**REPORT**



|  |  |
| --- | --- |
| **과목명** | 컴퓨터보안 |
| **학과** | 컴퓨터공학과 |
| **학번** | 12161658 |
| **이름** | 조재민 |
| **제출일자** | 2020.09.17 |

작업 환경:

* Macintosh 10.15.6에서 C++ 파일 작성 후, Windows 10에서 구동 확인.

파일 이름:

* 12161658.cpp, origin.bmp, stego.bmp

기본 로직:

24비트 Bmp파일의 구조는 최초 14 바이트의 비트맵 파일 헤더, 40 바이트의 비트맵 정보가 들어있고, 그 뒤로 각 3 Bytes (24 bits)크기의 RGB가 순차적으로 저장되어 있다. Steganography 기법을 사용하기 위해서는 최초 헤더 파일 54 바이트는 온전한 상태로 두고, RGB 각 3 Bytes 의 R, G, B 각각에 한 비트씩 글자를 숨기면 된다. 1 Byte의 R, G, B 각각 0 ~ 255의 값을 갖고있는데, Least significant bit (LSB)의 비트, 즉 색 변화에 가장 적은 영향을 줄 수 있는 만큼을 변경시켜 전체 사진을 보았을때 육안으로 변화가 생기지 않게 작업하였다.

앉아있는, 전화, 거리이(가) 표시된 사진

자동 생성된 설명Seekg함수를 이용하여 open 한 bmp파일 (origin.bmp) 파일의 가장 마지막으로 포인터를 옮긴 뒤, tellg 함수를 사용하여 해당 파일의 전체 크기를 계산한다. 파일 헤더와, 파일 인포는 #define으로 미리 14와 40의 크기를 지정해 두었다.

이러한 방식으로 실제 이미지 크기 즉 파일 사이즈 – 헤더 크기를 구할 수 있다.

실외, 텍스트, 스크린샷, 앉아있는이(가) 표시된 사진

자동 생성된 설명 입력받은 문자열의 크기만큼 반복문을 돌면서 8 비트씩 이동하며 버퍼에 각 마지막 LSB를 변경해주었다. 또한, ‘d’ 코멘드로 파일의 탐색을 할때 마지막 입력 위치를 알아내기 위하여 마지막 바이트에 공백을 추가해주는 연산을 해주었다.

실행 방법:

* 폴더 안에 컴파일된 exe파일과 origin.bmp 파일이 존재하여야한다.
* 명령 프롬포트를 켜고, exe파일과 origin.bmp 파일이 위치한 폴더로 이동한다.
* [filename].exe e 명령어 입력후 숨기고싶은 문자열 (엔터 전까지) 입력한다
* 폴더에 stego.bmp 파일이 생성된다.
* 명령 프롬포트에 [filename].exe d 명령어를 입력하면 stego.bmp파일에 숨겨진 문자열이 출력된다.

실행 방법) cmd창

스크린샷, 앉아있는, 테이블이(가) 표시된 사진

자동 생성된 설명

좌 origin.bmp, 우 stego.bmp 육안으로는 변경된게 보이지 않는다

스크린샷, 전자기기, 컴퓨터이(가) 표시된 사진

자동 생성된 설명