elicsir
Elevating Italian Computer Science Innovation and Research

Visual Cryptography for Color Images

Dalle immagini in bianco e nero alla percezione cromatica

Elettra Palmisano - Politecnico di Torino

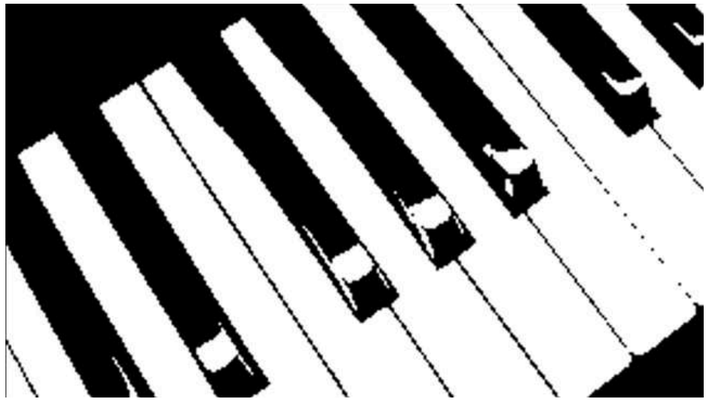
Mentore: Roberto De Prisco - Università degli studi di Salerno

Introduzione alla Visual Cryptography

Tecnica di *secret sharing* per condividere immagini, introdotta da Naor e Shamir nel 1994.

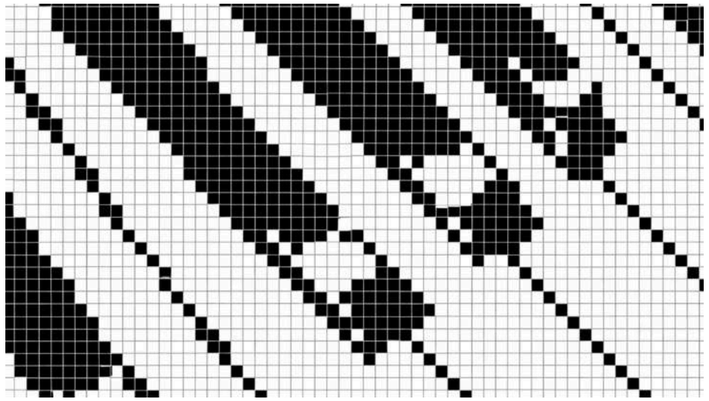
secret sharing → metodo crittografico che suddivide un dato sensibile in più frammenti chiamati *share*, distribuiti tra vari partecipanti. Il segreto può essere ricostruito solo unendo un insieme autorizzato di frammenti, impedendo a singoli individui e partecipanti non autorizzati di accedervi.

Introduzione alla Visual Cryptography



segreto

Introduzione alla Visual Cryptography



segreto

immagine = griglia di pixel

Introduzione alla Visual Cryptography

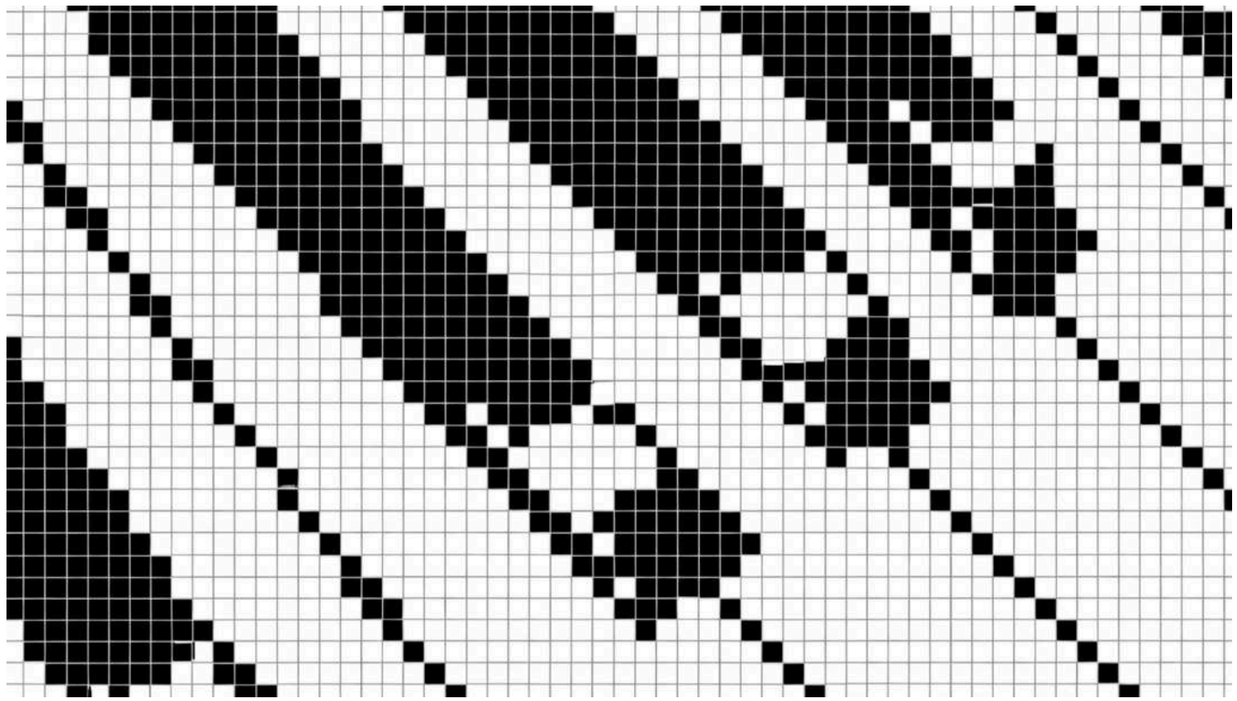
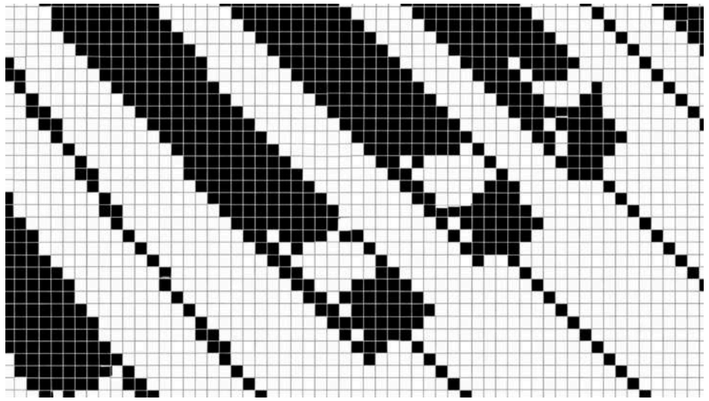


immagine = griglia di pixel

Ogni pixel corrisponde a un elemento M_{ij} di una matrice:

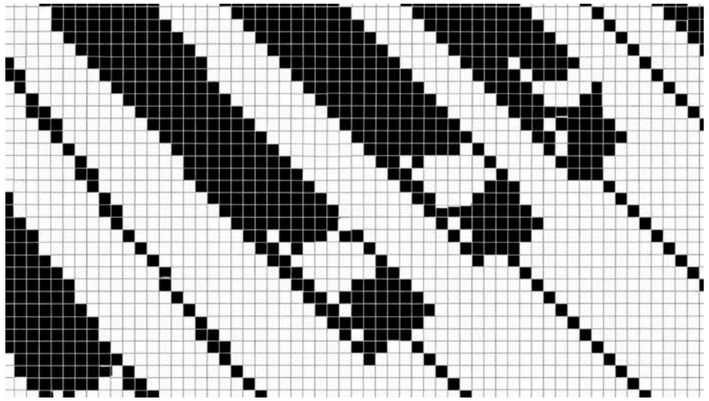
$$M = \begin{bmatrix} 1 & 1 & 1 & \dots \\ 0 & 1 & 0 & \dots \\ 1 & 0 & 1 & \dots \\ \dots & \dots & \dots & \dots \end{bmatrix}$$

Introduzione alla Visual Cryptography



segreto

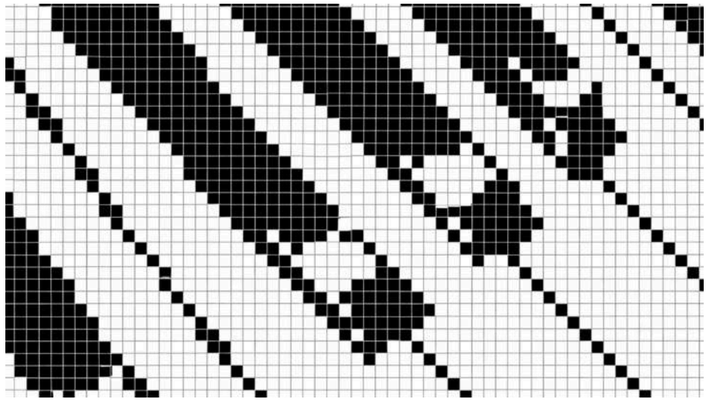
Introduzione alla Visual Cryptography



segreto

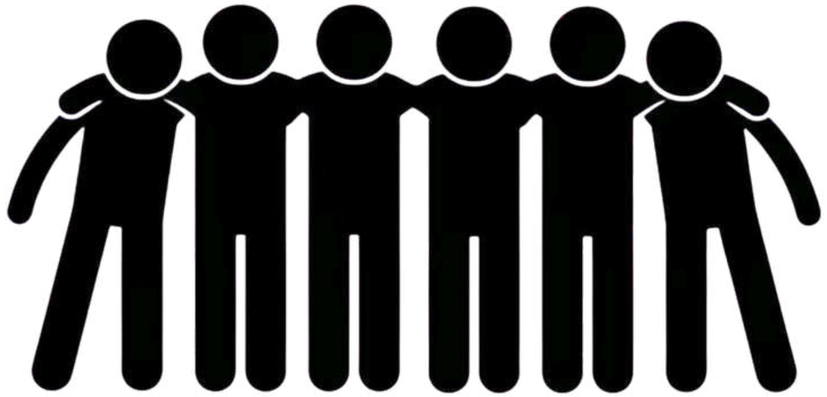
dealer

Introduzione alla Visual Cryptography



segreto

dealer

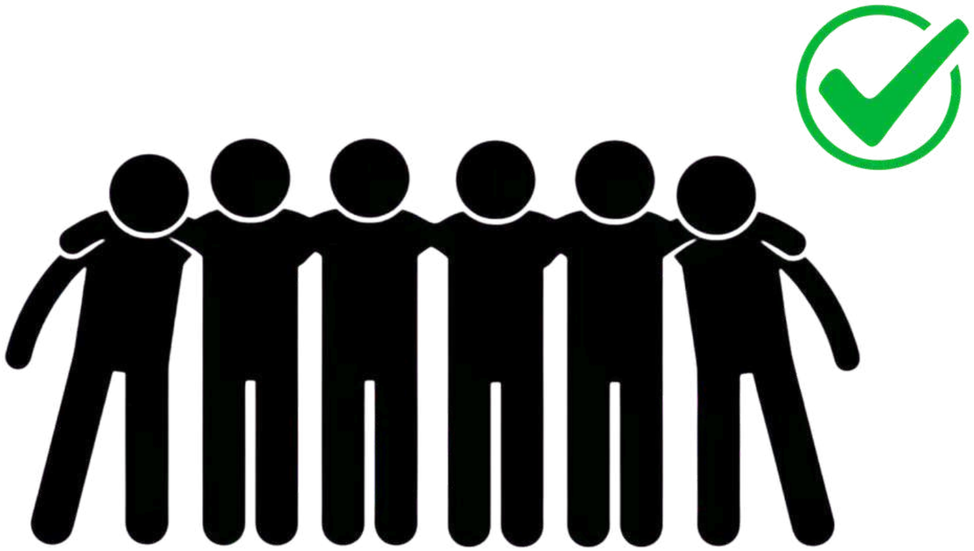


partecipanti

$$P = \{1, 2, \ldots, n\}$$

Struttura di accesso: insiemi Qualificati e Proibiti

dealer



partecipanti qualificati Q

Struttura di accesso: insiemi Qualificati e Proibiti

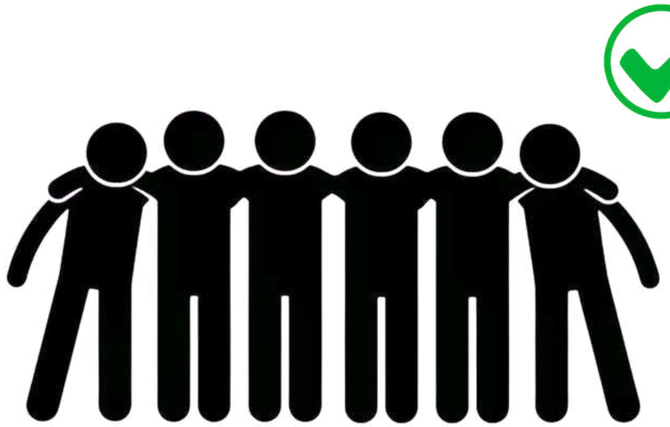
dealer

partecipanti proibiti F

Struttura di accesso: insiemi Qualificati e Proibiti

dealer

partecipanti proibiti F



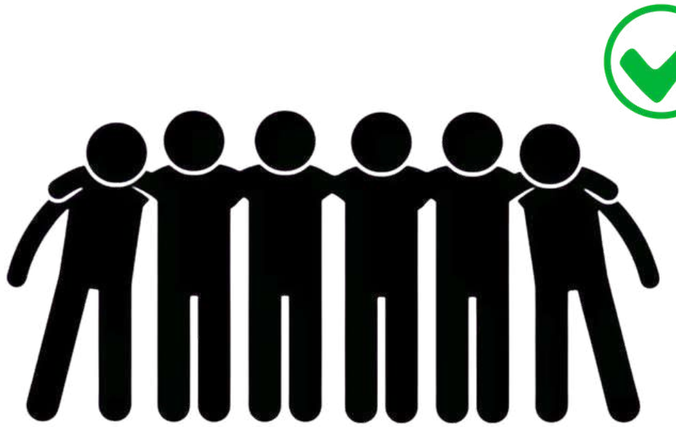
partecipanti qualificati Q

struttura di accesso (Q, F)

Struttura di accesso: insiemi Qualificati e Proibiti

dealer

partecipanti proibiti F



partecipanti qualificati Q

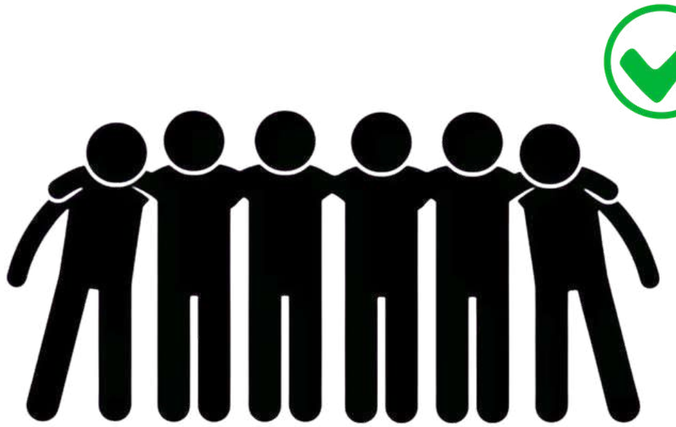
struttura di accesso (Q, F) **forte**:

- Q è monotonicamente crescente,
- F è monotonicamente decrescente,
- $Q \cup F = 2^P$

Struttura di accesso: insiemi Qualificati e Proibiti

dealer

partecipanti proibiti F



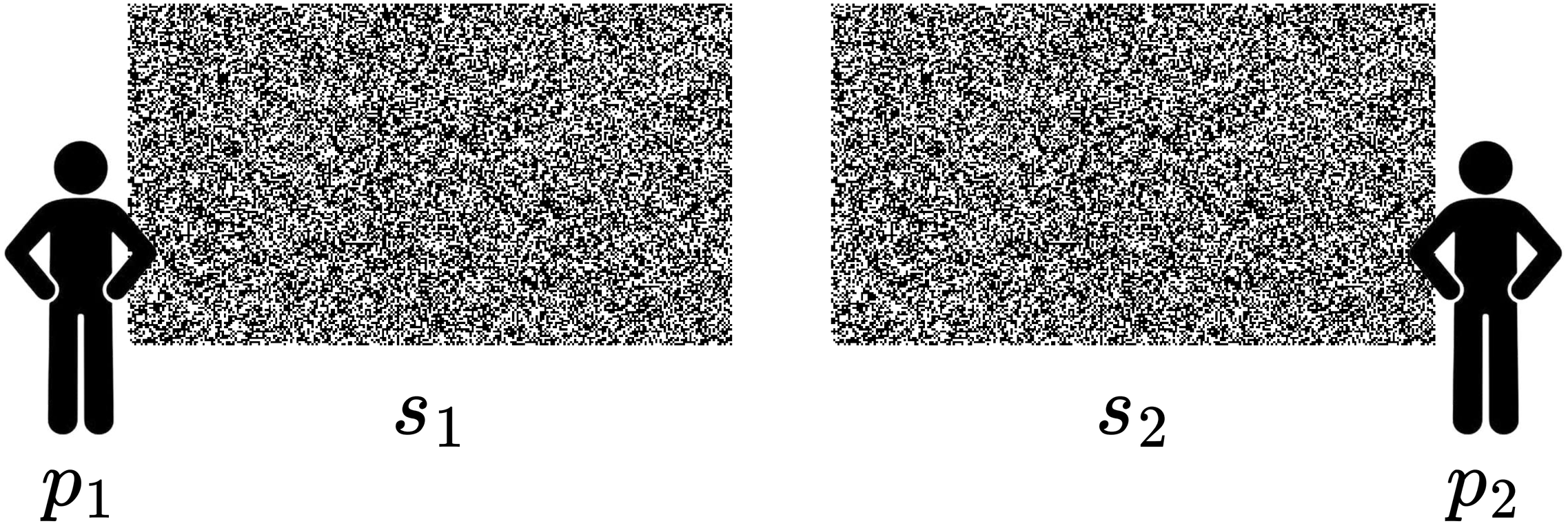
partecipanti qualificati Q

schema a soglia (k, n)

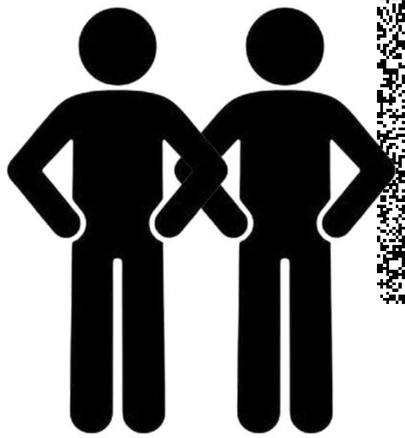
- Q : insiemi con almeno k partecipanti,
- F : insiemi con al massimo $k - 1$ partecipanti,

Cosa significa decodificare il segreto?

