면 백으로 표시한다.

$$c(H(V))=\begin{cases}Black, & \text{if } H(V)\ge d\\ White, & \text{if } H(V)\le d-\alpha m\end{cases} \tag{1}$$

(k,n) 시각암호의 가장 간단한 형태인 $(2,2)$ 시각암호를 예로 들면, 임계값 $d=4$, $\alpha=1/4$, share의 크기 $m=4$ 인 경우 2×2행렬 S는 각각 백화소를 위한 S_0, 흑화소를 위한 S_1을 식 (2)와 같이 정의할 수 있다.

$$S_0=\begin{bmatrix}0&1&1&1\\0&1&1&1\end{bmatrix}, S_1=\begin{bmatrix}1&0&1&1\\0&1&1&1\end{bmatrix} \tag{2}$$

여기서 각 행렬의 1행은 share 1을 위한 조합이 되고, 2행은 share 2를 위한 조합이 된다. 따라서 S_0와 S_1의 해밍가중치는 식 (3)과 같다.

$$\begin{aligned}&S_0\text{의 } H(V=(0,1,1,1))=3\\&S_1\text{의 } H(V=(1,1,1,1))=4\end{aligned} \tag{3}$$

이때 식 (4)와 같이 S_0, S_1의 각 열들을 교환하여 만들어진 부울 행렬들의 집합을 C_0, C_1이라 하자.

$$\begin{aligned}C_0&=\{S_0\text{의 열을 교환하여 생성된 행렬}\}\\C_1&=\{S_1\text{의 열을 교환하여 생성된 행렬}\}\end{aligned} \tag{4}$$

이 집합으로부터 비밀 정보의 화소가 백인 경우에는 임의의 C_0 부울 행렬을 각각의 share에 표시하고, 흑인 경우에는 C_1의 부울 행렬을 share에 표시하여 구성하게 된다.

[정의] (k,n) 시각암호 방식은 $n\times m$ 부울 행렬들의 두 집합 C_0, C_1으로 구성된다. 백화소를 분산하기 위해서 C_0의 행렬 중 하나를 임의로 선택하고, 흑화소를 분산하기 위해서 C_1의 행렬 중 하나를 임의로 선택한다. 선택된 행렬의 각 행은 한 개의 share에 대응시키고 행의 각 요소가 1이면 흑을, 0이면 백을 나타낸다. (k,n)시각암호의 유효한 해가 존재하기 위해서는 다음 세 가지 조건을 만족해야 한다.

조건 1. C_0에서 임의의 행렬 S에 대해서 n행 중 임의의 k행을 OR 연산했을 때 m차 벡터 V의 해밍 가중치는 $H(V)\le d-\alpha m$ 을 만족한다.

조건 2. C_1에서 임의의 행렬 S에 대해서 n행 중 임의의 k행을 OR 연산했을 때 m차 벡터 V의 해밍 가중치는 $H(V)\ge d$ 을 만족한다.

조건 3. $q<k$인 $\{1,2,\cdots,n\}$ 에 대한 임의의 부분집합 $\{i_1,i_2,\cdots,i_q\}$ 에 대해서 C_t내의 각 $n\times m$ 행렬을 $i_1,i_2,\cdots,i_q$ 행으로 한정시켜 얻어진 동일한 빈도의 동일한 행렬들을 포함한 2개의 $q\times m$ 행렬의 집합 D_t는 서로 구분할 수 없다. 단, $t\in\{0,1\}$.

조건 1과 조건 2는 share를 중첩했을 때, 복원된 영상에서 흑백을 구별하기 위한 대비를 나타내고, 조건 3은 k장 미만의 share를 중첩했을 때, 분산된 비밀화소가 흑인지 백인지를 구분할 수 없는 안전성을 보인다.

2.2 Yang의 부화소 비확장 모델

Yang은 확률적 분산방법을 사용하여 부화소를 생성하지 않는 방법을 제안했다[3]. 이 방법에서 p_0,p_1는 비밀영상의 흑백화소에 따라 생성된 share의 흑백 확률적 표시를 나타내며, $\beta=|p_0-p_1|$ 는 복원된 영상에서의 확률적 대비를 통해 시각적으로 인지할 수 있는 새로운 변수가 된다. <Table 1>은 Yang의 $(2,2)$시각암호 구조에서 각각의 share에 부화소를 생성하지 않는 비밀분산법을 보인다.

