Cyfrowy znak wodny

Ćwiczenie laboratoryjne

Cel

Celem ćwiczenia jest zapoznanie się z możliwościami zabezpieczania praw autorskich oraz autentyczności plików graficznych (zdjęć, grafik, itd.) przy pomocy ukrytego cyfrowego znaku wodnego. Do ćwiczeń wykorzystano wersję demonstracyjną programu Eikonamark firmy ALPHATECLTD oraz program testowy StirMark. Ćwiczenie należy wykonać w środowisku Windows.

Przygotowanie

- Należy pobrać plik **watermarking.zip** i rozpakować go w swoim katalogu domowym. W efekcie powinniśmy otrzymać katalog **Watermarking** z podkatalogami **Zad1**, **Zad2** i **Zad3**.
- Część poleceń wymaga współpracy z pozostałymi osobami w grupie.

Wyniki

Raport – odpowiedzi na pytania w zadaniach umieść w raporcie w pliku PDF.

Zad 1. Zabezpieczenie autentyczności i integralności obrazu

(1.1) W katalogu **watermarking** odnaleźć program **eikonamark.exe** i uruchomić go. Otworzyć plik [File \ Open] o nazwie **800C.jpg** z katalogu **Zad1**. Sprawdzić jego autentyczność i integralność. Z menu wybrać [Watermark \ Detect]. Klucz użytkownika ustawić na 100050. W polu Usage ustawić Authentication i zaznaczyć opcję Display Tampered Regions. Otrzymany plik graficzny należy zapisać pod nazwą **800M.jpg** (jakość 100). Następnie pliki **800C.jpg** i **800M.jpg** otworzyć w dowolnym edytorze graficznym. Ocenić jaki fragment obrazu oryginalnego został naruszony.

(1.2) Z Internetu pobrać dowolny plik jpg o rozmiarze 800x600 pikseli. Otworzyć go w programie **eikonamark** i osadzić w nim znak wodny zabezpieczający jego autentyczność i integralność [Watermark \ Embed]. W polu Invisible wybrać Watermark a w Usage wybrać Authentication. Ustawić znak najbardziej odporny na usuwanie (suwak Watermark level maksymalnie w prawo) a klucz ustalić według numeru stanowiska (stanowisko 1 - klucz 100001, stanowisko 2 - klucz 100002, ..., stanowisko 12 klucz - 100012). Otrzymany plik zapisać w formacie TIFF (jakość 100).

(1.3) Plik z osadzonym znakiem wodnym przekazać sąsiadowi, który ma dokonać na jego fragmencie manipulacji w dowolnym edytorze graficznym (np. przekleić fragment innego obrazu). Spreparowany plik odebrać od sąsiada i postarać się ustalić jaki fragment został uszkodzony (patrz pkt 1.1).

W raporcie umieść plik z zaznaczonym zmienionym fragmentem wraz z komentarzem.

Zad 2. Zabezpieczenie praw autorskich

(2.1) Z Internetu pobrać dowolny plik jpg o rozmiarze 800x600 pikseli. Otworzyć go w programie **eikonamark** i osadzić w nim znak wodny zabezpieczając swoje prawa autorskie jako jego właściciela - zakładamy, że prawdziwy właściciel nie dowie się o tym podczas trwania zajęć :). Wywołać osadzanie znaku [Watermark \ Embed], wybrać Invisible Watermark i Usage Copyright. UWAGA! klucz ustawiamy na 100050! Wybrać typ znaku Multibit Watermark, ustawić suwak na najmocniejszym podpisie i w polu Message podać dowolny 8 znakowy komunikat. Wygenerowany obraz zapisać w formacie TIFF (jakość 100). Plik z osadzonym znakiem wodnym przesłać do wszystkich osób w grupie.

(2.2) Wszystkie otrzymane od pozostałych osób obrazy z osadzonym znakiem wodnym zapisać w katalogu **Zad2**. W programie eikonamark wybrać przetwarzanie wsadowe [File \ Batch]. W zakładce Source wskazać katalog **Zad2** z plikami pozostałych osób. W zakładce Operation wybrać Detection i wejść do opcji. W opcjach klucz ustawić na 100050, wybrać Usage Copyright i Multibit Watermark. Otrzymany plik tekstowy **detect.log** został zapisany w katalogu **Zad2**.

Przeanalizuj zawartość pliku detect.log, wyniki obserwacji oraz treść pliku umieść w raporcie.

Zad 3. Metody ataku na cyfrowy znak wodny

Uwaga!!! – Programy działają poprawnie pod Windows XP, w Windows 7 lub 8 może być konieczne ponowne uruchomienie programu eikonmark.

W katalogu embeded umieszczono 4 pliki graficzne z osadzonym znakiem wodnym:

1200_1.jpg – obraz o rozmiarze 1200x771 z osadzonym najsłabszym znakiem wodnym;

1200_2.jpg – obraz o rozmiarze 1200x771 z osadzonym najmocniejszym znakiem wodnym;

400_1.jpg – obraz o rozmiarze 400x257 z osadzonym najsłabszym znakiem wodnym;

400_2.jpg – obraz o rozmiarze 400x257 z osadzonym najmocniejszym znakiem wodnym;

(3.1) W katalogu Zad3 uruchomić skrypt **crack.bat**. UWAGA! Operacje wykonywane podczas działania skryptu są bardzo czasochłonne (mogą trwać od kilku do kilkunastu minut). Skrypt pobiera kolejno obrazy z katalogu **embeded** i tworzy w katalogu **cracked** podkatalogi dla każdego pliku. Następnie generuje w podkatalogach pliki zmodyfikowane (obroty, filtracje, kompresje itd) na podstawie plików z katalogu **embeded**. W każdym podkatalogu zostanie również umieszczony plik **stirmark.log** zawierający opisy do poszczególnych modyfikacji.

(3.2) Uruchomić program **eikonamark**. Wybrać przetwarzanie wsadowe [File \ Batch]. W zakładce Source wskazać pierwszy podkatalog katalogu **cracked**. W zakładce Operation wybrać Detection i wejść do opcji. W opcjach klucz ustawić na 100050, wybrać Usage Copyright i Zero Bit Watremark. Otrzymany plik tekstowy **detect.log** został zapisany we wskazanym podkatalogu. Tę samą czynność powtórzyć dla pozostałych podkatalogów.

(3.3) Wykorzystując pliki **stirmark.log** i **detect.log** z odpowiednich podkatalogów katalogu **crack** porównać otrzymane wynik dla poszczególnych plików. Zrobić zestawienie:

1) ataków, na które odporne były poszczególne pliki,
2) ataków, na które odporne były wszystkie pliki,
3) ataków, na które żaden plik nie był odporny. Jaki wpływ na wyniki miała wielkość obrazu?, a jaki siła osadzonego znaku?

W raporcie umieść zestawienie oraz wyniki i wnioski.