BEZPIECZEŃSTWO I OCHRONA DANYCH

Steganografia

Cel:

Celem ćwiczenia jest zapoznanie się z przykładami ukrywania informacji w sposób niejawny.

Steganografia (gr. "ukryte pismo") jest metodą ukrywania informacji za pomocą innej informacji. Od kryptografii różni się tym, że fakt przesyłania tajnej informacji jest niejawny. Celem kryptografii jest zaszyfrowanie tajnej wiadomości, natomiast celem steganografii jest ukrycie samego faktu istnienia tajnej wiadomości. Dzięki temu nauka ta może mieć zastosowanie tam gdzie istnieje potrzeba sekretnej komunikacji.

Zastosowanie:

W przeszłości przykładami metod steganograficznych były: atrament sympatyczny, mikrokropki w czasach II wojny światowej. Obecnie metody steganograficzne używa się do sekretnej komunikacji rządowej, wojskowej, w biznesie, przy ochronie praw autorskich - poprzez dołączanie znaków wodnych. Steganografia może być również używana przy komunikacji grup przestępczych, np. poprzez przesyłanie niewinnie wyglądających zdjęć z tajnymi informacjami w nich zawartymi. Podejrzewa się, że metody te wykorzystywane są również przy przemycaniu narkotyków i broni, czy przy defraudacji pieniędzy.

Przesłanie tajnych informacji odbywa się przy pomocy nośnika danych zwanych **kontenerem**. W steganografii cyfrowej najczęściej używa się do tego plików graficznych, tekstowych, dźwiękowych oraz video. Kontenerem mogą być jednak również fale radiowe, pliki komputerowe, pole elektromagnetyczne, pakiety TCP/IP, trójwymiarowe figury geometryczne czy gry komputerowe.

Metody:

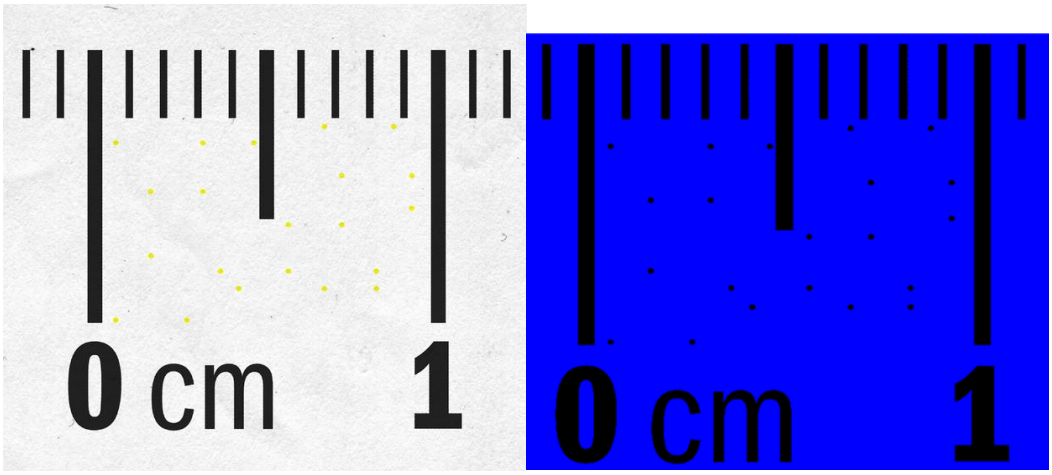
LSB (Least significant bit) - metoda najmniej znaczącego bitu.

Pliki audio, pliki video i pliki graficzne można zmodyfikować w taki sposób, że zmiany są niewidoczne dla ludzkiego oka i ucha, co wynika z niedoskonałości tych narządów. Przy wykorzystaniu metody LSB np. w przypadku plików graficznych w których stosowany jest 24-bitowy zapis kolorów, po 8 bitów dla 3 głównych składowych (red, green, blue) zmienia się umówioną ilość najmniej znaczących bitów (od prawej), na których ukrywamy tajną informację. Metodę tą można wykryć przy pomocy analizy histogramów, dlatego trzeba być ostrożnym przy wyborze ilości bitów, które podmieniamy. Podobnie można postąpić z plikami audio - zmiana najmniej znaczących bitów nie może być wykryta przy pomocy aparatu słuchowego.

Technika mikrokropek

Kolorowe drukarki umieszczają na wydruku dodatkowe żółte kropki o średnicy mniejszej niż milimetr, które są niewidoczne dla oka, a które można zobaczyć po odpowiedniej obróbce w programie graficznym. W takich kropkach zawierane są informacje o dacie i godzinie wydruku oraz numerze

seryjnym drukarki. Technikę mikrokropek stosuje się również metodą grawerowania laserowego m. in. w kasynach w celu zabezpieczenia przed podrabianiem żetonów, w motoryzacji znakując samochody, gdzie tysiące mikrokropek na powierzchni całego samochodu zawierają informację o numerach identyfikujących pojazd, są widoczne w nadfiolecie a ich całkowite usunięcie jest niemożliwe i jest zabezpieczeniem przy kradzieży samochodów.



Rysunek 1 Mikrokropki przy wydruku i te same widziane w kanale niebieskim w programie graficznym

Klasyfikacja:

Systemy steganograficzne dzielimy na:

1. **Steganografia czysta** - siła techniki opiera się na nieznajomości metody przez stronę atakującą. Systemy niepolecane ze względu na nie spełnianie zasady Kerckhoffsa ("System powinien być bezpieczny nawet wtedy, gdy wszystkie szczegóły jego działania - oprócz klucza - są znane")

2. **Steganografia z kluczem prywatnym** - metoda jest jawna, a strony komunikujące się używają klucza w sposób zależny od metody, istnieje problem przekazania klucza w bezpieczny sposób

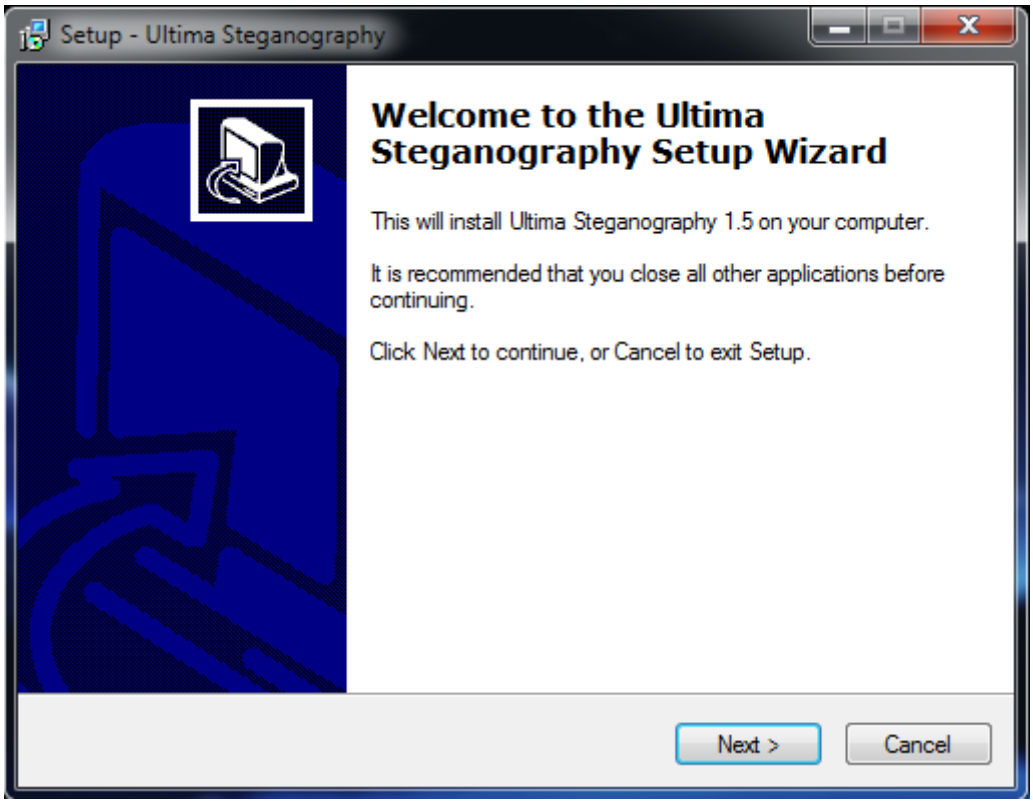
3. **Steganografia z kluczem publicznym** - używane są dwa klucze - publiczny i prywatny. Klucz publiczny, który jest jawny, wykorzystywany jest przy osadzeniu wiadomości w kontenerze, natomiast klucz prywatny przy jej wyodrębnianiu.

