Visual Cryptography

Tereza Hrubešová

Department of Algebra
Faculty of Mathematics and Physics
Charles University in Prague

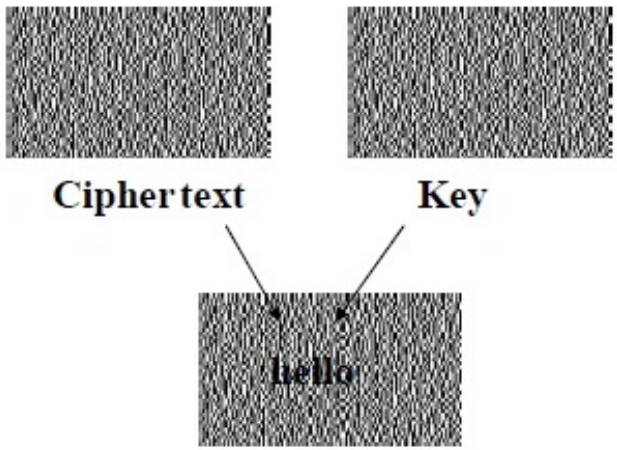
November 2015 / Fall School of Algebra

Visual Cryptography

- introduced by Naor and Shamir in 1994
- a type of cryptographic scheme which can decode concealed images by the human visual system
- perfectly secure
- decoding without any cryptographic computations
- a visual variant of the k out of n secret sharing problem

The Basic Model

- a printed page of ciphertext (indistinguishable from random noise)
- a printed transparency which serves as a secret key (indistinguishable from random noise)
- the original cleartext is revealed by placing the transparency with the key over the page with the ciphertext
- similar to a one time pad in the sense that each page of ciphertext is decrypted with a different transparency



The k out of n secret sharing problem

- n transparencies
- the original message is visible if any k (or more) of them are stacked together
- the original message is totally invisible if fewer than k transparencies are stacked together

The Model

- the message consists of a collection of black and white pixels (each pixel is handled separately)
- each original pixel appears in n modified versions (called shares), one for each transparency
- each share is a collection of m black and white subpixels
- the resulting structure can be described by an $n \times m$ Boolean matrix $\mathbf{S} = [s_{ij}]$ where $s_{ij} = 1$ iff the jth subpixel in the ith transparency is black

The Model

- the message consists of a collection of black and white pixels (each pixel is handled separately)
- each original pixel appears in n modified versions (called shares), one for each transparency
- each share is a collection of m black and white subpixels
- the resulting structure can be described by an $n \times m$ Boolean matrix $\mathbf{S} = [s_{ij}]$ where $s_{ij} = 1$ iff the jth subpixel in the ith transparency is black
- when transparencies $i_1, i_2, \ldots, i_r$ are stacked together, we see a combined share whose black subpixels are represented by the Boolean "or" of rows $i_1, i_2, \ldots, i_r$ in $\mathbf{S}$
- the grey level of this combined share is proportional to the Hamming weight $w_H(v)$ of the "or"ed m-vector v
- this grey level is interpreted by the visual system of the users as black if $w_H(v) \geq d$ and as white if $w_H(v) \leq d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha \geq 0$

Properties of (k, n) scheme

- Contrast
  - for $\mathbf{S}$ in $\mathbf{C_0}$ (white): $w_H(v) \leq d - \alpha m$
  - for $\mathbf{S}$ in $\mathbf{C_1}$ (black): $w_H(v) \geq d$
- Security
  - the two collections of $q \times m$ $(1 \leq q < k)$ matrices, formed by restricting $n \times m$ matrices in $\mathbf{C_0}$ and $\mathbf{C_1}$ to any q rows, are indistinguishable (in the sense that they contain the same matrices with the same frequencies)
- Uniformity
  - there is a function f such that for any matrix in $\mathbf{C_0}$ or $\mathbf{C_1}$ the Hamming weight of "or"ed q rows is $f(q)$

