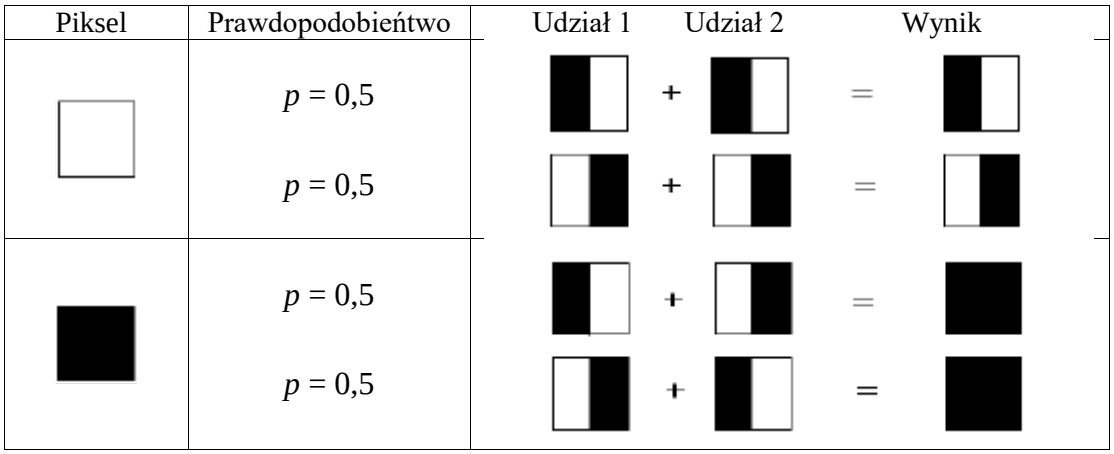
Kryptografia wizualna

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 przeźroczystych foliach udziały nakłada się na siebie. Zaproponowano kilka schematów takiego kodowania.

Rozważmy obraz czarno-biały (bez odcieni szarości). Składa się on z czarnych i białych pikseli, ułożonych w taki sposób, aby tworzyły zrozumiały dla człowieka obraz (słowo, symbol). Aby zakodować taki obraz za pomocą kryptografi wizualnej, należy każdy z pikseli pierwotnego obrazu podzielić na subpiksele (dla uproszczenia przyjmijmy w tej chwili, że każdy piksel dzielimy na dwa piksele, a obraz zaszyfrowany zostanie przy pomocy dwóch udziałów).



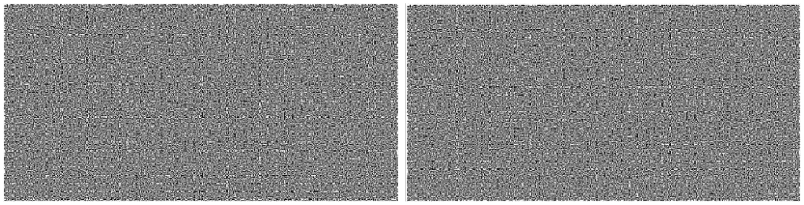
Rys. 1. Szyfrowanie białego i czarnego piksela

Jeśli dany piksel kodowanego obrazu jest biały, to do jego reprezentacji na dwóch udziałach zostanie losowo wybrana kombinacja dwóch subpikseli. Po odpowiednim nałożeniu obu udziałów otrzymamy wynik jak to pokazano na rys. 1. W obu przypadkach dla białego piksela widać, że wynikiem będą dwa subpiksele − czarny i biały obok siebie. Taka kombinacja da w efekcie wrażenie koloru szarego. Natomiast w przypadku piksela czarnego, w wyniku dostaniemy dwa czarne subpiksele obok siebie.

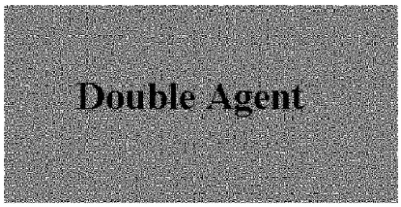
Żaden z udziałów, (które również są obrazami) nie zawiera żadnej widocznej informacji o obrazie pierwotnym (kodowanym), gdyż subpiksele są równomiernie rozłożone w poszczególnych udziałach: jeden biały subpiksel i jeden czarny na każdy piksel obrazu kodowanego. Te kombinacje (czarny/biały i biały/czarny) pojawiają się z prawdopodobieństwem 1/2, a więc na udziałach rozłożone są w sposób zupełnie losowy nie zdradzając żadnej informacji o obrazie pierwotnym. Kiedy udziały zostaną nałożone, białe obszary obrazu pierwotnego widoczne są jako szare obszary, natomiast rejony czarne w obrazie pierwotnym są czarne również w obrazie powstałym z nałożenia udziałów.

