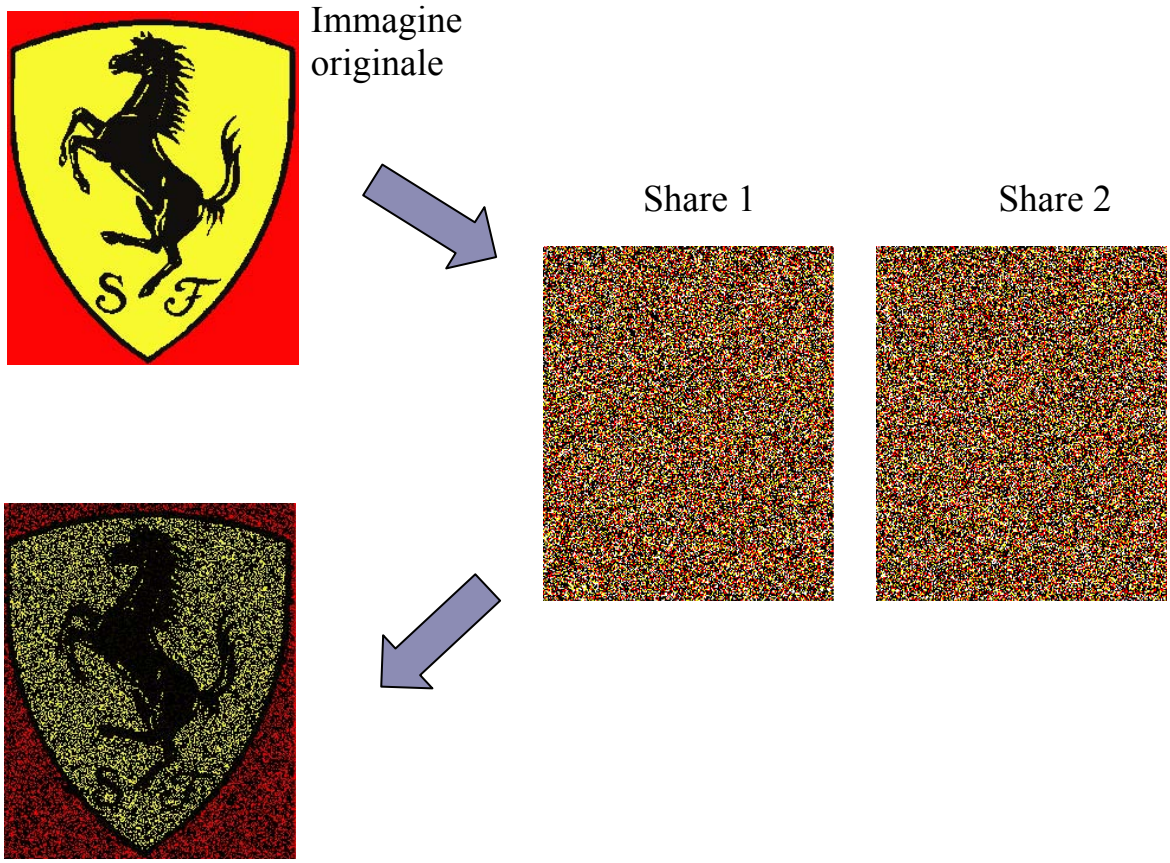
Crittografia Visuale

La crittografia visuale è una tecnica che realizza primitive crittografiche su immagini.La differenza principale, rispetto alle usuali tecniche di crittografia, consiste nel fatto che la fase di decodifica si basa esclusivamente sul sistema visivo umano, non richiedendo alcuna operazione né conoscenze particolari.Il classico scenario per la crittografia visuale consiste in:

un insieme P di n partecipanti;
un "dealer" D;
un segreto S (corrispondente ad un'immagine).

Il dealer è l'unico a conoscenza del segreto e vuole suddividerlo tra i vari partecipanti: a tal scopo genera n share (ognuna contenente un'informazione parziale su S) e le stampa su n lucidi che distribuisce ai partecipanti. Tali lucidi, sovrapposti, permetteranno di riconoscere l'immagine S.

Esempio di crittografia visuale con n=2 partecipanti.



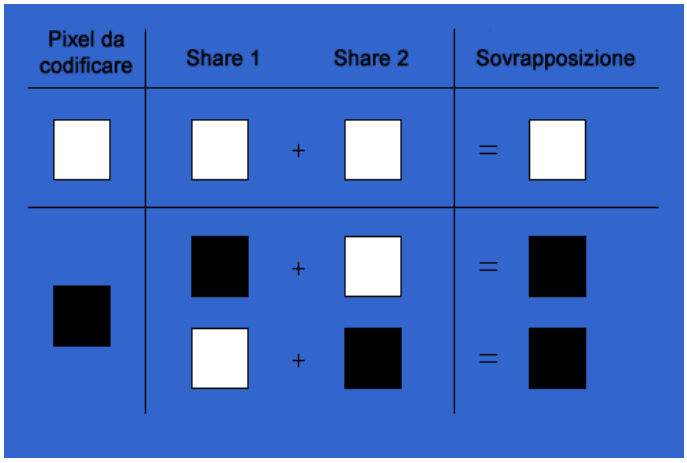
Lo schema a soglia (k,n)

Una generalizzazione di tale scenario è lo **schema di condivisione di un segreto a soglia (k,n)**, con k≤n. In questo schema se k=n si ottiene lo schema precedentemente descritto mentre se k<n, la ricostruzione del segreto può avvenire sovrapponendo k delle n share (qualunque esse siano).

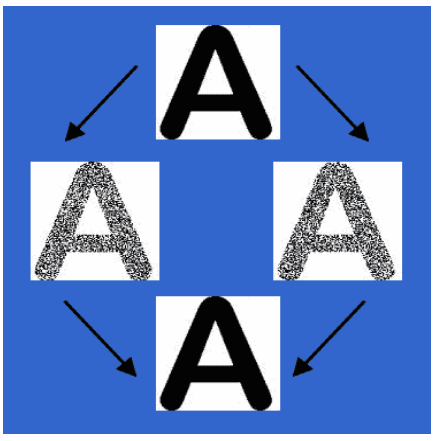
Un sottoinsieme di q partecipanti, con q<k, non ha quindi alcuna informazione sul segreto S.

Una possibile soluzione per uno schema a soglia (2,2) potrebbe essere la seguente:

- Un pixel bianco dell'immagine originale viene codificato con un pixel bianco in entrambe le share;
- Un pixel nero dell'immagine originale viene codificato con un pixel bianco in una share ed uno nero nell'altra



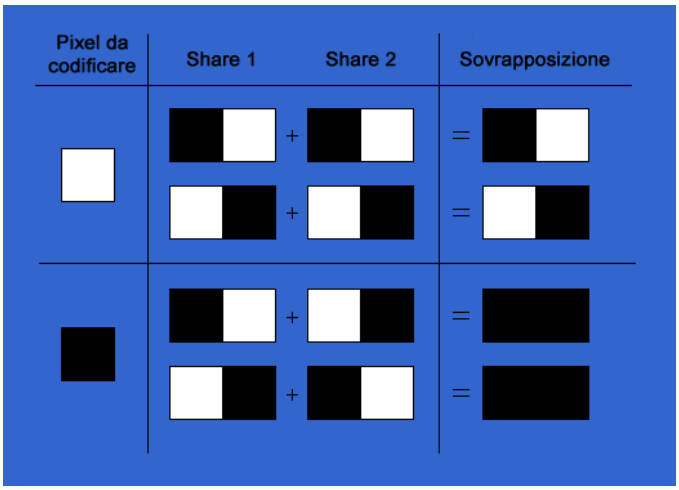
La soluzione descritta, però, dà origine ad uno schema non sicuro, in quanto su ognuna delle due share sono presenti sufficienti informazioni per recuperare gran parte dell'immagine originale. Infatti si osservi che un gruppo di pixel bianchi nell'immagine originale viene codificato con un gruppo di pixel bianchi nelle due share, mentre un gruppo di pixel neri viene codificato con un gruppo di pixel eterogenei, in quanto il bianco e il nero sono equamente distribuiti.



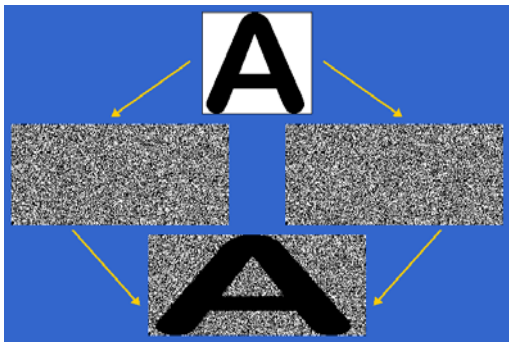
Una soluzione più sicura è data dallo schema di **Naor e Shamir** in cui ogni pixel p viene rappresentato, nella sua versione codificata, da due sottopixel:

- Se p è bianco, la coppia di sottopixel usata nella codifica è uguale per le due share, in modo da ottenere, dalla sovrapposizione, una coppia in cui un sottopixel è bianco e l'altro è nero;

- Se p è nero, la coppia di sottopixel utilizzata in una share è complementare a quella utilizzata nell'altra share, in modo che la sovrapposizione generi una coppia formata da due sottopixel neri.