Yang의 방법의 장점은 비밀영상의 픽셀 크기를 확장하지 않고 1대 1로 매핑할 수 있다는 점이다. 그렇지만 Yang의 방법도 k개의 share를 중첩시킬 경우 출력으로 얻어지는 영상은 백화소의 경우, 1/2 확률로 잡음이 포함되는 단점을 가지고 있다.

<표 1> Yang의 $(2,2)$ 비확장 비밀분산법

Pixel of the Secret Image	Share 1	Share 2	Recovered Result	Probability
□ (White)	□	□	□	$p_0=0.5$
	■	■	■	
■ (Black)	□	■	■	$p_1=0$
	■	□	■	

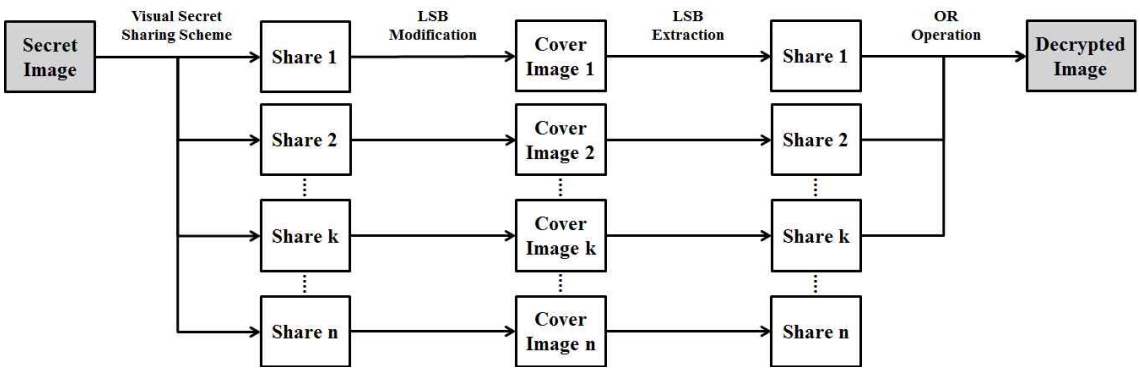
<Table 1> Yang's $(2,2)$ Non-expansion Secret Sharing Scheme

3. 기본적인 시각암호 응용 구조

시각암호 그 자체는 단순히 분산 영상만 이용하기 때문에 공격을 받기 쉽다. 따라서 비밀영상을 안전하게 공유하기 위한 방법 중 하나로 (Figure 1)과 같이 시각암호 방식으로 생성된 분산 영상의 정보를 커버영상에 은닉하는 데이터 은닉 기법을 적용했다.

원래 시각암호 기술에서는 각각의 share를 여러 곳에 분산 보관하게 하고 있으나 난수처럼 보이는 share가 의심을 살 수 있어 이를 평범하게 저장하는 방법이 있다면 안전성 향상에 큰 도움이 된다. 따라서 본 논문에서는 시각암호의 산물인 share를 여러 영상에 은닉함으로써 의심스러운 난수처럼 보이는 share 대신 의심스럽지 않은 보통영상을 분배하고 저장하게 하자는 것이 이 논문의 기본 골격이다. 그래서 비밀영상을 비밀 분산법에 의해 n개의 이진영상을 생성하고, 분산영상에 따라 각각 커버영상의 LSB(least

(그림 1) 기본적인 시각암호 응용구조



(Figure 1) Basic Application of Visual Cryptography Scheme

significant bit)를 수정한다. 물론 LSB 대신 다른 비트 플레인 위치에 정보를 은닉할 수도 있으나 편의상 LSB를 이용해 설명한다.

