시크릿 쉐어링 기반 비디오 스테가노그래피 통신의 강건성에 대한 연구

이상호*, 조영호(교신저자)**
*국방대학교 국방관리대학원 국방과학학부 사이버컴퓨터공학과
**국방대학교 국방관리대학원 국방과학학부 사이버컴퓨터공학과 교수
e-mail:sikh3402@naver.com, younghocho@korea.kr

A Study on the Robustness of Secret-Sharing-based Video Steganographic Communication

Sang-ho Lee*, Youngho Cho**
*Master's Course, Dept. of Cyber Security and Computer Engineering,
Korea National Defense University
**Professor, Dept. of Cyber Security and Computer Engineering,
Korea National Defense University

요 약

스테가노그래피는 메시지의 존재 자체를 감추는 은밀한 통신 기법으로, 최근 유투브와 같은 동영상 공유 플랫폼 환경에서의 활용성이 주목받고 있다. 하지만, 특정 플랫폼의 재인코딩 과정에서 스테가노그래피 매개체의 데이터가 훼손되면 은닉된 비밀메시지의 전달이 불가능해지며, 스테고 컨테이너플랫폼에 공유된 스테가노그래피 매개체가 스테그어날리시스 체계에 의해 탐지될 수도 있다. 본 연구에서는 이러한 제한사항을 해결하기 위해, 샤미르의 비밀 공유(Shamir's Secret Sharing)를 스테가노그래피와 결합하여 공유 플랫폼의 다수의 동영상에 분산 은닉하는 새로운 스테가노그래피 은닉 통신 프레임워크와 기법을 제안한다. 제안된 방법은 우선 비밀메시지를 암호화하여 분할한 후 다수의 커버 비디오 파일에 삽입하고 복구 메커니즘을 활용하여 임계값 미만의 비디오가 탐지 또는 노출되더라도 원본 비밀메시지가 유출되지 않음을 보장한다. 또한, 플랫폼의 공격적인 재인코딩으로 일부 비디오가 손상되더라도 데이터를 강건하게 복원할 수 있다. 초도실험에서 실제 유투브의 재인코딩 환경에서 제안기법의 은닉된 비밀메시지의 복원 성능을 평가하였으며, 실험 결과 일부 동영상이 손상되어도 최초 메시지의 복구 수 있음을 확인하였다.

1. 서론

스테가노그래피(Steganography)는 일반적인 디지털 콘텐츠에 비밀메시지를 은닉하는 기술이며 이를 기반으로 한 통신 방식을 스테가노그래피 은닉 통신이라 한다[1]. 최근 유투브와 같은 대규모 동영상 공유 플랫폼(이하 유투브)들이 높은 접근성과 확산력을 지녀 이러한 은닉 통신의 매력적인 전송 채널로 활용되고 있다[2].

그러나 이런 환경에서는 감시자 또는 불특정 다수가 해당 콘텐츠에 접근할 수 있으므로, 평문 형태의 은닉은 탐지될 위험성이 높기 때문에 수신자만 복원 가능한 형태의 암호화된 페이로드를 삽입하는 것이 탐지 회피를 위해 중요하다. 또한, 유투브의 업로드 과정에서 필요에 따라 재인코딩이 이루어지므로 은닉 삽입된 비트열에 오류가 발생할 수 있다. 특히, AEAD 계열 암호화는 무결성 검증을 포함하므로 하나의 비트 오류만 있어도 복호화가 거부되며, 실제 환경의 오류 양상은 산발 오류와 집중 오류가 공존하기에 이를 보완할 수 있는 설계가 요구된다. 즉, 한 개의 비디오에 모든 메시지를 삽입하는 방식은 단일 실패 지점을 형성해 특정 조건의 간섭만으로도 전체 복구가 실패할 수 있다.

기존 스테가노그래피 연구는 주로 삽입/탐지 기법의 은닉성 또는 단일 매체 내 강건성(Robustness)에 집중해 왔다. 반면에 유투브의 재인코딩을 전제로 산발·집중 오류가 공존하는 실제 조건에서 복수의 매체에 분산하고 오류 정정을 결합해 복구 가능성을 체계적으로 검증한 연구는 상대적으로 부족하다.

본 연구는 이러한 공백을 메우기 위해, 암호화된 페이로드를 Shamir Secret Sharing(SSS)으로 다수의 비디오에 분산하고 각 조각에 오류정정부호(ECC)를 결합하는 강건성 중심 분산 스테가노그래피 통신 구조를 제안한다. 이 구조는 산발 오류는 ECC로 보완하고, 집중 오류로 붕괴된 조각은 SSS의 임계값 k로 보완하여 단일 실패 지점의 가능성을 낮춘다.

