스테가노그래피 (steganography) 보안 기법과 그 한계의 극복방향

NewHeart

hahahia 진민화

2011. 12. 29

http://newheart.kr

목차

개요

사실 처음 스테가노그래피를 처음 접했을 때 그 전부터 파일안에 무언가를 숨기는게 없을까 하는 생각을 아주 예전부터 해왔는데 최근에 들어서 해킹대회를 통해 스테가노그래피라는 기법을 알게 되었고 과연 이 스테가노그래피가 어떠한 유래, 원리를 가지고 있는지 그리고 스테가노그래피가 가지고 있는 한계점을 찾아보고 그 한계점을 극복하기 위해서 어떠한 것들이 필요한지 분석을 해보았다. 그리고 이러한 분석을 통하여 대안의 기법을 연구해보는 취지에서 분석을 하였다. 또한 여러가지 제공되는 툴을 이용하여 어떠한 방식으로 파일이 이루어졌는지를 파악하는 작업을 하였다.

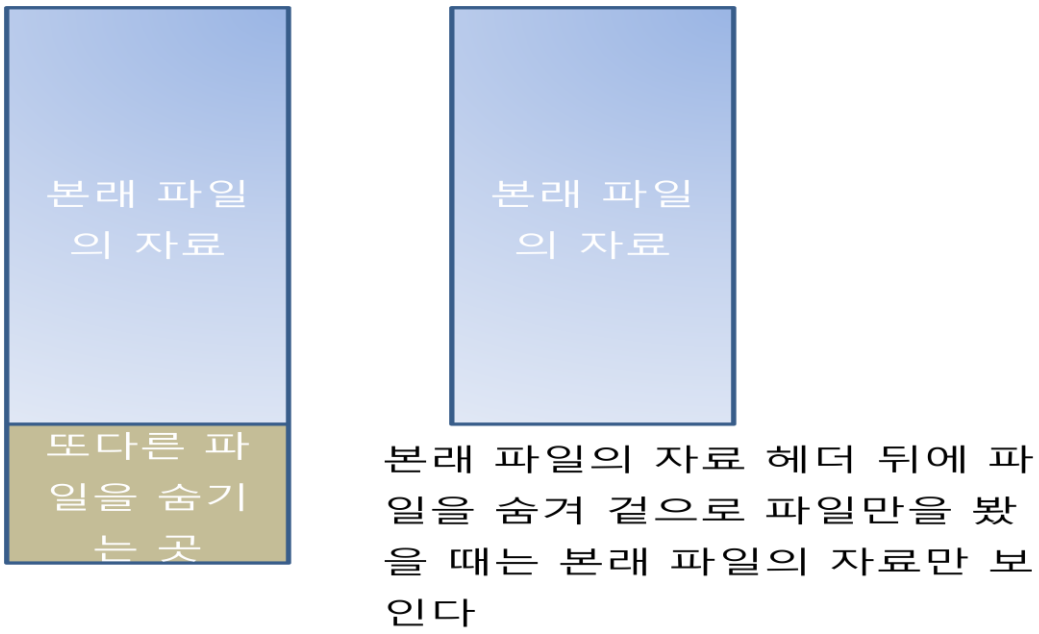
스테가노그래피의 유래

'스테가노그래피(steganography)'는 전달하려는 기밀 정보를 이미지 파일이나 MP3 파일 등에 암호화해 숨기는 심층암호 기술이다. 예를 들어 모나리자 이미지 파일이나 미국 국가 MP3 파일에 비행기 좌석 배치도나 운행 시간표 등의 정보를 암호화해 전달할 수 있다. 스테가노그래피(steganography)는 고대 그리스에서부터 이용되어온 것으로 현대 암호학에서 다루는 암호화(encryption)와는 다른 개념이다.
스테가노그래피의 유래는 기원전 5세기로 그리스의 왕 히스티에우스는 다이루스왕의 인질로 잡혀있었다. 그는 밀레투스에 있는 그의 양아들에게 밀서를 전달하는 방법으로 노예의 머리를 깎고서 그 머리에 메세지를 문신으로 썼다. 노예의 머리카락이 자라서 문신이 보이지 않게 되자 그는 노예를 밀레투스로 보냈다. 이것이 문서로 기록된 인류 최초의 Steganography다.