Rodzaje ataków na stegosystemy:

1. **Stego - only attack** - analityk dysponuje jedynie obrazem końcowym (kontenerem)
2. **Known cover attack** - atakujący ma dostęp do stegosystemu i oryginalnego kontenera
3. **Known message attack** - atakujący zna treść osadzonej informacji
4. **Chosen stego attack** - algorytm i stegosystemy są znane dla agresora

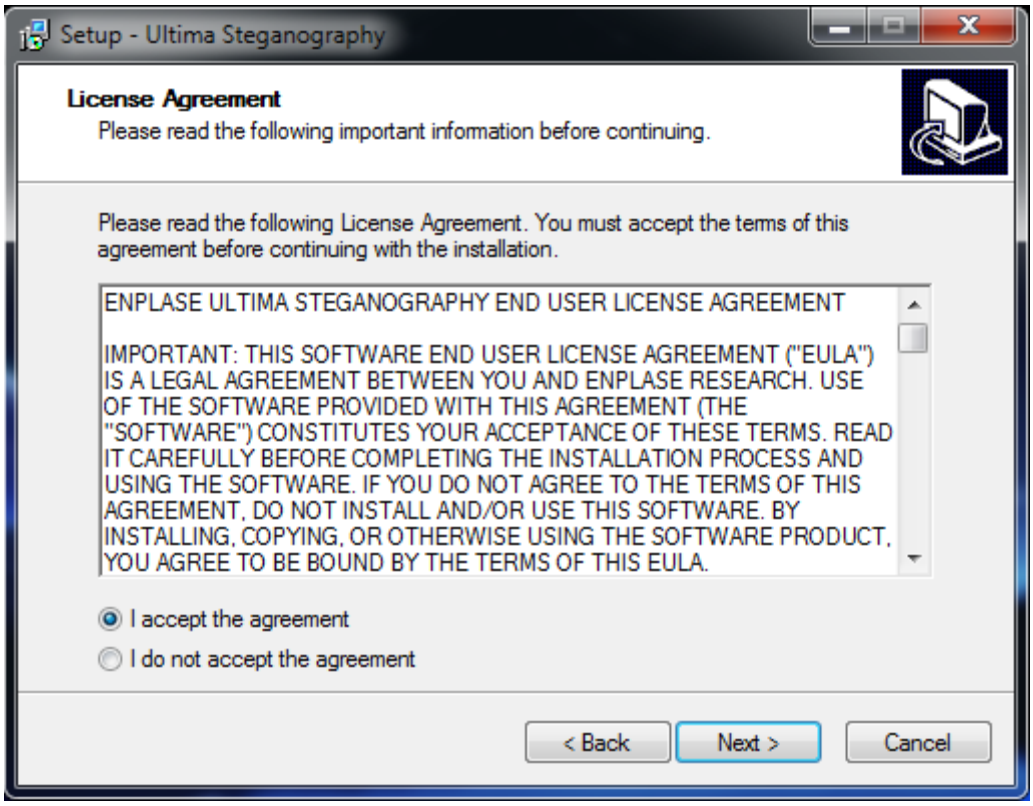
ĆWICZENIA