본 연구의 기여는 다음과 같다. 첫째, 유투브에서 강건성 중심

의 스테가노그패리 은닉 통신 프레임워크를 제시하여 블랙박스형 재인코딩 환경에서의 예측 불가능한 데이터 손실에 대응한다. 둘째, 실제 실험을 통해 제안한 프레임워크와 기법이 실제 유투브 재인코딩 채널의 영향에도 불구하고 안정적으로 비밀 메시지 복원이 가능함을 확인하고 오류 패턴에 따른 SSS, ECC의 효과를 분석하였다.

2. 배경지식 및 관련 연구

2.1 비디오 스테가노그래피의 강건성 관련 연구

비디오 스테가노그래피에서 강건성은 재인코딩, 채널 잡음 등 외부 요인에 따른 왜곡으로부터 삽입된 정보를 보호하는 것으로 관련된 연구는 다음과 같은 두 가지 유형으로 분류할 수 있다.

첫째, 안정적인 삽입 위치를 확보하기 위한 연구이다. 영상 데이터 중 채널의 변환 과정에서도 안정적으로 유지되는 영역을 식별하여 활용한다. Mstafa 등[3]은 코너 검출 알고리즘과 혼돈 변환 암호화 기법으로 메시지를 암호화하는 기법을 제안했다.

둘째, 복구 메커니즘을 결합하여 강건성을 확보하는 연구이다. 안정적인 위치 선정만으로는 모든 손실에 대응할 수 없기 때문에 ECC와 SSS 등의 기법을 결합하여 데이터의 손실을 대비한다. Zhang 등[4]은 이러한 복구 기술을 단일 비디오내 여러 프레임에 적용하여 일부 손상에 대해 대응하는 구조를 제안했다.

하지만 이러한 연구들은 몇 가지 문제점이 있다. 우선 안정적인 위치를 찾는 방법만으로는 재인코딩간 발생하는 모든 손실을 막을 수 없다. 복구 메커니즘을 강화하는 방법은 은닉성, 강건성, 수용 능력 간의 trade-off 문제에 직면한다. 복구 메커니즘을 추가할수록 강건성은 향상되지만, 이로 인해 비디오의 시각적 왜곡이 증가하거나 실질적인 메시지 수용 능력이 감소할 수 있다. 더 근본적으로, 이러한 모든 접근법은 통신 전체가 단일 비디오라는 매체에 종속된다는 한계를 가진다. 이는 다음 절에서 논의할 유투브와 같이 블랙박스형 재인코딩이 이루어지는 환경에서 반드시 고려해야 할 사항이다.

2.2 유투브 환경의 재인코딩 특징

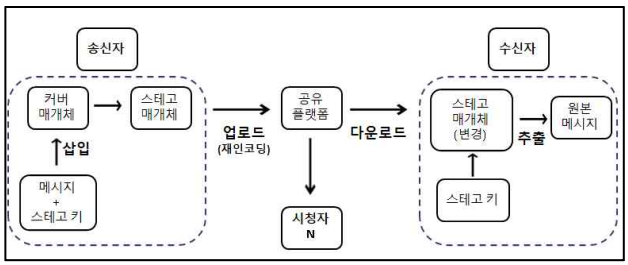
유투브(YouTube)는 업로드 시 특정 포맷을 권장한다. 유투브의 경우 H.264/AVC 코덱과 MP4 컨테이너, 4:2:0 색차 서브샘플링, 적응형 비트레이트 스트리밍(ABR)이 적용되어 대규모 트래픽을 처리하고, 이기종 단말기간의 호환성을 확보한다.

그러나 이러한 포맷으로의 재인코딩 과정은 은닉 데이터의 생존에 직접적인 손상을 준다. 즉, 4:2:0 색차 서브샘플링은 색차 정보를 줄여 은닉 신호를 약화시키고, 손실 압축 코덱과 양자화 과정은 미세한 삽입 신호를 파괴하며, ABR은 동일 콘텐츠를 여러 버전으로 변환·전송하는 과정에서 손상되는 양상이 다양하게 나타나 송신자가 예측하기 어렵게 만든다.

결국 이러한 처리 파이프라인은 내부 파라미터가 공개되지 않는 블랙박스형 채널로 기능한다. 따라서 최신 연구는 단순히 은닉성 확보를 넘어서, 불투명한 변환 환경을 전제로 한 강건성 확보 전략을 요구하게 된다.

