LABORATORIUM
PODSTAW KRYPTOGRAFII I STEGANOGRAFII

STEGANOGRAFIA

Wstęp

Zabezpieczenie informacji przy pomocy metod kryptograficznych jest obecnie standardem. Jednak gwałtowny wzrost mocy obliczeniowej i możliwości jakie może wnieść pojawienie się komputerów kwantowych stawiają pod znakiem zapytania przyszłość metod kryptograficznych. Rozwiązanie wielu problemów niesie steganografia. Steganografia jest nauka zajmującą się ochroną cennej informacji poprzez jej ukrycie w innej nie mającej wartości. W tabeli XX przedstawiono porównanie podstawowych właściwości i możliwości kryptografii i steganografii.

	Kryptografia	Steganografia
Przekształcenie informacji do postaci niezrozumiałej dla osób postronnych	tak	tak
Ukrycie informacji	nie	tak
Użycie klucza	tak	tak
Ukrycie fakty komunikacji	nie	tak
Zapewnienie anonimowości komunikujących się stron	nie	tak
Ilość przesyłanych informacji w procesie komunikacji	Porównywalna do ilości szyfrowanej informacji	Dużo większa od ilości szyfrowanej informacji
Potrzebny dodatkowy nośnik	nie	tak

Tabela XX. Porównanie podstawowych właściwości kryptografii i steganografii.

Steganografia tradycyjna

Projekt Absolwent na miarę czasu współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego;
Nr umowy UDA-POKL.04.01.01-00-421/10-01

Zanim nastąpił gwałtowny rozwój techniki cyfrowej, większość informacji była przekazywana analogowo. Najczęściej stosowanym nośnikiem był papier. Zadaniem steganografii tradycyjnej było ukrycie przekazu na takich nośnikach. Przykładami steganografii tradycyjnej są:

- Tatuowanie na skórze głowy (po odrośnięciu włosów tatuaż nie był widoczny).
- Pisanie ukrytego przekazu na glinianych tabliczkach, które następnie pokrywane były woskiem i zapisywane powtórnie innym nic nie znaczącym tekstem.
- Użycie atramentu sympatycznego, czyli cieczy, która nie pozostawiała śladów na papierze w momencie pisania, lecz była widoczna dopiero po wykonaniu pewnej określonej reakcji. Atrament sympatyczny dobierano w każdym rejonie świata niezależnie w zależności od dostępności. I tak w Chinach było to mleko, w Egipcie sok z cytryny (obie te ciecze ukazują się po podgrzaniu) lub też inne związki chemiczne.
- Jednym z najlepszych rozwiązań w tej dziedzinie była technika mikrokropek stosowana przez Niemców w czasie II Wojny Światowej. Polegała ona na pomniejszaniu zdjęcia do rozmiarów ok ½ x ½ milimetra czyli wielkości kropki w tekście drukowanym. Tak spreparowane zdjęcie wklejano w liście w miejscu kropki. Metoda ta dawała możliwość ukrycia dużej ilości informacji i jednocześnie była trudna do wykrycia. Z tych względów stosowana była powszechnie przez wywiad Niemiecki.
- Obecnym przykładem analogowych znaków wodnych jest znakowanie wodne banknotów.

Inne metody opierają się zwykle na ukrywaniu informacji w tekście pisanym. Polegają na umieszczaniu słów czy też znaków w odpowiednich miejscach tekstu, tak aby dobrze wkomponowywały się w treść dokumentu a jednocześnie pozwalały na jednoznaczne odczytanie wiadomości. Doskonałym przykładem jest samo wyjaśniający się akrostych. Pierwsze słowa kolejnych linijek po ułożeniu ich kolejno po sobie ułożą się w zdanie.

```
He must have had a special trick, said Robert K. Merton, for he
wrote such an amazing quantity of material that his friends were
simply astonished at his prodigious output of long manuscripts,
the contents of which were remarkable and fascinating, from the
first simple lines, over fluently written pages where word after
word flowed relentlessly onward, where ideas tumbled in a riot
of colorful and creative imagery, to ends that stopped abruptly,
```


Projekt Absolwent na miarę czasu współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego;
Nr umowy UDA-POKL.04.01.01-00-421/10-01

```
each script more curiously charming than its predecessors, each

line more whimsically apposite, yet unexpected.
```

