mgr inż. Kamil Kaczyński
Wojskowa Akademia Techniczna
Wydział Cybernetyki, Instytut Matematyki i Kryptologii

Kody korekcyjne w steganografii

Poprawnie zaprojektowany stegosystem powinien cechować się tzw. niewykrywalnością, która jest rozumiana jako brak możliwości rozróżnienia nośnika przenoszącego ukrytą treść od nośnika bez dołączonych danych. Prawdopodobieństwo wykrycia wykorzystania technik steganograficznych wzrasta wraz z ilością zmian wprowadzonych do oryginalnego nośnika. Zmniejszenie ilości wprowadzanych zniekształceń może zostać osiągnięte między innymi poprzez zastosowanie tzw. kodowania syndromami kodów korekcji błędów. Pierwszym algorytmem, w którym została wykorzystana ta technika, był algorytm F5 opracowany przez A. Westfelda. Zaproponowano w nim wykorzystanie liniowego kodu korekcji błędów — kodu Hamminga, czego efektem było drastyczne zmniejszenie liczby wprowadzanych zmian, a także zwiększenie odporności na dostępne techniki stegoanalityczne. Dodatkową zaletą kodowania syndromami jest także zwiększenie pojemności nośnika, przy jednoczesnym zmniejszeniu liczby wprowadzanych zmian. Warty podkreślenia jest fakt, iż nie tylko kody liniowe mogą być zastosowane do poprawienia właściwości istniejących algorytmów steganograficznych. Doskonałym rozwiązaniem może być wykorzystanie nieliniowych kodów binarnych, czy też kodów cyklicznych, które często posiadają znacznie większą ilość słów kodowych niż porównywalne kody liniowe. W niniejszym referacie przedstawione zostały zastosowania wybranych kodów korekcyjnych w steganografii, wraz ze wskazaniem i porównaniem ich najważniejszych cech, w szczególności sprawności osadzania.