W celu lepszego zrozumienia koncepcji kryptografii wizualnej rozważmy poniższy przykład. Żaden z udziałów (rys. 2) nie zdradza żadnej infromacji o obrazie pierwotnym. Po nałożeniu na siebie udziałów otrzymujemy informację pierwotną (rys. 3). Obszary białe na

obrazie pierwotnym są teraz widoczne jako szare, a obszary czarne pozostały czarne i ukazują zakodowany obraz.



Rys. 2. Udział 1 (z lewej) oraz udział 2 (z prawej)



Rys. 3. Wynik (udział 1 + udział 2)

Mimo, iż kryptografia wizualna jest stosunkowo młodą gałęzią kryptografii, ma szanse szybko znaleźć zastosowania praktyczne.

Rozważmy skrytkę bankową. Załóżmy, że trójka przyjaciół składa w skrytce dużą sumę pieniędzy, którą w przyszłości będą mogli odebrać tylko we trójkę. Jedną z metod zagwarantowania, iż tylko wszyscy razem będą mogli otworzyć skrytkę może zapewnić kryptografia wizualna. Komputer mógłby wygenerować kod otwierający skrytkę i przekształcić go w trzy udziały. Tylko nałożenie wszystkich trzech udziałów ujawni kod (klucz) otwierający skrytkę.

Innym zastosowaniem może być przesyłanie tajnych wiadomości. Jeżeli przesyłamy wiadomości w postaci udziałów, wtedy nawet, jeśli któryś z udziałów zostanie przechwycony, żadne informacje nie zostaną ujawnione.

W ramach kryptografi wizualnej opracowano kilka schematów progowych. Schemat opisuje sposób, w jaki obraz będzie kodowany i rozkodowywany. Przykładowo, istnieje schemat *r* z *n*, który mówi, że obraz zostanie zakodowany przy użyciu *n* udziałów i dowolne *r* udziałów musi zostać nałożone na siebie, aby rozkodować obraz. Jeśli ilość nałożonych na siebie udziałów jest mniejsza od *r*, to zakodowany obraz nie zostanie ujawniony. Inny schemat może określać pewne podzbiory udziałów, które należy nałożyć na siebie, aby rozkodować informację. Załóżmy, że obraz zakodowano za pomocą 4 udziałów: A, B, C i D. Schemat może określać, iż tylko nałożenie udziałów B i C rozkoduje informację. Żadna inna kombinacja udziałów nie pozwoli odtworzyć zaszyfrowanego obrazu.

Schematy, które opisano poniżej opisane są za pomocą macierzy. Używane są dwa zbiory macierzy. Jeden służy do zaszyfrowania białych pikseli (C_0), drugi do zaszyfrowania pikseli czarnych (C_1). Macierze w tych zbiorach mają rozmiar $n \times m$: każdy piksel pierwotnego obrazu jest szyfrowany przez *m* subpikseli, udziałów natomiast będzie *n*. Macierze tworzymy dla wszyskich permutacji kolumn w każdym zbiorze. Jako przykład rozważmy następujące zbiory dla schematu stopnia (2, 2):

$$C_0 = \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}$$

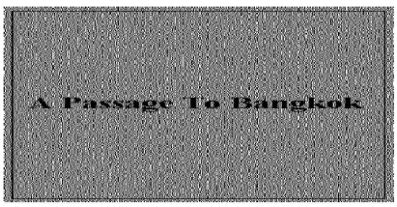
$$C_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

Rys.4 Układ dwóch subpikseli

W przykładzie tym $n = 2$ i $m = 2$. Podczas szyfrowania białego piksela wybierana jest losowo jedna macierz ze zbioru C_0. Nie ma znaczenia, którą macierz wybierzemy, gdyż w wyniku operacji nałożenia (or) rzędów otrzymamy 1 czarny subpiksel i 1 biały piksel. Daje to wagę 1: odcień szarości. Po wybraniu macierzy, każdy z udziałów koduje biały piksel jednym rzędem macierzy. Podobnie postępujemy w przypadku piksela czarnego. Jedna z macierzy C_1 jest wybierana losowo. Każda macierz daje w wyniku złożenia rzędów 2 czarne piksele. Daje to wagę 2: czarny piksel. Każdy udział koduje pierwotny piksel jednym z rzędów macierzy. Połączenie udziałów ujawnia zaszyfrowany obraz.