The parameters of a scheme

- m – the number of pixels in a share, we would like m to be as small as possible
- α – the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original picture, we would like α to be as large as possible
- r – the size of the collections $\mathbf{C_0}$ and $\mathbf{C_1}$, $\log r$ represents the number of random bits needed to generate the shares and does not effect the quality of the picture

2 out of 2 visual secret sharing problem

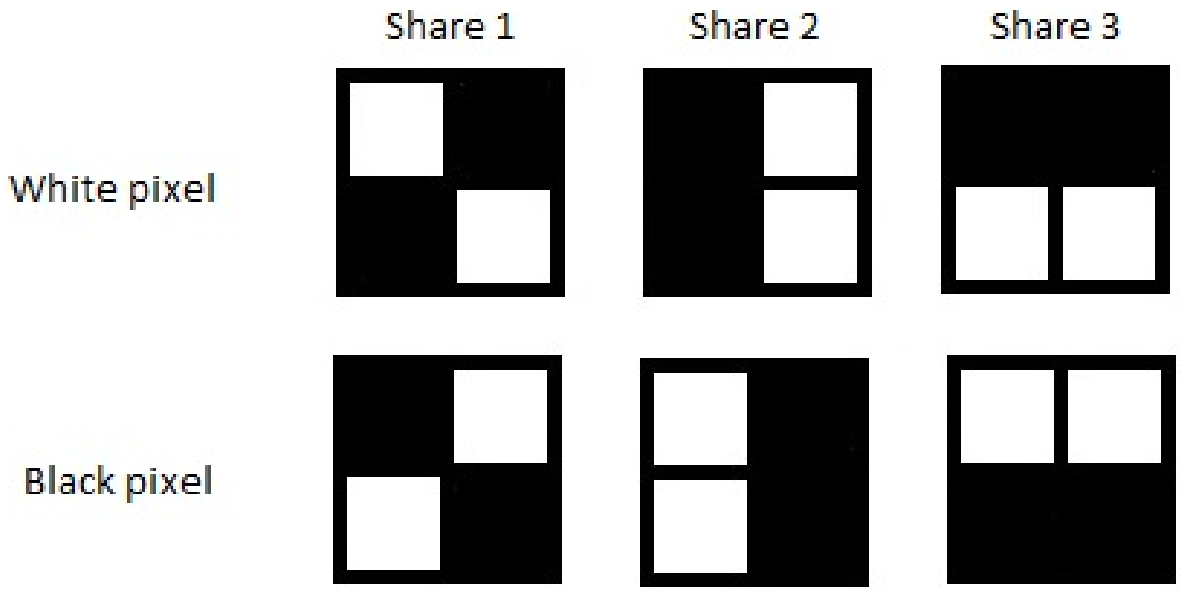
- a white pixel is shared into two identical arrays from the list
- a black pixel is shared into two complementary arrays from the list
- when two shares are stacked together, the result is either medium grey (which represents white) or completely black (which represents black)

3 out of n ($n \geq 3$) visual secret sharing problem

- $\mathbf{B}$ – the $n \times (n-2)$ matrix which contains only 1's
- $\mathbf{I}$ – the identity $n \times n$ matrix
- $\mathbf{BI}$ – the $n \times (2n-2)$ matrix obtained by concatenating $\mathbf{B}$ and $\mathbf{I}$
- $\mathbf{c(BI)}$ – the Boolean complement of the matrix $\mathbf{BI}$
- $\mathbf{C_0} = \{$all the matrices obtained by permuting the columns of $\mathbf{c(BI)}\}$
- $\mathbf{C_1} = \{$all the matrices obtained by permuting the columns of $\mathbf{BI}\}$