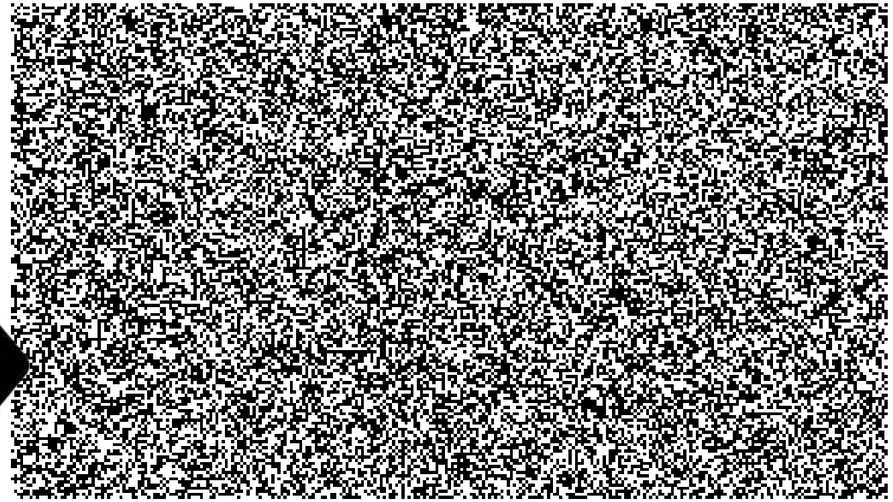
Decodifica del segreto



Decodifica del segreto

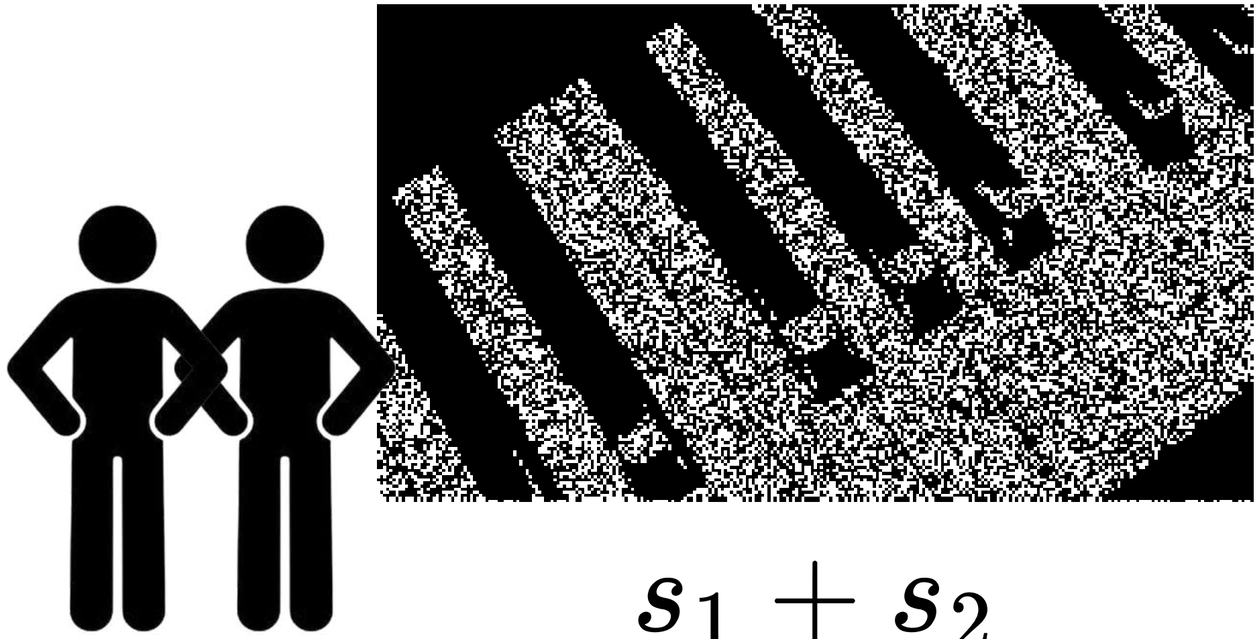


partecipanti qualificati (Q)



$$s_1 + s_2$$

Decodifica del segreto

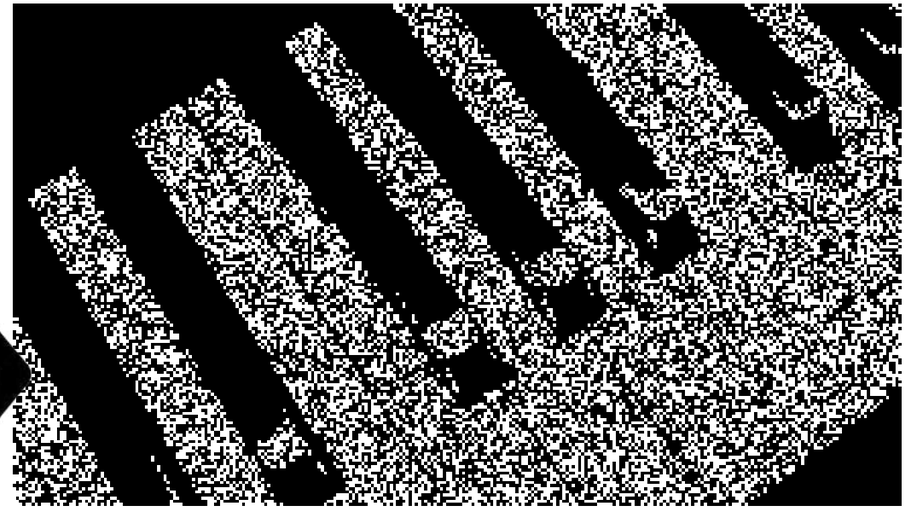


$s_1 + s_2$

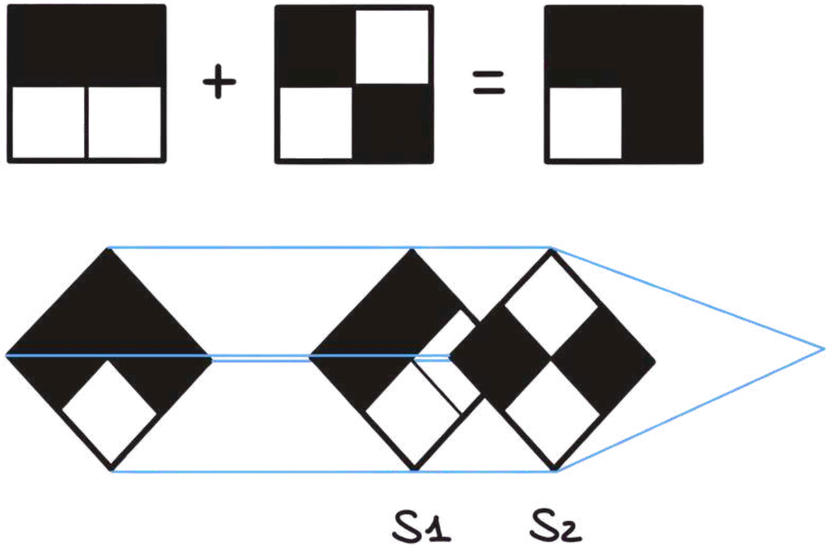
partecipanti qualificati (Q)

Decodifica del segreto

partecipanti qualificati (Q)

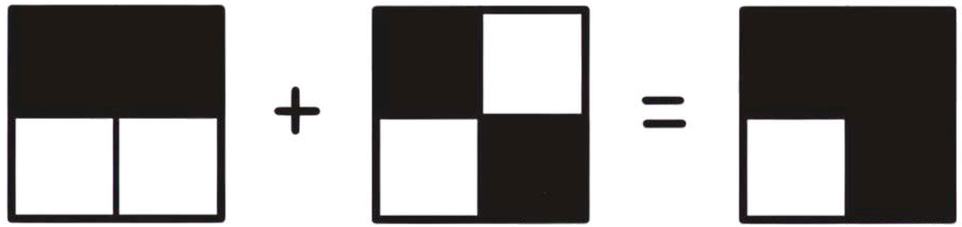


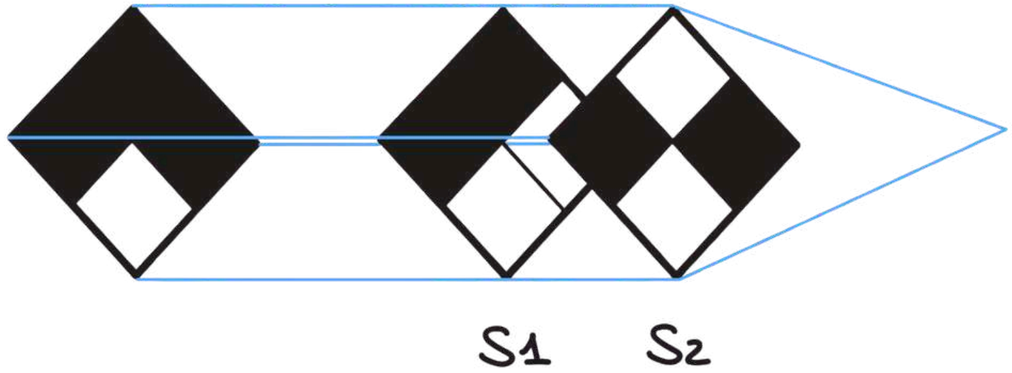
$s_1 + s_2$



Decodifica del segreto

L’operazione di sovrapposizione delle share è assimilabile a calcolare l’or tra i valori dei pixel sovrapposti.

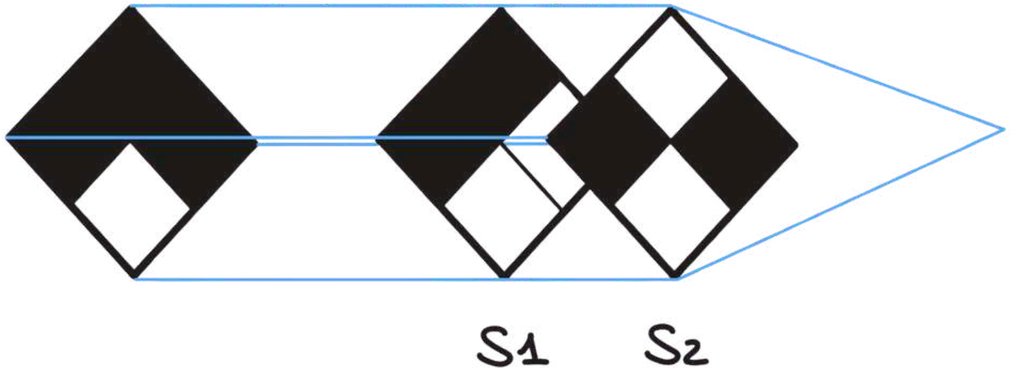




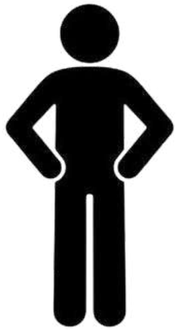
Decodifica del segreto

L’operazione di sovrapposizione delle share è assimilabile a calcolare l’or tra i valori dei pixel sovrapposti.

1	1	+	1	0	=	1	1
0	0		0	1		0	1



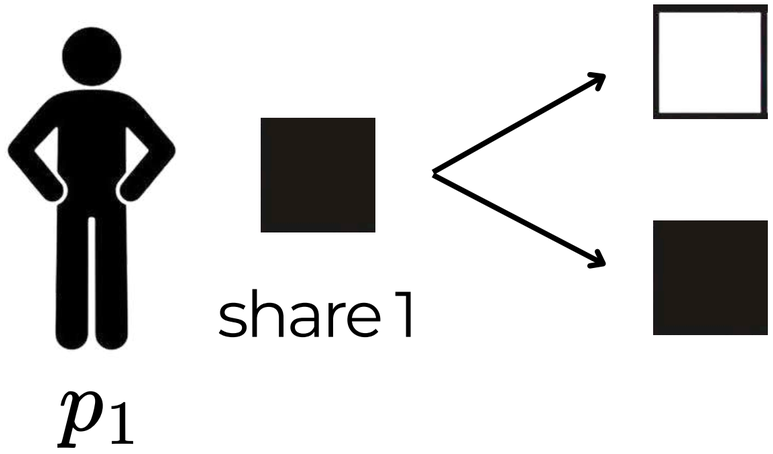
Decodifica del segreto



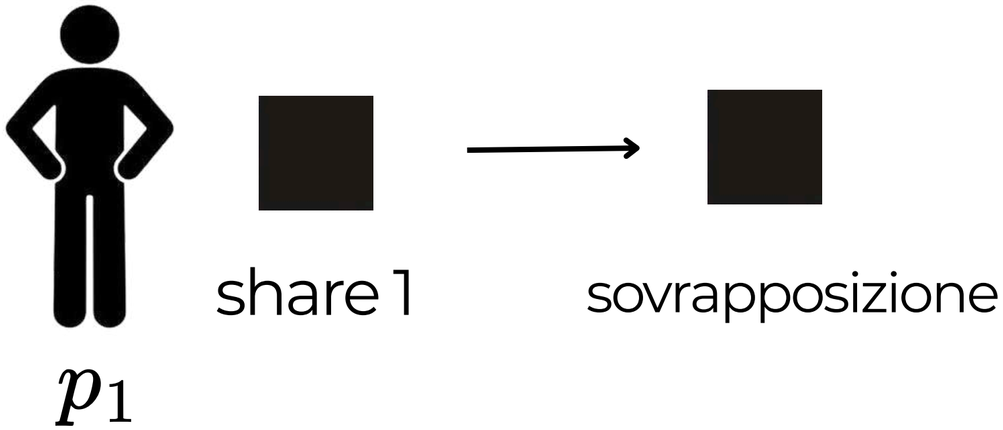
share 1

p_1

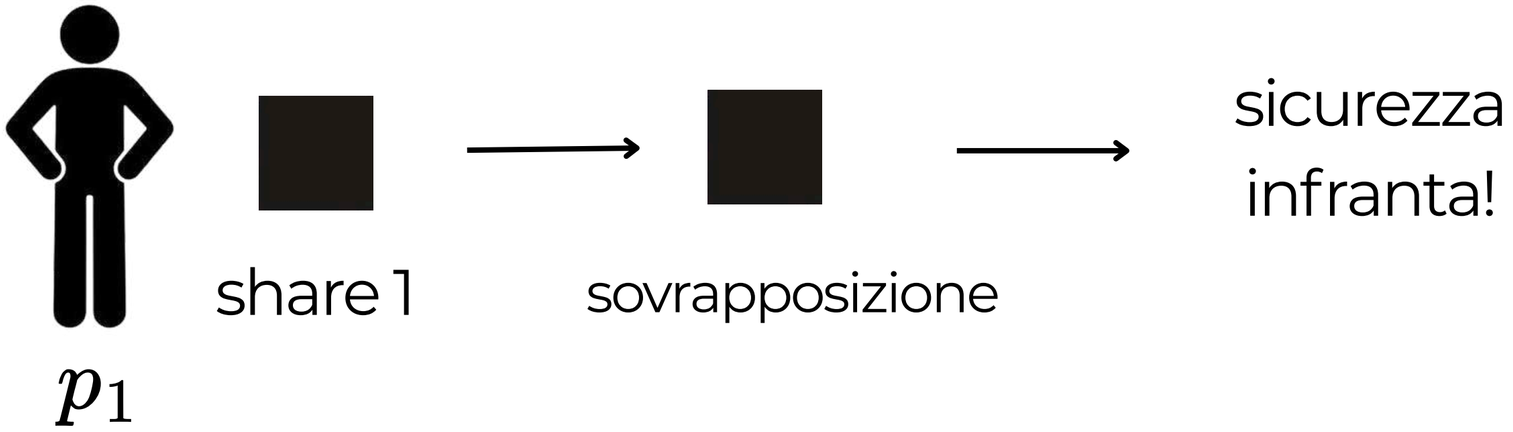
Decodifica del segreto



Decodifica del segreto



Decodifica del segreto



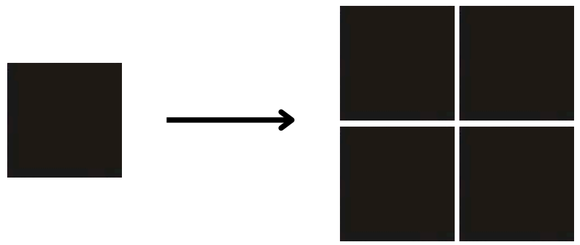
Visual Cryptography Deterministica

Visual Cryptography Deterministica

Ogni pixel dell'immagine segreta viene espanso in un blocco di m sub-pixel.