Oczywiście stosowano nie tylko pierwsze słowa poszczególnych linijek do ukrycia informacji. Często były to pierwsze lub drugie litery wybranych słów, różnej wielkości odstępy w tekście (pojedyncza spacja to binarne zero, podwójna to binarna jedynka) czy też użycie innych białych znaków. Warto również wspomnieć o technice nakłuwania liter w tekście. Nakłuciami oznaczano kolejne litery tajnego przekazu. Wiadomość taka mogła być z łatwością odczytana „pod światło", gdyż wówczas nakłucia były doskonale widoczne. W innej pozycji odczytanie wiadomości nie było możliwe.

Steganografia cyfrowa

Rozwój techniki cyfrowej spowodował przeniesienie steganografii również na tą dziedzinę. Steganografia cyfrowa daje o wiele większe możliwości ukrycia informacji niż tradycyjna. Bazuje ona, bowiem na dokonywaniu subtelnych zmian w oryginalnym medium w taki sposób, aby ludzkie oko nie było w stanie ich wykryć. Ponadto Internet umożliwia o wiele bardziej swobodny przepływ informacji. Można wręcz umieścić przekaz na publicznym serwerze pozostając anonimowym. Osoba, która jest adresatem wiadomości również może ją niepostrzeżenie odczytać. W przypadku wykrycia informacji przez osoby niepowołane mogą one poznać treść, lecz trudno będzie im ustalić adresata oraz nadawcę. Tak więc niejednokrotnie odczytanie wiadomości może się okazać dla intruza bezużyteczne, ponieważ nie będzie wiedział kogo ona dotyczy.

Nośnikiem ukrytej informacji może być dowolny rodzaj pliku. Najczęściej wykorzystywane są do tego celu pliki multimedialne. Mają one duże rozmiary a ponadto trudno jest wychwycić drobną modyfikację oryginału. Pozwala to na ukrycie dużej paczki danych przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa.

Istnieje wiele sposobów ukrywania treści. W zależności od wykonywanych operacji możemy podzielić je na kilka kategorii:

- Substytucji
- Transformacyjne
- Modyfikacji widma
- Widma rozproszonego
- Zniekształceniowe
- Statystyczne
- Generacji nośnika

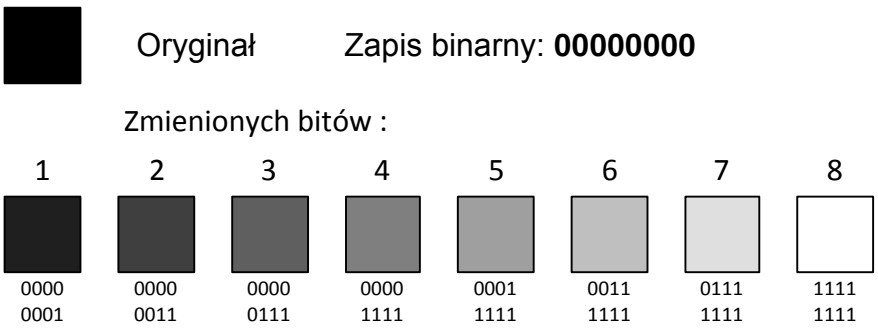
Metody substytucji

Projekt Absolwent na miarę czasu współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego;
Nr umowy UDA-POKL.04.01.01-00-421/10-01

Zasada działania metod substytucji polega na dołączaniu do istniejących danych bitów ukrywanej wiadomości. Najczęściej osiągane jest to poprzez zastąpienie najmniej znaczących bitów ukrywaną informacją. Bity te zazwyczaj przenoszą jednie szum – możemy więc je traktować jako zapis szumu występującego w sygnale. Zmiany wykonane w tej części zapisu nie wnoszą istotnych zmian do całego zapisu, więc mogą być dowolnie modyfikowane i przenosić znaczące ilości danych. Jednak ze względu na ich marginalne znaczenie bardzo często ulegają zniszczeniu podczas konwersji zapisu. Do metod substytucji należą:

Metoda najmniej znaczących bitów – LSB (ang. Least Significant Bit) polegająca na podmienieniu jednego lub kilku najmniej znaczących bitów bitami ukrywanymi.

