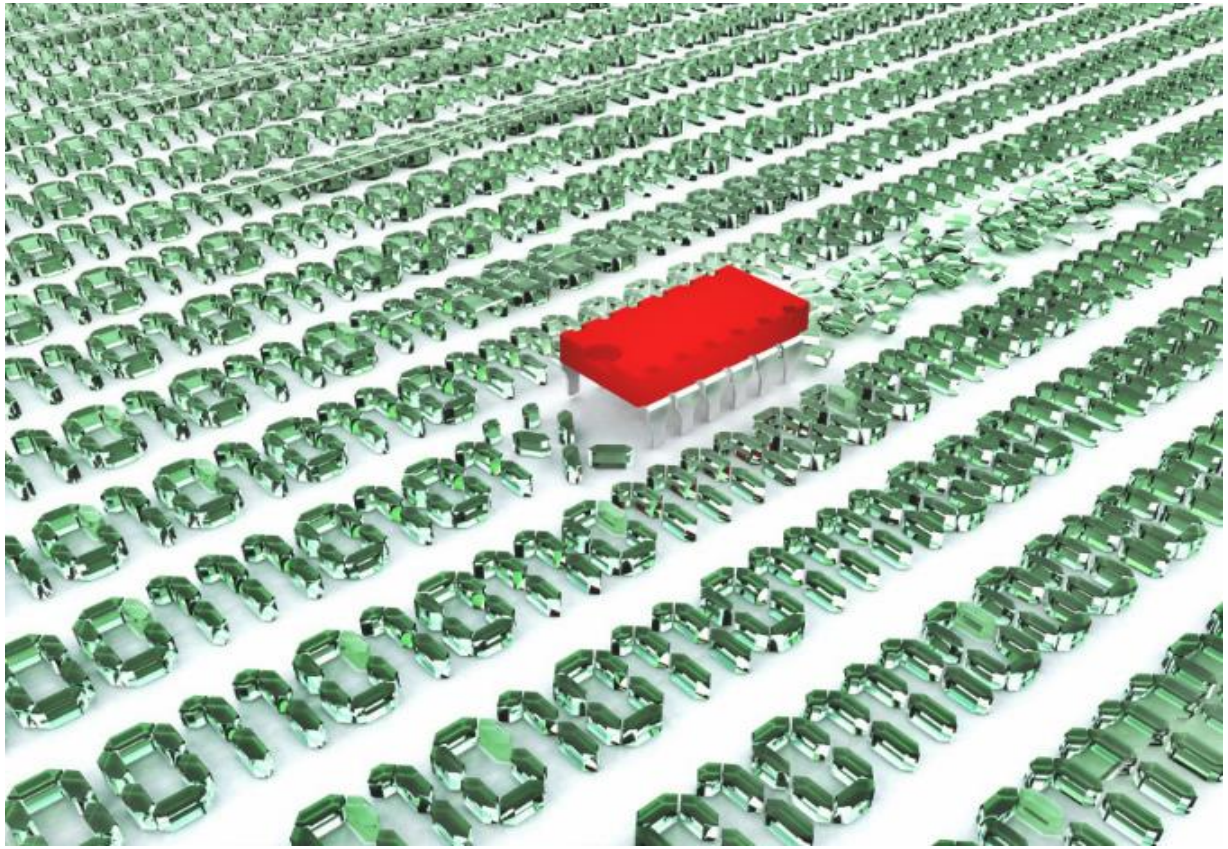
STEGANOGRAPHY

2019.07.08
Y.M.Jeon



스테가노그래피 (steganography)

1. 감추다 (stegos) + 글 (graphie)의 합성어
2. 스테가노그래피 파일은 두 파일로 구성
   - 비밀 메시지를 저장하고 있는 파일을 호스트 파일
   - 호스트 파일 안에 숨겨진 비밀 문서는 페이로드

1. 워터마킹 (*watermarking*)