실제 공유되는 영상은 비밀 정보가 삽입된 커버영상 $1,2,\cdots,k,\cdots,n$ 으로 시각적으로 변화가 적은 LSB가 변조되기 때문에 사용자는 커버영상만 인지할 뿐 삽입된 분산영상을 인지하기 어렵다. 비밀영상을 복호화 하기 위해서는 k개 이상의 커버영상에서 LSB를 추출하여 각각의 share $1,2,\cdots,k$ 를 OR 연산한다. 이로써 시각적으로 구별이 가능한 비밀영상이 복호화 된다.

4. 제안된 시각암호 응용 구조

제안된 시각암호 응용 구조는 모든 share를 비밀분산법에 의해 생성하는 것이 아니라 (Figure 2)와 같이 share 1부터 $n-1$까지를 커버영상에서 추출해내는 방법을 적용함에 중점을 둔다. 커버 용도로 사용되는 영상에서 LSB 정보로 share 1을 생성한다. 즉, share 1을 생성하는데 커버영상 1의 LSB 정보가 그대로 사용되었을 뿐 실제로 커버영상 1에 훼손이 가해지지 않았음을 알 수 있다. 커버영상 2에서도 LSB 정보가 share 2로 사용될 뿐 전혀 훼손이 없다. 이렇게 $n-1$개의 share가 각각의 커버영상 LSB 정보로부터 자연스럽게 생성된다. 그렇다면 n번째 share는 다음과 같이 생성한다. 우선 share 1부터 share $n-1$까지를 XOR 연산해 얻은 이진영상과 비밀영상을 XOR 연산한 결과를 share n이라 한다. 그리고 수정이 되는 영상은 LSB가 share n으로 치환된 커버영상 n뿐이다.

(k,n) 시각암호 기술을 사용하여 전체 n개 share로 비밀분산 할 때, 조건 3을 만족하여 $k-1$개의 모든 조합이 비밀영상을 유출하지 않도록 share를 비밀분산 하는 방법과 다르게, 제안된 시각암호 응용 구조는 모든 share $1,2,\cdots,n$를 XOR 연산해야만 비밀영상을 복호화 할 수 있는 (n,n) 구조이다.

예를 들어, 커버영상 1의 LSB 값이 다음과 같다고 하자.

1 0 1 0 1 0 1 1 1 0 0 0 1 0 0 0 1

커버영상 2의 LSB 값은 다음과 같다고 하자.

0 0 1 0 1 0 1 1 1 0 0 0 1 0 0 1 1

커버영상 3의 LSB 값은 다음과 같다고 하자.

1 1 1 0 0 0 1 0 1 0 0 0 1 0 1 0 1

3개의 영상을 이용해 다음의 비밀영상 정보

0 0 0 0 0 0 1 1 1 0 0 1 1 0 0 0 1

를 숨기고자 한다. 이때 우선 커버영상 1과 커버영상 2의 LSB 값을 XOR하면

1 0 1 0 1 0 1 1 1 0 0 0 1 0 0 0 1

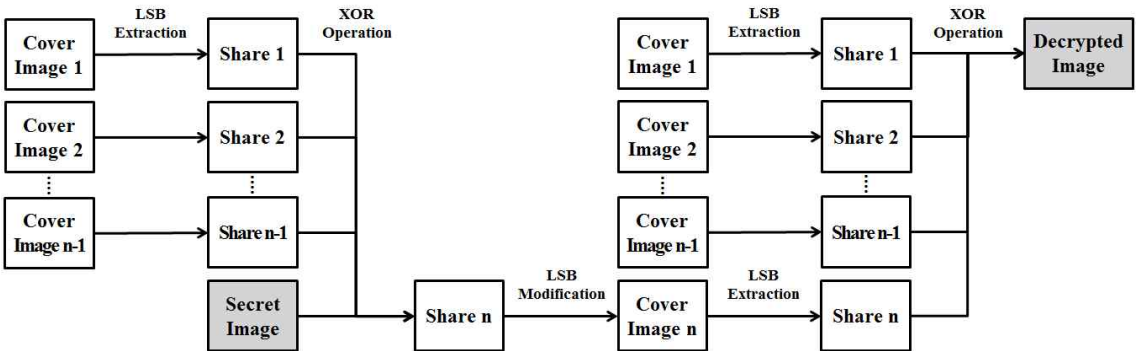
$\oplus$

0 0 1 0 1 0 1 1 1 0 0 0 1 0 0 1 1

=

1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0

(그림 2) 제안된 시각암호 응용 구조



(Figure 2) Proposed Application of Visual Cryptography Scheme

을 얻는다. 이때 커버영상 1과 2에는 손상을 가하지 않는다는 전제가 깔려있다. 위에서 얻은 이진영상 정보와 비밀영상의 값을 XOR 연산하면

$$
\begin{array}{c}
1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0 \\
\oplus \\
0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1 \\
= \\
1\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1
\end{array}
$$

