Steganografia – jak ukryć galaktykę w Babiej Górze

*William J. PEARSON**

*Narodowe Centrum Badań Jądrowych

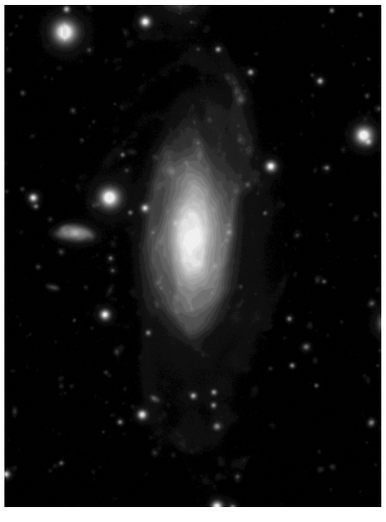
Tłumaczenie: *Anna DURKALEC*

Zdarza się, że chcemy komuś przekazać informację w tajemnicy. Ukrytą tak sprytnie, żeby żadna niepożądana osoba nie mogła jej zrozumieć, a nawet zauważyć. Może to być poufna wiadomość od szpiega, informacje przekazywane pomiędzy sojusznikami w czasie działań wojennych albo sekretny list miłosny. Od czasu do czasu zwariowany astrofizyk chciałby też mieć możliwość ukrycia zdjęcia galaktyki w typowym zdjęciu przedstawiającym pejzaż górski.

Przekazywanie ukrytych wiadomości nie jest nowym problemem – dobrze ponad 2000 lat temu Juliusz Cezar używał prostej metody „przesuwania" alfabetu do szyfrowania swoich listów i notatek. Oczywiście w miarę upływu czasu techniki szyfrowania stały się bardziej zaawansowane, a tajne wiadomości trudniejsze do wykrycia. Każdy z nas wie, że tak prosta rzecz jak sok z cytryny pozwala na napisanie niewidzialnej wiadomości. Są na to również bardziej wyszukane sposoby, wykorzystujące rzadziej spotykane substancje chemiczne. A to był dopiero początek. Wraz z pojawieniem się komputerów metody umożliwiające zaszyfrowanie i ukrycie wiadomości stały się jeszcze bardziej skomplikowane. Przedstawię tu jedną z nich. Pozwala ona na ukrycie informacji w obrębie cyfrowego obrazu.

Ukrytą wiadomość można napisać fenoloftaleiną, a odczytać dzięki oparom amoniaku lub węglanu sodu. Nie próbujcie tego w domu.

Babia Góra. Zdjęcie z wakacji.
Autorzy: A. Durkalec / W.J. Pearson



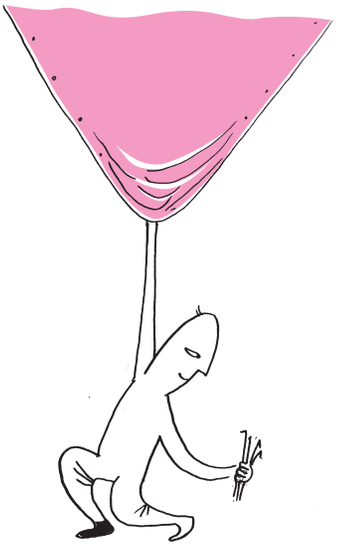
Galaktyka ukryta w Babiej Górze
Autorzy: W.J. Pearson / T. Goto / H. Matsuhara w ramach przeglądu nieba HSC/AKARI-NEP

Współcześnie większość zdjęć, zarówno tych wykonywanych telefonem komórkowym, jak i zdjęć galaktyk wykonywanych za pomocą teleskopów, zapisuje się na matrycy CDD (*charge–coupled device*). W obu przypadkach zdjęcia są zapisywane i przechowywane w postaci dwuwymiarowych tablic pikseli. Każda z tych tablic zawiera informację o kolorze w postaci trzech lub czterech wartości: koloru czerwonego, zielonego i niebieskiego (RGB), RGB z przezroczystością (RGBA) albo kolorów cyjanu, magenty, żółtego i czarnego (CMYK). W przypadku RGB każdy kolor przyjmuje jedną z 256 wartości, od 0 do 255, która przechowywana jest jako wartość 8 bitów ($2^8 = 256$). Niewielkie zmiany tych wartości są niezauważalne dla ludzkiego oka. Na przykład zmiana wartości czerwieni piksela o 2 odpowiada zmianie barwy o 1%. I właśnie ten fakt możemy wykorzystać do ukrycia wiadomości w obrazie – dokonując niewielkich zmian w wartościach liczb niosących informację o kolorze.

Rozważmy obraz, dla którego kolor lewego górnego piksela ma wartości RGB 123, 151 i 188. W 8–bitowym kodzie binarnym te liczby zapisuje się jako `01111011`, `10010111` i `10111100`. Dla uproszczenia rozważmy tylko kanał czerwony, czyli kanał R: `01111011`. Zamieniając ostatnie cztery cyfry tej liczby na zera, otrzymamy `01110000`, czyli w systemie dziesiętnym liczbę 112. W przybliżeniu zmieniliśmy więc wartość koloru czerwonego o około 10% (oryginalny kolor w systemie RGB miał wartość 123). Oczywiście moglibyśmy zmienić pierwsze cztery cyfry binarne na zero, wówczas otrzymalibyśmy `00001011` lub w systemie dziesiętnym 11, co jest w przybliżeniu zmianą o 90% w stosunku do oryginalnej wartości. Ponieważ zmiana pierwszych czterech cyfr binarnych powoduje dużą różnicę w kolorze, a zmiana ostatnich czterech małą, możemy uznać pierwsze cztery cyfry binarne za znaczące, a ostatnie cztery za nieistotne. Tylko zmiana cyfr nieistotnych nie rzuci się za bardzo w oczy.