1. Zainstaluj program „Ultima Steganography”.

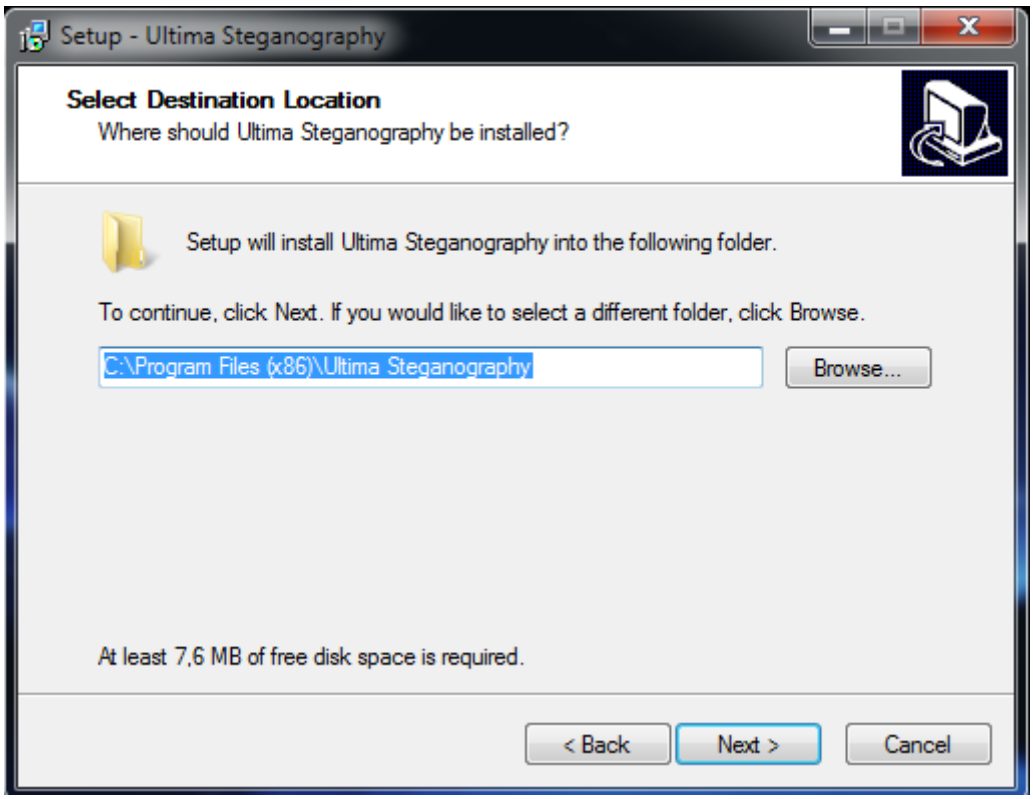


Po otworzeniu kreatora: Kliknij przycisk *Dalej*

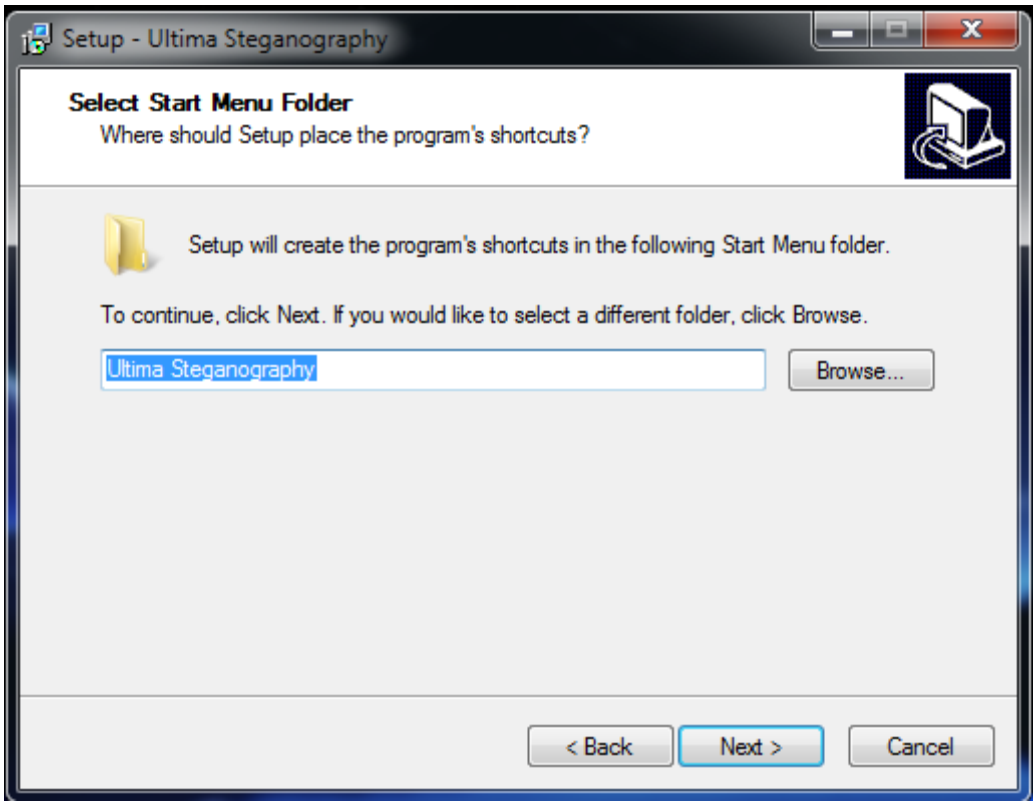
Otwiera się okno wyboru zadania:



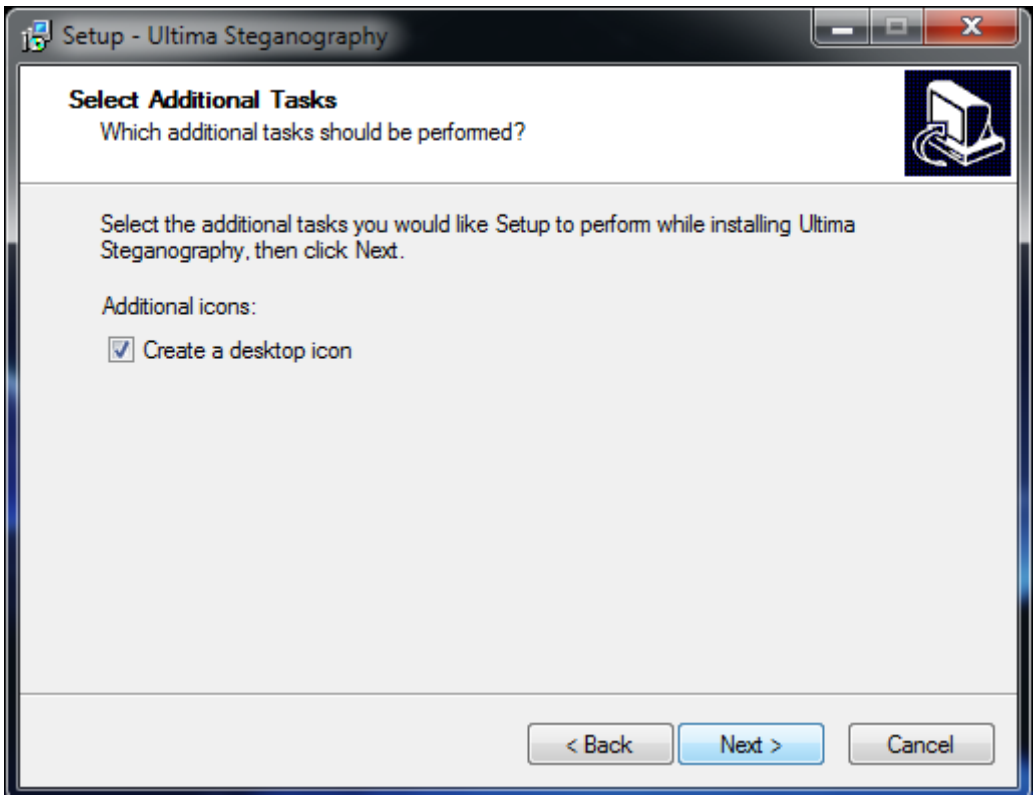
Akceptujemy Licencje i klikamy przycisk „Next”



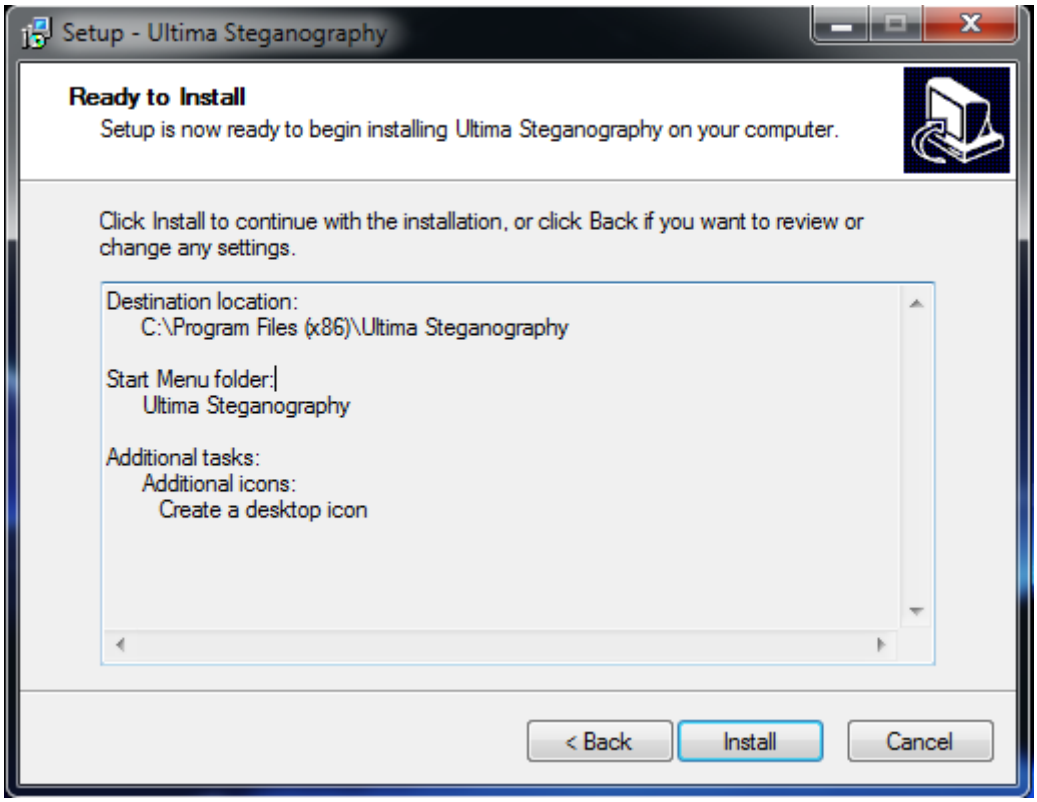
Określamy miejsce docelowe instalacji i klikamy przycisk „Next”