스테가노그래피 기법

스테가노그래피(steganography) 라고도 불리는 정보 은닉 (information hiding) 기법은 비밀정보를 임의의 커버이미지 (cover image) 에 숨겨 전송한다. 이 기법은 일반적으로 커

버이미지의 픽셀 (pixel) 값을 변경하여 다른 사람들이 비밀정보의 은닉 유무를 인지할 수 없도록 한다. 말 그대로 파일 안에 또 다른 파일을 숨기는 방식을 이용한다. 중요한 데이터를 숨겨서 전송하는 방법으로서 제3자가 보기에는 중요한 데이터가 아닌 일반 데이터를 전송하는 것처럼 보인다. 이렇게 해서 제3자에게 전송되는 데이터가 비밀데이터라는 사실을 숨길 수 있게 되어 암호화보다 더욱 안전한 것이다. 때로는 가장 단순한 것이 최상의 기술일 수 있다라는 말이 바로 이 스테가노그래피 기법에 걸 맞는 말이다.



스테가노그래피 기법을 통한 파일이 숨겨지는 과정을 나타냄.

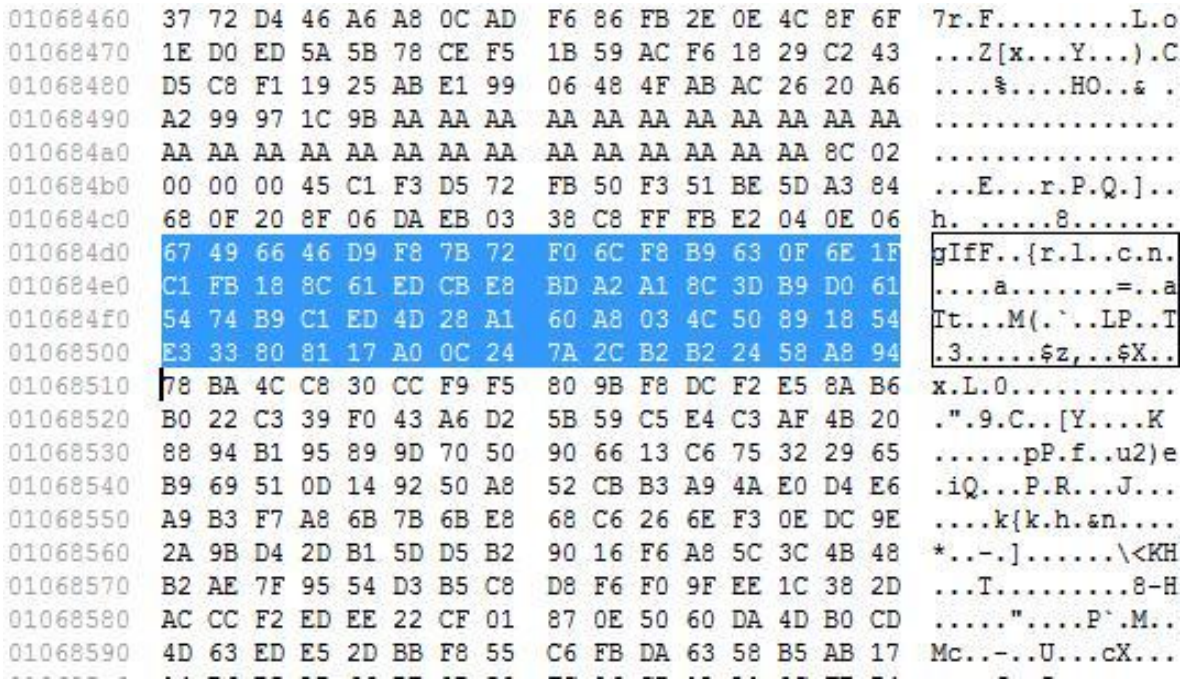
스테가노그래피를 활용할 수 있는 방향

기본적으로 스테가노그래피는 목적대로 중요한 데이터를 일반 데이터에 숨겨서(은닉) 안전하게 전송하는데 사용된다. 또한, 일반데이터의 저작권을 보호하기 위하여 사용되고 복제방지추적으로도 사용된다. 사실 이 스테가노그래피 기법은 테러리스트나 혹은 군대에서 중요 군사내용이나 비밀작전 등을 전송하는데 사용한다.
또한 스테가노그래피는 삽입되는 일반데이터의 저작권을 보호하기 위하여 사용된다. 이는 멀티미디어 데이터에 제작자의 중요 정보를 삽입하는 것이다. 제작자의 중요정보를 삽입함으로써 스테가노그래피가 설정된지를 모르는 제3자 멀티미디어 데이터를 변환하여 조작하였을 경우, 내부에 삽입된 데이터를 추출하여 진위여부를 파악 할 수 있다.