Visual Cryptography Deterministica

Ogni pixel dell'immagine segreta viene espanso in un blocco di m sub-pixel.

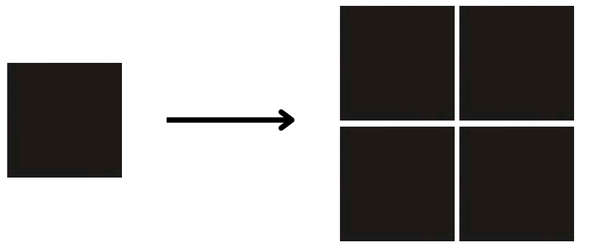


1 pixel
(segreto)

m sub-pixel
(share)

Visual Cryptography Deterministica

Ogni pixel dell'immagine segreta viene espanso in un blocco di m sub-pixel.



1 pixel
(segreto)

m sub-pixel
(share)

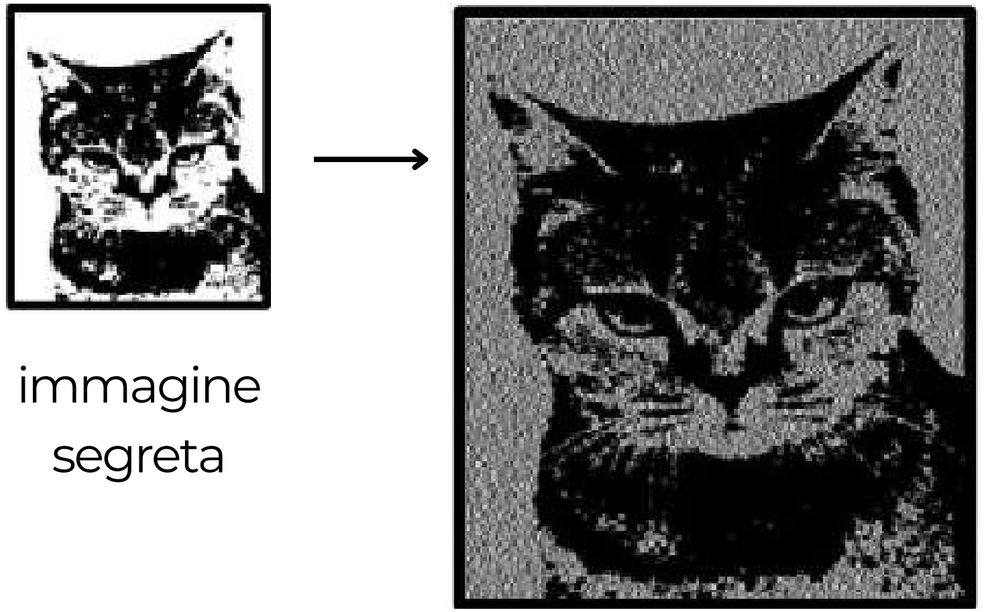
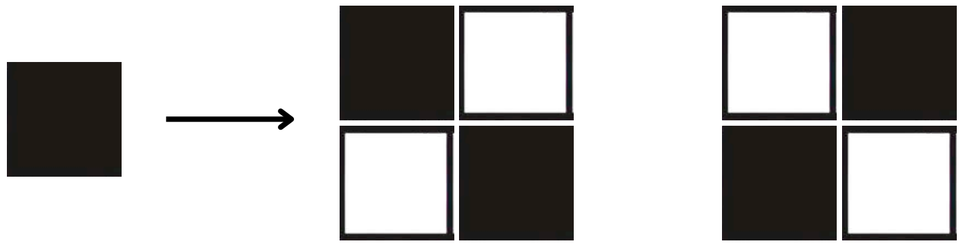


immagine
segreta

immagine
ricostruita

Visual Cryptography Deterministica

Ogni pixel dell'immagine segreta viene espanso in un blocco di m sub-pixel.



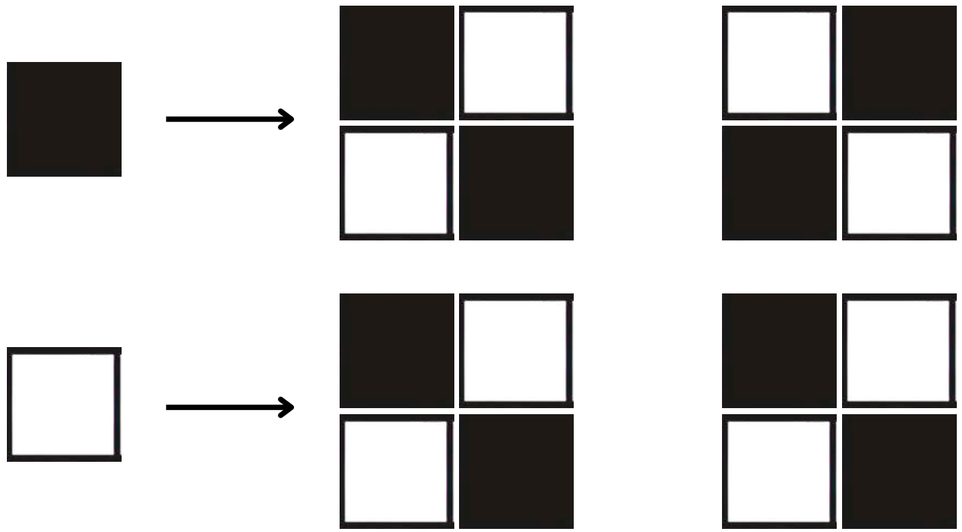
1 pixel segreto

share 1

share 2

Visual Cryptography Deterministica

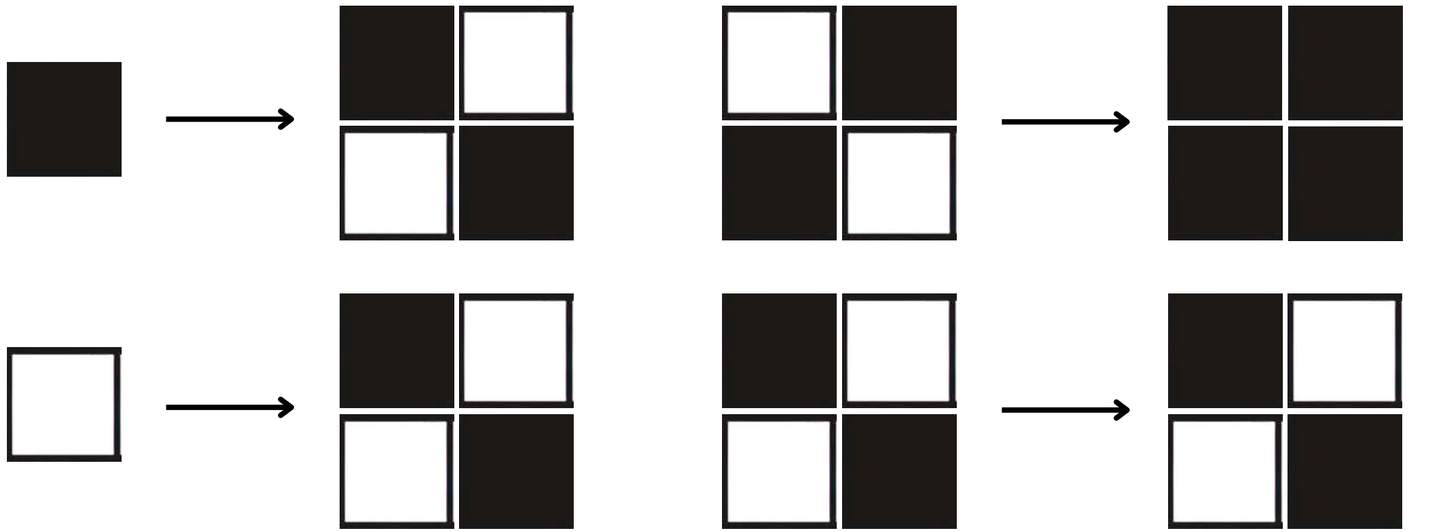
Ogni pixel dell'immagine segreta viene espanso in un blocco di m sub-pixel.



1 pixel segreto | share 1 | share 2

Visual Cryptography Deterministica

Ogni pixel dell'immagine segreta viene espanso in un blocco di m sub-pixel.

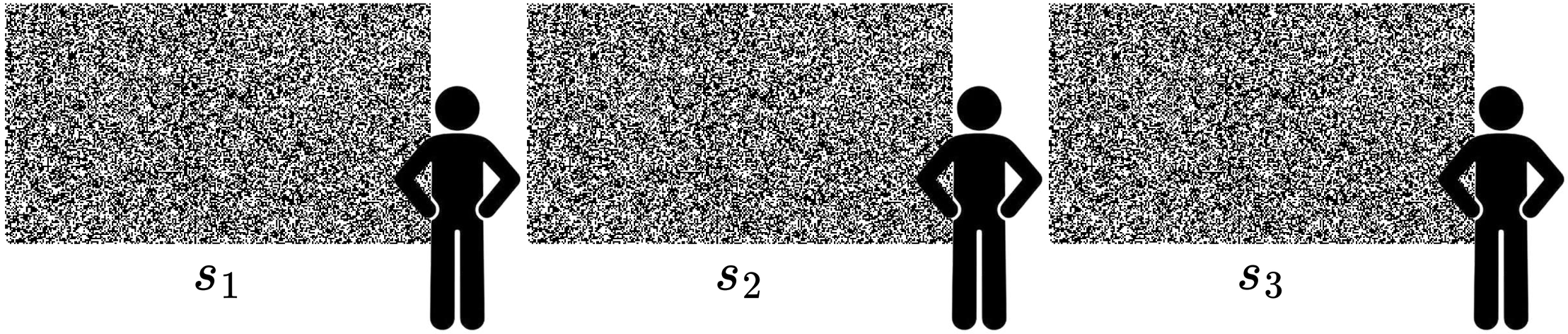


1 pixel segreto | share 1 | share 2 | ricostruzione

Esempio (3, 3)-threshold VCS, m = 4

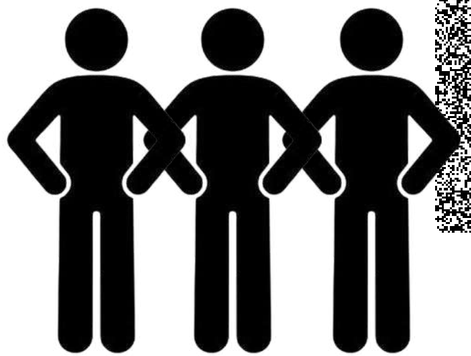
Esempio (3, 3)-threshold VCS, m = 4

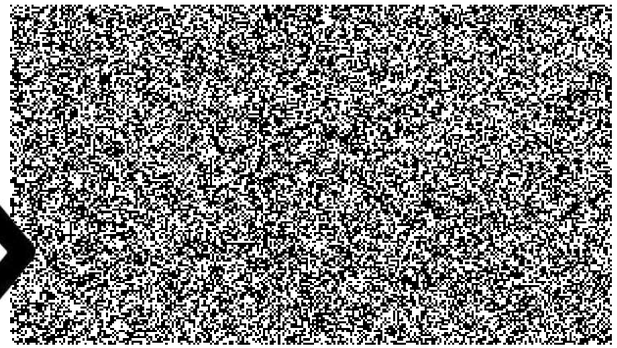
- 3 partecipanti → 3 share
- 1 pixel segreto → 4 sub-pixel nelle share



Esempio (3, 3)-threshold VCS, m = 4

- 3 partecipanti → 3 share
- 1 pixel segreto → 4 sub-pixel nelle share



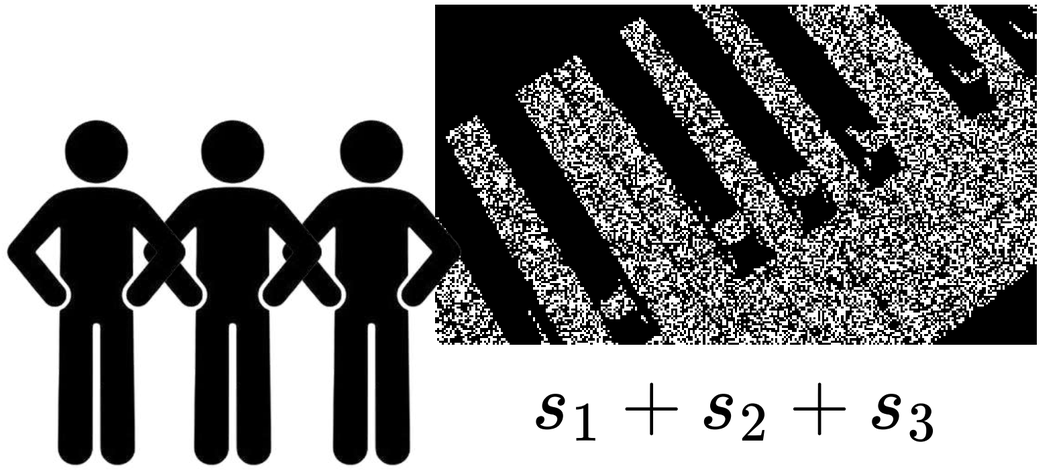


$s_1 + s_2 + s_3$

partecipanti qualificati (Q)

Esempio (3, 3)-threshold VCS, m = 4

- 3 partecipanti → 3 share
- 1 pixel segreto → 4 sub-pixel nelle share



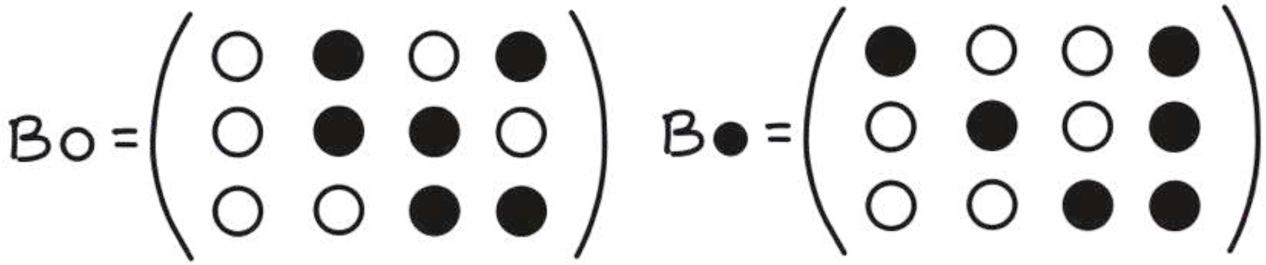
$s_1 + s_2 + s_3$

partecipanti qualificati (Q)

Come fa il dealer a generare le share?