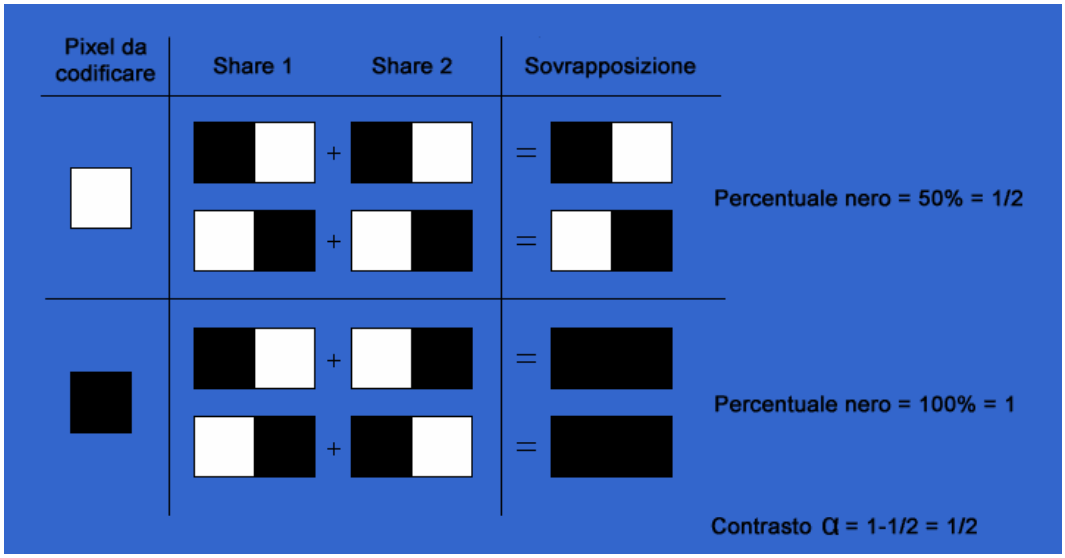
La soluzione appena descritta è un caso particolare del più generico schema di crittografia visuale (VCS, Visual Cryptography Scheme) che rappresenta un pixel p con m sottopixel. Il parametro **m** viene detto espansione del pixel.La sicurezza di questo schema è dovuta al fatto che, osservando una coppia di sottopixel in una share, non è possibile risalire al colore del corrispondente pixel nell'immagine originale.Infatti tale coppia sarà costituita da un sottopixel bianco ed un sottopixel nero, indipendentemente dal colore del pixel originale.Si noti che la rappresentazione di un pixel con due sottopixel dà luogo ad un'immagine di dimensione doppia (in altezza o in larghezza) rispetto all'immagine originale, il che corrisponde ad una deformazione dell'immagine stessa.
Oltre alla deformazione dell'immagine, tale tecnica comporta anche una perdita di contrasto, poiché un pixel nero verrà rappresentato da due sottopixel neri, ma un pixel bianco verrà rappresentato da un sottopixel bianco ed uno nero (la vicinanza dei due sottopixel appare, all'occhio umano, come una sorta di grigio).



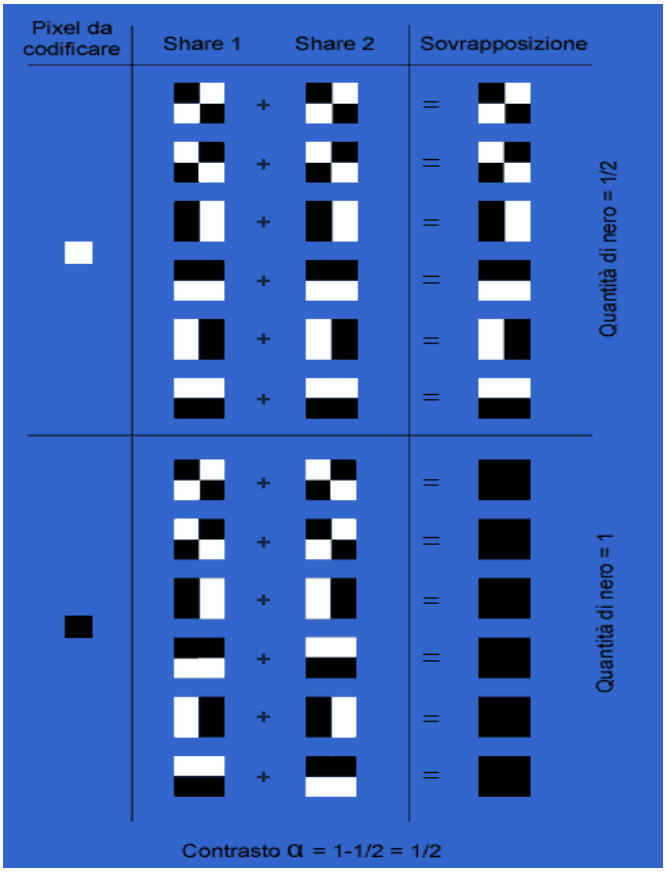
In un VCS indicheremo con:

- α il contrasto dell'immagine ricostruita dalla sovrapposizione delle share.
- 1-α la perdita di contrasto dell'immagine ricostruita rispetto all'originale.
-

Un VCS ottimale dovrebbe massimizzare α per ridurre al minimo la perdita di contrasto.



Vediamo ora un esempio di schema a soglia (2,2) con **m**=4



Tale soluzione può essere utile per mantenere le proporzioni dell'immagine originale, benché l'immagine ricostruita risulti quattro volte più grande. Come si può notare dalla figura, sovrapponendo i pixel delle due share otteniamo, per un pixel nero, 4 sottopixel neri, mentre per un pixel bianco, 2 sottopixel neri e 2 sottopixel bianchi.

Riepilogando, i principali parametri di un VCS sono:

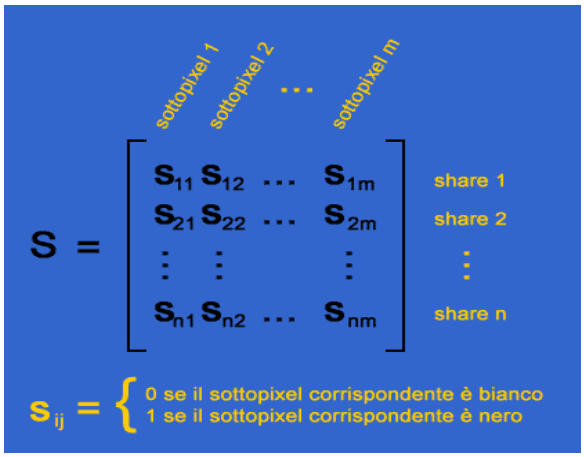
- **m**, espansione del pixel. Si desidera minimizzare questo parametro per ridurre lo spazio occupato dall'immagine;
- α, contrasto nell'immagine ricostruita. Si desidera massimizzare questo parametro per ridurre al minimo la perdita di contrasto (1-α). Il valore teorico massimo di questo parametro è 1, benché Naor e Shamir abbiano dimostrato che uno schema funzionante ha un contrasto massimo pari a ½. Lo schema a soglia (2,2) ha, quindi, un contrasto ottimale.

Modello di crittografia visuale per immagini in bianco e nero

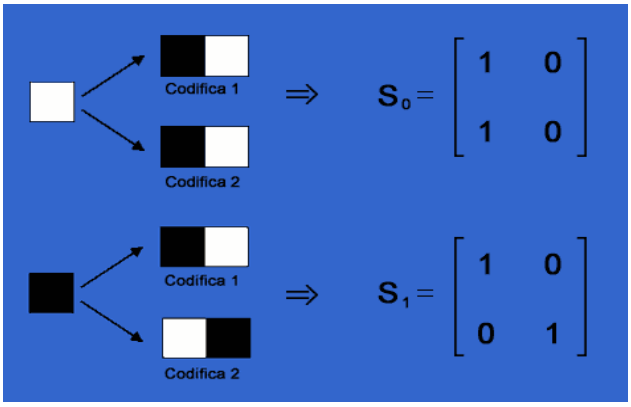
Per rappresentare la codifica di un pixel dell'immagine originale si fa uso di una matrice booleana S di dimensioni n x m.L'elemento di posizione (i,j) indica il colore del j-esimo sottopixel nella i-esima share (e quindi relativa all'i-esimo partecipante).Il valore booleano '1' indica il colore nero mentre il valore '0' indica il colore bianco.

Vediamo ora due esempi:

1) Una matrice n x m con indicazione delle righe e delle colonne.