그리고 또한 이 스테가노그래피를 통해 악성코드를 다른 파일에 숨겨서 전송하는 기법을 통해 악성코드를 확장시킬 때도 사용되고, 실제로도 최근에 스파이 활동에서 이 스테가

노그래피 기법을 이용해 첩보활동을 하다가 적발된 경우도 있었다. 9.11 테러의 경우, 오사마 빈 라덴이 알 카에다 테러조직에게 비행기 도면 등을 전송할 때 모나리자 사진에 숨겨 메일로 전송한 것으로 알려져 있다. 또한 북한 지령으로 국내에서 간첩 활동을 벌인 혐의로 공안당국에 적발된 사례가 있는데 비밀 메시지를 스테가노그래피 기법을 통하여 전해져 활동한 것으로 알려져 있다.

스테가노그래피의 단점과 극복방향

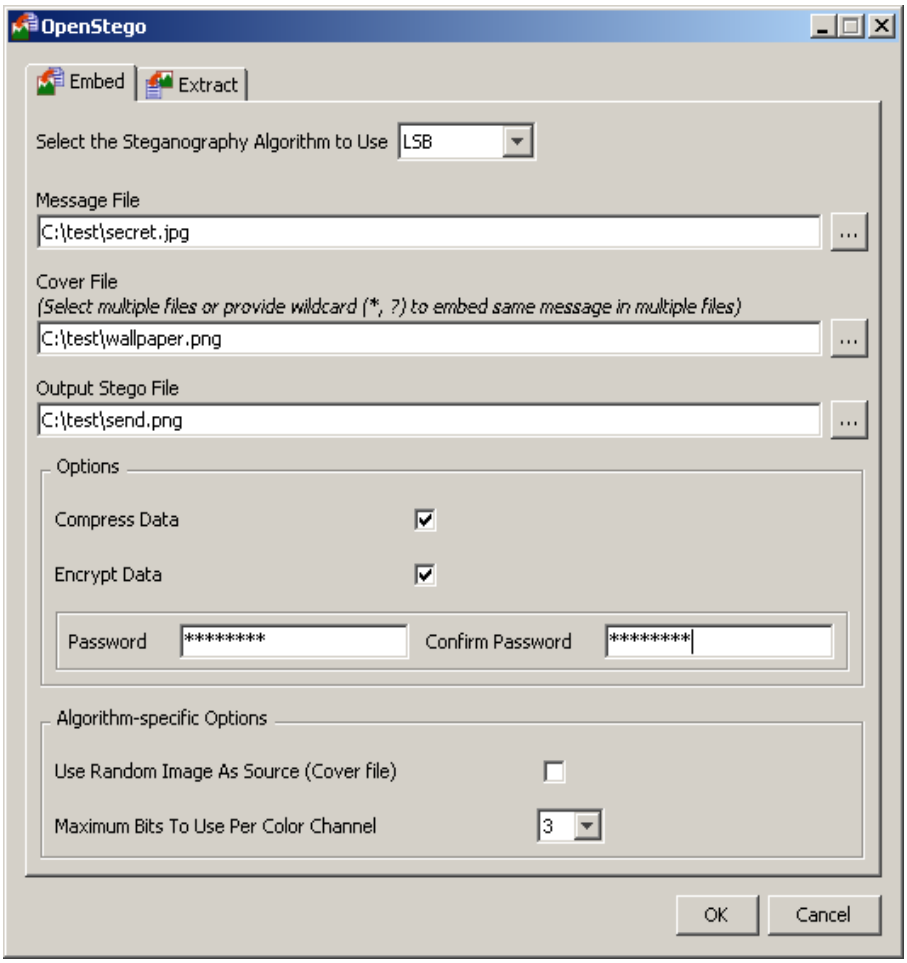
사실 스테가노그래피의 최대 단점이라고 할 수 있는 부분은 파일 안에 파일을 넣기 때문에 용량상에 부분에서 의심가는 부분이 당연히 생기기 마련이고 들키기가 쉽다는 단점이 있다. 그리고 또하나의 단점은 이 기법을 이용하여 파일을 숨기고자 했을 때 숨기려는 파일은 대부분 암호화가 되어있지 않기 때문에 바로 툴을 이용해서 파일을 뜯어낼 수가 있다. 그러면 이 스테가노그래피의 단점을 극복하기 위해서는 이 파일상의 용량을 줄이는 측면에서 최대한을 줄여 파일을 전송하는 방법이 가장 효과적일 것이다.
그렇다면 이러한 두가지의 단점을 극복하기 위해서는 먼저 첫번째로 보여지는 파일의 첫 부분과 은닉하려는 파일사이에 은닉하려는 파일의 헤더정보를 파악하고 은닉하려는 파일의 존재유무를 파악하게 되는데 이 부분에서 헤더 정보를 암호화를 시키는 것이다. 예를 들어



