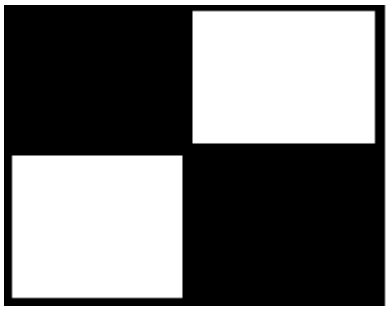
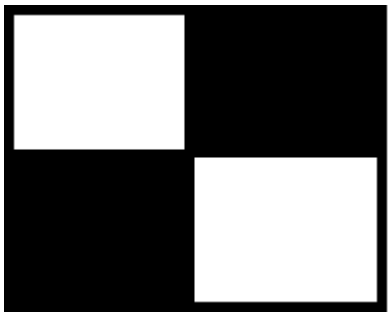
Kryptografia Wizualna

Rozszerzeniem dziedziny dzielenia sekretu jest kryptografia wizualna. W najprostszej wersji polega ona na utworzeniu z obrazu binarnego (takiego którego piksele mają tylko wartość 0 lub 1) zawierającego sekretną wiadomość, dwóch graficznych udziałów które po nałożeniu na siebie pozwalają odkryć sekret. Istotne jest to, że z pojedynczego udziału nie ma możliwości przywrócenia nawet najmniejszej części pierwotnego sekretu. Algorytm ten jest więc bezpieczny teorio-informacyjne.

Do utworzenia obu udziałów należy użyć specjalnych bloków pikseli, np.:



(a) blok 1



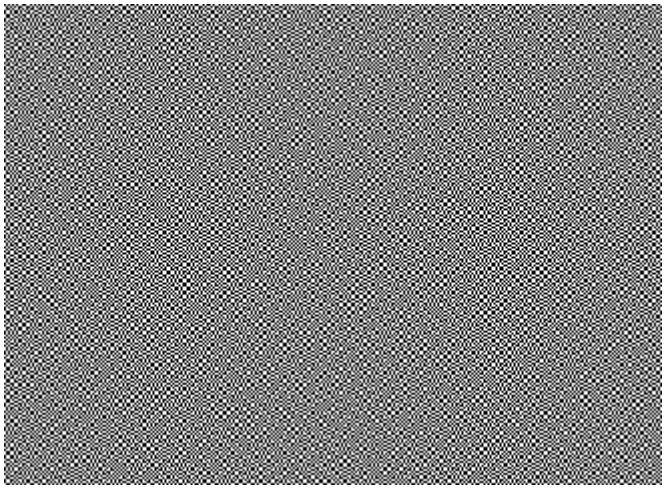
(b) blok 2

Każdemu pikselowi obrazu wejściowego odpowiada 4 pikselowy blok na obu udziałach (oznacza to, że oba udziały są 2 razy wyższe i 2 razy szersze niż obraz wejściowy). Jeżeli w obrazie wejściowym czytany jest piksel biały, w pierwszym udziale ustawiany jest blok (a), a w drugim (b), lub w pierwszym udziale ustawiany jest blok (b), a w drugim (a) – wybór jest losowy. Jeżeli czytany piksel jest czarny w pierwszym i drugim udziale ustawiany jest blok (a), lub w pierwszym i drugim udziale ustawiany jest blok (b) – wybór kombinacji również jest losowy. Istnieją inne rodzaje bloków do tworzenia udziałów, jak np.:

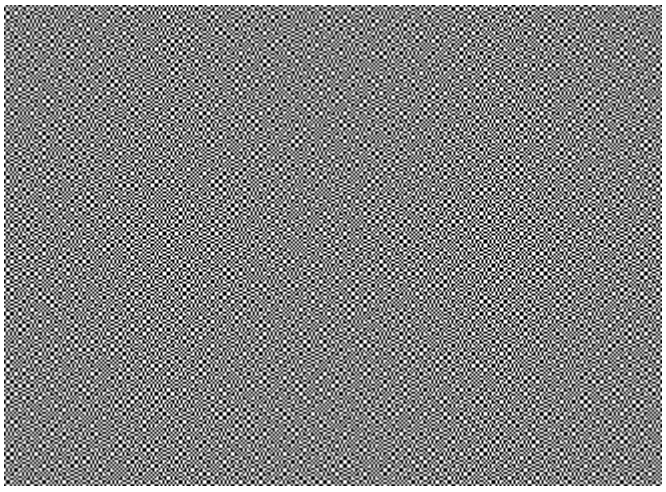
Ale powodują one odpowiednio zniekształcenia w pionie lub poziomie przy odtwarzaniu sekretu. Poniżej przykład sekretu, udziałów i odtworzenia sekretu z udziałów z użyciem bloków (a) i (b):

Obraz oryginalny:

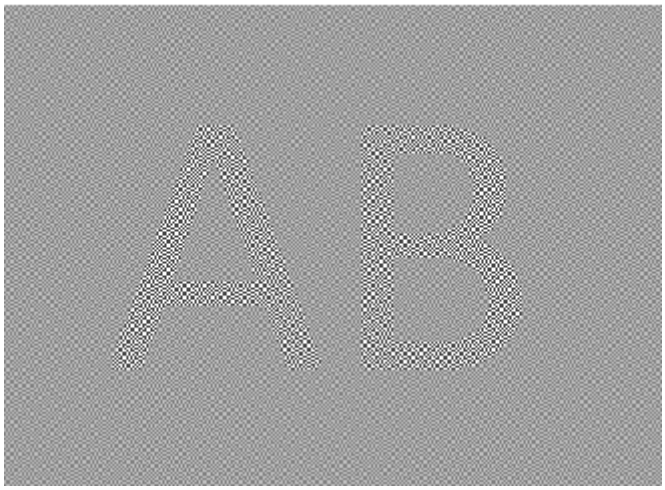
Udział 1:



Udział 2:



Nałożenie udziału 1 na udział 2:



Zadanie:

Wasz zespół przechwycił 10 różnych obrazów. 2 z nich są udziałami sekretnego obrazka zawierającego hasło, reszta to przypadkowy szum. Znajdźcie sekretne hasło. Jeśli uda Wam się wykonać to zadanie, otrzymacie za nie 80 punktów.