2) Due matrici S_0 e S_1 relative ad uno schema a soglia (2,2) con **m**=2



In generale la sovrapposizione delle share di r partecipanti (con $r \leq n$) equivale all'OR booleano delle r corrispondenti righe di S. Il pixel risultante dalla sovrapposizione delle share viene rappresentato come un vettore V di **m** valori, uno per ciasciun sottopixel. Il numero di '1' presenti nel vettore V è detto ***peso di Hamming***, e si indica con **H(V)**.
Indicando con il parametro **d** ($1 \leq d \leq m$) il numero di sottopixel neri utilizzati per rappresentare un pixel nero, risulta che:

- per ogni vettore V, se $H(V) \geq \mathbf{d}$, il sistema visivo umano riconosce come nero il pixel rappresentato da V.

- per ogni vettore V, se $H(V) < (\mathbf{d} - \alpha)\cdot\mathbf{m}$, il pixel sarà visto come bianco.

VCS per strutture a soglia

Uno schema a soglia (k,n) consiste di due collezioni di matrici C_0 e C_1, di dimensione n x m.
Gli insiemi C_0 e C_1 contengono tutte le possibili matrici che codificano, rispettivamente, un pixel bianco e un pixel nero, in uno schema ad n partecipanti ed espansione **m**.
Per condividere un pixel bianco del segreto, il dealer sceglie casualmente una delle matrici in C_0, mentre per condividere un pixel nero sceglie casualmente una delle matrici in C_1. La matrice scelta per condividere il pixel definisce il colore degli **m** sottopixel in ciascuna delle n share.
Scegliendo arbitrariamente una matrice S_0 in C_0 (rispettivamente una matrice S_1 in C_1), è possibile generare tutte le matrici in C_0 (risp. in C_1) mediante permutazioni delle colonne di S_0 (risp. S_1). Per questo motivo, S_0 ed S_1 vengono dette ***matrici di base.***

La soluzione è considerata valida se si ha che:

1. Per ogni matrice S in C_0, il vettore V risultante dall'OR di un qualsiasi insieme di k righe soddisfa la relazione $H(V) < (\mathbf{d} - \alpha)\cdot\mathbf{m}$ (il pixel appare bianco);

2. Per ogni matrice S in C_1, il vettore V risultante dall'OR di un qualsiasi insieme di k righe soddisfa la relazione $H(V) \geq \mathbf{d}$ (il pixel appare nero);

3. Considerato un insieme $Q=\{i_1, i_2, ..., i_q\}$, con $q<k$ ed i cui elementi indicano q partecipanti, si definiscano D_0 e D_1 come le collezioni di matrici, di dimensioni q x m, ottenute, rispettivamente, dalla restrizione delle matrici in C_0 e C_1 alle q righe referenziate da Q. Scelta una matrice in $(D_0 \cup D_1)$, non si ha alcuna informazione addizionale per stabilire se proviene da D_0 o D_1.

Schema a soglia (2,n)

Lo schema a soglia (2,n) può essere realizzato direttamente costruendo gli insiemi C_0 e C_1 nel seguente modo:

C_0 = tutte le possibili permutazioni delle colonne della matrice n x n

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix}$$

C_1 = tutte le possibili permutazioni delle colonne della matrice n x n

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$

Calcolando l'OR di due righe di una matrice in C_0, si ottiene un vettore con un unico elemento uguale ad '1' ed n-1 elementi uguali a '0'.
Calcolando, invece, l'OR di due righe di una matrice in C_1, si ottiene un vettore con 2 elementi uguali ad '1' ed n-2 elementi uguali a '0'.
Tale differenza ci dà la possibilità di distinguere un pixel bianco da un pixel nero.

I parametri di questo schema assumono i seguenti valori:

- $\mathbf{d} = 2$
- $\mathbf{m} = n$
- $\alpha = 2/\mathbf{m} - 1/\mathbf{m} = 1/\mathbf{m} = 1/n$

Schema a soglia (3,n)

La costruzione di uno schema a soglia (3,n) avviene nel seguente modo:
sia B una matrice di dimensione n x (n-2) formata da tutti '1' e sia I la matrice identità di dimensione n x n.
Si generi la matrice BI, di dimensione n x (2n-2), ottenuta dalla concatenazione di B ed I.

C_0 e C_1 verranno costruite come segue:

C_0 = tutte le matrici ottenute permutando le colonne di S_0=c(BI), complemento bit a bit di BI;

C_1 = tutte le matrici ottenute permutando le colonne di S_1=BI.

Le matrici appartenenti agli insiemi C_0 e C_1 godono delle seguenti proprietà:

- Ogni singola riga contiene n-1 sottopixel neri ed n-1 sottopixel bianchi;
- Ogni coppia di righe ha n-2 sottopixel neri nelle stesse posizioni e 2 sottopixel neri in posizioni diverse;
- L'OR su una qualsiasi tripla di righe prese da una matrice in C_0, è caratterizzato da n sottopixel neri;
- L'OR su una qualsiasi tripla di righe di una matrice in C_1, è caratterizzato da (n+1) sottopixel neri.

Supponendo di porre n pari a 4 avremo:

$$B = \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \qquad I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$S_1 = BI = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad S_0 = c(BI) = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Nell'esempio dello schema a soglia (3,4), appena visto, i parametri assumono i seguenti valori:

- **d** = 5
- **m** = 6
- $\alpha = 5/6 - 4/6 = 1/6$

Soluzione ottimale per uno schema a soglia (n,n)

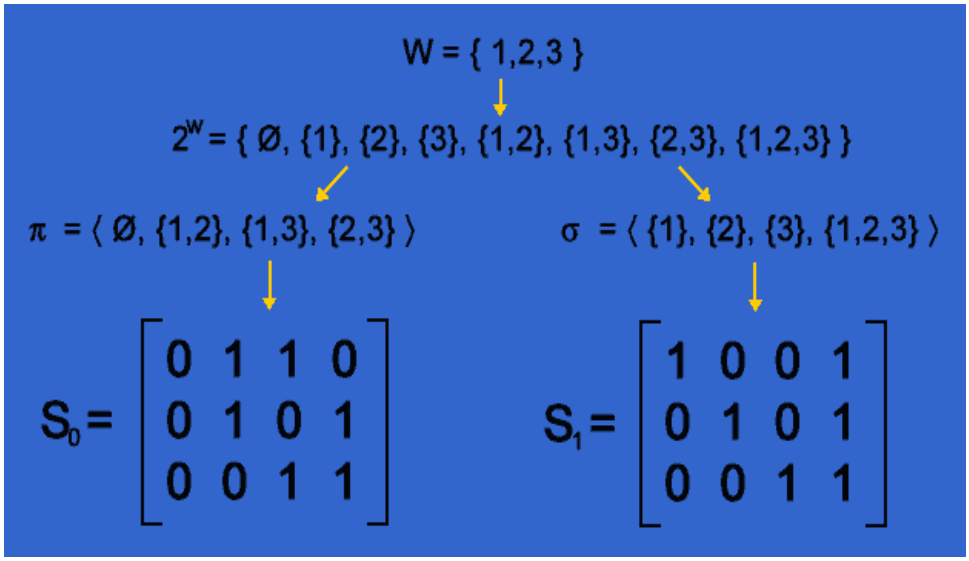
Si consideri l'insieme W={1,2,...,n} con il relativo insieme 2^w, formato da tutti i 2^n possibili sottoinsiemi di W, e si indichino con π e σ, rispettivamente, la lista formata dagli elementi di 2^w di cardinalità pari e la lista formata dagli elementi di 2^w di cardinalità dispari.

Posto **m** = $|\pi| = |\sigma| = {}^{2n-1}$, si costruiscono le matrici S_0 e S_1, di dimensione n x m, nel seguente modo:

$S_0[i,j]=1$ se e solo se $i \in \pi j$, dove con πj si intende il j-esimo elemento di π ;

$S_1[i,j]=1$ se e solo se $i \in \sigma j$, dove con σj si intende il j-esimo elemento di σ.

Vediamo un esempio con n=3:



Lo schema appena analizzato è caratterizzato da un contrasto $\alpha = \frac{1}{2}^{n-1}$.

Tale soluzione è ottimale poiché vale il seguente teorema (dimostrato da Naor e Shamir) :

TEOREMA. In ogni schema a soglia (n,n) si ha $\alpha \leq \frac{1}{2}^{n-1}$ e **m** $\geq 2^{n-1}$

VCS per strutture di accesso generali

Finora si sono esaminati schemi a soglia (k,n), dove il segreto poteva essere ricostruito da qualsiasi sottoinsieme dei partecipanti di cardinalità almeno k.Talvolta si richiede che il segreto possa essere ricostruito solo da alcuni specifici sottoinsiemi dell'insieme dei partecipanti, detti autorizzati (qualified); i sottoinsiemi non abilitati alla ricostruzione del segreto si dicono proibiti (forbidden). La coppia (sottoinsiemi autorizzati, sottoinsiemi proibiti) determina una struttura di accesso.

Si consideri l'insieme dei partecipanti P={p1,p2,...,pn} con il relativo insieme 2p, formato da tutti i possibili sottoinsiemi di P. Avremo che:

- $\mathbf{Q} \subseteq 2p$, indica la famiglia dei sottoinsiemi di partecipanti qualificati a ricostruire il segreto.
- $\mathbf{F} \subseteq 2p$, indica la famiglia dei sottoinsiemi di partecipanti NON qualificati a ricostruire il segreto.
- La coppia **(Q,F)** è detta ***struttura di accesso dello schema***.
- Un partecipante p è detto ***essenziale*** se esiste un sottoinsieme di P che non può ricostruire il segreto senza la share di p.