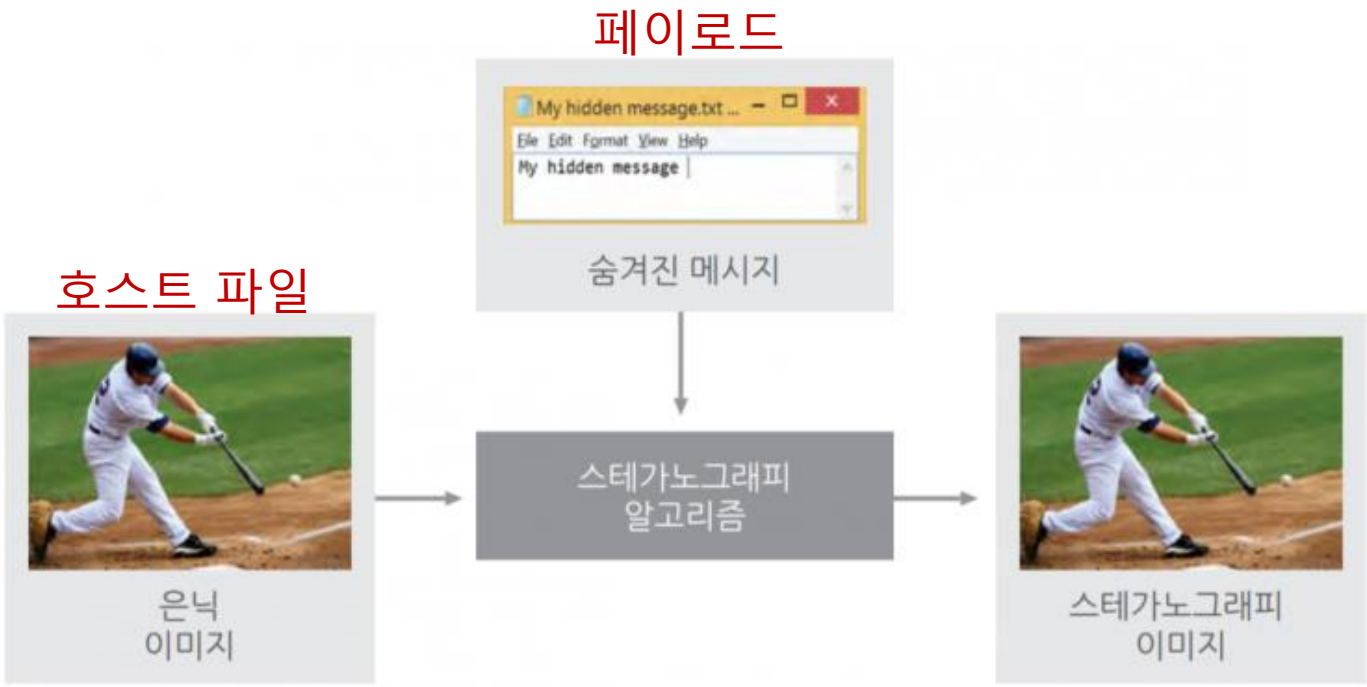
- 사진이나 동영상 같은 각종 디지털 데이터에 저작권 정보와 같은 비밀 정보를 삽입하여 관리하는 기술

2. 크립토그래피 (*cryptography*)

- 암호화 알고리즘을 작성하여 상대방이 이해할 수 없도록 메시지를 작성하고 그 안에 비밀을 삽입하는 기술

3. 스테가노그래피 (*steganography*)

- 정상적으로 보이는 객체 안에 메시지를 숨기는 기술



1. 호스트 파일의 유형에 따라 이미지, 오디오, 영상 파일로 나뉜다.

2. 동영상, 사진, 오디오 파일을 사용하는 이유는 파일에 상당한 양의 불필요한 데이터가 있기 때문이다.

3. 이러한 불필요한 데이터를 노이즈 (*noise*) 라고 한다.

4. 페이로드 파일은 꼭 텍스트 기반일 필요 없이 다양한 조합이 가능하다.

5. 삽입 기법과 수정 기법 2가지 기법으로 나뉜다.

1. 삽입 기법

- 파일 데이터를 변경하지 않고 추가 데이터를 파일 앞이나 뒤에 붙이는 방식으로 이미지에 영향을 주지 않는다.

