Marta Walenczykowska

Streszczenie

W ostatnich latach można zauważyć dynamiczny rozwój steganografii. Okazuje się, że poza szyfrowaniem danych można je dodatkowo zabezpieczyć przez ich ukrycie. Połączenie tych dwóch metod jest skutecznym i coraz powszechniej stosowanym sposobem ochrony danych. Większość obecnych na rynku aplikacji wykorzystuje właśnie takie połączenie. Aby prawidłowo odczytać ukryte informacje, należy zauważyć fakt ich zamaskowania i złamać algorytm steganograficzny oraz dokonać dekryptażu.

W artykule omówiono możliwości wykorzystania dostępnych w Internecie darmowych aplikacji steganograficznych stosowanych do ukrywania wrażliwych danych. Przeanalizowano używane w nich algorytmy ukrywania informacji oraz ich odporność na ataki steganograficzne. Omówiono między innymi: Contraband, F5.jar, Invisible Secrets 2.1, MP3 Steno, Securengine Professional 1.0, JPHS i S-Tools. Przedstawiono również wartość obliczonych współczynników MSE (*mean square error* – błąd średniokwadratowy) oraz współczynnik PSNR (*peak signal to nosie ratio* – szczytowy stosunek sygnału do szumu) w celu przedstawienia wprowadzonych przez programy zniekształceń.

W celu lepszego zrozumienie tekstu w artykule omówiono pojęcia: nośnik, plik nośny, stegoplik oraz stegoobraz. Na zakończenie zwrócono uwagę na kilka podstawowych zasad, których należy przestrzegać, aby stosowane programy zapewniły oczekiwany poziom bezpieczeństwa ukrywanych danych.