Każdy rodzaj multimediów posiada zapis w którym jego elementy składowe posiadają wartości opisywane liczbowo. Obraz może być zapisany w postaci grafiki rastrowej – czyli kolekcji pikseli, z których każdy ma określone położenie na obrazie oraz barwę. Barwa opisywana jest przy pomocy wartości liczbowych. W przypadku obrazów czarno-białych barwa piksela zapisana jest na jednym bicie. Wartość 0 oznacza kolor czarny a wartość 1 kolor biały. Zmiana wartości zmienia kolor piksela. W przypadku obrazów reprezentowanych w skali szarości, kolor każdego piksela zapisywany jest na 8 bitach co daje 256 różnych możliwości. Wartość 0 oznacza kolor czarny a wartość 255 kolor biały. Zwiększanie wartości liczbowej reprezentującej kolor powoduje jego rozjaśnianie. Niewielka zmiana wartości spowoduje wprowadzenie niewielkich zmian w odcieniu modyfikowanego piksela co z reguły pozostaje niezauważalne dla ludzkiego oka. Jako że chcemy do nośnika dołączyć wartości bitów, najprościej jest podmienić pewne bity przechowujące wartość kolory piksela na bity ukrywanej informacji. Jako że zależy nam na tym by wprowadzone zmiany były jak najmniejsze to podmieniamy wartości najmniej znaczących bitów, gdyż ich zmiana w najmniejszym stopniu wpływa na zmianę koloru danego piksela. Wpływ zmiany wartości kolejnych bitów na zmianę barwy czarnego piksela zaprezentowano na rysunku S2.



Rysunek S2. Wpływ ilości modyfikowanych bitów na barwę.

W przypadku obrazu kolorowego, mamy do dyspozycji większą ilość bitów, gdyż każdy kolor reprezentowany jest niezależnie a jego wartość zapisywana jest przynajmniej na

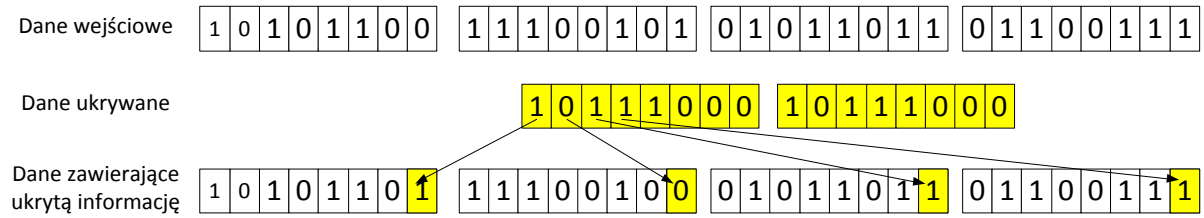
Projekt Absolwent na miarę czasu współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego;
Nr umowy UDA-POKL.04.01.01-00-421/10-01

8 bitach. Mamy 3 kolory: czerwony, zielony, niebieski. Oko ludzkie wykazuje różną wrażliwość na zmiany poszczególnych kolorów. Nie należy więc modyfikować wszystkich składowych barwnych w jednakowym stopniu. Dla każdej składowej należy dobrać odpowiednią dla niej ilość modyfikowanych bitów.

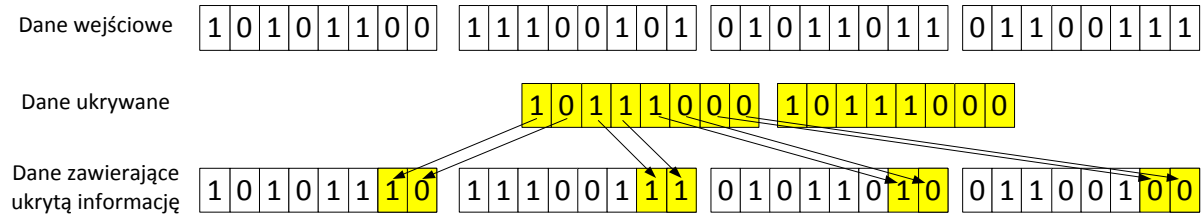
W przypadku dźwięku, podstawowym elementem jest próbka (jest odpowiednikiem piksela w obrazie). Jej wartość jest również zapisywana liczbowo i oznacza amplitudę fali dźwiękowej w danym momencie (jest to równoważne wychyleniu membrany głośnika odtwarzającego ten sygnał) Zasady modyfikacji są takie same jak w przypadku obrazu.