을 얻는다. 따라서 이 정보가 share 3이 된다.

이 share 3을 커버영상 3의 LSB 값으로 치환하면 된다. 즉, 커버영상 1과 커버영상 2의 LSB 값은 그대로 두고 커버영상 3의 LSB 값만 고친 셈이다. 비밀영상을 복원하려면 커버영상 1과 커버영상 2, 그리고 치환된 커버영상 3의 LSB 값에 대해 XOR 연산을 다음과 같이 시행하면

$$
\begin{array}{c}
1\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,0\,0\,0\,1 \\
\oplus \\
0\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1 \\
\oplus \\
1\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1 \\
= \\
0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1
\end{array}
$$

비밀영상을 온전히 얻게 된다.

만일 치환된 커버영상 3의 LSB 값이 비밀영상의 정보를 유출하지 않는다면, 더 엄밀히 말하자면 share 1과 share 2, share 1과 share 3, share 2와 share 3을 XOR 연산했을 때 비밀영상 정보를 유출하지 않는다면 굳이 잡음을 생성하는 Yang의 방법을 쓸 이유가 없다. 당연히 share 1과 share 2는 XOR 연산을 해도 비밀영상 정보와 무관하므로 정보를 유출할 가능성이 없다. 그러나 share 3은 비밀영상과 관련이 있으므로 share 1, share 2는 각각 share 3과의 XOR 연산을 통해 정보를 유출할 수 있는지 확인할 필요가 있으며, 이는 실험의 (Figure 11-12)를 통해 검증하였다. 따라서 커버영상 1, 커버영상 2, 치환된 커버영상 3의 LSB 중 단 하나라도 빠지면 비밀영상을 복호화 할 수 없다.

또한 비밀메세지의 인덱스에 따라 카운트 되는 모든 커버영상을 수정해야 하는 김천식의 방법[11]과 다르게 제안된 방법은 n개의 커버영상 가운데 하나의 영상만 LSB를 수정하고 $n-1$개의 커버영상을 훼손하지 않고 LSB를 그대로 사용하므로 steganalysis에서 검색될 가능성이 $1/n$이 된다.

5. 실 험

예제와 같이 (3,3) 구조로 부화소가 생성되지 않는 제안된 방법을 적용했다.

(Figure 3)에 이진 비밀영상이 주어졌다.

(Figure 4, 5, 6)은 각각 커버영상 1, 2, 3이다.

(Figure 7)은 비밀영상, 커버영상 1의 LSB (share 1), 커버영상 2의 LSB(share 2)를 XOR 연산한 결과(share 3)이며,

(Figure 8)은 커버영상 3의 LSB를 (그림 7)로 치환한 영상이다.

(Figure 9)에서는 각각 커버영상 1, 커버영상 2, 수정된 커버영상 3 의 LSB를 추출하여 XOR 연산을 통해 손실 없이 비밀영상을 그대로 복원함을 볼 수 있다.

(Figure 10)은 Yang의 방법을 적용하여 복호화 된 영상으로, (Figure 9)와 비교해 보면 백화소에 잡음이 생성됨을 확인할 수 있다.

(Figure 11)은 share 1과 share 3을 XOR 연산한 영상,

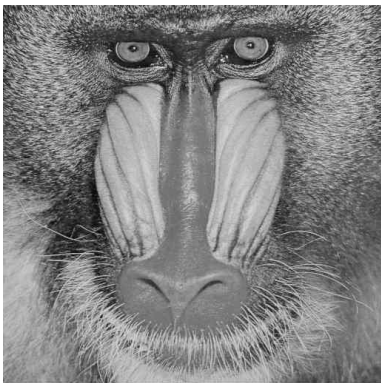
(Figure 12)는 share 2와 share 3을 XOR 연산한 영상으로, (Figure 11-12)를 통해 연산 값이 무작위로 나타남을 확인 할 수 있기 때문에, 각각 영상의 LSB 정보만 사용할 때 share 3와 조합을 통해 정보를 유출하지 않음을 검증한다.