Esempio (3, 3)-threshold VCS, m = 4

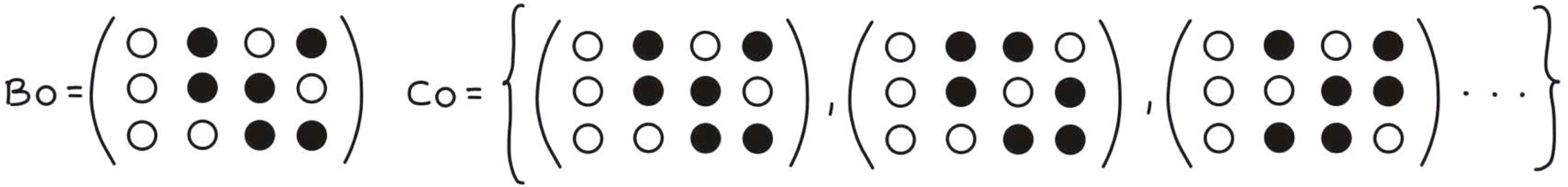
Il dealer genera due matrici di dimensione $n \times m$, chiamate **matrici di base**.



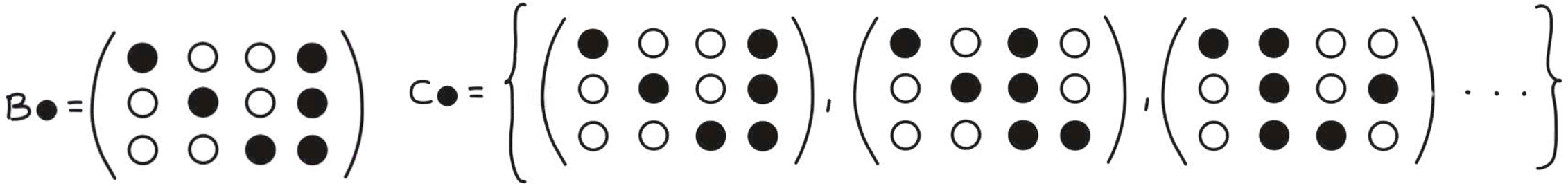
per i pixel bianchi per i pixel neri

Esempio (3, 3)-threshold VCS, m = 4

Il dealer costruisce i **set di matrici di distribuzione** ottenuti dalla permutazione delle colonne delle matrici di base:



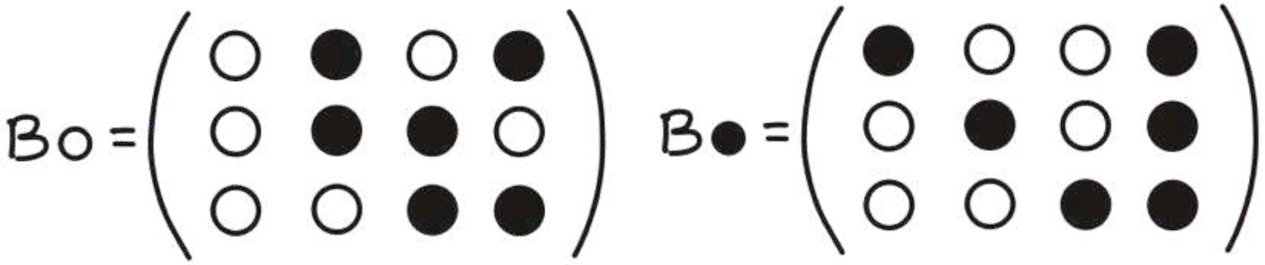
per i pixel bianchi



per i pixel neri

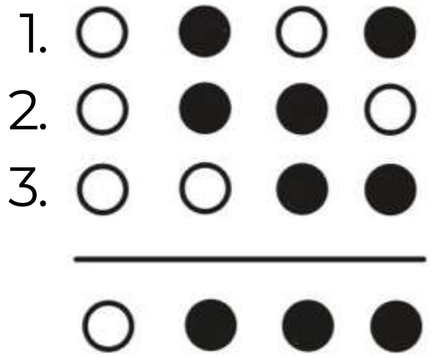
Esempio (3, 3)-threshold VCS, m = 4

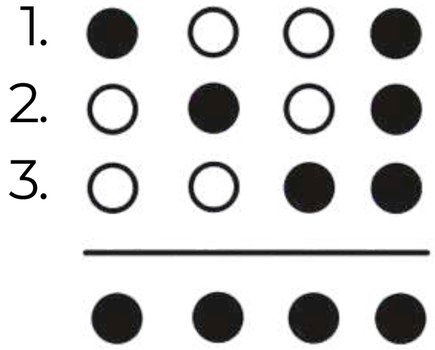
Proprietà di contrasto



per i pixel bianchi

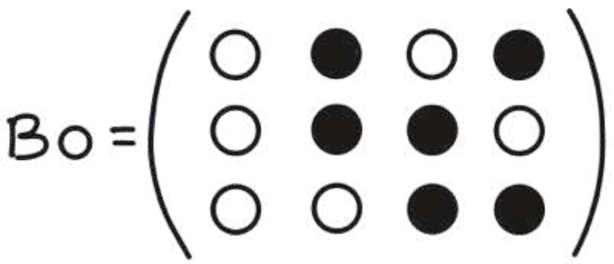
per i pixel neri



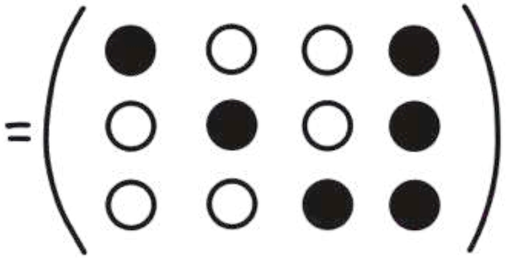


Esempio (3, 3)-threshold VCS, m = 4

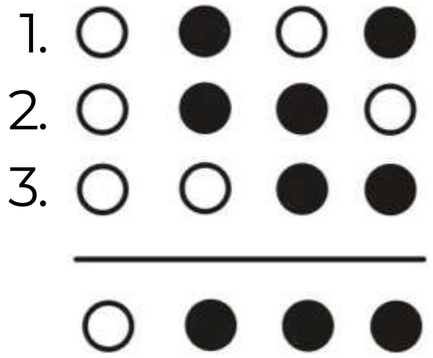
Proprietà di contrasto

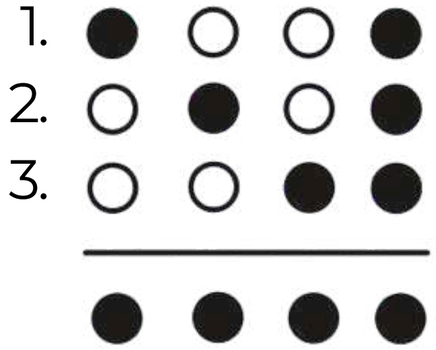


per i pixel bianchi



per i pixel neri



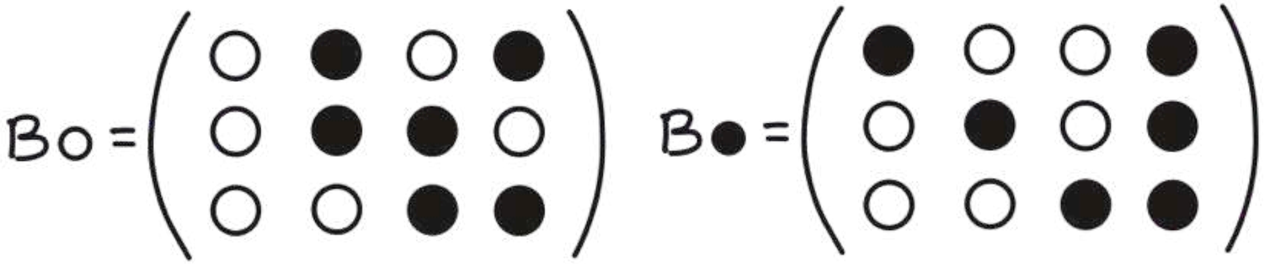


Esistono due soglie l e h con $0 < l < h < m$ tali che per ogni insieme qualificato Q :

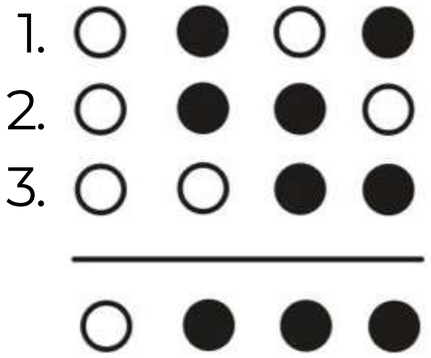
- Se il pixel segreto è **bianco** → il blocco sovrapposto ha al **massimo** l subpixel **neri**.
- Se il pixel segreto è **nero** → il blocco sovrapposto ha **almeno** h subpixel **neri**.

Esempio (3, 3)-threshold VCS, m = 4

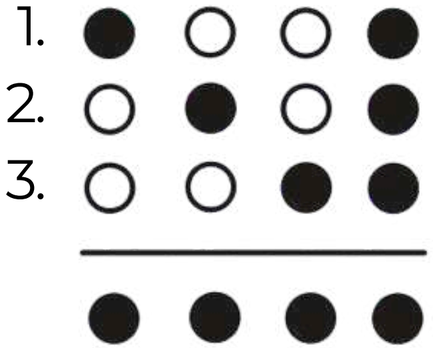
Proprietà di contrasto



per i pixel bianchi per i pixel neri



$l = 3$



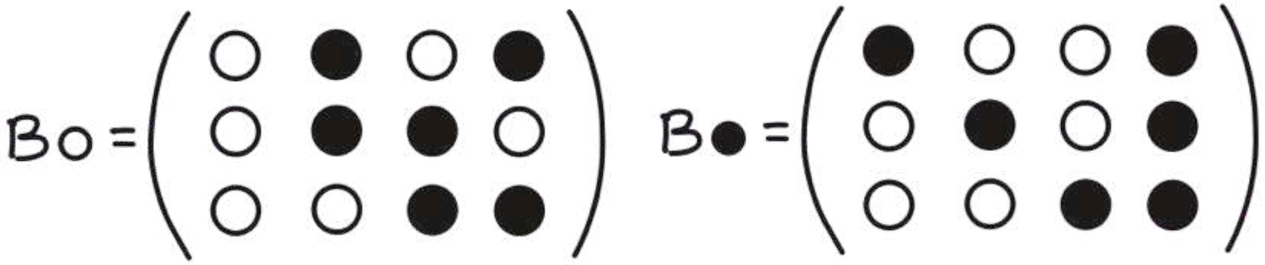
$h = 4$

Esistono due soglie l e h con $0 < l < h < m$ tali che per ogni insieme qualificato Q :

- Se il pixel segreto è **bianco** → il blocco sovrapposto ha al **massimo** l subpixel **neri**.
- Se il pixel segreto è **nero** → il blocco sovrapposto ha **almeno** h subpixel **neri**.

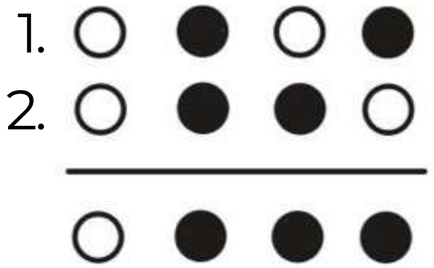
Esempio (3, 3)-threshold VCS, m = 4

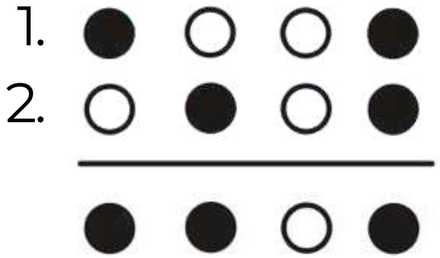
Proprietà di sicurezza



per i pixel bianchi

per i pixel neri



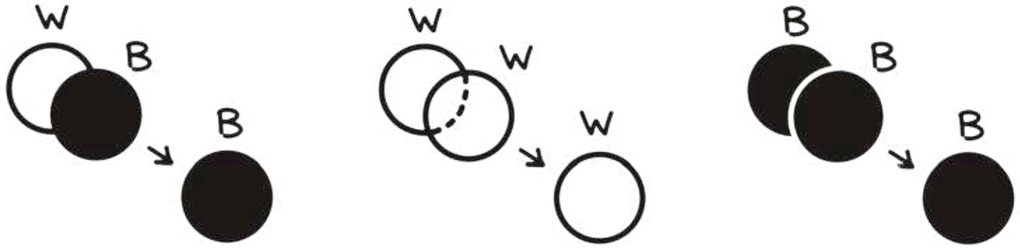


Per ogni insieme proibito F
le **distribuzioni** ottenute come risultato della sovrapposizione delle share risultano **indistinguibili** per pixel bianchi e neri.

Visual Cryptography per immagini a colori

Visual Cryptography per immagini a colori

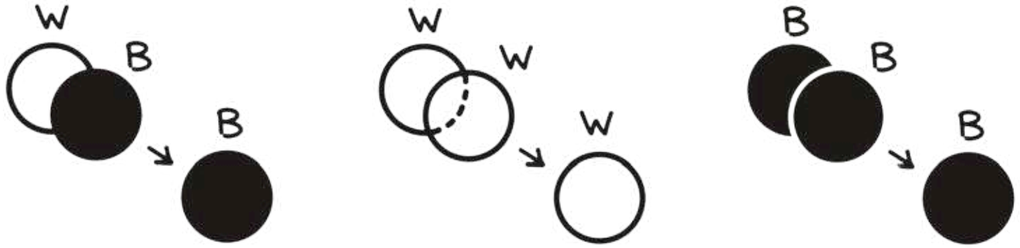
- B/W → $\Sigma = \{black, white\}$



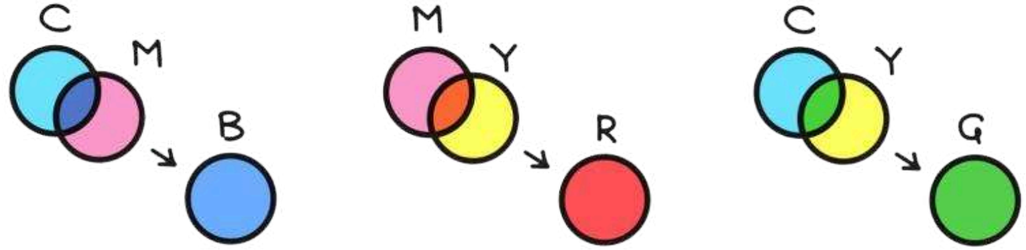
- Colori → $\Sigma = \{0, 1, \ldots, c-1\}$

Visual Cryptography per immagini a colori

- B/W → $\Sigma = \{black, white\}$

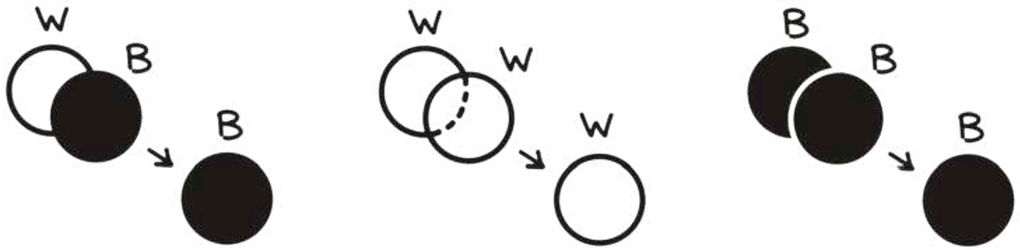


- Colori → $\Sigma = \{0, 1, \ldots, c-1\}$

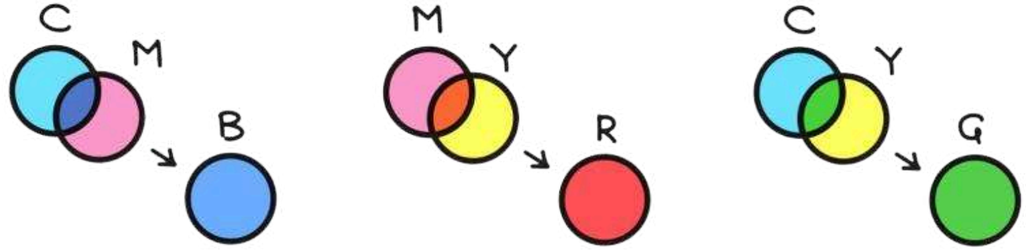


Visual Cryptography per immagini a colori

- B/W → $\Sigma = \{black, white\}$



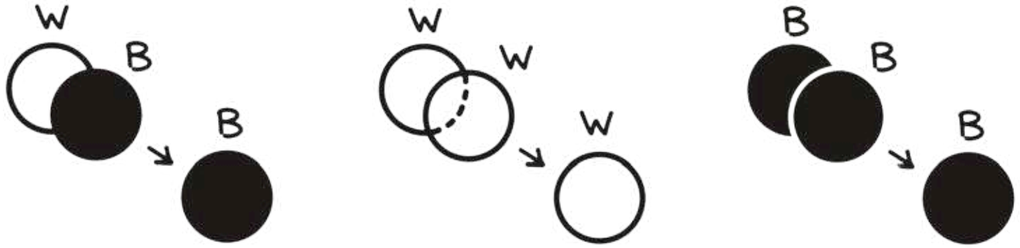
- Colori → $\Sigma = \{0, 1, \ldots, c-1\}$