Generalna zasada jest taka: im więcej bitów modyfikujemy tym więcej informacji możemy ukryć (uzyskać większą pojemność steganograficzną). Jednak im więcej bitów zmodyfikujemy tym bardziej będą widoczne wprowadzone zmiany.

Schematycznie zasada działania metody LSB została przedstawiona na rysunku S3, S4 i S5.

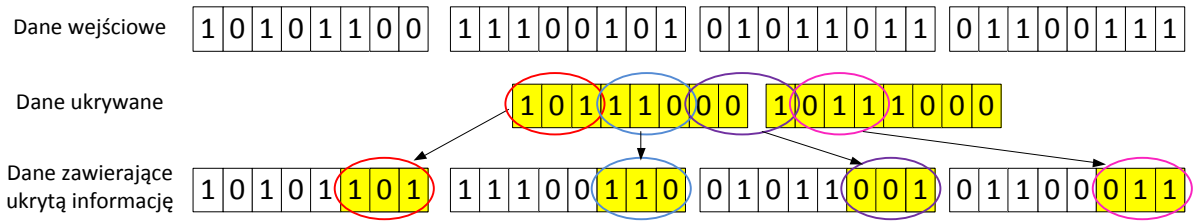


Rys S3. Ukrywanie danych metodą LSB przy wykorzystaniu jednego najmniej znaczącego bitu każdej próbki nośnika.



Rys S4. Ukrywanie danych metodą LSB przy wykorzystaniu dwóch najmniej znaczących bitów każdej próbki nośnika.

Projekt Absolwent na miarę czasu współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego;
Nr umowy UDA-POKL.04.01.01-00-421/10-01



Rys S4. Ukrywanie danych metodą LSB przy wykorzystaniu trzech najmniej znaczących bitów każdej próbki nośnika.

Istotne jest by sprawdzić czy dane, które chcemy ukryć zmieszczą się w nośniku (kontenerze) w którym chcemy je ukryć. Dodatkową informację ukrywamy jedynie w obszarze danych (wartościach próbek), nie wolno modyfikować nagłówka pliku.

ZADANIA

1. Opracuj program komputerowy ukrywający i odczytujący informację w obrazie metodą najmniej znaczących bitów. Zapewnij możliwość wczytywania obrazu z pliku, wczytywania pliku danych do ukrycia (w dowolnym formacie) oraz zapisania pliku wynikowego. Zapewnij obsługę plików w skali szarości oraz kolorowych. Ilość najmniej znaczących bitów, która będzie wykorzystywana będzie podawał użytkownik. Zadaniem programu będzie sprawdzenie czy ukrywana informacja zmieści się w nośniku przy użyciu zadeklarowanej ilości najmniej znaczących bitów.
2. Ukryj w wybranym obrazie dane przy wykorzystaniu różnej ilości najmniej znaczących bitów. Porównaj efekty, określ przy jakiej ilości wykorzystywanych bitów zmiany zaczynają by widoczne.
3. Wykonaj ponownie doświadczenie z punktu drugiego. Tym razem użyj zestawu różnych obrazów. Jeden z nich powinien zawierać duże jednobarwne powierzchnie, drugi powinien zawierać dynamicznie zmienną zawartość (duża ilość różnorodnych, niejednorodnych elementów) np. fotografia drzewa, łąki kwiatów, trzeci niech będzie szkicem wykonanym ołówkiem. Określ czy wszystkie obrazy jednakowo nadają się do ukrywania w nich danych, czy też występują pomiędzy nimi różnice.
4. Ukryj w nośniku dowolny tekst. Przekaż koledze nośnik.
5. Spróbuj odczytać informację z pliku otrzymanego od kolegi. Próbuj wykorzystywać różne ilości najmniej znaczących bitów. Oceniaj automatycznie otrzymaną zawartosc w celu określenia czy jest to poprawny tekst. Użyj metod oceniania znanych Ci z zajęć kryptoanalizy.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt Absolwent na miarę czasu współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego;
Nr umowy UDA-POKL.04.01.01-00-421/10-01