본 실험에서는 share 3개를 사용한 예를 들었지만, share 수가 증가하더라도 모든 share들이 서로 상관관계가 없는 독립적인 영상들이라면 (n,n) 시각암호 기술을 안전하게 구현하는데 전혀 문제가 없음을 보일 수 있다. 즉, $n-1$개의 share들이 서로 독립이라면 이것들의 XOR 결과는 비밀영상과 역시 독립이므로 비밀영상과의 XOR 결과인 share n은 다른 모든 share들과 독립이다. 따라서 어느 경우라도 $n-1$개의 모든 share들의 조합으로부터 비밀영상을 복구하는 것은 불가능하다.

(그림 3) 비밀영상

(Figure 3) Secret Image

(그림 4) 커버영상 1



(Figure 4) Cover Image 1

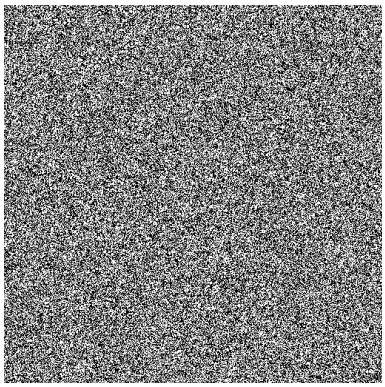
(그림 5) 커버영상 2

(Figure 5) Cover Image 2

(그림 6) 커버영상 3

(Figure 6) Cover Image 3

(그림 7) Share 3



(Figure 7) Share 3

(그림 8) 수정된 커버영상 3

(Figure 8) Modified Cover Image 3

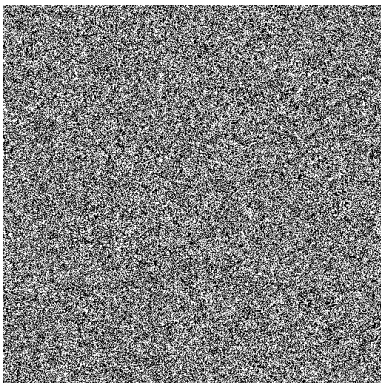
(그림 9) 복호화 된 영상

(Figure 9) Decrypted Image

(그림 10) Yang의 방법으로 복호화 된 영상

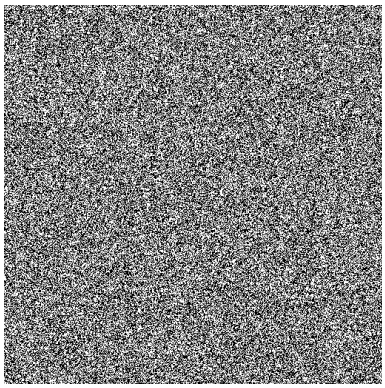
Figure 10) Decrypted Image by Yang's Method

(그림 11) Share 1과 Share 3의 XOR 영상



(Figure 11) XOR Image of Share 1 and Share 3

(그림 12) Share 2와 Share 3의 XOR 영상



(Figure 12) XOR Image of Share 2 and Share 3

6. 결 론

기본적인 시각암호 구조는 n개의 분산된 영상에 비밀영상을 나누어 담기 때문에 분산영상의 개수만큼 커버영상을 변조해야 한다. 하지만, 본 논문에서 제안한 시각암호 구조는 시각암호 방식에 steganography 기법을 응용한 방법으로 커버영상 $n-1$장을 온전히 수정하지 않은 채 조합된 정보를 이용하여 다른 하나의 비밀 분산된 영상을 생성하기 때문에 기본적인 방식에 비해 훨씬 steganalysis가 어렵게 만들어 공격으로부터 향상된 안전성을 제공한다. 또한 기존 시각암호를 사용한 구조에서 복원된 영상은 확률적으로 잡음을 생성했지만, 제안된 시각암호의 구조는 비밀영상을 온전히 복원할 수 있음을 보였다. 다만, 각각의 share들이 상호 독립적이어야 한다는 조건이 필요하나 이것은 영상들의 LSB 값들이 거의 상호 독립적이므로 전혀 부담스러운 전제조건이 되지 못한다.