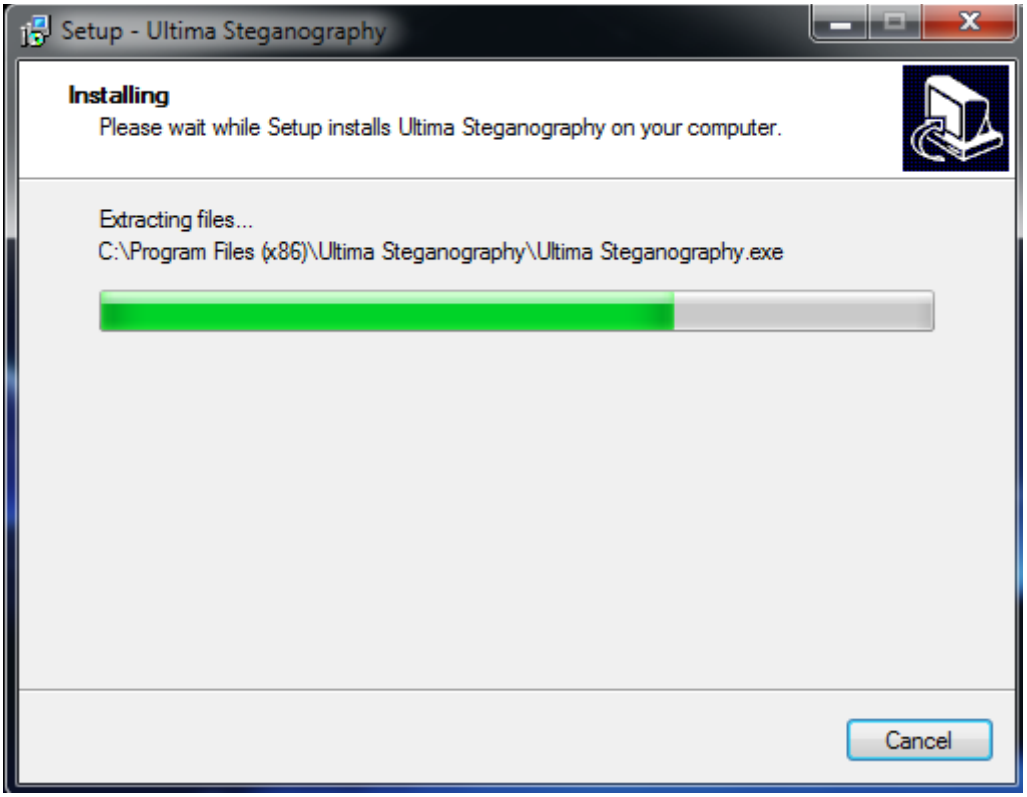
Możemy zmienić nazwę folderu wyświetlanego w menu „start”
Przechodzimy dalej klikając przycisk „Next”



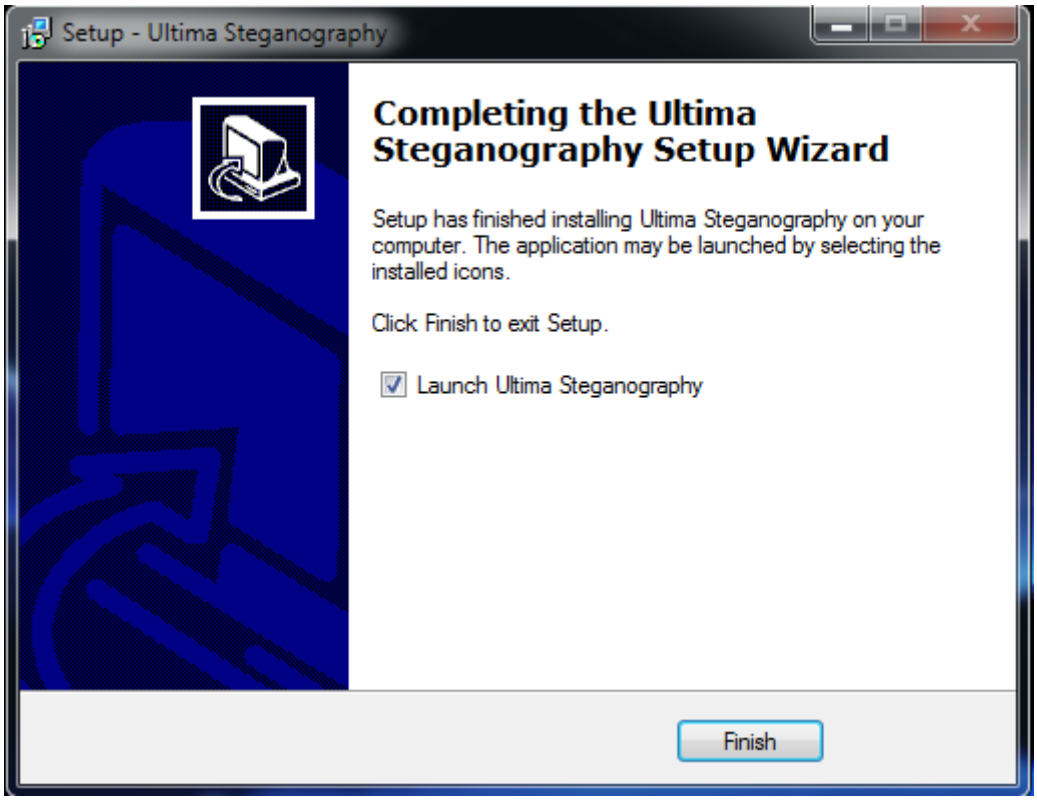
W kolejnym kroku upewniamy się że zostanie utworzony skrót na pulpicie i przechodzimy dalej klikając przycisk „Next”



Instalator podsumowuje zebrane informacje, jeżeli jesteśmy pewnie klikamy przycisk „Install”