  Formalmente, p è essenziale se $\exists\ X \in \mathbf{F} \mid X \cup \{p\} \in \mathbf{Q}$
- **Q** è detto ***monotono crescente***, se aggiungendo un partecipante ad un sottoinsieme qualificato, questo continua ad essere qualificato.

  Formalmente, **Q** è monotono crescente se $\forall\ X \in \mathbf{Q}$ e $\forall\ p \in P\text{-}X$ si ha che $X \cup \{p\} \in \mathbf{Q}$.

- **F** è detto ***monotono decrescente***, se sottraendo un partecipante ad un insieme non qualificato, questo continua ad essere non qualificato.

  Formalmente, **F** è monotono decrescente se $\forall\ X \in \mathbf{F}$ e $\forall\ X' \subset X$ si ha che $X' \in \mathbf{F}$.

- Una struttura di accesso (**Q**, **F**) è detta ***forte*** se **Q** è monotono crescente e **F** è monotono decrescente.
- L'insieme $\mathbf{Q_0} = \{ A \in \mathbf{Q} \mid \forall\ A' \subset A, A' \notin \mathbf{Q}\}$ è la famiglia minimale di tutti i sottoinsiemi qualificati.

  In altre parole, $\mathbf{Q_0}$ è costituito da quei sottoinsiemi qualificati tali che ogni partecipante è indispensabile, nell'ambito del sottoinsieme di appartenenza, per la ricostruzione del segreto.

- Se (**Q, F**) è una struttura forte, $\mathbf{Q_0}$ si dice ***base*** e **Q** è chiusura di $\mathbf{Q_0}$,
  cioè : $\mathbf{Q} = \{ C \subseteq P \mid \exists\ B \subseteq C: B \in \mathbf{Q_0}\}$.

  In altri termini, ogni insieme in **Q** è ottenuto aggiungendo ad un insieme di $\mathbf{Q_0}$, un sottoinsieme di P.

La coppia (Q,F) è considerata struttura di accesso valida se sono verificate le seguenti condizioni:

1. ogni insieme qualificato $X = \{i_1, i_2, ..., i_p\} \in \mathbf{Q}$ può recuperare l'immagine condivisa sovrapponendo le share dei partecipanti appartenenti all'insieme. Formalmente, per ogni $S \in C_0$, il vettore V, corrispondente all'OR delle righe $i_1, i_2,..., i_p$ di S, soddisfa la relazione $H(V) \leq d - \alpha \cdot m$, mentre per ogni $S \in C_1$ risulta $H(V) \geq d$;

2. ogni insieme non qualificato $Y=\{i_1, i_2, ..., i_q\}$ non ha nessuna informazione sull'immagine considivisa. Formalmente, si definiscano D_0 e D_1 come le collezioni di matrici, di dimensioni q x m, ottenute, rispettivamente, dalla restrizione delle matrici in C_0 e C_1 alle q righe referenziate da Y. Scelta una matrice in $(D_0 \cup D_1)$, non si ha alcuna informazione addizionale per stabilire se proviene da D_0 o D_1.

Vediamo ora un semplice esempio:

Si supponga n=4 e P={1,2,3,4}. Si definiscano:

Q= { {1,2}, {2,3}, {3,4}, {1,2,3} }

F= { {1}, {2}, {3}, {4}, {1,3}, {1,4}, {2,4} }

Si ricava che:

$\mathbf{Q_0}$= { {1,2}, {2,3}, {3,4} }

La struttura di accesso (**Q,F**) definita NON è una struttura forte (infatti, {1,2} è qualificato mentre {1,2,4} non lo è).

Le matrici di base S_0 ed S_1 sono:

$$S_0 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \qquad S_1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Dalle matrici di base otteniamo: **m**=3 e α=1/3.

Nelle seguenti tabelle sono riportati gli insiemi qualificati e non con i relativi pesi di Hamming.

Le tabelle mostrano inoltre che, per ogni insieme qualificato, H(V) varia a seconda che V sia ricavato da S_0 o da S_1; tale valore, invece, non cambia per gli insiemi non qualificati. Sugli insiemi restanti il comportamento non è definito.

Insiemi qualificati	**H(V) in So**	**H(V) in S1**
{1,2}	2	3
{2,3}	1	2
{3,4}	2	3
{1,2,3}	2	3

Insiemi proibiti	H(V) in S0	H(V) in S1
{1}	2	2
{2}	1	1
{3}	1	1
{4}	2	2
{1,3}	2	2
{1,4}	3	3
{2,4}	2	2

Insiemi restanti	H(V) in S0	H(V) in S1
{2,3,4}	2	3
{1,2,4}	3	3
{1,3,4}	3	3
{1,2,3,4}	3	3

Crittografia per immagini a toni di grigio

Fino ad ora è stato studiato il caso di immagini composte esclusivamente da due toni di grigio il bianco ed il nero utilizzando lo schema di Naor e Shamir (*VCS*). Ora vedremo come codificare immagini formate da **g** toni di grigio. Inizieremo con un esempio di codifica di un immagine formata da **g**=3 toni di grigio (bianco, nero, grigio) utilizzando lo schema(2,2) m=4 utilizzato precedentemente per la codifica di immagini in bianco e nero riadattato a questo caso.

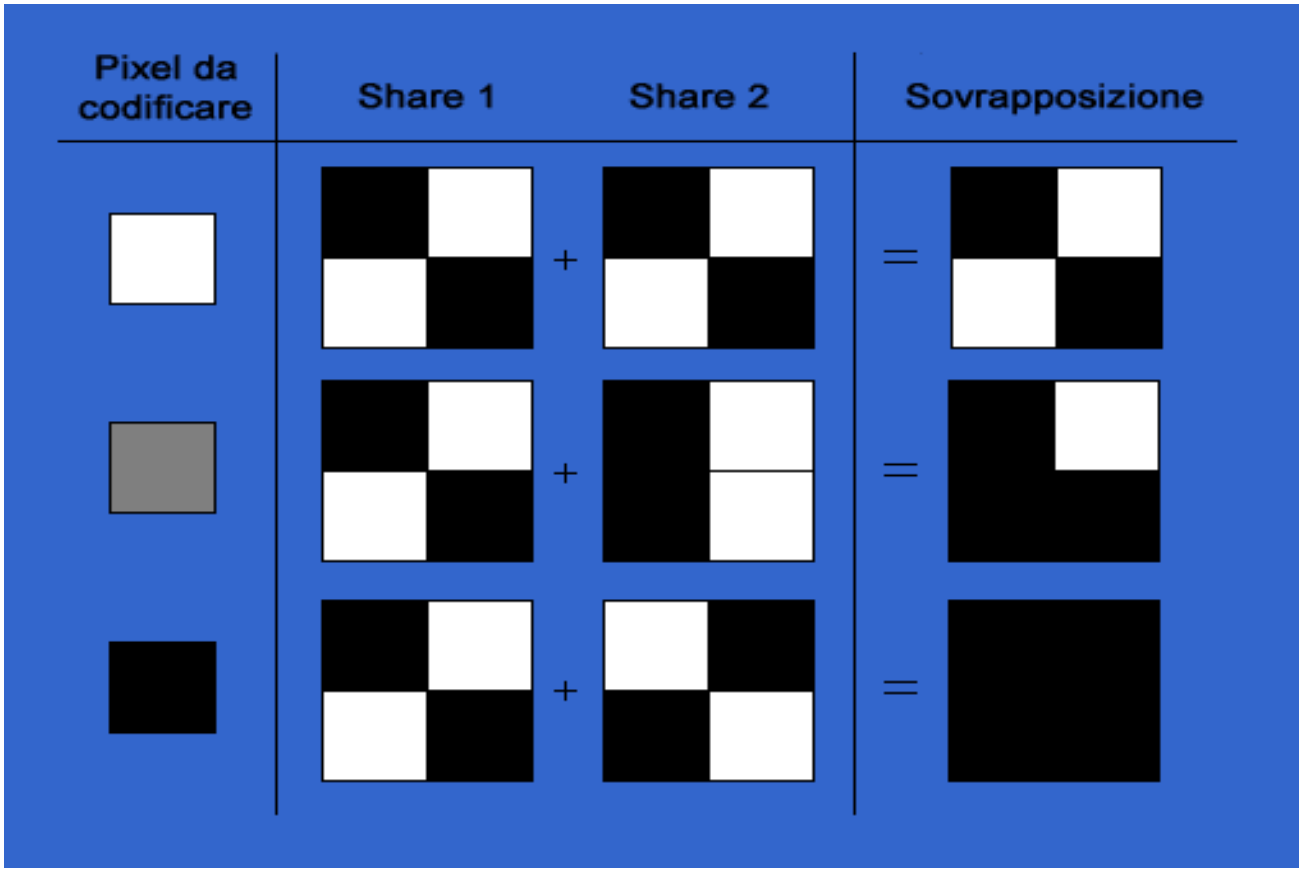


fig.1 esempio di codifica di immagini a **g**=3 toni di grigio

Si noti come, nella figura, le share e la loro sovrapposizione (immagine codificata) siano composte esclusivamente da pixel bianchi e neri; è la loro composizione a generare zone che appaiono all'occhio umano come diverse zone di grigio. Si noti inoltre come la sovrapposizione delle due share per la codifica di un pixel bianco dia come risultato due sottopixel neri e due sottopixel bianchi, la sovrapposizione delle due share per la codifica del pixel grigio dia come risultato tre sottopixel neri ed uno bianco e la sovrapposizione delle due share per la codifica di un pixel nero dia come risultato quattro sottopixel neri.
La figura contiene una sola codifica per ogni tono di grigio. In realtà, ogni tono è rappresentato da una matrice di base: le permutazioni delle colonne di tali matrici generano tutte le possibili codifiche dei corrispondenti toni di grigio.
Osservando la figura che segue possiamo notare che le modifiche apportate allo schema precedente non influisca minimamente sulla sicurezza dello schema.