Jeśli zastosujemy ten sam pomysł dla wszystkich pikseli obrazu, wówczas zmiana koloru będzie niezauważalna dla przeciętnego obserwatora (poza pewnymi problemami, o których za chwilę). Sprytny Czytelnik już pewnie wie, jak tę słabość wykorzystać. Obraz pozornie nie zmieni się, jeżeli pozostawimy nienaruszone cztery pierwsze cyfry z 8–bitowych wartości binarnych opisujących kanały RGB. Pozostałe cztery cyfry możemy więc dowolnie zmieniać i wykorzystać je do przekazania tajnej wiadomości. W ten sposób możemy na przykład ukryć zdjęcie galaktyki wewnątrz niepozornego zdjęcia z wakacji.

Patrząc na zamieszczone na marginesie zdjęcie Babiej Góry, można by pomyśleć, że jest to po prostu niskiej jakości zdjęcie, być może nadmiernie skompresowane. W rzeczywistości ukrywa ono w sobie obraz galaktyki. Wystarczy wziąć znaczące cyfry binarne zdjęcia galaktyki i odrzucić cyfry nieistotne. W kolejnym kroku



podmienić nieistotne cyfry binarne zdjęcia Babiej Góry na istotne cyfry binarne zdjęcia galaktyki. I voila! Ukryliśmy obraz galaktyki w zdjęciu z wakacji.

Niestety cała procedura, zarówno ukrycie zdjęcia galaktyki, jak i jej odkodowanie, powoduje utratę jakości obu obrazów. Zastąpienie czterech nieistotnych cyfr binarnych oryginalnego zdjęcia spowodowało, że góra stała się blokowa, a gładkie przejścia kolorów stały się gwałtowne i ostre. To samo widać na odzyskanym obrazie ukrytej galaktyki, gdzie gładkie ramiona spiralne stają się zbite i szorstkie.

To nie jedyna wada tej metody. Ukryta informacja może zostać przechwycona, jeśli niepożądana osoba ma dostęp do oryginalnego obrazu. Odjęcie oryginalnego obrazu od tego, który edytowaliśmy poprzez zmiany kolorów, w prosty sposób ujawni naszą tajną informację. Niska rozdzielczość edytowanego obrazu może również nas zdemaskować, skłaniając kogoś do bliższego przyjrzenia się zawartym w nim danym. Wówczas wszystkie nasze tajemnice mogą zostać ujawnione.

Oczywiście możemy naszą wiadomość ukryć bardziej dyskretnie. Edytując mniejszą liczbę nieistotnych cyfr: na przykład zmieniając tylko ostatnie dwie cyfry binarne zamiast czterech ostatnich. Wtedy obraz będzie mniej uszkodzony. Niestety w takim przypadku znacznie zmniejszymy przestrzeń do ukrycia informacji, co oznacza, że będziemy mogli przesłać mniej danych lub będziemy musieli rozbić naszą sekretną wiadomość na więcej obrazów.

Ostatecznie jednak możemy ukryć galaktykę w Babiej Górze.

Zadania

Przygotował Dominik BUREK

M 1729. Prostokąt został podzielony na kilka przystających trójkątów prostokątnych. Czy zawsze pewne dwa sąsiadujące trójkąty z podziału tworzą (bez przemieszczania) prostokąt?
Rozwiązanie na str. 8

M 1730. Liczby $1, 2, \ldots, 2022$ są wypisane na tablicy. W każdej sekundzie zmazujemy cztery liczby postaci a, b, c, $a+b+c$ i zastępujemy je liczbami $a+b$, $b+c$, $c+a$. Udowodnić, że proces ten musi skończyć się po mniej niż 9 minutach.
Rozwiązanie na str. 9

M 1731. Liczby całkowite dodatnie a i n są takie, że n dzieli a^2+1. Udowodnić, że istnieje liczba całkowita dodatnia b taka, że $n(n^2+1)$ dzieli b^2+1.
Rozwiązanie na str. 10

Przygotował Andrzej MAJHOFER

F 1061. Metalową kulę o promieniu R umieszczono w jednorodnym polu elektrycznym $\vec{E}$. Po wyłączeniu pola w kuli wydzieliło się ciepło Q. Ile ciepła wydzieliłoby się w metalowej kuli o promieniu równym $2R$ po wyłączeniu pola $\vec{E}$?
Rozwiązanie na str. 15

F 1062. Dwie gwiazdy o masach m_1 i m_2 tworzą układ podwójny. Okres, z jakim obiegają ich wspólny środek masy, wynosi T. Ile wynosi odległość między gwiazdami R?
Rozwiązanie na str. 17