Hex로 mp3파일안에 또다른 gif그림파일을 은닉한 부분을 보여줌

현재 이 mp3파일에는 스테가노그래피 기법을 통해 gif형식의 그림파일이 있다. 지금 블

록설정한 부분이 파일의 형식(즉 확장자)를 나타내는 부분인데 이 부분을 통하여 또다른 gif형식의 파일이 존재할 수 있다는 점을 파악 할 수 있다. 하지만 이 부분만을 암호화를 시킬 수 있다면 실제로 Hex로 분석을 하더라도 본래 보여지는 파일 내부에 또 다른 gif 형식의 파일이 있다는 것을 숨길 수가 있을 것이다.
그리고 비밀정보의 양이 많을수록 커버이미지 픽셀 값들의 변화량 또한 증가하여 숨겨진 비밀정보는 쉽게 드러나게 된다. 이와 같은 취약점을 해결하기 위하여, 커버 이미지를 변화시키지 않은 대신 액자 (frame) 를 이용해 비밀 정보를 숨긴 후, 커버 이미지에 그 액자를 덧붙여 전송하는 새로운 이미지 스테가노그래피 기법을 생각해 볼 수가 있다. 제안한 기법은 사람들이 액자나 이모티콘 (emoticon) , 저작권 (copyright) 등을 이용해 사진을 꾸민 뒤 인터넷에 올리는 원리를 응용하여, 비밀 정보를 숨긴 액자를 커버 이미지에 장식하여 전송하는 방법을 이용하면 또 다른 대안책이 될 수 있다.
또한 OpenStego 사이트를 통하여 기존 파일에 대하여 비밀번호를 걸 수 있는 프로그램이 있어서 내부에 있는 파일을 확인하기 위해서는 사용자가 걸어놓은 비밀번호를 알아야 은닉한 파일을 볼 수 있게 하는 방안도 나와 있다.



OpenStego 프로그램을 통한 메시지 파일과 커버 파일 사이에 비밀번호를 설정하는 과정

reference

- 스테가노그래피 : 숨겨진 사이버세상의 진실을 찾다, 도경화, 전자정부포커스 제97호 (2004. 가을) pp.18-23
- http://news.donga.com/3/all/20110826/39812978/1 , 동아일보(북한 간첩이 메시지를 보낸기법(스테가노그래피)
- http://www.openstego.info/