3. 제안 기법

3.1 연구문제 정의 및 설계 목표

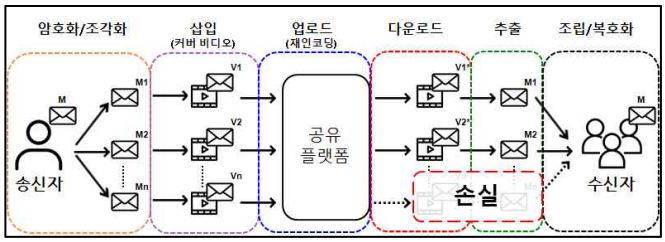


[그림 1] 유투브에서의 비디오 스테가노그래피 통신 모델

본 연구는 위와 같은 기존기법들의 제한사항을 해결하기 위해 유투브 환경에서의 강건한 비디오 스테가그래피 은닉 통신 문제를 정의하고 설계 목표를 수립하였다. [그림 1]은 유투브 환경을 도식화한 것으로 업로드 과정에서 재인코딩 과정과 불특정 다수가 매체에 접근 가능함을 보여준다.

이러한 상황에서 성공적인 비디오 스테가노그래피 통신에 두 가지 구조적 위험에 직면한다. 첫째, 재인코딩 과정은 삽입된 비트열에 오류를 유발하여 암호화된 메시지의 복원을 어렵게 한다. 둘째, 단일 커버 비디오 의존 구조는 오류가 해당 비디오에 집중될 때 추출 실패로 이어질 수 있다. 따라서 본 연구는 재인코딩으로 인한 오류가 존재하더라도 메시지 복원이 가능하도록 하는 강건성 향상을 목표로 한다.

3.2 제안기법의 동작단계 및 설계



[그림 2] 유투브 내 다중 매개체 활용 구조(N번 비디오 손실)

제안 프레임워크는 비밀 메시지를 다수의 비디오에 분산하여 삽입함으로써, 일부 조각이 손상되더라도 임계값 이상의 유효 조각을 확보하면 원본 메시지를 확인할 수 있도록 설계되었다. [그림 2]는 본 연구에서 제안하는 구조를 나타낸 것으로 암호화, 조각화, 삽입 단계를 거치며 복구는 역순을 따른다. 이와 같은 구조는 일부 비디오에서 조각 복구가 실패되더라도 복원이 가능케하

며, 결과적으로 전체 시스템의 강건성을 향상시킨다.

3.2.1 암호화 단계

첫 단계인 암호화 단계의 목표는 원문 메시지 M의 기밀성과 무결성을 확보하는 데 있다. 패스프레이즈 P와 무작위 솔트(salt)는 PBKDF2-HMAC-SHA256에 입력되어 충분한 반복 횟수를 통해 256비트 대칭키 K를 안전하게 생성한다 [5]. 이렇게 생성된 키 K는 ChaCha20-Poly1305 인증 암호(AEAD) 알고리즘에 사용되어, 원문 M을 암호문 C로 변환하고 무결성을 검증하기 위한 인증 태그(τ)를 함께 생성한다. 또한, 알고리즘은 각 세션마다 재사용되지 않는 nonce를 입력으로 사용하므로 같은 키를 동일한 메시지에 재사용하더라도 별개의 암호문이 생성된다[6].

3.2.2 조각화 단계

암호화된 메시지는 단일 비디오에 의존하지 않고 복수의 비디오에 안전하게 분산되기 위해 조각화 과정을 거친다. 이 단계의 핵심 목표는 복원력 확보이다.

먼저, 암호문 C는 Shamir의 (n, k) 비밀 공유 기법을 적용하여 n개의 조각으로 나누어진다. n개의 조각 중 임계값인 최소 k개의 조각이 확보되면 라그랑주 보간법을 통해 복원함으로써 원문 C를 회복할 수 있으며, k−1개 이하의 조각만으로는 원문에 대한 어떠한 추가 정보도 유출되지 않는다[7].

추가적으로, 각 조각은 Reed-Solomon(RS) 오류정정부호(ECC)로 인코딩되어 유투브 재인코딩이나 전송 과정에서 발생할 수 있는 국소적 손상에도 복구 가능성을 확보한다. 그 결과, 제안된 메시지는 암호학적으로 안전할 뿐만 아니라 실제 환경에서의 물리적 손상에 대한 복원력까지 확보할 수 있다[8].

3.2.3 삽입 단계

조각화된 메시지는 전체 길이에 걸쳐 선택된 프레임 집합에 배정된다. 각 할당 프레임은 YCrCb로 변환한 뒤 휘도(Y) 채널에 Haar DWT를 적용하고, 저주파(LL) 대역에만 은닉한다. LL은 재인코딩·전송 과정에서의 보존성이 높아 강건성에 유리하고, 손실 압축에서 쉽게 소거되는 LH/HL/HH는 사용하지 않는다 [9].