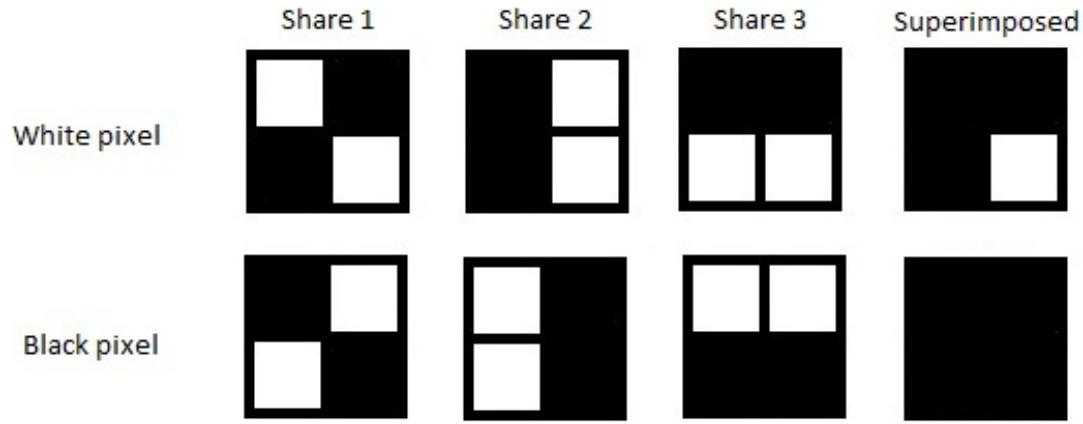
(3,3) Scheme Example

- $\mathbf{BI} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$, $\mathbf{c}(\mathbf{BI}) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$
- permutation is $\{2, 3, 4, 1\}$



(3,3) Scheme Example – Contrast

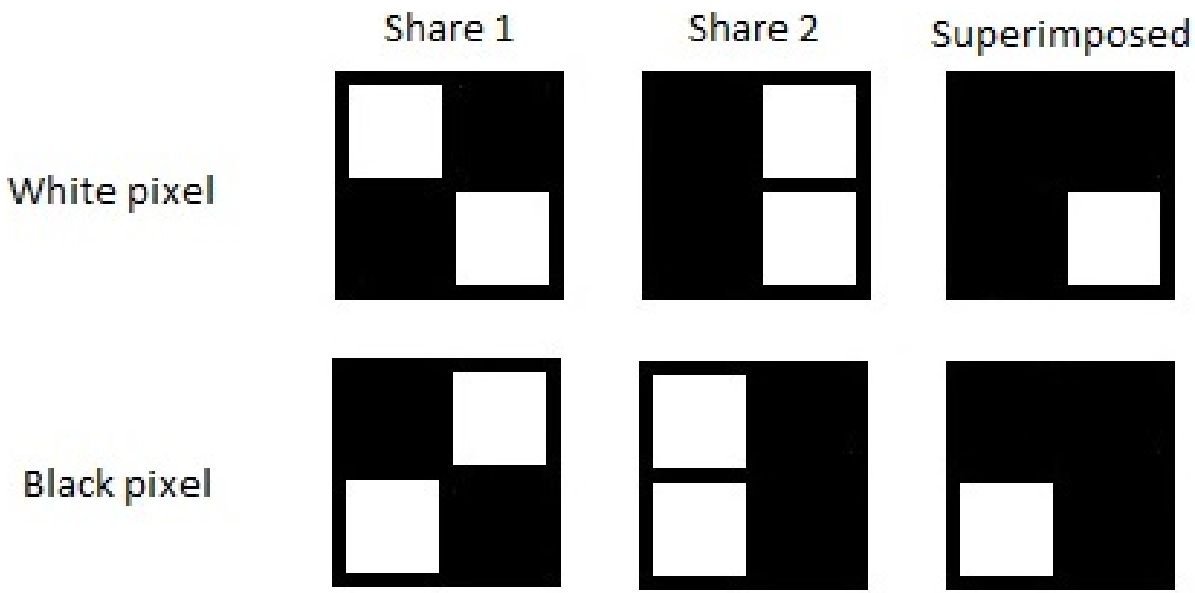
- $\alpha = \frac{1}{4}$



- can also be seen by Hamming weight:
  - black: $\mathbf{BI} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$, $w_H(v) = 4$
  - white: $\mathbf{c(BI)} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$, $w_H(v) = 3$