Opisany powyżej schemat stopnia (2,2), to przypadek, w którym dwa z dwóch utworzonych udziałów potrzebne są do rozszyfrowania informacji. Implementacja tego schmatu (i innych) stwarza dodatkowy problem. Możliwe jest zaimplementowanie schematu stopnia (2,2) z pikselami ułożonymi jak na rysunku 4 Problem, jaki pojawia się przy takiej implementacji polega na tym, że każdy piksel szyfrowanego obrazu jest kodowany przez dwa piksele ułożone na każdym z udziałów w pionie lub w poziomie, co daje w wyniku zniekształcony obraz. Przypadek ten ilustrują rysunki 5 oraz 6. Zniekształcone obrazy pojawiają się również przy schematach gdzie $n = 4, 6$ i innych.

Rys. 5. Obraz oryginalny



Rys. 6. Zniekształcony obraz rozszyfrowany

Aby rozwiązać ten problem, do zakodowania pojedynczego piksela można zastosować 4 subpiksele tworzące kwadrat w taki sposób, żeby zniekształcenia były minimalne. Aby

zaimplementować schemat stopnia (2,2) przy użyciu 4-subpikselowej reprezentacji, można użyć następujących macierzy:

$$C_0 = \left\{ \begin{bmatrix} 0011 \\ 0011 \end{bmatrix}, \begin{bmatrix} 1100 \\ 1100 \end{bmatrix}, \begin{bmatrix} 0101 \\ 0101 \end{bmatrix}, \begin{bmatrix} 1010 \\ 1010 \end{bmatrix}, \begin{bmatrix} 0110 \\ 0110 \end{bmatrix}, \begin{bmatrix} 1001 \\ 1001 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \begin{bmatrix} 1001 \\ 0110 \end{bmatrix}, \begin{bmatrix} 0110 \\ 1001 \end{bmatrix}, \begin{bmatrix} 0011 \\ 1100 \end{bmatrix}, \begin{bmatrix} 1100 \\ 0011 \end{bmatrix}, \begin{bmatrix} 0101 \\ 1010 \end{bmatrix}, \begin{bmatrix} 1010 \\ 0101 \end{bmatrix} \right\}$$

Rys. 7. Organizacja pikseli zapobiegająca zniekształceniom obrazu − złożenia udziałów dla białego piksela

Aby zaszyfrować biały piksel wybieramy losowo jedną macierz ze zbioru C_0 i piksele z poszczególnych rzędów przydzielane są do udziałów. Po nałożeniu udziałów otrzymamy 2 białe i 2 czarne piksele, co da wrażenie koloru szarego.

Aby zaszyfrować czarny piksel, wybieramy jedną macierz ze zbioru C_1 i poszczególne udziały otrzymują po jednym rzędzie macierzy. Po złożeniu obrazów otrzymamy 4 czarne piksele.

Schemat stopnia (3,3) może być zaimplementowany z wykorzystaniem układu subpikseli z rys. 7. W tym przypadku używamy następujących macierzy:

$$C_0 = \left\{ 24 \text{ macierze otrzymane poprzez permutację kolumn macierzy } \begin{bmatrix} 0011 \\ 0101 \\ 0110 \end{bmatrix} \right\}$$

$$C_1 = \left\{ 24 \text{ macierze otrzymane poprzez permutację kolumn macierzy } \begin{bmatrix} 1100 \\ 1010 \\ 1001 \end{bmatrix} \right\}$$

Aby zakodować biały piksel, wybieramy losowo macierz ze zbioru C_0 , a poszczególne udziały otrzymują rzędy macierzy. Podobnie postępujemy w przypadku kodowania piksela czarnego.

W schemacie stopnia (3,3), podobnie jak w przypadku schematu stopnia (2,2), żaden z udziałów nie zdradza żadnej informacji z oryginalnego obrazu (macierze wybierane są losowo). Również złożenie dwóch udziałów nie zdradza obrazu szyfrowanego, gdyż każdy piksel oryginalnego obrazu reprezentowany jest przez jeden biały i trzy czarne piksele, dając w wyniku równomiernie rozłożony kolor ciemno szary. Dopiero złożenie wszystkich trzech udziałów pozwala na odtworzenie obrazu zaszyfrowanego. Białe piksele reprezentowane są przez 3 czarne i jeden biały subpiksel (wrażenie ciemno szarego), a czarne przez 4 czarne subpiksele (wrażenie czarnego).

Prowadzone są również badania nad zastosowaniem kryptografii wizualnej do kodowania obrazów w skali szarości, obrazów kolorowych oraz dodatkowego ukrywania szyfrowanej treści. Przykładowy program obrazujący zasadę działania kryptografi wizualnej, pobrać można ze strony http://compsci.snc.edu/cs460_archive/2003/busspr/, lub obejrzeć dołączony na płycie.