은닉된 비트 b는 양자화 지수 변조(QIM, Quantization Index Modulation) 방식으로 삽입된다. QIM은 계수를 특정 간격(Δ)으로 양자화하고 삽입할 비트 값에 따라 정해진 격자에 배치하는 방식이다. 이때 Δ 값이 작으면 은닉성이 향상되지만 손상에 취약해지고, 값이 크면 강건성은 증가하나 은닉성이 저하되는 절충이 존재한다 [10].

이후 강건성을 더욱 높이기 위해 동일한 비트를 복수의 LL 계수 위치에 중복 삽입하였고, 삽입이 완료된 프레임은 역 DWT와 색 공간 복원을 거쳐 재조립된다.

3.2.4 추출 및 복호화 단계

이 단계는 삽입의 역순으로 진행된다. 송신자는 비디오에서 프레임 조각을 추출하고 각 프레임의 휘도 채널을 DWT로 분해하여 얻은 LL 계수에서, QIM 복조 규칙에 따라 비트를 판별한다. 삽입간에 각 비트는 시·공간적으로 중복 기록되었으므로, 추출 시 동일한 비트에 대해 복수 후보가 얻어진다. 최종 비트 $\hat{b}_k$는 다수결 규칙(majority voting)을 통해 결정되며, 이는 일부 삽입 위치가 손상되더라도 가장 가능성이 높은 값으로 수렴한다.

재구성된 비트열은 바이트 단위로 변환된 뒤, 삽입 단계에서 적용된 ECC로 디코딩된다. ECC는 바이트 단위 오류와 손실을 일정 범위까지 정정할 수 있으므로, 비트 오류율(BER)을 낮추고 유효한 조각 복구율을 향상시킨다. 이후 유효조각이 임계값 k개 이상 확보되면, SSS 복원 절차를 통해 암호문 $\hat{C}$가 재구성된다.

마지막으로, 재구성된 암호문 $\hat{C}$는 사전 공유된 키 K로 복호화가 수행된다. 이 과정에서 인증 태그를 검증하여 무결성을 확인하며 검증 실패 시 복호화는 거부되고, 성공 시에만 최종 원문 메시지 M이 수신자에게 전달된다.

4. 초도 실험

4.1 실험 목적 및 방법

본 실험의 목적은 유투브와 같이 블랙박스형 재인코딩이 이루어지는 유투브 환경에서 메시지의 복원 여부를 통해 제안 프레임워크의 강건성을 검증하는데 있다.

실험은 512/1024B 크기의 메시지를 ChaCha20-Poly1305로 암호화한 후 SSS(n=10, k=7)로 분할하고, 각 조각에 RS(255,223) 부호를 적용하여 10개의 커버 비디오에 삽입하였다. QIM 양자화 간격(Δ)은 64, 72, 80을 사용했으며, 공간 중복도 r=11, 시간 분산 96프레임으로 설정하였다. 삽입된 비디오를 유튜브에 업로드 후 다운로드하여 재인코딩을 거친 뒤, 역과정을 통해 데이터를 추출하고 복원 성능을 측정하였다. 변화를 준 파라미터는 양자화 간격과 메시지 크기로서 일반적으로 양자화 간격이 클수록, 메시지의 크기가 작을수록 강건성은 증가하지만 각각 은닉성, 수용능력과 trade-off 관계를 가진다.

평가지표로는 다음 세 가지를 사용했다.

- 초기 유효조각비율(pre-ECC): 오류 정정 적용 전 무결성 검증을 통과한 조각의 비율
- 최종 유효조각비율(post-ECC): 오류 정정 적용 후 무결성 검증을 통과한 조각의 비율

• Bit Error Rate(BER): 원본 메시지와 복원 메시지를 비교해 잘못 복원된 비트의 비율

기존 연구와의 공정 비교는 다음과 같은 한계가 있다. 첫째, 유투브의 재인코딩 정책은 블랙박스로 운영되며 지속적으로 변경된다. 둘째, 대부분의 비디오 스테가노그래피 관련 연구들의 구현 코드가 공개되지 않아 동일 조건에서의 재현이 불가능하다.

4.2 실험 결과 및 분석

초도 실험 결과와 분석은 다음과 같다.