Cierpliwie czekamy aż instalator zakończy swoją pracę



Po zakończonej instalacji klikamy przycisk „Finish” i uruchamiamy program

2. Obsługa programu :

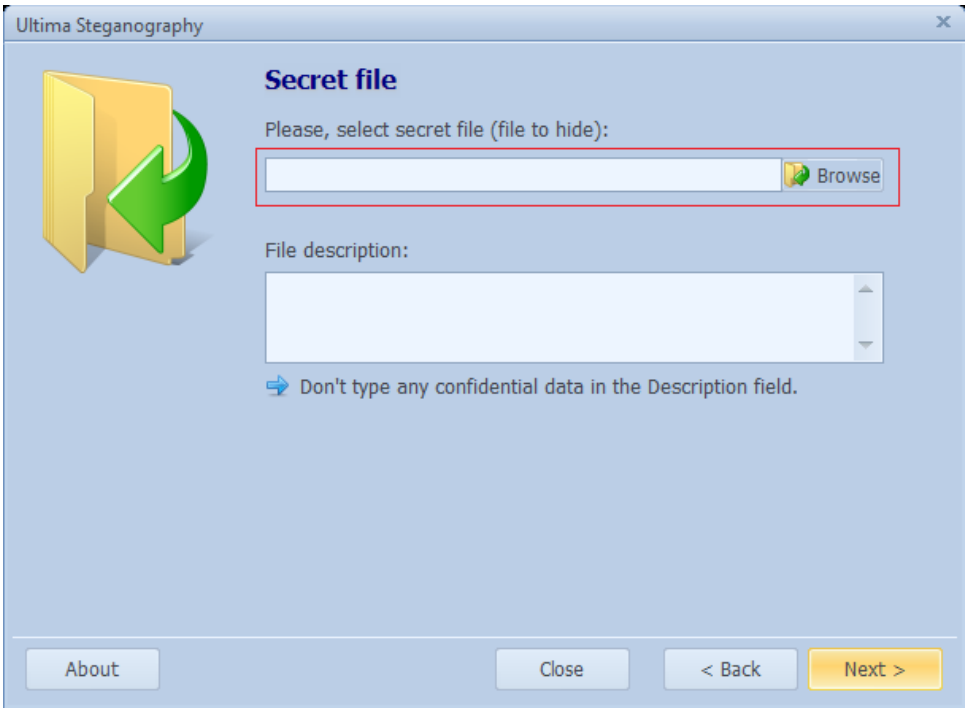
Po uruchomieniu programu ukazuje nam się okno:

Klikamy przycisk „Continue ustni the limited version”

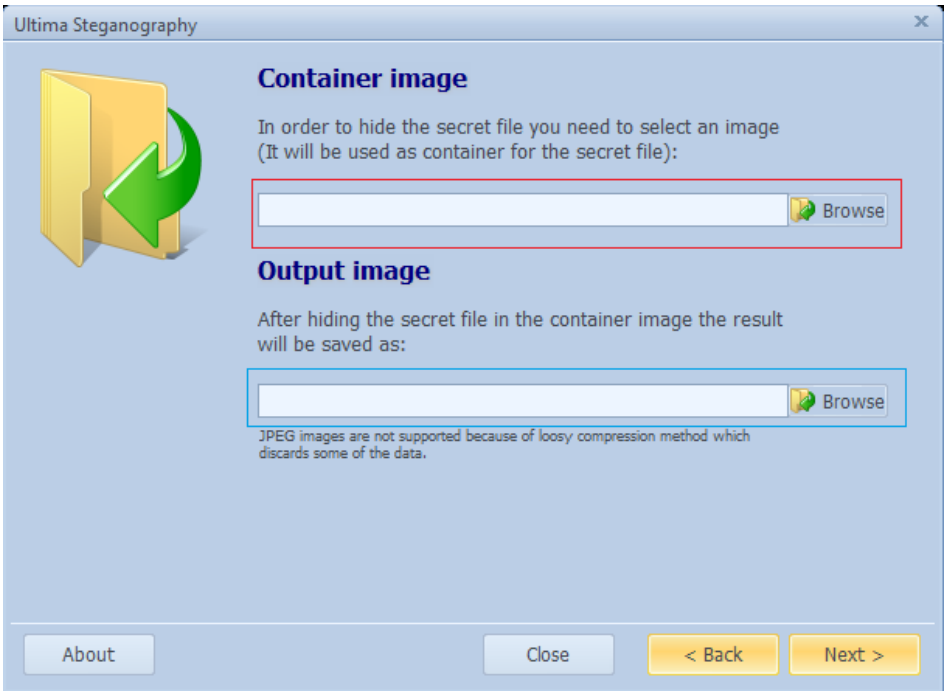
Pojawia się menu w którym mamy następujące opcje:

a) Hide a file In an image - opcja ta służy do ukrywania naszej informacji w obrazku.
b) Extract hidden file from an image – ta opcja służy do odzyskania ukrytej informacji.

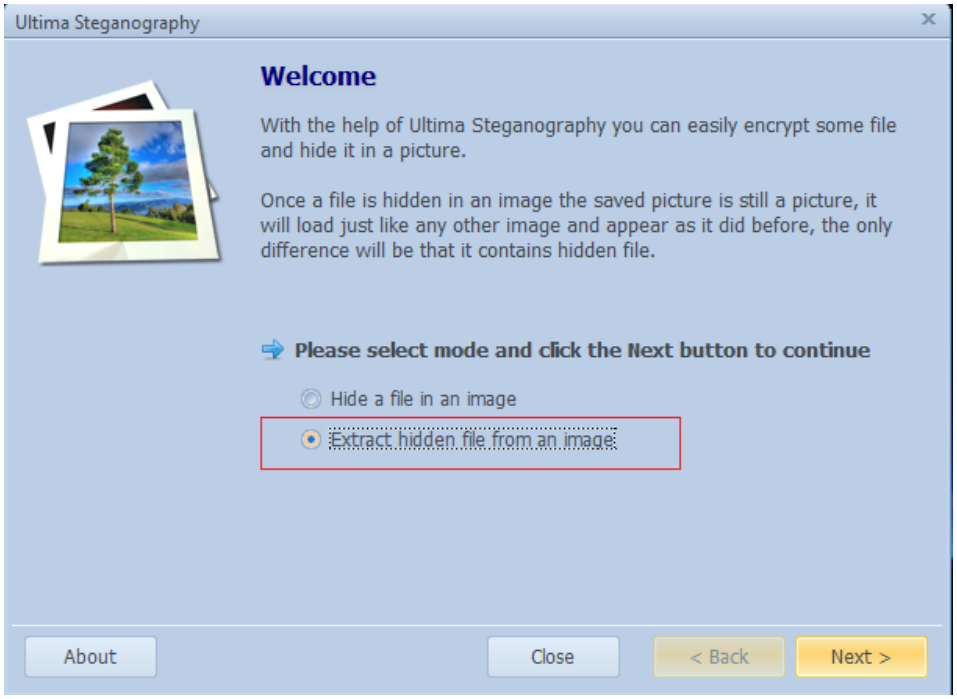
Zaznaczamy opcje a) i przechodzimy dalej klikając przycisk „Next”



W polu zaznaczonym czerwoną ramką wybieramy plik który chcemy ukryć, w folderze „Przykład 1” znajduje się przykładowy obraz „ukrywany” z którego możemy skorzystać.