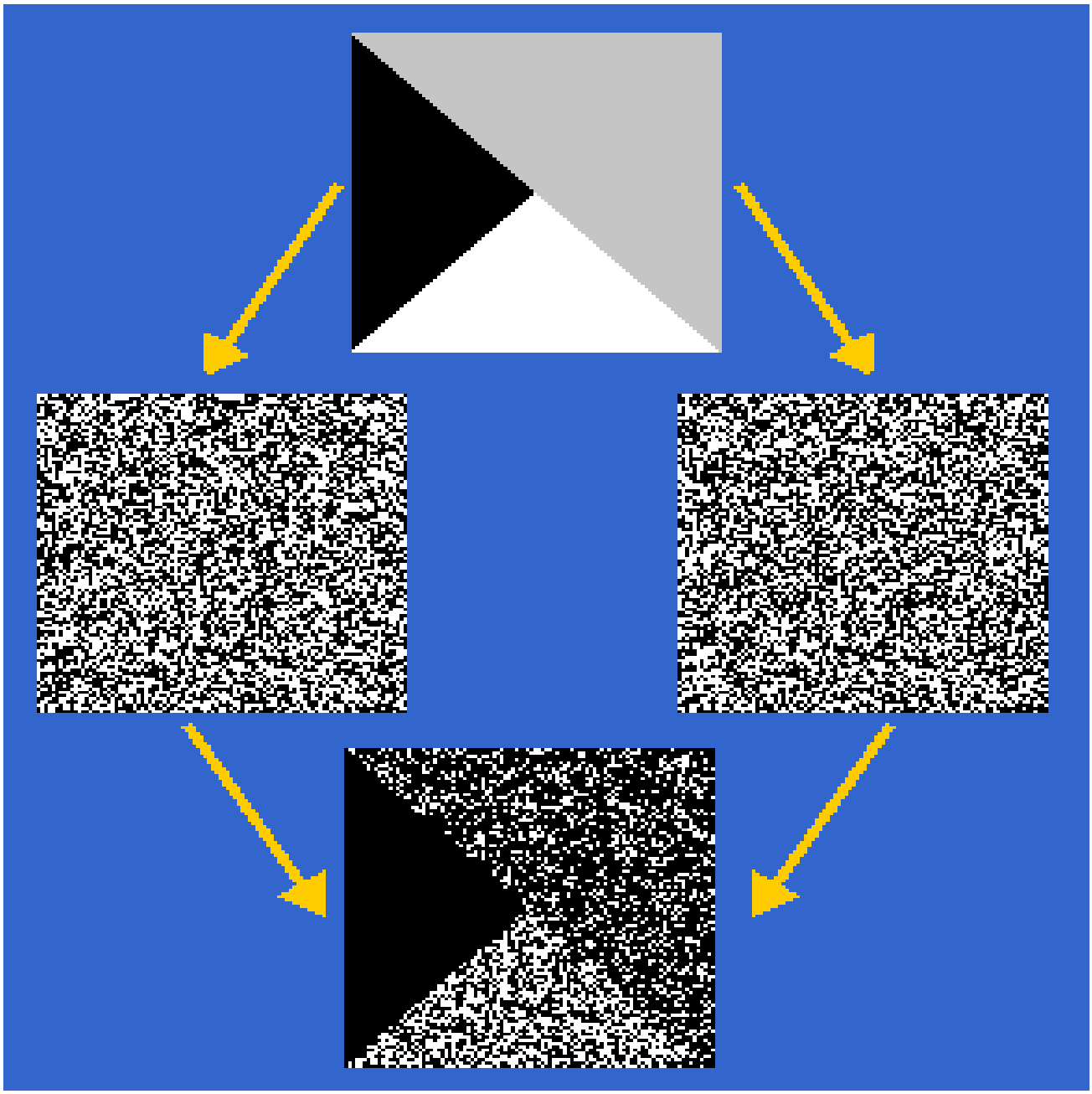


fig.2 immagine a g=3 toni di grigio

Possiamo facilmente verificare che avendo una sola delle due share non abbiamo nessuna informazione su come era l'immagine originariamente. Sovrapponendo le due share invece riusciamo a ricostruire l'immagine originale distinguendo le tre zone di colore diverso.

g-GVCS (Gray Visual Cryptography a g toni di grigio)

Ora vedremo più approfonditamente come è fatto lo schema di crittografia visuale per immagini formate da **g** toni di grigio (*g-GVCS*).
I parametri utilizzati saranno:

- **g** che rappresenta il numero di toni di grigio che formano l'immagine (ovviamente se **g**=2 si avrà il caso particolare di due toni di grigio il bianco ed il nero già ampiamente trattato),
- $\boldsymbol{\alpha_i}$ che rappresenta il contrasto relativo tra i-esimo e l'(i+1)-esimo tono di grigio,
- $\mathbf{d_i}$ parametro che differenzia la codifica del tono g_i dal tono g_{i+1},

- **$G_0,G_1,\ldots..,G_{g-1}$** sono le matrici di base utilizzate per la costruzione degli insiemi di matrici $C_0,C_1,\ldots..,C_{g-1}$ rappresentative dello schema.
-

Inoltre lo schema per essere valido deve rispettare le seguenti proprietà:

1. ogni insieme di p partecipanti (con p>k) è in grado di ricostruire l'immagine originale. Formalmente, si consideri V come il vettore risultante dall'OR di k o più righe di una matrice G. Per i=0,1,...,g-1 e per ogni matrice G in C_i, il vettore V soddisfa la relazione $H(V) < (d_i - \alpha_i)\cdot m$, mentre per ogni matrice G in C_{i+1}, il vettore V soddisfa la relazione $H(V) \geq d_i$;
2. ogni insieme di partecipanti di dimensione q< k, non è in grado di reperire alcuna informazione sull'immagine originale. Definendo formalmente D_i, per i=0,1,..., g-1, come le g collezioni di matrici, di dimensioni q x m, ottenute dalla restrizione delle matrici in C_i alle q righe corrispondenti ai q partecipanti considerati. Scelta una matrice in $(D_0 \cup D_1 \cup ... \cup D_{g-1})$, non si ha alcuna informazione addizionale per stabilire da quale dei g insiemi Di provenga.

La prima proprietà ci garantisce che avendo a disposizione un numero di share (partecipanti) p maggiore del numero di share (partecipanti) k, utili per ricostruire il segreto S, la cui sovrapposizione ci permette di riconoscere il tono g_i dal tono g_{i+1} e quindi di ricostruire il segreto.
La seconda proprietà invece ci garantisce la sicurezza dello schema, infatti se abbiamo a disposizione un numero di share q inferiore la numero minimo di share k utili per ricostruire il segreto S non abbiamo nessuna informazione aggiuntiva per capire il segreto.

Ovviamente lo schema *g-VCS* può applicare anche a strutture con partecipanti qualificati e partecipanti proibiti che deve rispettare le seguenti proprietà:

1. ogni insieme qualificato $X = \{i_1, i_2, ..., i_p\} \in Q$ può recuperare l'immagine condivisa sovrapponendo le share dei partecipanti appartenenti all'insieme. Formalmente, si consideri V come il vettore risultante dall'OR delle righe $\{i_1, i_2, ..., i_p\}$ di una matrice G. Per ogni $G \in C_i$, il vettore V soddisfa la relazione $H(V) < (d_i - \alpha_i)\cdot m$, mentre per ogni $G \in C_{i+1}$ risulta $H(V) \geq d_i$;
2. ogni insieme non qualificato $Y= \{i_1, i_2, ..., i_q\}$ non ha nessuna informazione sull'immagine condivisa. Formalmente, si definiscano D_i, per i=0,1,...,g-1, come le collezioni di g matrici, di dimensioni q x m, ottenute dalla restrizione delle matrici in C_i alle q righe referenziate da Y. Scelta una matrice in $(D_0 \cup D_1 \cup ... \cup D_{g-1})$, non si ha alcuna informazione addizionale per stabilire da quale dei g insiemi D_i provenga.