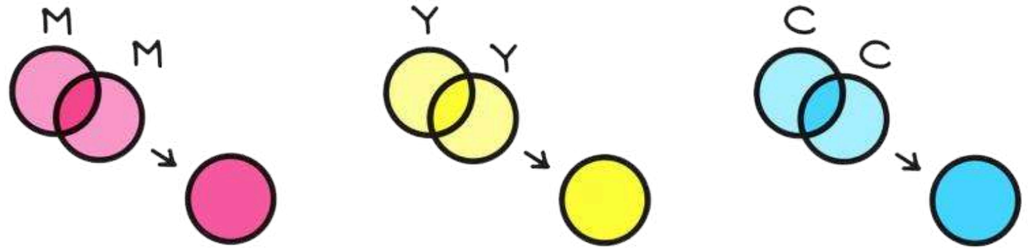
*Cosa succede sovrapponendo pixel di **colori differenti**?*

Visual Cryptography per immagini a colori

- B/W → $\Sigma = \{black, white\}$



- Colori → $\Sigma = \{0, 1, \ldots, c-1\}$

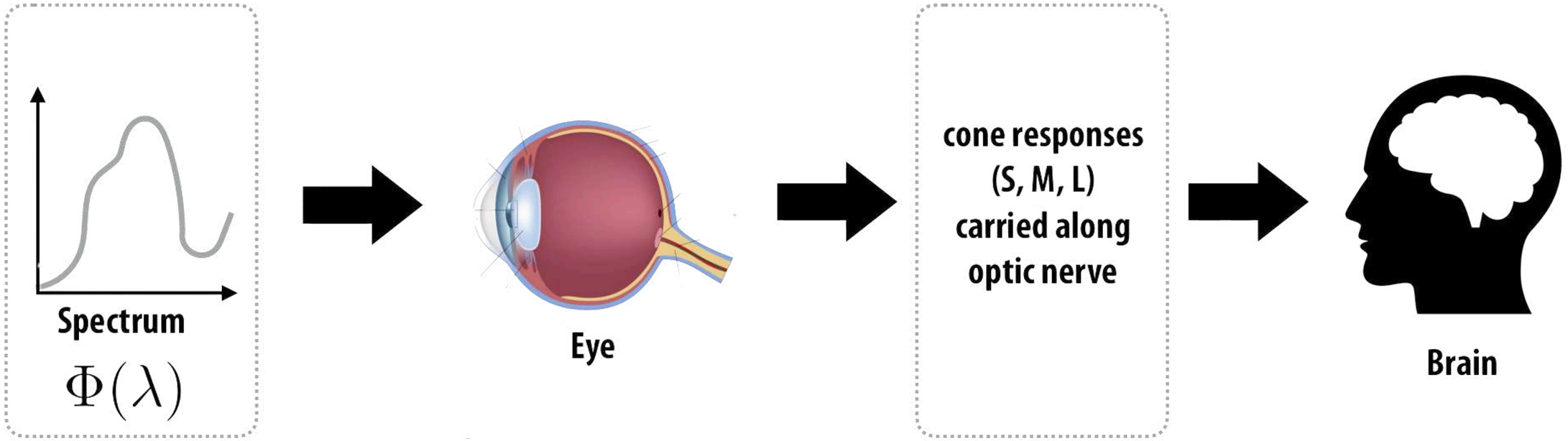


Fenomeno del Darkening

*Cosa succede sovrapponendo pixel dello **stesso colore**?*

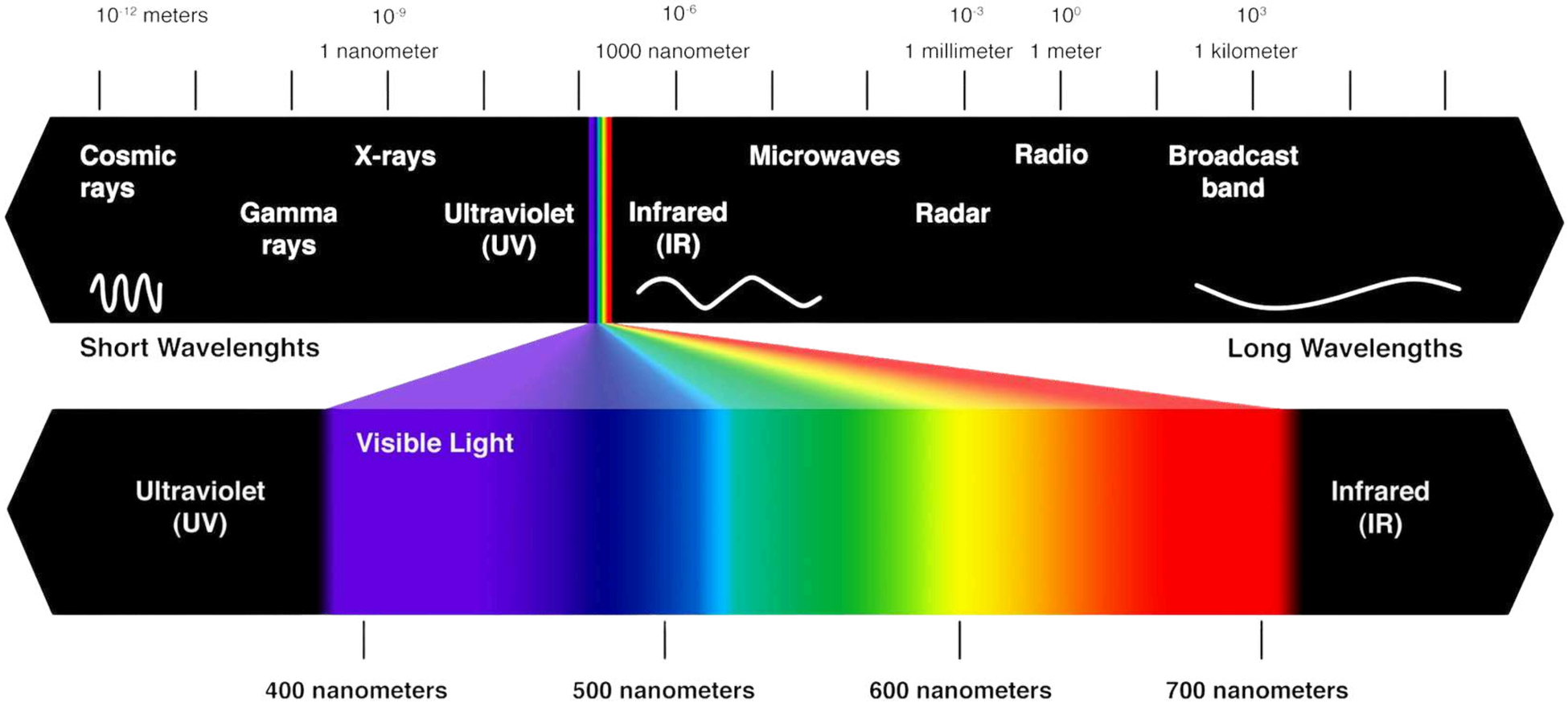
Cosa succede sovrapponendo pixel ***colorati****?*

Visual Cryptography per immagini a colori

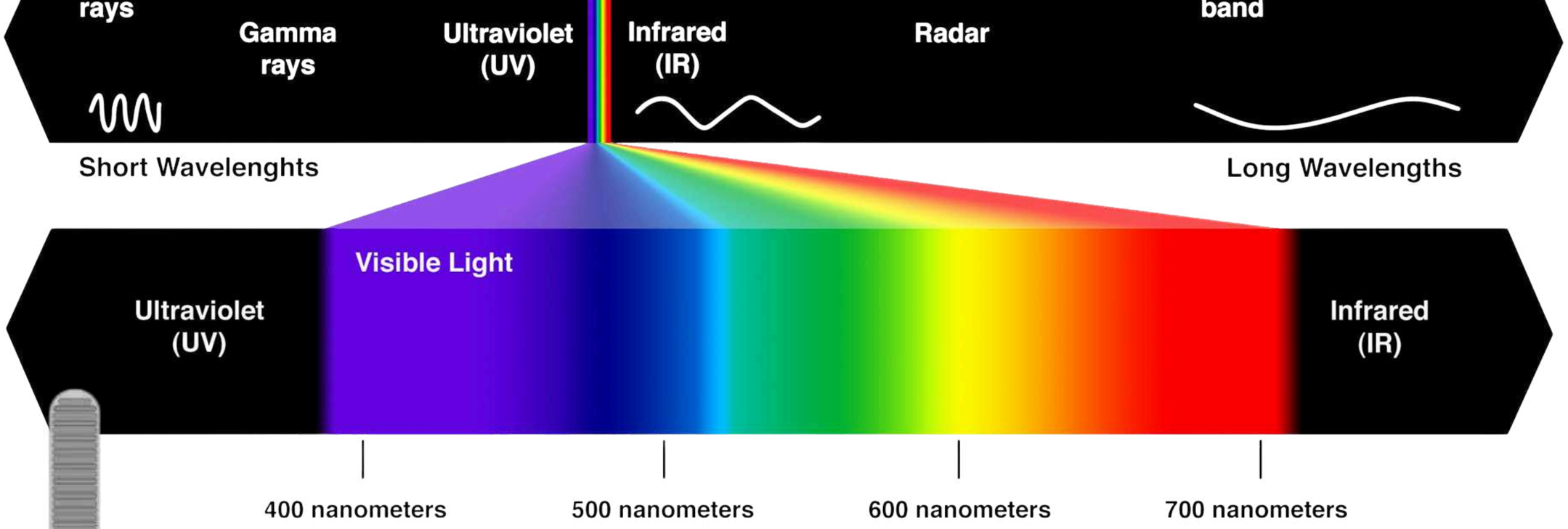


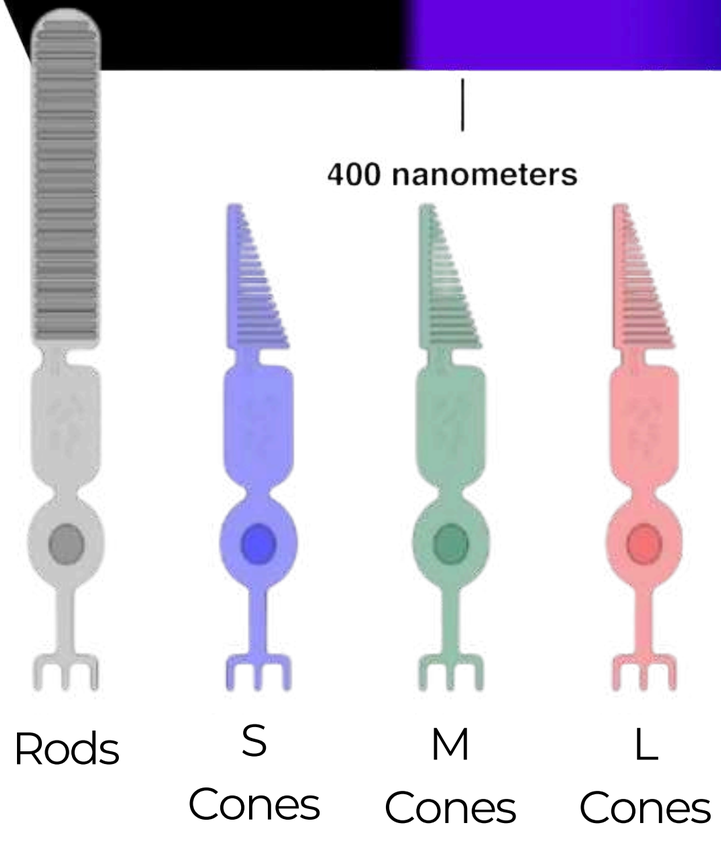
Il colore è una **percezione** generata dal nostro sistema visivo in risposta alle diverse lunghezze d'onda della luce visibile.

Visual Cryptography per immagini a colori



Il colore è una **percezione** generata dal nostro sistema visivo in risposta alle diverse lunghezze d'onda della luce visibile.



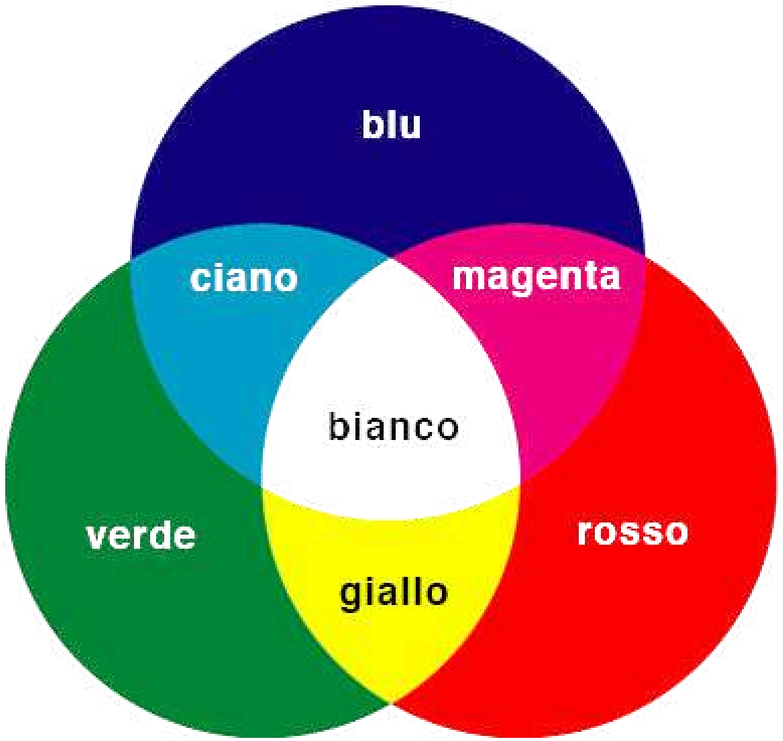


Quando la luce colpisce l'occhio umano, questo comprime lo spettro luminoso in tre risposte, corrispondenti ai tre tipi di coni presenti nella retina:

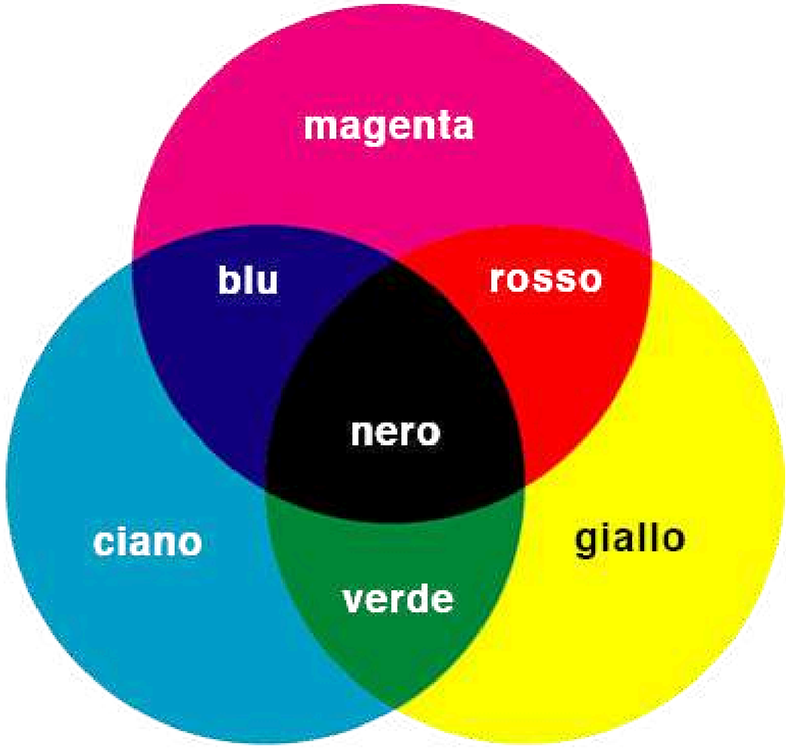
- S → Short (~420 nm) → blu / viola
- M → Medium (~530 nm) → verde
- L → Long (~560 nm) → rosso

Modelli di colore

Un modello di colore è un sistema formale che permette di rappresentare tutti (o una parte de) i colori percepibili dall'uomo.