W polu oznaczonym czerwoną ramką wybieramy plik który będzie „kontynerem" przechowującym nasz ukryty obrazek, możemy wybrać plik „transportowy" który znajduje się w folderze „Przykład 1". Natomiast w polu oznaczonym niebieską ramką wybieramy miejsce zapisu u nazwę pliku wyjściowego. Po poprawnym wybraniu plików otrzymujemy plik w którym jest ukryty nasz sekretny obrazek.



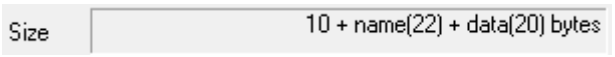
Możemy odzyskać nasz ukryty plik uruchamiając ponownie program i w menu wybierając tym razem opcje „Extract hidden file from an image" i podając scieżkę dostępu to pliku wyjściowego.

Open Puff 4.0

Ukrywanie danych

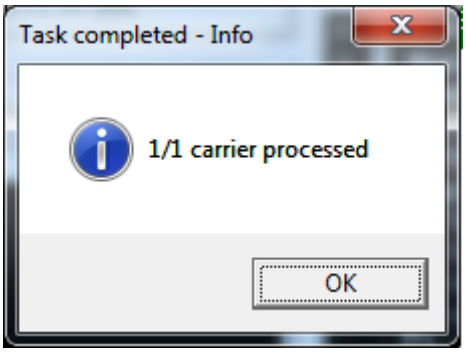
1. Otwórz program Open Puff (OpenPuff.exe) znajdujący się na dysku i przejdź do punktu 3. Jeśli programu nie ma na dysku pobierz program ze strony http://embeddedsw.net/OpenPuff_Steganography_Home_pl.html
2. Rozpakuj pobrany plik zip w dowolnej lokalizacji, program jest gotowy do użytku.
3. Po uruchomieniu aplikacji, w sekcji „steganography" kliknij przycisk „Hide".
4. W sekcji „(1) Insert 3 uncorrelated data passwords (Min:8, Max: 32)"
   a) w polu Cryptography (A) wpisz hasło: P@ssw0rd
   b) w polu Crptography (B) wpisz hasło: qwertyui
   c) w polu Scrambling (C) wpisz hasło: Steganografia
   Program zabezpiecza się przed wzajemnym zbyt dużym podobieństwem hasłem, przy pomocy obliczania odległości Hamminga, jeśli wartość pola „Password check" jest podświetlona na zielono to znaczy że wszystko jest w porządku

5. W dowolnym miejscu na dysku utwórz plik „Ukrywana_wiadomosc.txt", napisz w nim swoje imię i nazwisko oraz numer grupy. Zapisz i zamknij plik.
6. W sekcji „(2) Data (Max: 256 Mb)" kliknij „Browse" i wybierz plik który utworzyłeś w punkcie 5. Program poinformuje cię o rozmiarze pliku który wybrałeś



7. W sekcji „(3) Carrier selection [Order sensitive]" kliknij "Add" I wybierz dowolny plik w formacie png. Gdy dodasz plik, program poinformuję cię ile miejsca można użyć do ukrywania informacji, oraz ile miejsca zostanie wykorzystane.

8. Jeśli liczba dostępnego miejsca (Selected) jest mniejsza od liczby potrzebnego miejsca do zakodowania informacji (Total) należy wybrać kolejny plik .
9. W sekcji „(4) Bit selection options" rozwiń opcję, znajdujące się po lewej stronie napisu „Png (Image)" i wybierz opcję „1/5 (20%) – Medium"
10. Kliknij przycisk „Hide Data!" i wybierz docelową lokalizację aby ukryć dane. Jeśli dane zostały ukryte, program nas o tym poinformuje.



11. Zamknij program.

Wyodrębnianie danych

1. Otwórz program Open Puff znajdujący się na dysku.
2. Po uruchomieniu aplikacji, w sekcji „steganography" kliknij przycisk „Unhide".
3. W sekcji „(1) Insert 3 uncorrelated data passwords (Min:8, Max: 32)"
   a) w polu Cryptography (A) wpisz hasło: P@ssw0rd
   b) w polu Crptography (B) wpisz hasło: qwertyui
   c) w polu Scrambling (C) wpisz hasło: Steganografia
   UWAGA! Podane hasła muszą być identyczne do tych, które były użyte przy ukrywaniu informacji"
   Program zabezpiecza się przed wzajemnym zbyt dużym podobieństwem hasłem, przy pomocy obliczania odległości Hamminga, jeśli wartość pola „Password check" jest podświetlona na zielono to znaczy że wszystko jest w porządku

4. W sekcji „(2) Carrier selection [Order sensitive]" kliknij "Add Carriers" I wybierz plik w którym są ukryte informacje. Program poinformuje nas o maksymalnym rozmiarze danych ukrytym w wybranym plik.

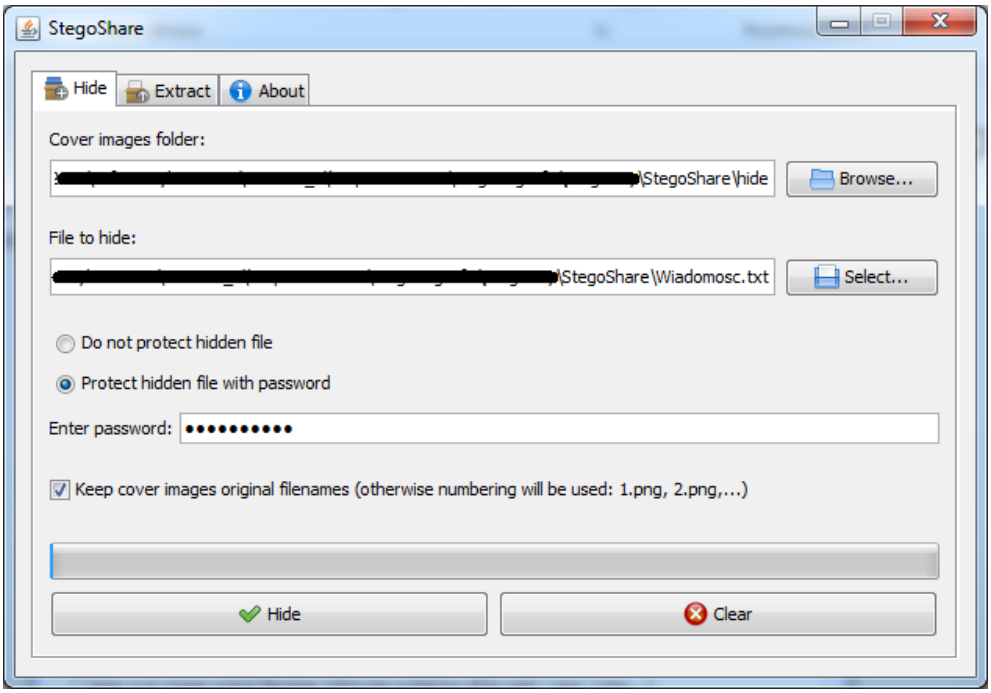
5. W sekcji „(3) Bit selection options" wybierz format pliku oraz liczbę bitów na których są ukryte informacje. W naszym przypadku format pliku to png a liczba bitów to „1/5 (20%) – Medium".
6. Kliknij „Unhide" i wybierz lokalizację zapisu ukrytej informacji która zostanie wyodrębniona. Program wyświetli nam raport, klikamy „Done"
7. Program utworzył nam w wybranej lokalizacji plik „Ukrywana_wiadomosc.txt"

- **Zadanie**: Przy pomocy innego (dostępnego) formatu pliku ukryj inną wiadomość i przekaż ją do kolegi. Spróbuj przy użyciu tego programu ukryć obraz w innym obrazie.
  Gdy otrzymasz wiadomość od kolegi, wyodrębnij z niej zapisane informacje.
  Wskazówka Możesz używać dowolnych haseł, które spełnią wymagania stawiane przez program.
  Program może ukrywać dane w plikach o następujących orzszerzeniach: 3gpp, Aiff, Bitmap, Flv, Jpeg(jpg), Mp3, Mp4, Mpg, Next/Sun, Pcx, Pdf, Png, Swf, Tga, Vob, Wave.