La prima proprietà garantisce che la totalità dei partecipanti di un insieme qualificato riescono a ricostruire il segreto, la seconda invece garantisce che la totalità dei partecipanti di un insieme proibito (non qualificato) non è in grado di ricostruire il segreto.

Ora verrà presentata una tecnica per costruire una struttura per la codifica di immagini a **g** toni di grigio. Per fare ciò si parte da una struttura di accesso per immagini in bianco e nero ad espansione **m**.
Di tale struttura si prenderanno in considerazione le matrici di base S^0 e S^1 di dimensione n×m per costruire le matrici di base $G_0,G_1,\ldots,G_{g-1}$ di dimensione $n\times(g-1)\cdot m$ della nuova struttura per immagini a **g** toni di grigio. La costruzione della generica matrice G_i è definita come segue: G_i =

S0 **o** S0 **o** …. **o** S0 **o** S1 **o** S1 **o** …. **o** S1, dove **o** indica la concatenazione tra le matrici S0 S1, con S0 concatenato g-(i+1) volte e con S1 concatenato i volte. Nell'esempio seguente mostreremo più in dettaglio questa tecnica.
Prenderemo innanzitutto in considerazione un VCS(2,3) ed m=2, per adattarlo al nostro caso un g-GVCS(2,3) con m=2, g=4, insieme dei qualificati (qualified) Q = {{1,2},{2,3},{1,2,3}} ed insieme dei proibiti (forbidden) F = {{1},{2},{3},{1,3}} mostrato nella figura che segue.

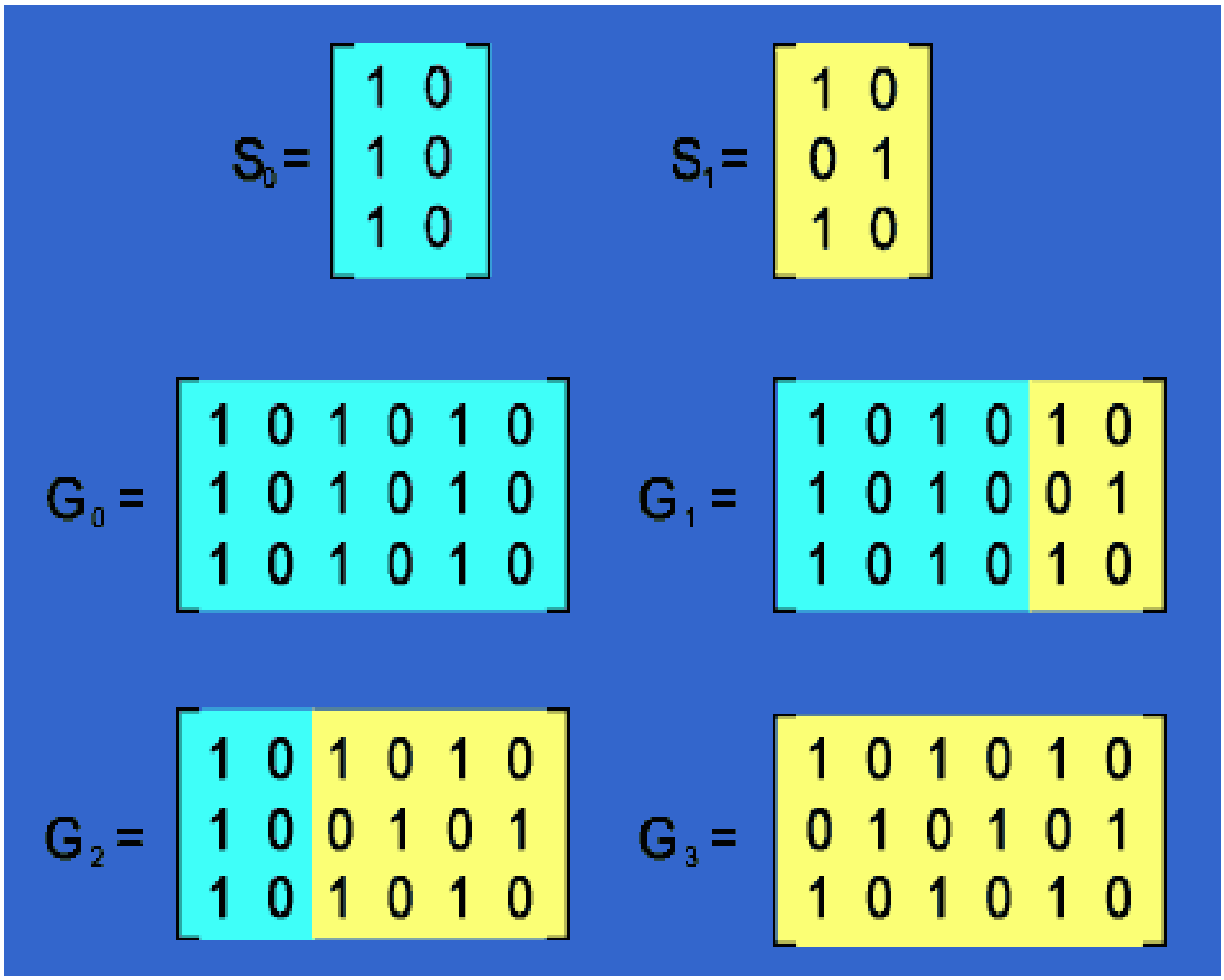


fig.3 schema g-GVCS(2,3) con m=2, g=4

Dalla figura si comprende più facilmente come vengono costruite le matrici di base $G_0,G_1,\ldots,G_{g-1}$, ad esempio la matrice G_1 viene costruita concatenando g-(i+1) (4-(1+1)) volte la matrice S^0 e i (1) volte la matrice S^1. Si può inoltre notare che la sovrapposizione delle share di un insieme qualificato ci permette di capire quale era il tono di grigio dell'immagine originale, infatti se ad esempio prendiamo la prima e la seconda riga di ogni matrice e di volta in volta facendone l'or avremo ogni volta un risultato diverso (un numero diverso di sottopixel neri), invece le share di un insieme proibito ci darà sempre lo stesso risultato ovvero tre sottopixel neri e tre sottopixel bianchi. Ricordiamo che un 1 rappresenta un sottopixel nero ed uno zero rappresenta un sottopixel bianco.

Modello di crittografia per immagini a colori

Prima di parlare del modello di crittografia per immagini a colori faremo un breve accenno alla sintesi additiva e sottrattiva dei colori.
La sintesi additiva parte da uno sfondo nero (totale assenza di colore) e proiettandovi sopra inizialmente un fascio di luce rossa e successivamente un fascio di luce verde e la zona dove i due colori si sovrappongono apparirà un terzo colore: il giallo, ed infine proiettando un fascio di luce blu e dove il blu ed il giallo si sovrappongono apparirà un colore azzurro turchese detto ciano mentre dalla sovrapposizione del blu apparirà un colore rosso purpureo detto magenta ed infine dalla sovrapposizione dei tre fasci di luce apparirà il colore bianco

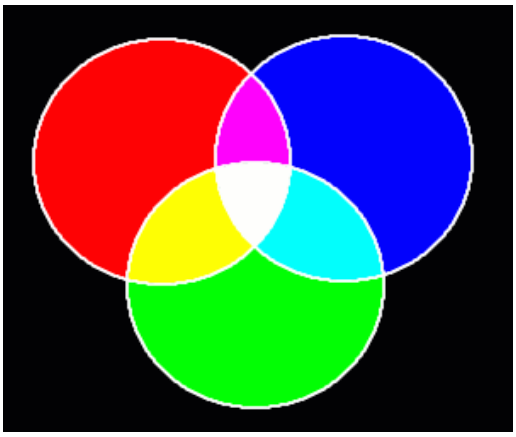


fig.4 sintesi additiva

Si noti che anche la sovrapposizione di un colore primario (rosso,verde e blu) con il risultato della sovrapposizione degli due dà come risultato il colore bianco e sono detti colori complementari, è facile notare che il complementare del rosso è il ciano, il complementare del blu è il giallo ed infine il complementare del verde è il magenta.

Nella sintesi sottrattiva avviene esattamente l'opposto, si parte innanzitutto da uno sfondo bianco e appoggiandoci sopra di volta in volta dei lucidi con i colori complementari del caso precedente ed avremo ad ogni passaggio uno dei colori primari del caso precedente fino ad arrivare alla totale assenza di colore ovvero il nero.

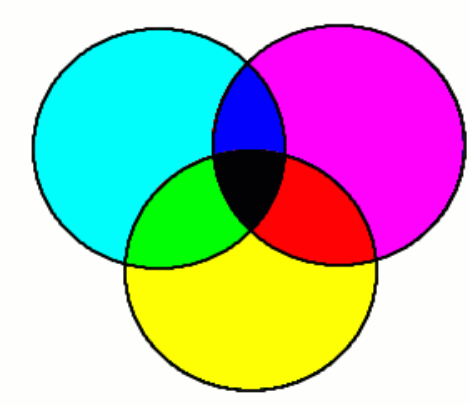


fig.5 sintesi sottrattiva

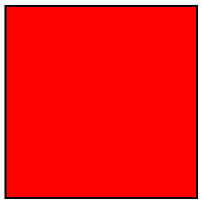
La discussione che segue si basa sulla sintesi sottrativa in quanto nel nostro caso sono le share sovrapposte a ridare l'immagine originale e verranno usati solo tre colori il rosso il verde ed il blu, una loro opportuna miscelazione darà poi tutti gli altri colori.

