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

Algorytm steganograficzny PM1 wykorzystujący trójkowy kod Hamminga

W 1998 roku R. Crandall opublikował wpis na *steganography mailing list*, wskazując na możliwość poprawienia efektywności algorytmów steganograficznych przez wykorzystanie kodów korekcyjnych w procesie osadzania wiadomości. W szczególności, poprzez wykorzystanie kodów liniowych istnieje możliwość skonstruowania systemu steganograficznego opartego o tzw. osadzanie macierzowe (z ang. *matrix embedding*). W systemie takim wiadomość jest przekazywana z wykorzystaniem syndromu wybranego kodu korekcji błędów. Niech C będzie kodem o długości n i o k elementach informacyjnych, posiadającym macierz kontroli parzystości H i zdolność korekcyjną t. Niech x będzie wektorem uzyskanym po zastosowaniu funkcji przypisywania symboli do elementów nośnika i $s \in F_q^{n-k}$ oznacza tajną wiadomość. Poniższy schemat pozwala osadzić $n-k$ symboli, dokonując przy tym co najwyżej t zmian w każdym bloku składającym się z n symboli.

$$Emb(x,s) = x - e_L = y$$
$$\mathrm{Ext}(y) = Hy.$$

Algorytm PM1 (Plus Minus 1) jest rozwinięciem algorytmu LSB, cechującym się nie tylko zwiększoną odpornością na ataki stegoanalityczne, ale także wysoką pojemnością steganograficzną. Operacja osadzania wiadomości w pikselu obrazu x_i wymaga wykonania operacji $x_i + c$, gdzie $c \in \{0, +1, -1\}$, co oznacza, że wiadomość jest przenoszona przez dwa najmniej znaczące bity piksela obrazu, w odróżnieniu do algorytmu LSB, w którym zmianie ulega jedynie najmniej znaczący bit piksela obrazu. Postać funkcji osadzającej w naturalny sposób wskazuje, że najbardziej optymalne jest wykorzystanie symboli z $\mathbb{Z}_3$, gdzie funkcja wyodrębniająca ma postać

$$\mathrm{Ext}(y_i) = y_i \bmod 3.$$

W niniejszym referacie przedstawiona została modyfikacja algorytmu PM1, w którym zastosowano tzw. kodowanie syndromami poprzez wykorzystanie syndromów trójkowego kodu Hamminga $(13, 10)$. Zastosowanie kodowania macierzowego pozwoliło na znaczące poprawienie podstawowych parametrów algorytmu PM1, takich jak średnie zniekształcenie i współczynnik osadzania, co w efekcie pozwoliło także na uzyskanie wysokiej sprawności osadzania, blisko o 44% większej niż w przypadku algorytmu zmodyfikowanego w oparciu o binarny kod Hamminga $(7, 4)$. Zmniejszenie liczby zmian wprowadzanych do nośnika spowodowało znaczące zmniejszenie wrażliwości algorytmu na podstawowe ataki stegoanalityczne, takie jak stegoanaliza RS, czy też atak Chi-kwadrat. Zastosowany w algorytmie trójkowy kod Hamminga może zostać także użyty do modyfikacji innych algorytmów steganograficznych, pozwalając na poprawę ich głównych parametrów i jednoczesne zwiększenie osiąganej przez nie sprawności osadzania.