Podstawy Ochrony Danych – laboratorium AGC
Kryptografia wizualna

Cel ćwiczenia laboratoryjnego: Poznanie metody szyfrowania wykorzystującą schematy progowe.

Materiały do laboratorium: materiały z wykładu oraz inne podane przez prowadzącego.

Zadanie:

Ideą kryptografii wizualnej jest możliwość bezpiecznego zaszyfrowania informacji takiej jak tekst, pismo ręczne czy obrazy, w taki sposób, aby możliwe było jej odszyfrowanie przy pomocy tylko i wyłącznie wzroku. W swojej podstawowej postaci, pojedynczy obraz dzielony jest na dwa obrazy zwane udziałami. Zaszyfrowana informacja (obraz) ukazuje się po nałożeniu na siebie obydwu udziałów. Na konferencji Eurocrypt'94 Naor i Shamir opisali sposób kodowania czarno-białych obrazów przy pomocy *n* udziałów. Dekodowanie odbywa się za pomocą wzroku, gdy umieszczone na przezroczystych foliach udziały nakłada się na siebie. Zaproponowano kilka schematów takiego kodowania gdzie, jeden piksel zastępowany jest dwoma, czterema lub dziewięcioma pikselami.

Zadanie:

Implementacja **najprostszej wersji algorytmu**, dla obrazu czarno-białego 100x100 pikseli, podział na dwa udziały, a po złożeniu udziałów brak korekcji zniekształcenia formatu i pozostawienie zaszumienia.

Brak sprawozdania – programy będą sprawdzane na zajęciach.