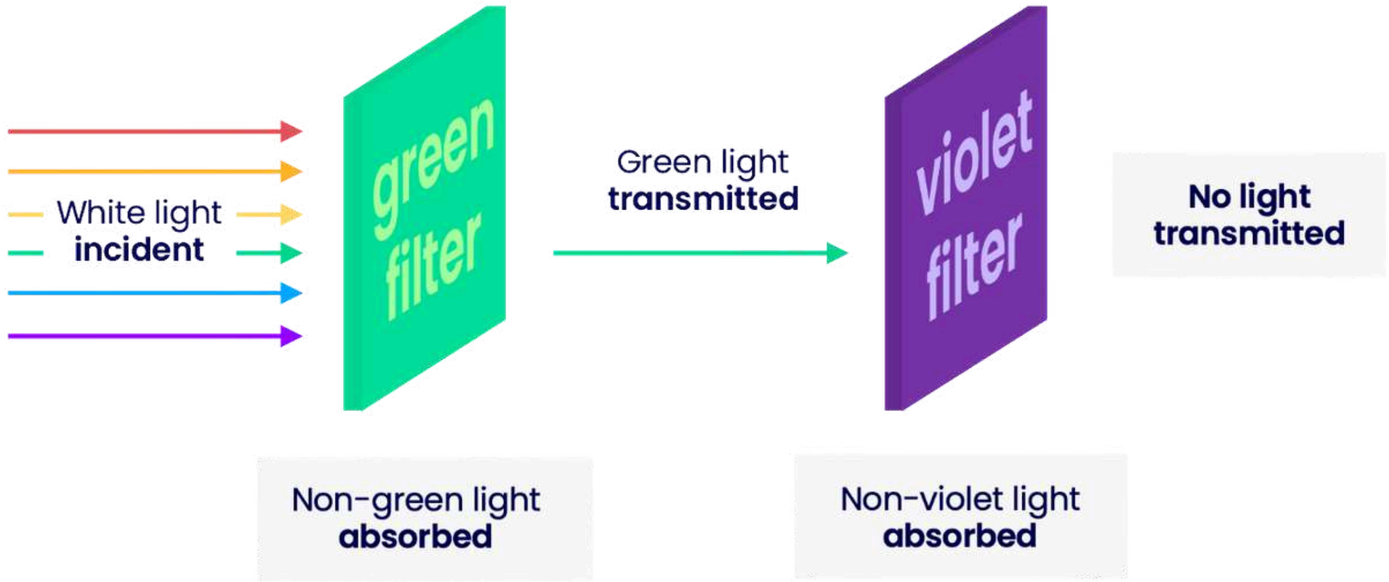
sintesi additiva

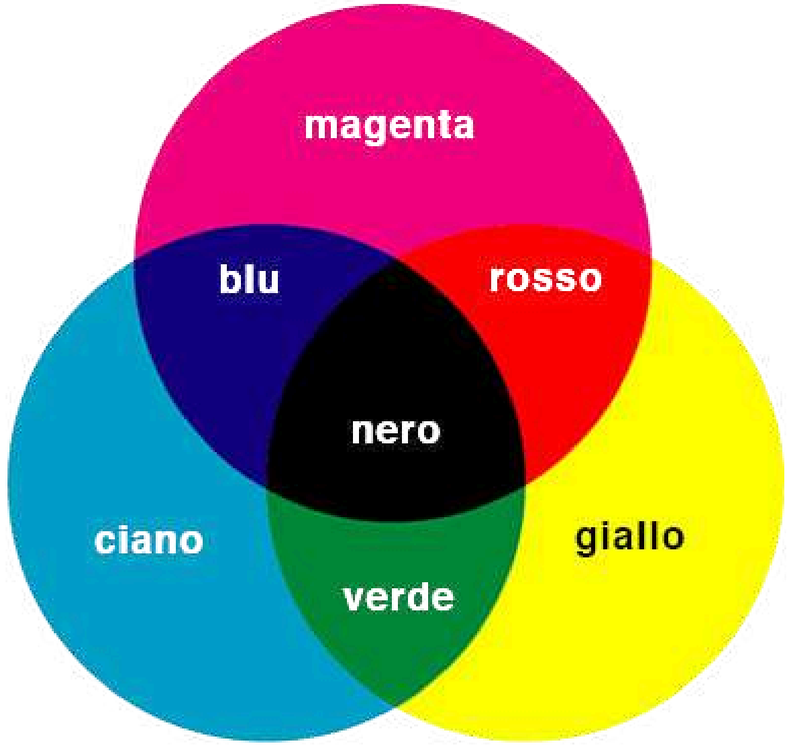


sintesi sottrattiva

Modello sottrattivo

Nel modello sottrattivo i colori sono generati per filtraggio di luce.

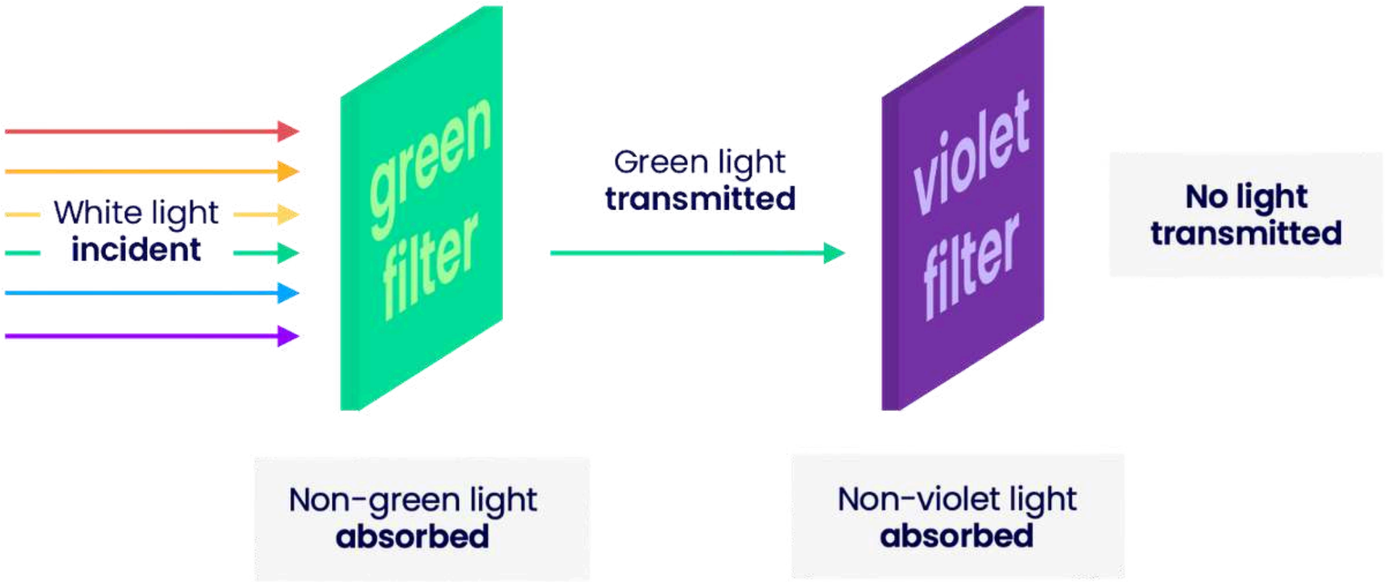


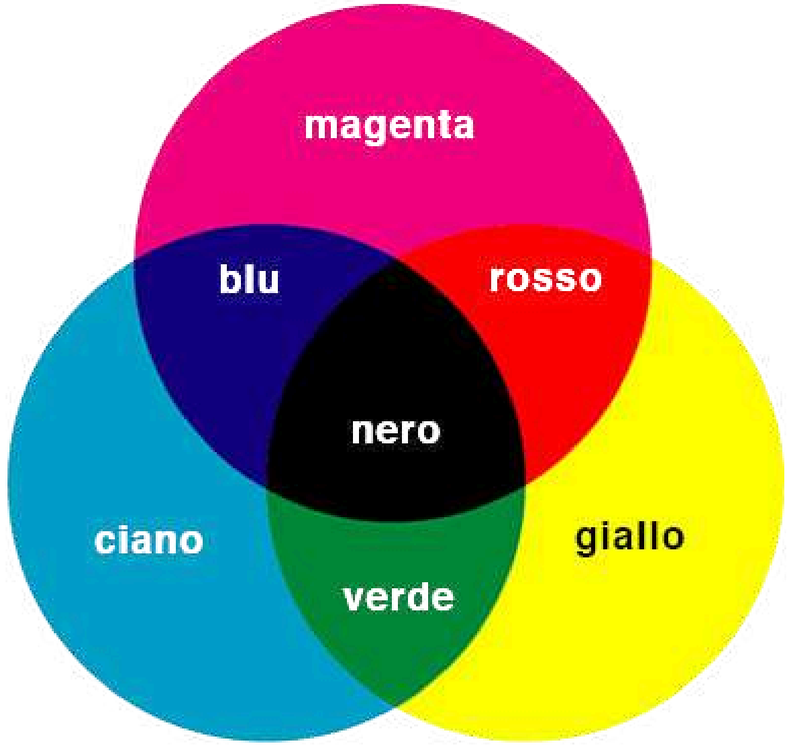


sintesi sottrattiva

Modello sottrattivo

Nel modello sottrattivo i colori sono generati per filtraggio di luce.





sintesi sottrattiva

Nelle trasparenze la ricostruzione del colore avviene per filtraggio cumulativo.

Sovrapposizione cromatica

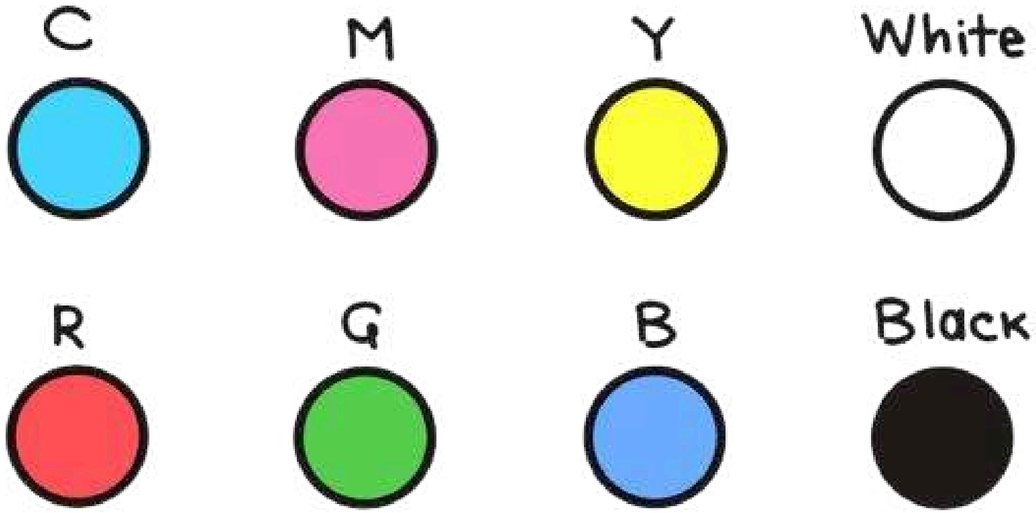
Sovrapposizione cromatica

Ogni colore è rappresentato da una tripla $C = (x, y, z) : \ 0 \leqslant x, y, z \leqslant 1$

Sovrapposizione cromatica

Ogni colore è rappresentato da una tripla $C = (x, y, z) : \ 0 \leqslant x, y, z \leqslant 1$

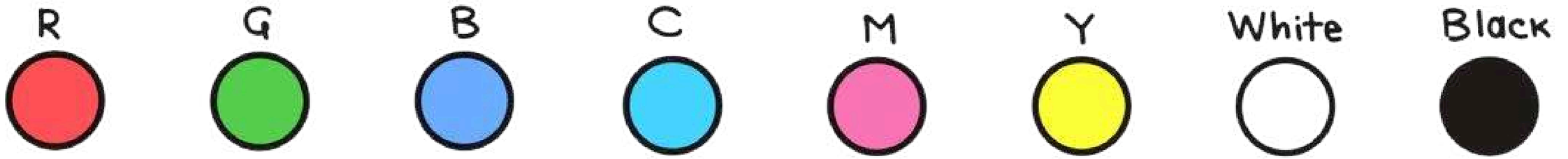
set ristretto di colori: gli 8 colori ideali ad intensità piena



Godono della proprietà di essere **chiusi** rispetto all'operazione di **sovrapposizione**.

Sovrapposizione cromatica

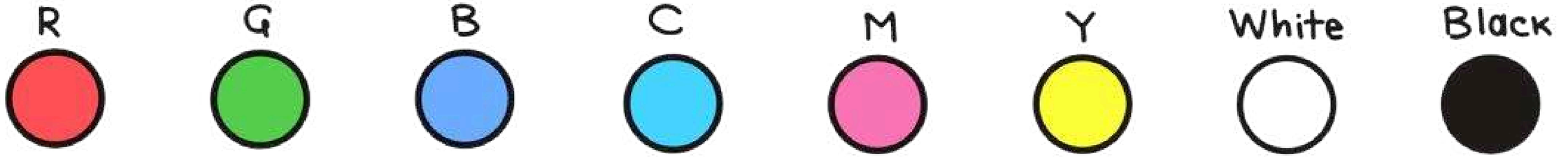
Ogni colore è rappresentato da una tripla $C = (x, y, z) : \ 0 \leqslant x, y, z \leqslant 1$



$(1, 0, 0)$ $(0, 1, 0)$ $(0, 0, 1)$ $(0, 1, 1)$ $(1, 0, 1)$ $(1, 1, 0)$ $(1, 1, 1)$ $(0, 0, 0)$

Sovrapposizione cromatica

Ogni colore è rappresentato da una tripla $C = (x, y, z) : \ 0 \leqslant x, y, z \leqslant 1$



$(1, 0, 0)$ $(0, 1, 0)$ $(0, 0, 1)$ $(0, 1, 1)$ $(1, 0, 1)$ $(1, 1, 0)$ $(1, 1, 1)$ $(0, 0, 0)$

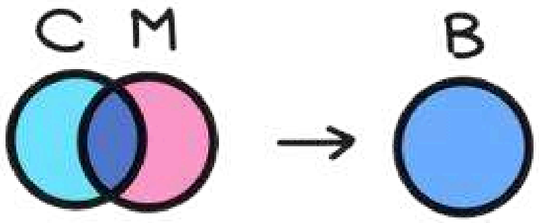
Dati due colori C_1 e C_2 , la loro sovrapposizione è descritta dall'operatore:

$$add\,(C_1, C_2) = (x_1 x_2, y_1 y_2, z_1 z_2)$$

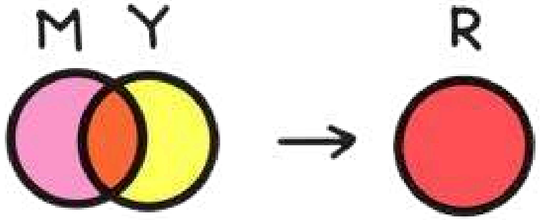
Sovrapposizione cromatica

Dati due colori C_1 e C_2 , la loro sovrapposizione è descritta dall'operatore:

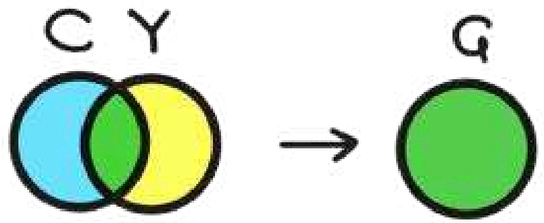
$$add\,(C_1, C_2) = (x_1 x_2, y_1 y_2, z_1 z_2)$$



$add\,((0,1,1),(1,0,1)) = (0,0,1)$



$add\,((0,1,1),(1,1,0)) = (0,1,0)$

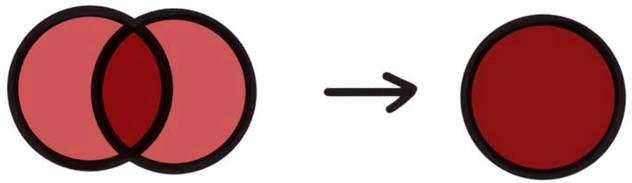


$add\,((1,0,1),(1,1,0)) = (1,0,0)$

Sovrapposizione cromatica

colori non ideali: *sovrapposizione di pixel non ad intensità piena*

$(0.80, 0, 0)$



$(0.80, 0, 0)$

$$add\left((0.8, 0, 0), (0.8, 0, 0)\right) = (0.64, 0, 0)$$

Fenomeno del Darkening

Sovrapposizione cromatica

colori non ideali: *sovrapposizione di pixel non ad intensità piena*

$(0.80, 0, 0)$ $(0.64, 0, 0)$ $(0.51, 0, 0)$ $(0.41, 0, 0)$ $(0.33, 0, 0)$ $(0.26, 0, 0)$

Fenomeno del Darkening

Modello generale

Modello generale

La sovrapposizione di pixel colorati segue le vere leggi ottiche:

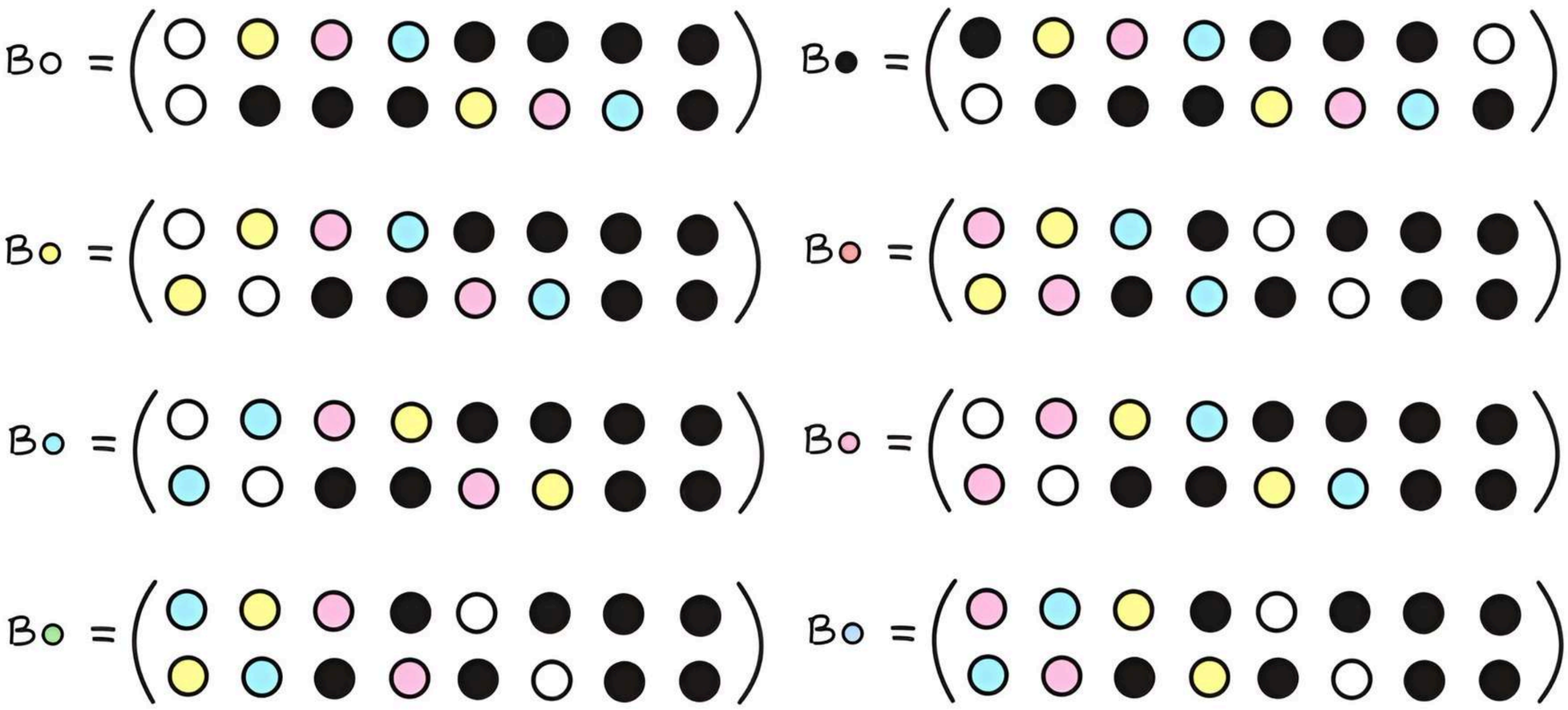
- pixel colorati possono essere sovrapposti senza limitazioni
- il *darkening* è considerato

Modello generale

8 color (2,2)-threshold scheme

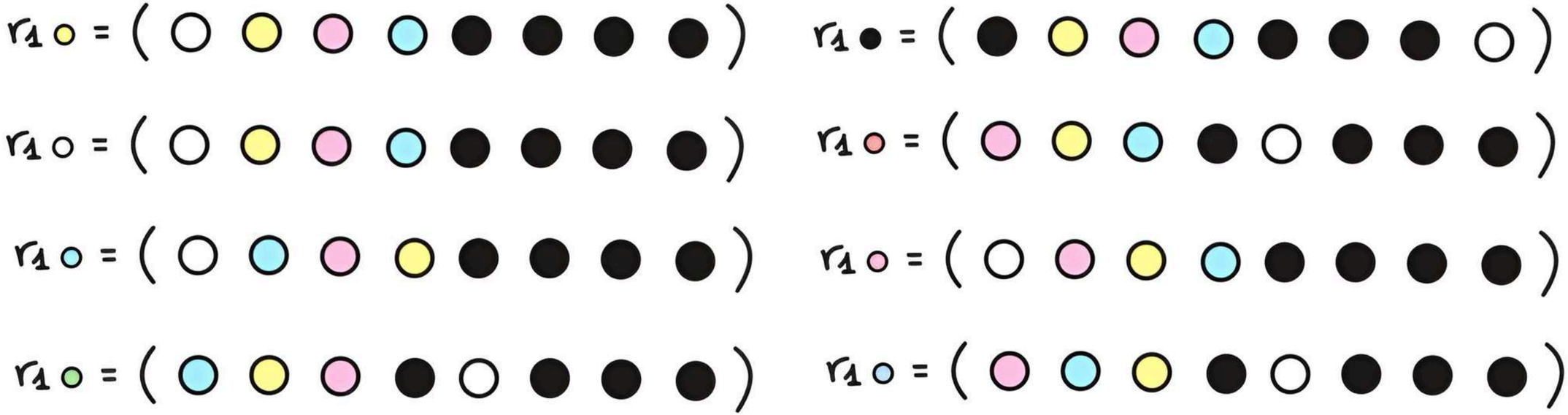
Modello generale

8 color (2,2)-threshold scheme



Modello generale

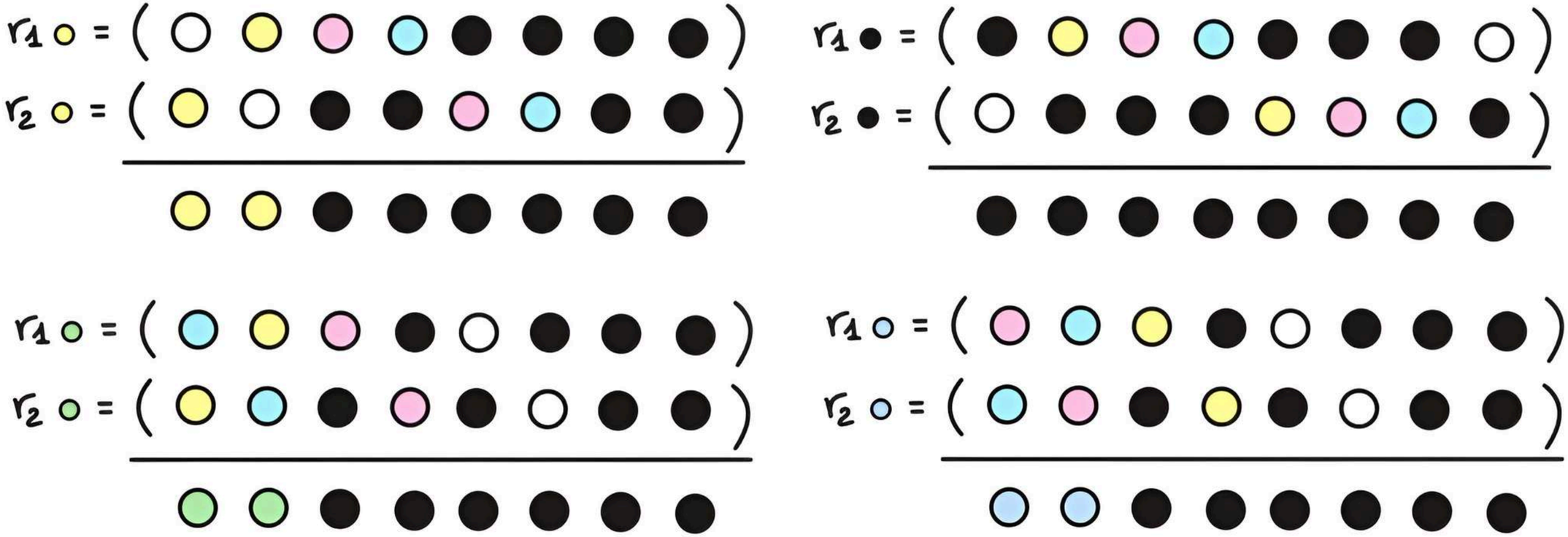
8 color (2,2)-threshold scheme



proprietà di sicurezza

Modello generale

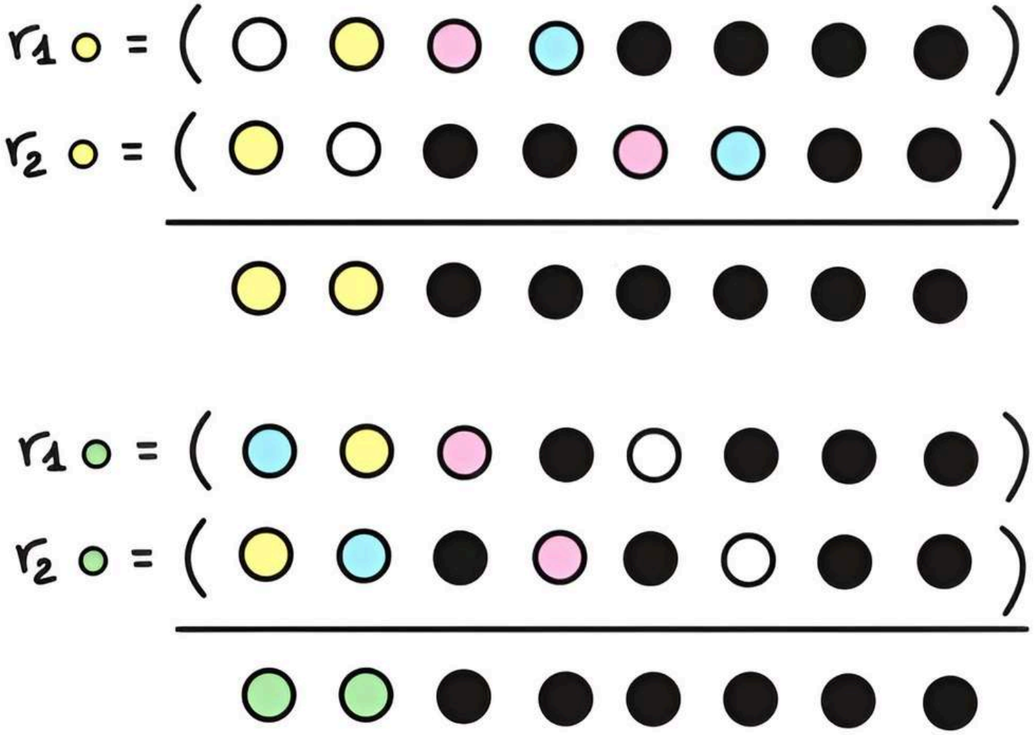
8 color (2,2)-threshold scheme



proprietà di contrasto

Modello generale

8 color (2,2)-threshold scheme



Affinchè il colore i sia percepito, ogni gruppo qualificato Q deve vedere:

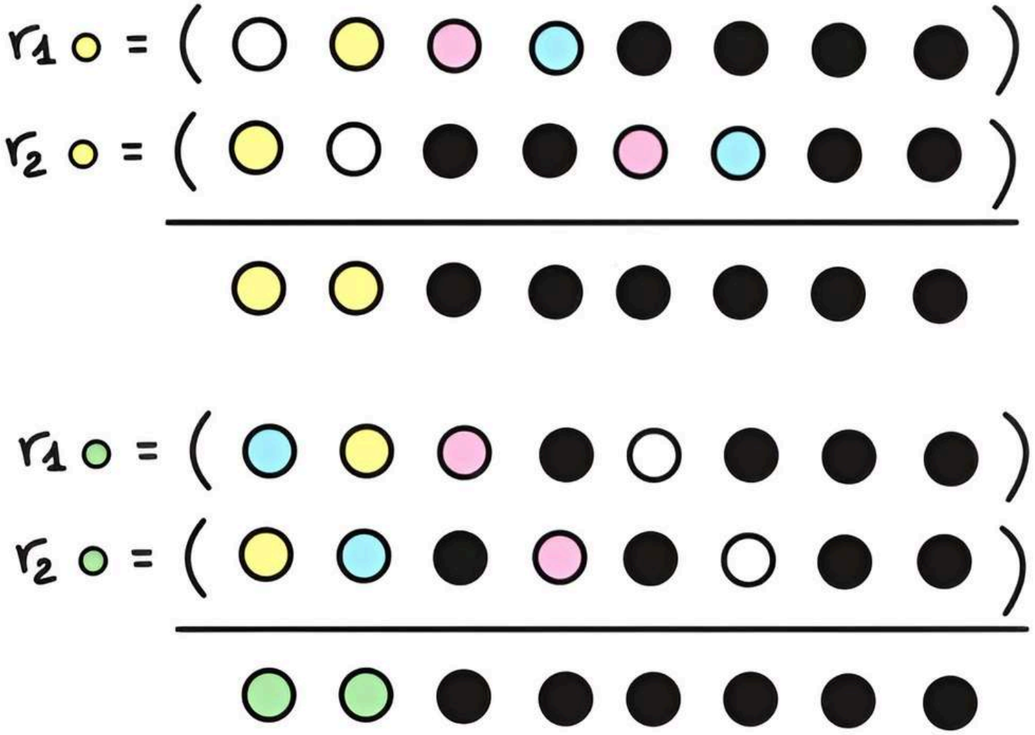
- almeno h subpixel del colore i
- al massimo l subpixel di qualsiasi altro colore $j \neq i$

e deve valere: $0 < l < h < m$

proprietà di contrasto

Modello generale

8 color (2,2)-threshold scheme



Affinchè il colore i sia percepito, ogni gruppo qualificato Q deve vedere:

- almeno h subpixel del colore i
- al massimo l subpixel di qualsiasi altro colore $j \neq i$

e deve valere: $0 < l < h < m$

$$h = 2, l = 0$$

proprietà di contrasto

Il metodo di Hou

Il metodo di Hou

Fase 1: Pre-elaborazione dell'immagine segreta

Fase 2: Generazione delle share

Fase 3: Fusione (Merge)

Il metodo di Hou

Fase 1: Pre-elaborazione dell'immagine segreta

a) **Scomposizione cromatica:** L'immagine viene divisa nei canali indipendenti Ciano, Magenta e Giallo.

immagine segreta

decomposizione nei 3 primari

Il metodo di Hou

Fase 1: Pre-elaborazione dell'immagine segreta

b) **Conversione Halftone** (Mezzatinta): L'halftone riduce le sfumature continue a punti discreti (inchiostrati o trasparenti).

Il metodo di Hou

Fase 1: Pre-elaborazione dell'immagine segreta

b) **Conversione Halftone** (Mezzatinta): L'halftone riduce le sfumature continue a punti discreti (inchiostrati o trasparenti).

immagine segreta

C M Y

conversione halftone

Il metodo di Hou

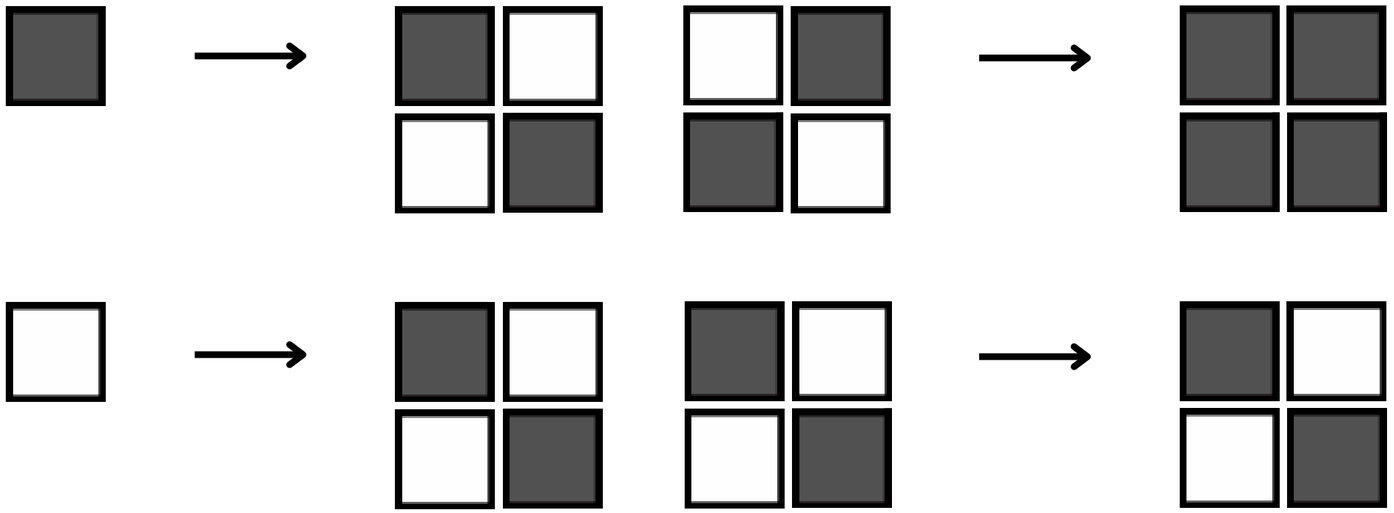
Fase 2: Generazione delle share

Indipendentemente per ogni canale vengono generate 2 share con pixel expansion $m = 4$.