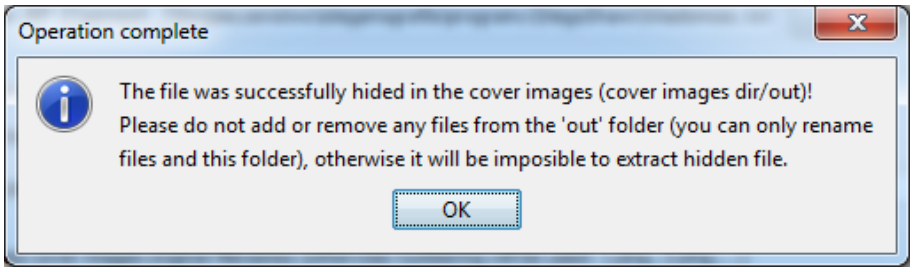
StegoShare

Ukrywanie danych

1. Otwórz program StegoShare (StegoShare.jar) znajdujący się na dysku. Jeśli programu nie ma na dysku pobierz go ze strony http://stegoshare.sourceforge.net/download.html
2. Ściągnij dowolny plik graficzny/pliki graficzne o rozszerzeniu png lub jpg, które posłużą jako kontener informacji.
3. Po uruchomieniu aplikacji, w zakładce „Hide" naciśnij „Browse" i wybierz folder w którym znajdują się pliki pobrane w poprzednim punkcie. Będą to nasze nośniki danych.
4. W dowolnym miejscu na dysku (oprócz lokalizacji podanej w 3. Punkcie) utwórz plik „Ukrywana_wiadomosc.txt", napisz w nim swoje imię i nazwisko oraz numer grupy. Zapisz i zamknij plik.
5. W zakładce „Hide" naciśnij „Select" i wybierz plik utworzony w poprzednim punkcie.
6. Zaznacz opcję „Protect hidden file with password".
7. W polu "Enter password" wpisz: P@ssw0rd
8. Zaznacz opcję „Keep cover images original filenames…". Tak mniej więcej wygląda obraz programu przed wykonaniem następnego kroku:



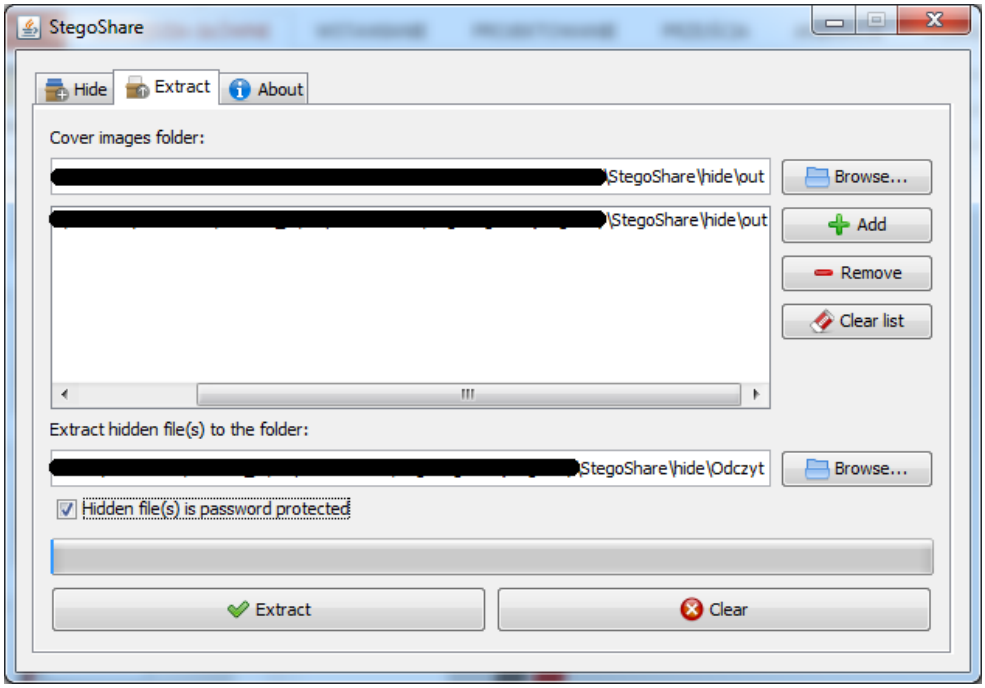
9. Naciśnij przycisk "Hide". Gdy program pomyślnie zakończy ukrywanie informacji w kontenerze, pokaże nam się komunikat:



10. Jeśli program wyrzuci komunikat błędu, będzie to prawdopodobnie spowodowane złym formatem plików kontenera, lub niewystarczającą ich ilością. W takim przypadku, napraw ten błąd, poprzez zmianę plików kontenera.
11. Zamknij program.
12. Pliki z ukrytym plikiem graficznym znajdują się w folderze „out” w lokalizacji którą wskazaliśmy w punkcie 3.

Wyodrębnianie danych

1. Otwórz program StegoShare znajdujący się na dysku.
2. Po uruchomieniu aplikacji, w zakładce „Extract” naciśnij „Browse” i wybierz folder w którym znajdują się pliki z ukrytymi danymi.
3. Naciśnij przycisk „Add”.
4. Poniżej napisu „Extract hidden file(s) to the folder:” naciśnij „Browse” i wybierz lokalizację w której zostanie zapisana wyodrębniona wiadomość.
5. Zaznacz opcję „Hidden file(s) is password protected” (Jeśli przesyłana informacji nie była chroniona hasłem, nie zaznaczaj tej opcji). Wygląd programu przed przejściem do kolejnego kroku:



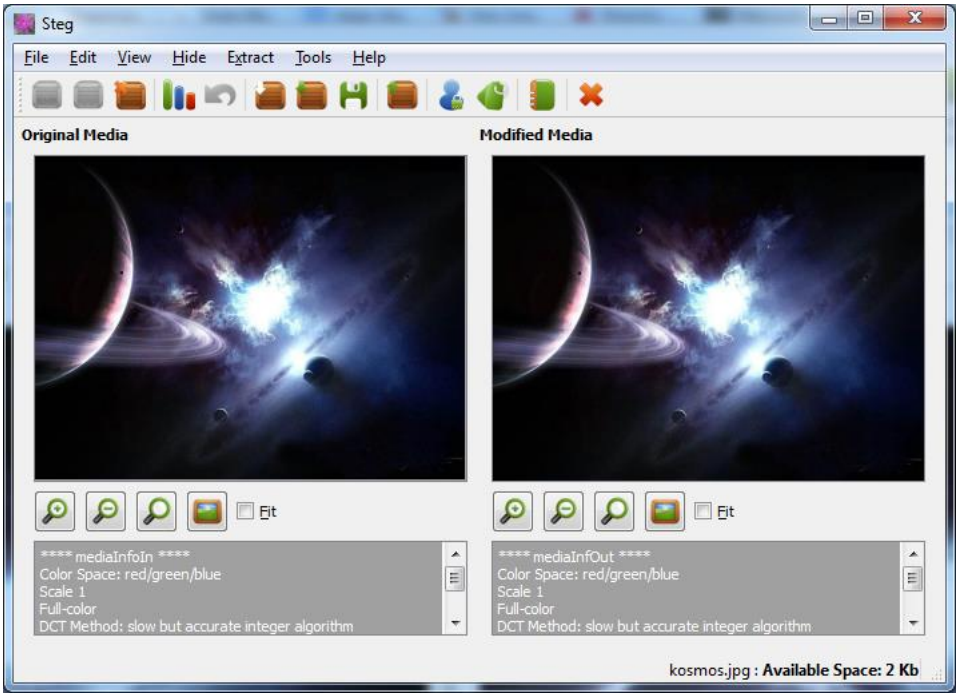
6. Naciśnij „Extract”.

7. Pojawi się nowe okno. Wpisz hasło: P@ssw0rd
8. W lokalizacji wskazanej w punkcie 4. Została wyodrębniona wiadomość ukryta w nośniku.
9. Zamknij program.

STEG

Ukrywanie danych

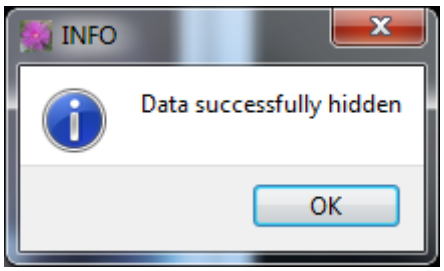
1. Otwórz program Steg (steg.exe) znajdujący się na dysku i przejdź do punktu 3. Jeśli programu nie ma na dysku pobierz go ze strony http://steg.drupalgardens.com/stegdownload
2. Rozpakuj pobrany plik zip w dowolnej lokalizacji, program jest gotowy do użytku.
3. Po uruchomieniu programu wybierz „File->Open JPEG image”.
4. Wybierz plik z dysku o rozszerzeniu .jpg który będzie kontenerem danych. Okno programu będzie wyglądało mniej więcej w ten sposób:



W sekcji „Original Media” widzimy oryginalny obraz wraz z podstawowymi informacjami. W sekcji „Modified Media” widzimy obraz, który posiada w sobie ukrytą wiadomość (o ile już ją ukryliśmy). Dzięki temu możemy porównać stary jakości obrazu.

5. W dowolnym miejscu na dysku utwórz plik „Ukrywana_wiadomosc.txt”, napisz w nim swoje imię i nazwisko oraz numer grupy. Zapisz i zamknij plik.
6. W programie Steg wybierz „Tools->RSA key-pair generator”.
7. W nowo otwartym oknie wybierz lokalizację w której zostanie zapisana para klucz: Twój klucz publiczny i Twój klucz prywatny.
8. Wyślij swój klucz publiczny do odbiorcy ukrywanej wiadomości.
9. W programie Steg wybierz „Edit->Configuration…”
10. W zakładce „Common Options” zaznacz opcję „Embed a text massege”.
11. W polu poniżej wpisz “Gratuluje poprawnego odczytania wiadomości”.
12. W „Crypto Mode” wybierz „Asymmetric Signed (hide or extract)”.
13. W polu „Public Key” naciśnij „…” i wskaż klucz publiczny odbiorcy.

14. W polu „Private Key” naciśnij „…” i wskaż swój klucz prywatny.
15. W zakładce „Special Options” zaznacz wszystkie możliwe opcje.
16. Dla wszystkich opcji „Use component” ustaw wartość 1.
17. Naciśnij „OK”.
18. Wybierz „Hide -> Hide Noise” i porównaj straty w jakości obrazu. (Polecenie Hide Noise służy do wypełnienia dostępnego miejsca przykładowymi danymi).
19. Wybierz „Edit -> Revert”.
20. Wybierz „Hide->Hide Data”.
21. Wybierz lokalizację pliku utworzonego w punkcie 5. Po udanym ukryciu danych, program nas o tym poinformuje:

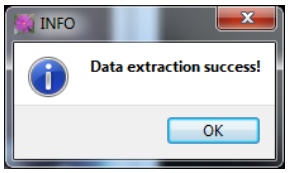


22. Naciśnij „Ok” i w programie wybierz „Hide -> Save”. Wybierz lokalizację gdzie zostanie zapisany zmodyfikowany obraz z ukrytym plikiem tekstowym.
23. Wyślij utworzony plik w punkcie 22 do odbiorcy
24. Zamknij program.

Wyodrębnianie danych

Założenie: Przed przystąpieniem do wyodrębniania danych, powinieneś utworzyć parę kluczy RSA. Zostało to opisane w punktach 6-7 w paragrafie „Ukrywanie danych”. Twój klucz publiczny powinien posłużyć do realizacji punktu 13. tamtego paragrafu.

1. Otwórz program Steg znajdujący się na dysku.
2. Po uruchomieniu programu wybierz „File->Open JPEG image”. Wybierz plik który ma w sobie ukryte dane.
3. Wybierz „Edit -> Configuration..”.
4. W zakładce „Common options” w polu „Crypto Mode” wybierz „Asymmetric Signed (hide or extract)”.
5. W polu „Public Key” naciśnij „…” i wskaż klucz publiczny nadawcy.
6. W polu „Private Key” naciśnij „…” i wskaż swój klucz prywatny.
7. W zakładce „Special Options” zaznacz wszystkie możliwe opcje.
8. Dla wszystkich opcji „Use component” ustaw wartość 1.
9. Naciśnij „OK”.
10. Wybierz „Extract -> Extract Data..” i określ lokalizację w której chcesz zapisać ukryte dane. Gdy wszystko przebiegło pomyślnie, program nas o tym poinformuje:



11. W lokalizacji wskazanej w punkcie 10. Zostaną utworzone 4 pliki. W pliku „Ukrywana_wiadomosc.txt” jest imię i nazwisko nadawcy, w pliku „Ukrywana_wiadomosc.txt.txt” jest wiadomość dołączona w punktach 10-11 sekcji „Ukrywanie danych”.
12. Zamknij program.

Zadanie: Spróbuj, przy użyciu programu Steg, ukryć dane zaszyfrowane symetrycznie. (**Podpowiedź:** do tego potrzebne będę jedynie klucze publiczne)
Zadanie: Spróbuj, przy użyciu programu Steg, ukryć dane zaszyfrowane asymetrycznie bez podpisu. (**Podpowiedź:** Aby ukryć dane wystarczy nam klucz publiczny odbiorcy. Przy wyodrębnianiu danych potrzebujemy nasz klucz prywatny).