Un generico colore c è definito da una tripla (r,g,b) dove r, g e b rappresentano le quantità rosso, di verde e di blu che caratterizzano il colore ed ogni elemento della tripla è approssimato da un intero appartenente all'intervallo [0,255].

È facile notare che c(0,0,0) dà come risultato il colore nero (ovvero assenza di colore),

invece la tripla c(255,255,255) dà come risultato il colore bianco

una con uno dei tre elementi con il valore massimo e gli altri due a zero dà come risultato il colore primario corrispondente in questo caso c(255,0,0) il rosso



un valore diverso dal massimo darà una diversa tonalità di colore in questo caso c(100,0,0)

Si può inoltre osservare che se ogni elemento della tripla assume il valore x in questo caso si avrà un tono di grigio la cui intensità dipenderà appunto dal valore di x.

A questo punto possiamo definire l'operatore di SOMMA tra due colori, che nient'altro sarebbe poi che la sovrapposizione di un pixel di colore c1=(r1,g1,b1) ad un altro pixel di colore c2=(r2,g2,b2), definita come segue:

c=SOMMA(c1,c2)=(r1*r2 mod 255, g1*g2 mod 255, b1*b2 mod 255).

Ora possiamo parlare dello schema per la crittografia visuale per immagini a colori (**CVCS**).
In questo caso il segreto **S** sarà un'immagine a colori formata da c $\{x_1,\ldots,x_c\}$ colori, quindi ogni pixel dell'immagine **S** sarà di uno di questi colori. Dopo la codifica di **S** ogni suo pixel verrà codificato da m sottopixel. Il colore di un sottopixel è scelto nell'insieme $\{x_1,\ldots,x_c\}$ U {NERO,BIANCO}; di conseguenza una share può essere considerata come un vettore di m elementi nel suddetto insieme. Per la rappresentazione di n share, si può ricorrere ad una matrice di dimensione n x m, dove, per l'appunto, ogni riga corrisponde ad una share. Con tale matrice il dealer è in grado di individuare una possibile distribuzione delle share ad n partecipanti; infatti si può pensare che all'i-esimo partecipante venga data la i-esima riga della matrice.
Considerato un vettore V di colori, il peso di Hamming generalizzato per i, indicato con Hi(V) per i=1,...,c, corrisponde al numero di elementi in V uguali ad i.
Si definiscano $0 \leq l < h \leq m$ lo schema per la codifica di immagini formate da c colori (**c-CVCS**) è formato da matrici c matrici C1,….Cc i cui elementi sono valori appartenenti all'insieme $\{x_1,\ldots,x_c\}$ U {NERO,BIANCO} debbono rispettare le seguenti proprietà:

1. Considerato un insieme qualificato $X \in Q$, per ogni matrice M scelta in C_i (per $i \in \{x1,x2,\ldots xc\}$) si ha che $H_i(SOMMA(MX)) \geq h$ e $H_j(SOMMA(MX)) \leq l$, per qualunque $j \neq i$. In altri termini, sovrapponendo, con l'operatore di somma, le righe della matrice ottenuta dalla restrizione di M rispetto ad X (cioè la matrice MX), il peso di Hamming del vettore risultante assume un valore tale da permettere di distinguere il colore i da tutti gli altri

2. Considerato un insieme non qualificato $Y \in F$, la collezione $D_i = \{ MY \mid M \in C_i \}$ di matrici di dimensione $|Y| \times m$, con $i=1,...,c$ contiene matrici uguali. In altri termini, l'insieme delle matrici $|Y| \times m$, ottenute dalla restrizione di M rispetto ad Y, è tale che, dalla sovrapposizione delle righe dei suoi elementi, non si ha alcuna informazione addizionale per distinguere il colore i dagli altri

Osserviamo infine che la qualità di un CVCS è misurata in funzione di m (espansione dei pixel) e del contrasto α definito come il rapporto (h-l)/(h+l).

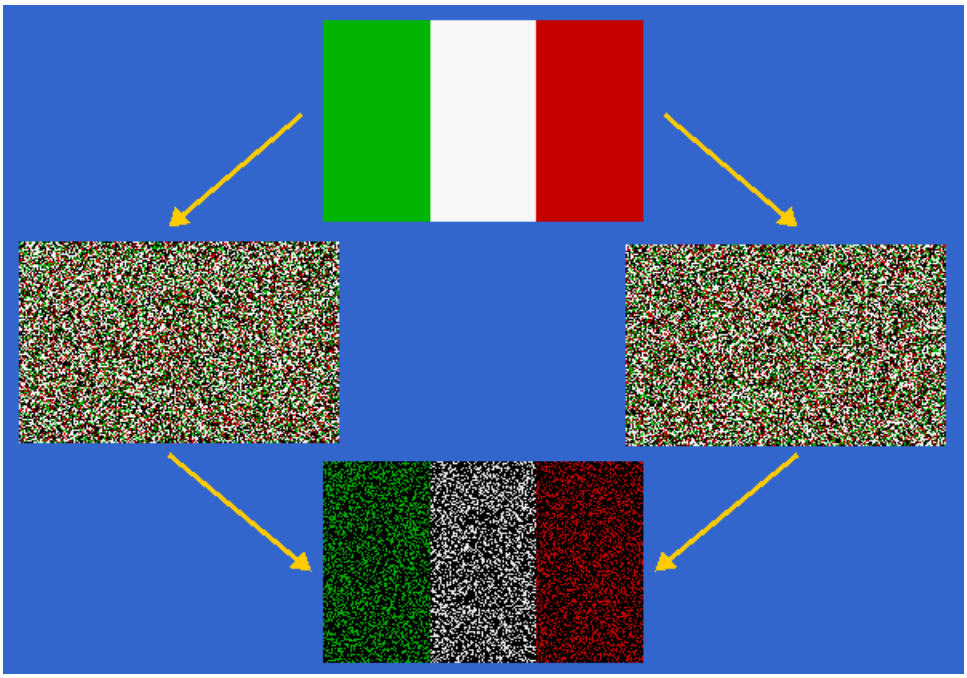


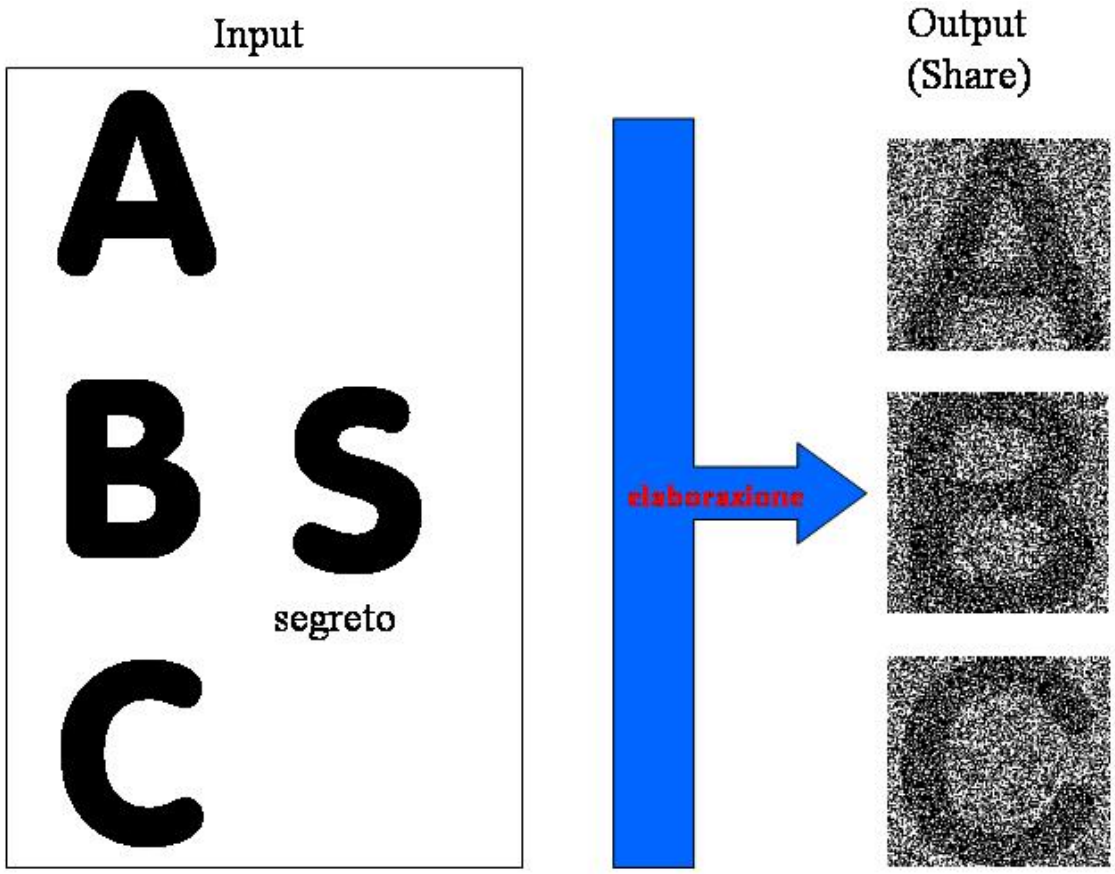
Fig.6 esempio di codifica di un'immagine a colori