2. 수정 기법

- 이미지 파일에서 Red, Green, Blue를 나타내는 RGB값의 최하위 비트(LSB)를 수정하는 기법

Steganography TOOL

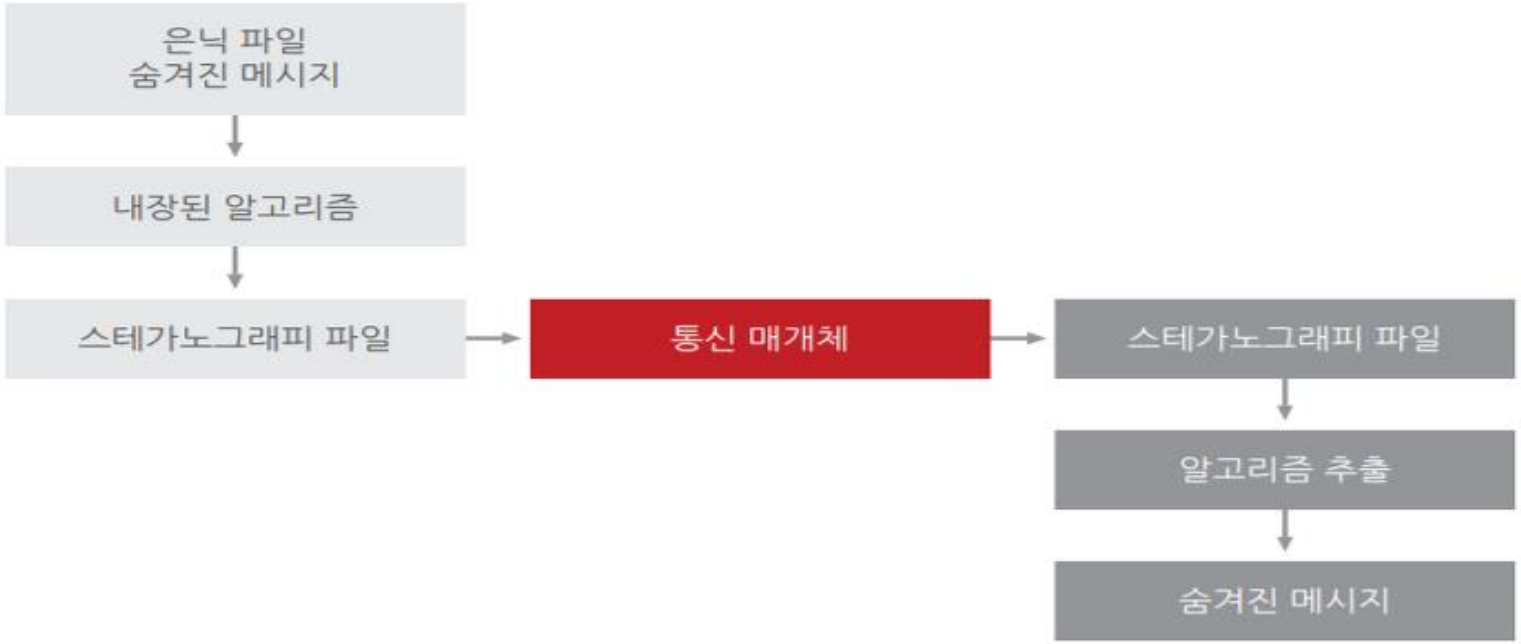
StegSpy : 파일에 숨겨진 파일이 있는지 탐지하는 도구

Openstego : 이미지 파일 안에 다른 파일을 숨기는 도구

Stegsolve : LSB를 이용한 이미지의 비밀 정보를 볼 수 있는 도구

Stegcracker : 이미지의 데이터를 숨길 때 사용된 암호 크랙 도구

MP3stego : MP3 파일에 정보를 숨기는 도구



분석 과정

1. 커버 파일을 헥스 파일분석기(*HxD , WinHex* 등)을 이용하여 분석

2. *StegSpy*를 이용하여 숨겨진 데이터 유무 판단

3. 이미지 파일이면 *StegSolve* 등의 도구를 사용하여 *LSB* 등을 시도

- 이미지 파일이 아니면 *binwalk*를 이용하여 파일 안에 숨겨진 파일이 있는지 분석

4. 숨겨진 데이터 추출

QnA