(3,3) Scheme Example – Security

- superimposing less than 3 shares does not reveal if secret pixel is white or black
- Hamming weight of 2 superimposed shares is always 3



A general k out of k scheme

- $m = 2^{k-1}$, $\alpha = \frac{1}{2^{k-1}}$, $r = 2^{k-1}!$
- a ground set $W = \{e_1, e_2, \ldots, e_k\}$ of k elements
- even cardinality subsets of W $\pi_1, \pi_2, \ldots, \pi_{2^{k-1}}$
- odd cardinality subsets of W $\sigma_1, \sigma_2, \ldots, \sigma_{2^{k-1}}$
- $k \times 2^{k-1}$ matrices $\mathbf{S_0}$ and $\mathbf{S_1}$:
  - $\mathbf{S_0}[i,j] = 1$ iff $e_i \in \pi_j$
  - $\mathbf{S_1}[i,j] = 1$ iff $e_i \in \sigma_j$
- the collections $\mathbf{C_0}$ and $\mathbf{C_1}$ are obtained by permuting all the columns of the corresponding matrix

A general k out of k scheme – Example

- $(4,4)$ scheme, $m = 8$, $\alpha = \frac{1}{8}$
- $W = \{1,2,3,4\}$
- Even cardinality subsets:
  $\{\{\},\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},\{1,2,3,4\}\}$
- Odd cardinality subsets:
  $\{\{1\},\{2\},\{3\},\{4\},\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$
- $\mathbf{S_0} = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$, $w_H(v) = 7$
- $\mathbf{S_1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$, $w_H(v) = 8$

A general k out of k scheme

Lemma

The above scheme is a k out of k scheme with parameters $m = 2^{k-1}$, $\alpha = \frac{1}{2^{k-1}}$ and $r = 2^{k-1}!$.

Theorem

In any k out of k scheme $\alpha \leq \frac{1}{2^{k-1}}$ and $m \geq 2^{k-1}$.

A general k out of n scheme

- Let C be an uniform k out of k visual secret sharing scheme with parameters m, r, α
  - $\mathbf{C_0} = \mathbf{T_1^0}, \mathbf{T_2^0}, \ldots, \mathbf{T_r^0}$
  - $\mathbf{C_1} = \mathbf{T_1^1}, \mathbf{T_2^1}, \ldots, \mathbf{T_r^1}$
  - there is a function $f(q)$ such that for any matrix $\mathbf{T_i^t}$ where $t \in \{0, 1\}$ and $1 \leq i \leq r$ and for every $1 \leq q \leq k-1$ rows of $\mathbf{T_i^t}$ the Hamming weight of the "or" of the q rows is $f(q)$
- Let H be a collection of l functions $(h_1, \ldots, h_l)$ such that
  1. $\forall h \in H$ we have $h : \{1, \ldots, n\} \to \{1, \ldots, k\}$
  2. for all subsets $B \subset \{1, \ldots, n\}$ of size k and for all $1 \leq q \leq k$ the probability that a randomly chosen $h \in H$ yields q different values on B is the same (denote this probability by β_q)

A general k out of n scheme

We construct from C and H a k out of n scheme C' as follows:

- each $1 \leq t \leq r^l$ is indexed by a vector $(t_1, t_2, \ldots, t_l)$ where each $1 \leq t_i \leq r$
- the matrix $\mathbf{S_t^b}$ for $t = (t_1, t_2, \ldots, t_l)$ where $b \in \{0, 1\}$ is defined as