향후 Color Image, Video, Audio등을 응용한 시각암호 구조에 대한 연구를 진행하고자 한다.

References

[1] M. Naor and A. Shamir, "Visual cryptography", Lecture Notes in Computer Science, vol. 950, pp. 1-12, 1995.

[2] Mi-Ra Kim, Ji-Hwan Park, Sang-Woo Park, and Kwang-Jo Kim, "Secret Sharing Scheme Using Visual Cryptography", Journal of The Korea Institute of

Information Security & Cryptology, vol. 7, no. 4, pp. 37-50, December 1997
[3] C.-N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognition Letters, vol. 25, no. 4, pp. 481 - 494, March 2004.
[4] C.-N. Yang, P.-W. Chen, H.-W. ,and C. Kim, "Aspect ratio invariant visual cryptography by image filtering and resizing," Personal and Ubiquitous Computing, Published online, April 2012.
[5] F. Liu, T. Guo, C. Wu and L. Qian, "Improving the visual quality of size invariant visual cryptography scheme," Journal of Visual Communication and Image Representation, vol. 23, no. 2, pp. 331-342, February 2012.
[6] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography", IEICE Transactions on Fundamentals, vol. E82-A, no, 10, pp. 2172-2177, October 1999.
[7] N. Chhabra, "Visual cryptographic steganography in Images," International Journal of Computer Science and Network Security, vol. 12, no. 4, pp. 126-131, April 2012.
[8] Hye-Joo Lee and Ji-Hwan Park, "An Extension of Visual Cryptography and Its Application into Digital Watermark", Journal of Korea Multimedia Society, vol. 1, no. 1, pp. 80-89, 1998
[9] Eun-Jun Yoon, Hae-Soon Ahn, Ki-Dong Bu, and Kee-Young Yo, "A Frequency Domain based Steganography using Image Frame and Collage", The Institute of Electronics Engineers of Korea - Computer and Information, vol. 47, no. 6, pp. 86-92, November 2010
[10] Jin-Kyoung Heo, "Distributed Security for Web Application Contents Protection", Journal of Digital Contents Society, vol. 9, no. 1, pp. 123-130, March 2008
[11] Cheonshik Kim, Eun-Jun Yoon, You-Sik Hong, and Hyoung Joong Kim, "Secret Sharing Scheme using Gray Code based on Steganography", The Institute of Electronics Engineers of Korea - Computer and Information, vol. 46, no. 1, pp. 96-102, January 2009

장 시 환

2010년 : 강원대학교
산업공학과 (공학사)
2010년~현 재 : 고려대학교
정보보호대학원 (석사과정)

관심분야 : Visual Cryptography, Steganography, Watermarking, DRM

최 용 수

1998년 : 강원대학교
제어계측공학과 (공학사)
2000년 : 강원대학교
제어계측공학과 (공학석사)
2006년 : 강원대학교
제어계측공학과 (공학박사)

2006년~2007년: 연세대학교
첨단융합건설연구단 연구교수
2007년~현 재: 고려대학교
정보경영전문대학원 연구교수
2008년~현 재: 대한전자공학회
컴퓨터소사이어티 논문편집위원장
관심분야 : Multimedia Hashing, Information Hiding, Watermarking, Steganography

김 형 중

1978년 : 서울대학교
전기공학과 (공학사)
1986년 : 서울대학교
제어계측공학과 (공학석사)
1989년 : 서울대학교
제어계측공학과 (공학박사)

1990년~2006년: 강원대학교 교수
1992년~1993년: USC Univ. 방문교수
2007년~현 재: 고려대학교 정보보호대학원 교수
관심분야 : Watermarking, Parallel Computing, Image Hashing, Data Compression, Steganography