Il metodo di Hou

Fase 2: Generazione delle share

Indipendentemente per ogni canale vengono generate 2 share con pixel expansion $m = 4$.



pixel segreto

share 1

share 2

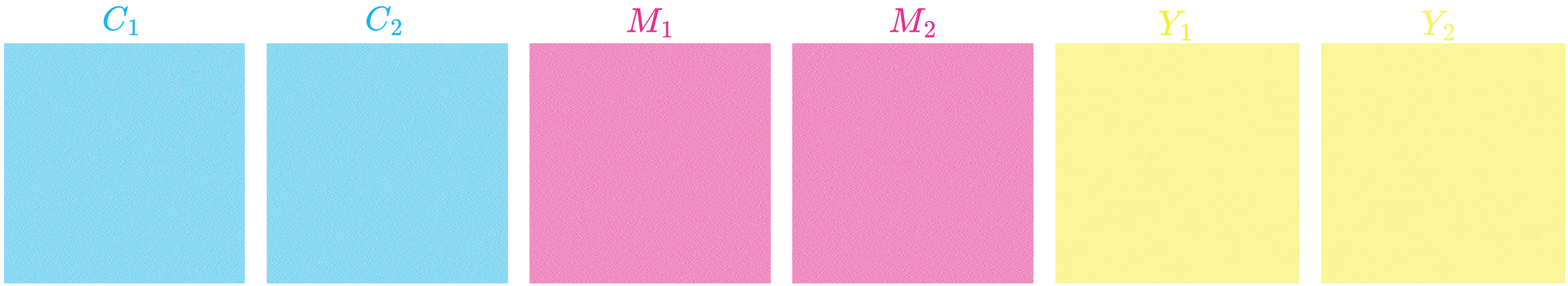
sovrapposizione

Ogni blocco da 4 subpixel contiene esattamente 2 subpixel trasparenti e 2 inchiostrati.

Il metodo di Hou

Fase 2: Generazione delle share

Indipendentemente per ogni canale vengono generate 2 share con pixel expansion $m = 4$.

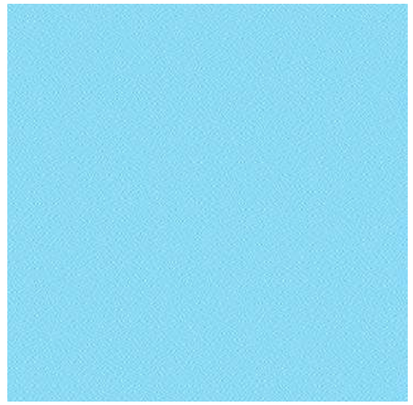
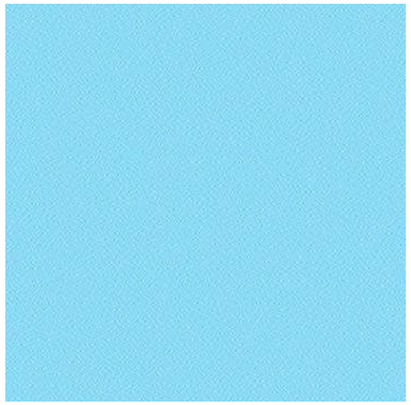


6 share temporanee

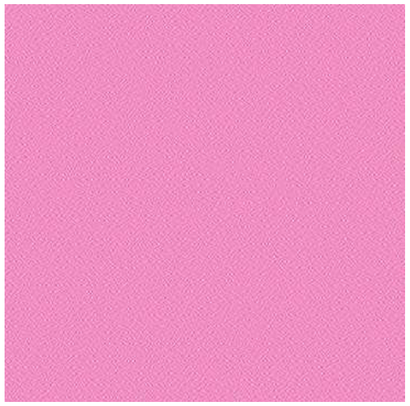
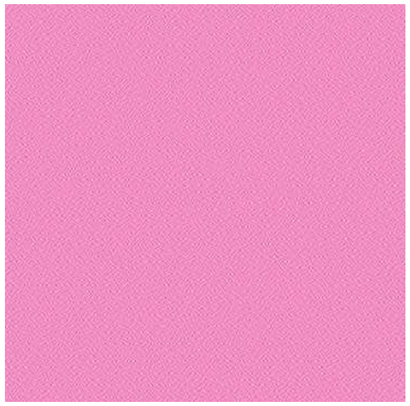
Il metodo di Hou

Fase 2: Generazione delle share

C C_1 C_2 Y Y_1 Y_2

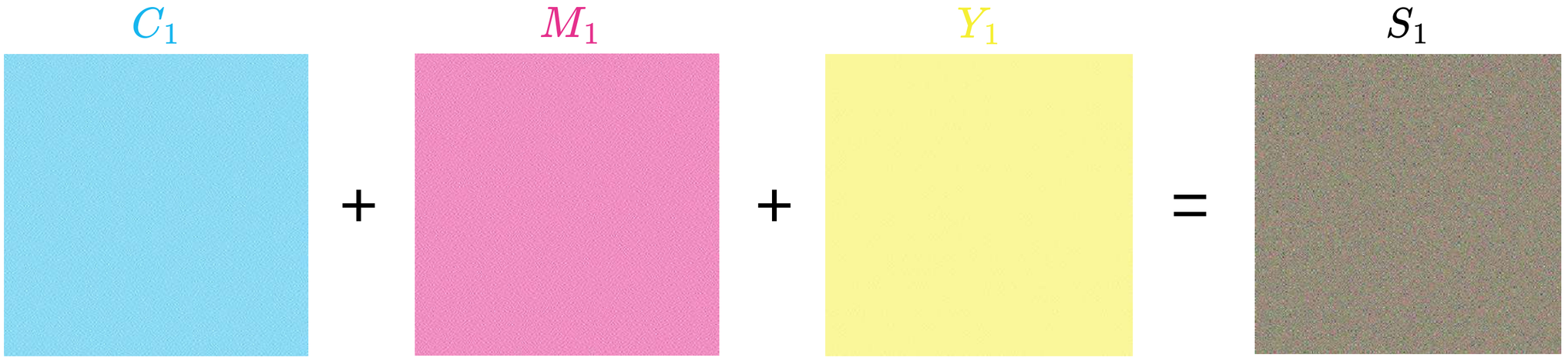




M M_1 M_2

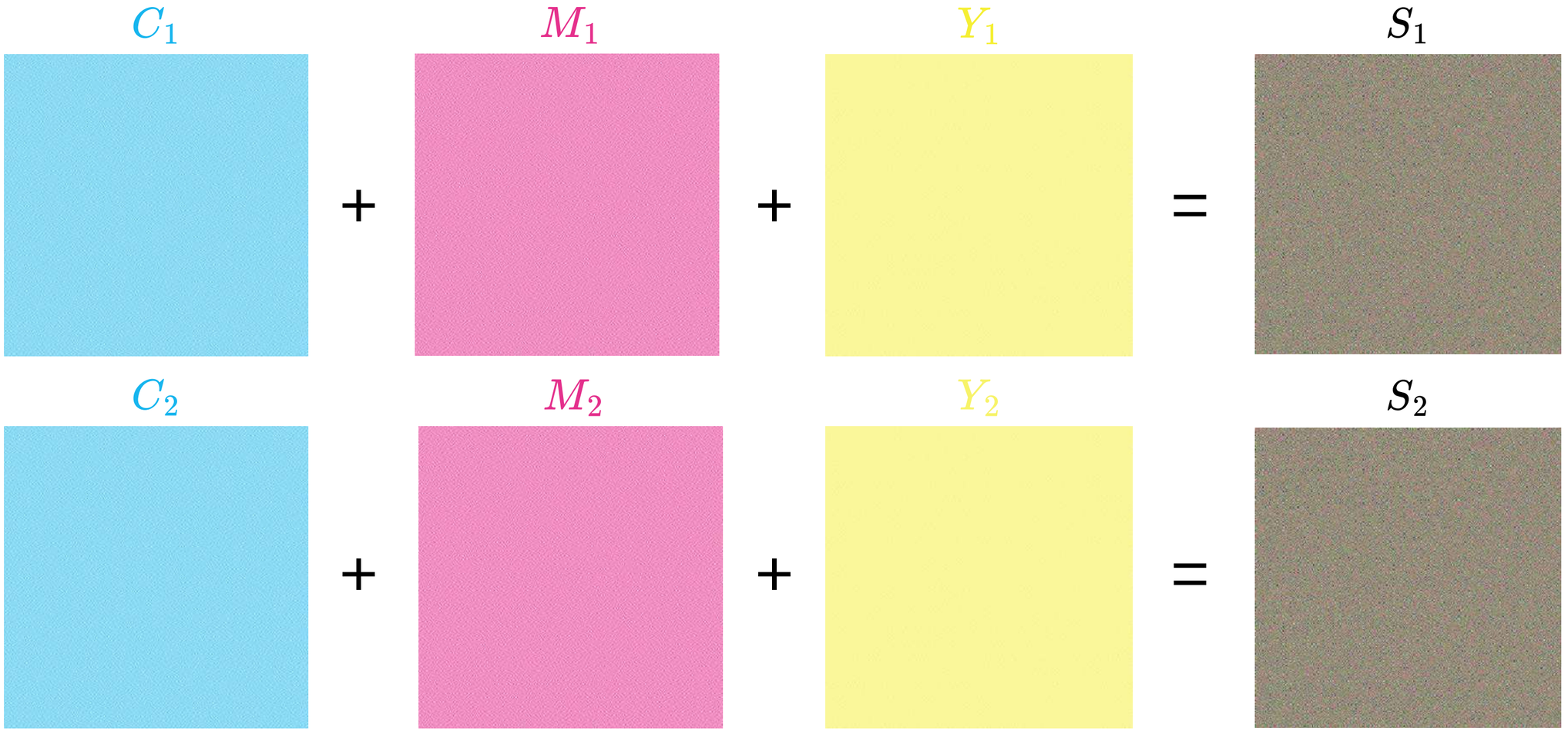
Il metodo di Hou

Fase 3: Fusione (Merge)



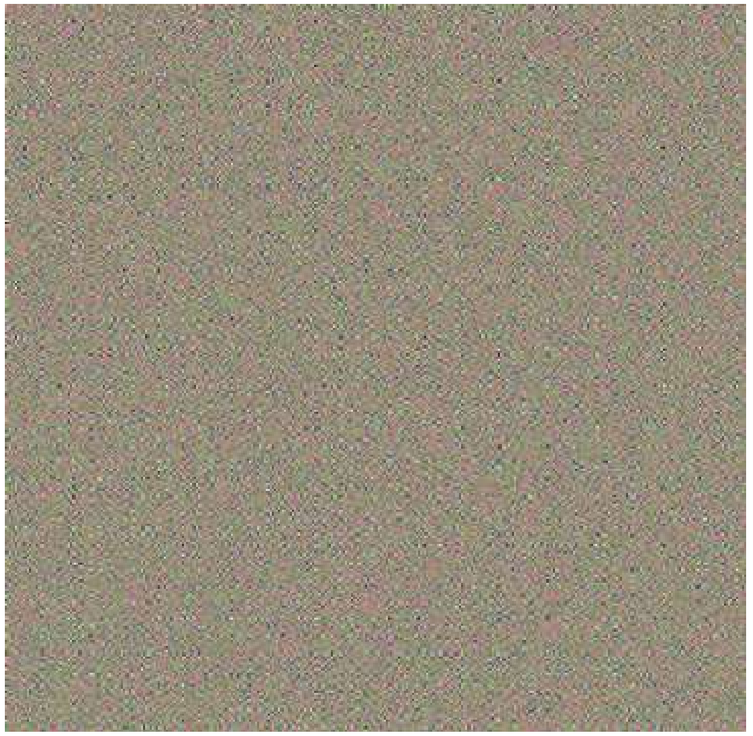
Il metodo di Hou

Fase 3: Fusione (Merge)

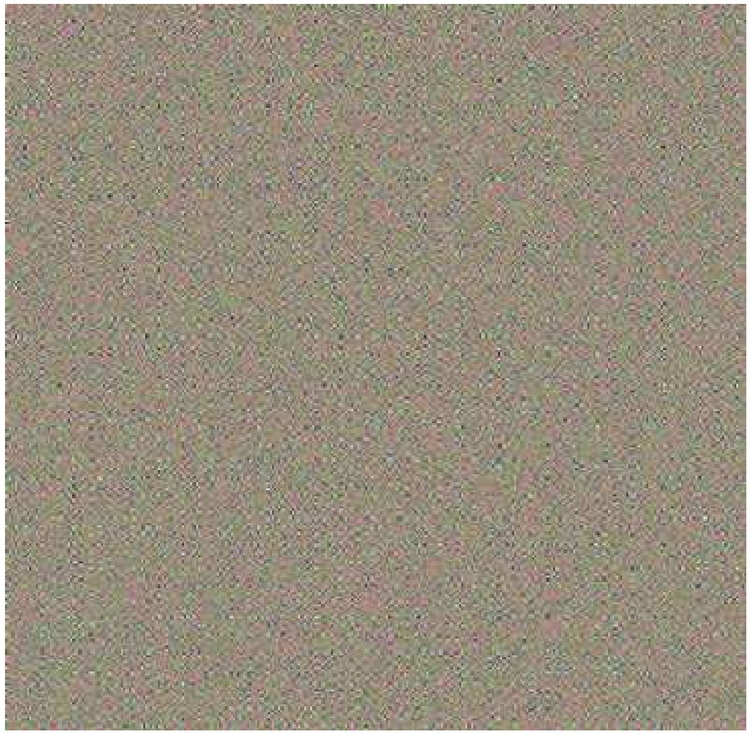


Il metodo di Hou

immagine segreta



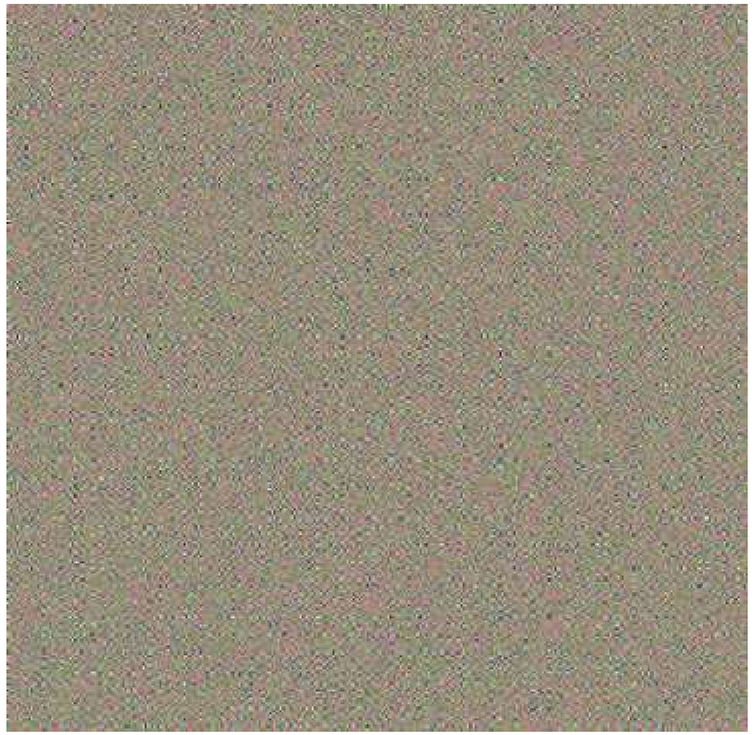
S_1



S_2

Il metodo di Hou

immagine
segreta



$S_1 + S_2$

Il metodo di Hou

immagine
segreta

$S_1 + S_2$

Riferimenti

- M. Naor, A. Shamir, "*Visual Cryptography*", 1995.
- E. R. Verheul, H. C. A. van Tilborg, "*Constructions and Properties of k out of n Visual Secret Sharing Schemes*", 1997.
- H. Koga, H. Yamamoto, "*Proposal of a Lattice-Based Visual Secret Sharing Scheme for Color and Gray-Scale Images*", 1998.
- C. Blundo, A. De Bonis, A. De Santis, "*Improved Schemes for Visual Cryptography*", 2001.
- Y.-C. Hou, "*Visual Cryptography for Color Images*", 2003.
- C.-N. Yang, "*New Visual Secret Sharing Schemes Using Probabilistic Method*", 2004.
- S. Cimato, R. De Prisco, A. De Santis, "*Colored Visual Cryptography without Color Darkening*", 2007.
- R. De Prisco, A. De Santis, "*Color Visual Cryptography Schemes for Black and White Secret Images*", 2013.
- R. De Prisco, A. De Santis, "*On the Relation of Random Grid and Deterministic Visual Cryptography*", 2015.