첫째, 제안 기법은 [표 1]과 같이 양자화 계수와 메시지 크기가 변화하는 환경에서 제안 기법이 잘 동작하여 메시지 복원에 성공했다. 64/512와 64/1024의 경우 오류 정정 전 유효 조각의 비율이 각각 40%로 SSS의 임계값인 70%에 미치지 못하는 실패조건이었지만 ECC 적용 이후 유효 조각 비율이 80%로 증가하여 메시지 복원에 성공했다. 파라미터의 특징을 보면 메시지 크기가 512바이트로 작은 경우, 1024바이트 보다 유효 조각 비율이 높거나 같은 경향을 보였다. 양자화 계수의 경우 80/1024의 이상치를 제외하면, 계수가 커질수록 유효 조각 비율이 높거나 같은 걸 볼 수 있어 강건성에 미치는 영향을 확인할 수 있다.

[표 1] 파라미터별 복구율

파라미터(Δ/M)	메시지 복원 여부	초기 유효조각비율 (pre-ECC)	최종 유효조각비율 (post-ECC)
64/ 512	복원 성공	40%	80%
72/ 512	복원 성공	50%	80%
80/ 512	복원 성공	60%	80%
64/ 1024	복원 성공	40%	80%
72/ 1024	복원 성공	50%	80%
80/ 1024	복원 성공	50%	70%

* SSS임계값은 (10, 7)로 70%이상 유효 조각 확보시 복원 가능

둘째, 유투브 재인코딩 환경에서 단일 매체에 기반한 은닉통신의 복원 실패 가능성이 증가함을 확인했다. [표 2]를 보면 재인코딩 이후 비트 오류는 전체 비디오에 균등하게 발생하지 않고 특정 비디오(#2)에만 집중되는 패턴을 보였으며, 일부 비디오(#3,9)에는 오류가 전혀 발생하지 않았다. 이는 블랙박스 환경의 예측 불가능성을 보여주며 다중 매체에 기반한 은닉통신의 필요성을 보여준다.

[표 2] BER(%)

파라미터 (Δ/M)	64/ 512	72/ 512	80/ 512	64/ 1024	72/ 1024	80/ 1024
#1	0.74	0	0	1.20	0.06	1.88
#2	1.09	0.51	2.94	13.05	5.33	9.86
#3	0	0	0	0	0	0
#4	0	0	0	0	0	0.04
#5	0.11	0	0	0.01	0	0
#6	0.31	0.02	0.03	0.29	0.06	0.01
#7	0.51	1.23	0.93	0.25	0.89	0.60
#8	0	0	0.02	0	0	0
#9	0	0	0	0	0	0
#10	0.02	0.07	0	0.05	0.01	0

* 비트오류율로 0에 가까울수록 원본과 유사

5. 결론 및 향후 연구

본 연구는 SSS를 스테가노그래피와 결합하여, 단일 실패 지점 문제와 재인코딩 환경에서의 데이터 손상 문제를 최소화하는 분산형 프레임워크를 제안했다. 실험 결과, 제안 기법은 일부 비디오가 손상된 상황에서도 메시지 복원을 성공했다. 향후 연구 방향은 다음과 같다. 첫째, 다양한 파라미터 조합에 따른 다른 스테가노그래피의 특징에 대해 실험하여 강건성, 은닉성, 수용능력간의 trade-off에 대해 평가하여 최적의 파라미터 조합을 검증할 계획이다. 둘째, 데이터셋의 표본을 확대하여 실험에서 관찰된 비디오의 특징과 오류율을 정량적으로 분석하여 더욱 강건한 스테가노그래피 은닉통신에 대해 연구할 예정이다.

참고문헌

[1] Neil F. Johnson et al., "Exploring steganography: Seeing the unseen," computer 31.2, 2008.

[2] P Fan et al., "Robust video steganography for social media sharing based on principal component analysis," EURASIP Journal on Information Security 2022.1, 2022.

[3] RJ Mstafaet al., "A new video steganography scheme based on Shi-Tomasi corner detector," IEEE Access 8, 2020.

[4] Y Zhang et al., "Novel video steganography algorithm based on secret sharing and error-correcting code for H. 264/AVC," Tsinghua Science and Technology 22.2, 2017.

[5] B Kaliski. PKCS# 5: Password-based cryptography specification version 2.0. No. rfc2898, 2000.

[6] Y Nir et al., ChaCha20 and Poly1305 for IETF Protocols, No. rfc7539, 2015.

[7] A Shamir. "How to share a secret," Communications of the ACM 22.11, 1979.

[8] IS Reed et al., "Polynomial codes over certain finite fields," Journal of the society for industrial and applied mathematics 8.2, 1960.

[9] WK Pratt. Digital image processing. Wiley-interscience, 2007.

[10] B Chen et al., "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," IEEE Transactions on Information theory 47.4, 2002.