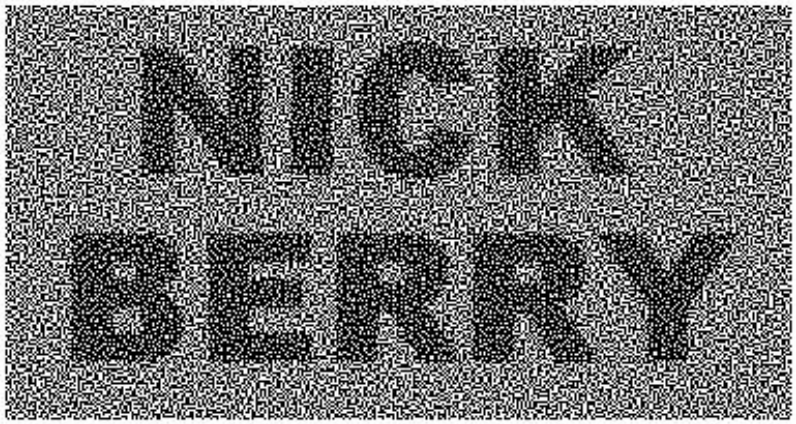
$$\mathbf{S_t^b}[i, (j, u)] = \mathbf{T_{t_u}^b}[h_u(i), j]$$

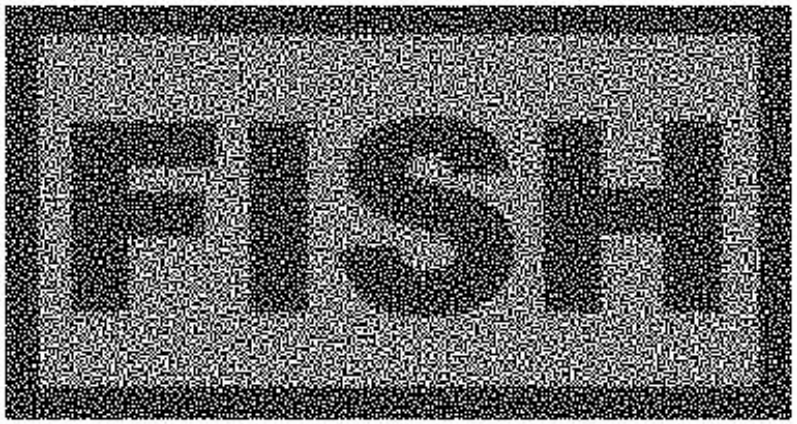
Lemma

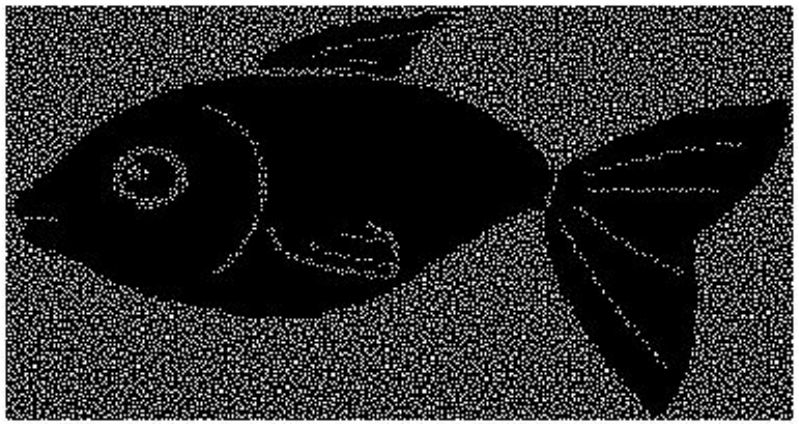
If C is a scheme with parameters m, α, r, then C' is a scheme with parameters $m' = ml, \alpha' = \alpha\beta_k, r' = r^l$.

Visual Steganography

- the two source images, a third secret image we want to encode

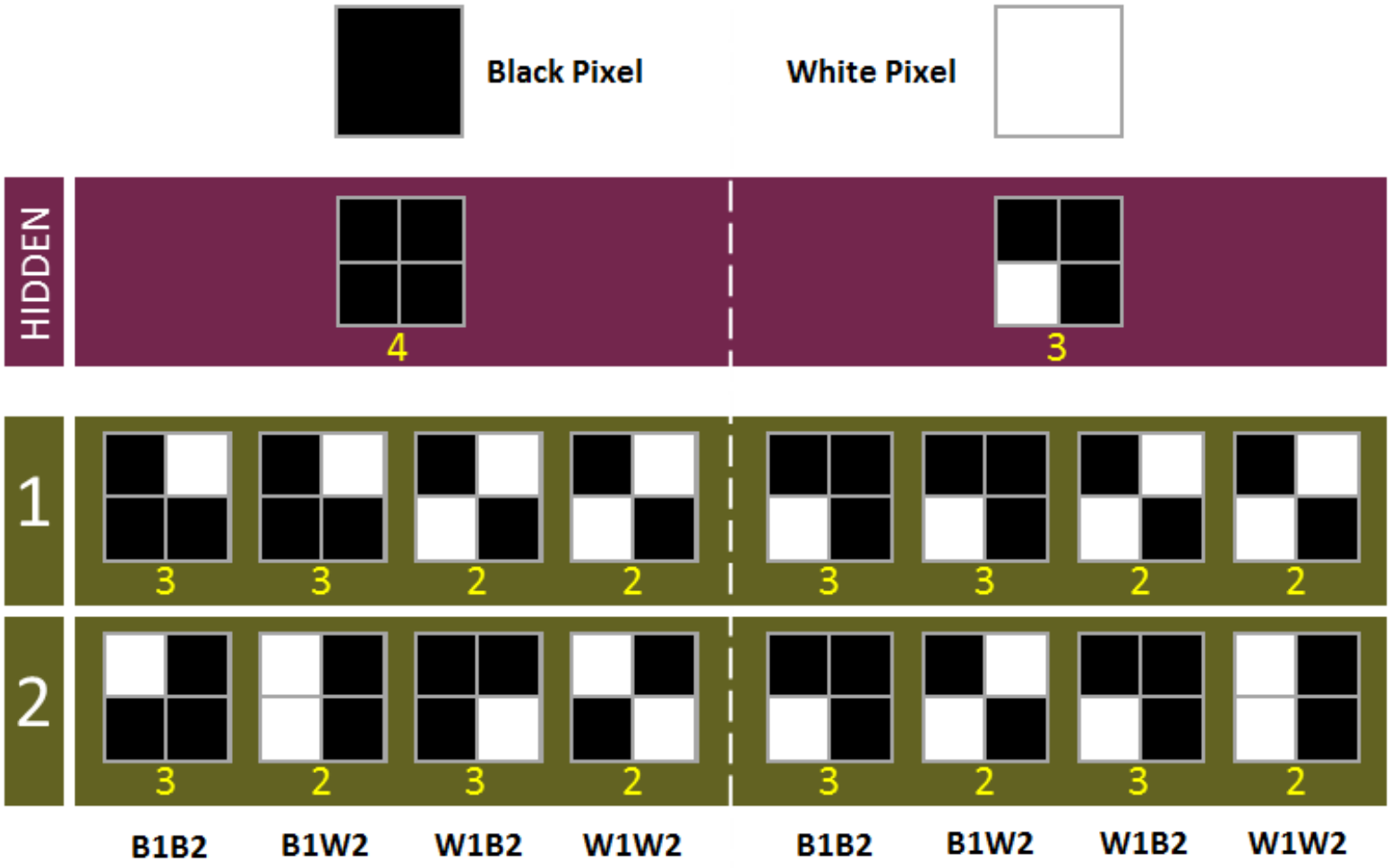






Visual Steganography

- we divide each pixel into (2 x 2) subpixels



References

- M. Naor and A. Shamir, Visual Cryptography, in “Advances in Cryptology – Eurocrypt ’94”, A. De Santis Ed., Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp. 1–12, 1995.
- http://www.datagenetics.com/blog/november32013/
- http://www.cs.jhu.edu/ fabian/courses/CS600.624/slides/ /VisualCrypto.pdf