Crittografia visuale estesa

Il fine ultimo della crittografia visuale estesa ha come scopo quello di rimediare la problema che si viene a formare durante l'utilizzo della crittografia visuale.
Mentre nella crittografia visuale standard il risultato della crittografia sono una serie di immagini che non hanno nessun senso .
La crittografia visuale estesa vuole invece cercare di inserire le informazioni di un determinato segreto all'interno di una serie di immagini che mantengono il loro stato naturale quindi immagine che alla apparenza hanno un senso .
Questo avviene grazie ad un processo che prevede all'interno di un sistema di elaborazione oltre al nostro segreto anche una serie di immagini .
Il sistema di elaborazione prende prima tutte le immagini inserite e le tratta come se fossero segreti indipendenti e utilizza il processo descritto nella crittografia visuale standard. Una volta terminato il processo di creazione delle share con il sistema spiegato nella parte precedente il sistema di elaborazione crea una matrice di espansione dei pixel che ha il compito di modificare le share create precedentemente.

La modifica consiste nel diminuire il grado di contrasto delle immagini che serviranno da scambio e che devono mantenere un loro senso per inserire le informazioni del nostro segreto.
La matrice di trasformazione o di espansione dei pixel calcola il grado di contrasto delle share delle immagini di scambio , calcola il grado di contrasto delle share del segreto .
Inoltre calcola la posizione dei pixel appartenenti al segreto e li mette a confronto con le posizione dei pixel delle immagini di scambio in modo da poter decidere quale porzione di immagine deve essere modificata dalla matrice .
Una volta calcolato tutto questo il sistema sostituisce le parti del nostro segreto ormai suddivise in share all'interno delle immagini di senso compito e rielabora le share ricreando le immagini di senso compiuto.

- Dato il vettore **x** contenente tutti gli x_T (numero dei sottopixel esattamente neri nelle Share i per $i \in T$)
- Dato il vettore **r** contenente tutti gli r_s (numero dei sottopixel neri necessari per ricostruire il *Segreto*)
- $Mx = r$
    - dove $M = (m_{S,T})_{\emptyset \neq S,T \subseteq \{1,\ldots,n\}}$
    - $m_{S,T} = 1$ se $S \cap T \neq \emptyset$ & $m_{S,T} = 0$ altrimenti
    - $m = \sum 2^{|T|-1}$ con $T \in S$



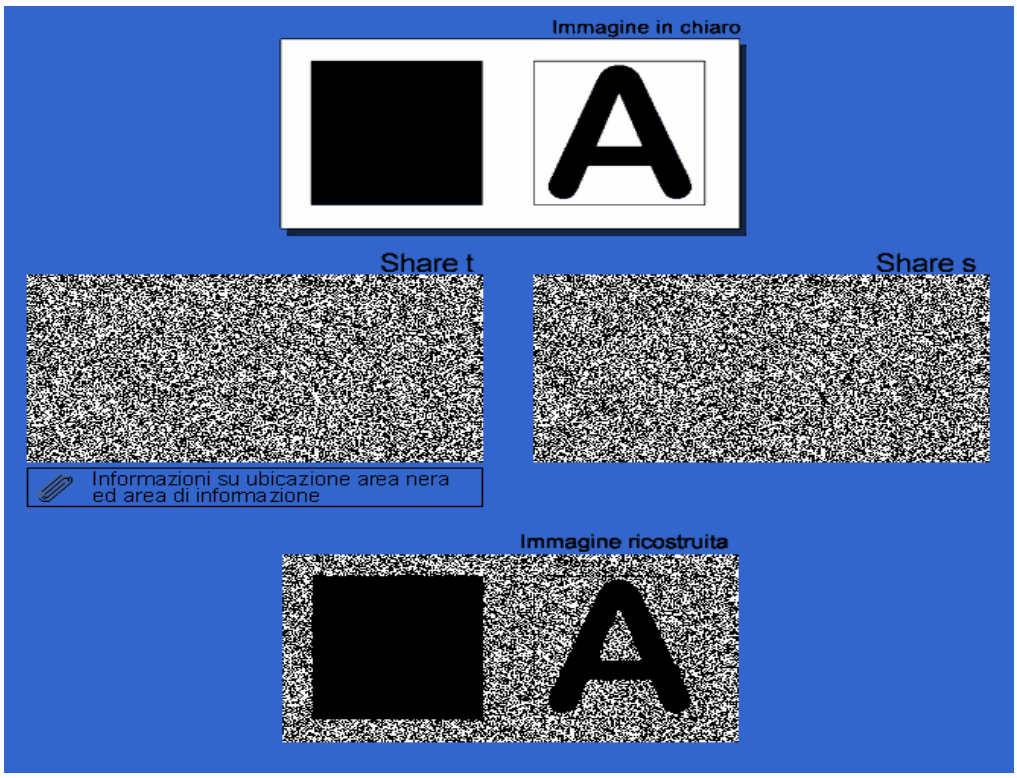
La matrice ammette soluzioni non negative se e solo se per ogni $S \subseteq \{1, \ldots, n\}$

- $\sum_{S \subseteq T \subseteq \{1,\ldots,n\}} (-1)^{|S|+|T|} r_T \leq 0$ è soddisfatta (non-negatività)
- $\sum_{\substack{S \subseteq T \subseteq \{1,\ldots,n\} \\ |S| \equiv |T| \bmod 2}} b_T \leq \sum_{\substack{S \subseteq T \subseteq \{1,\ldots,n\} \\ |S| \not\equiv |T| \bmod 2}} w_T$ è soddisfatto
  - $\emptyset \neq T \subseteq \{1, \ldots, n\}$ definendo $\delta_T = b_T - w_T$
- $$m \geq b_{\{1,\ldots,n\}} \geq \sum_{\emptyset \neq T \subseteq \{1,\ldots,n\}} \delta_T 2^{|T|-1}$$

- $x_{\{1,\ldots,n\}} = \sum (-1)^{|T|+1} r_T$
- $\alpha_T = (b_T - w_T) * m^{-1}$
- $\sum 2^{|T|-1} \alpha T \leq 1$

Autenticazione visuale

Come nella crittografia classica anche la crittografia visuale ha cercato di creare sistemi di autenticazione.
Il fine è quello di poter inviare informazioni e poterne autenticare il contenuto senza avere il minimo dubbio del fatto che l'informazione in possesso possa essere stata manomessa.
Per fare questo la crittografia visuale introduce il concetto di area nera.
Nello scambio di informazioni tra due utenti il mittente inserisce all'interno delle informazioni da inviare un area nera o più aree nere, questo dato viene stabilito su un canale sicuro tra mittente e destinatario.
Fatto ciò il mittente crea le share con il sistema della crittografia e le invia al destinatario .
Siccome dalle share è impossibile capire quel informazione fa parte dell'area nera e quale fa parte dell'area di informazione allora cercando di modificare il contenuto dell'informazione si va ad alterare il contenuto dell'area nera che nel momento della ricomposizione non apparirà più uniformemente nera .
Questo sistema permette al destinatario di capire se l'informazione in suo possesso è autentica oppure no .



Identificazione Visuale

Argomento che nel corso del tempo ha preso piede è quello del identificazione visuale.
L'identificazione visuale ha come scopo quello i capre se un determinato utente è autorizzato oppure no a venire a conoscenza del segreto.
Questo avviene tramite uno scambio di informazioni tra un sistema che deve identificare e un utente che deve essere identificato.
Il processo nella sua forma base e molto semplice ma ha posto le basi per una versione molto più elaborata di cui discuteremo più avanti.

Durante la fase di inizializzazione, S prepara un immagine in cui appaiono **N** quadrati colorati (i colori usati da S devono essere tutti facilmente distinguibili) e la trasmette ad U. Il protocollo prevede che, ad ogni identificazione, S scelga d quadrati a caso tra gli N dell'immagine e generi un lucido nero con **d** quadrati trasparenti corrispondenti ai d quadrati scelti dall'immagine originale. Quando U riceve il lucido, lo sovrappone all'immagine in suo possesso, e risponde ad S inviando l'insieme dei colori visualizzati (l'ordine dei colori nella risposta di U non ha importanza). Il verificatore S accetta U solo se la risposta è corretta per tutti i d quadrati. Si indichi con ***l*** il numero massimo di volte che l'immagine inviata da S ad U (formata da quadrati colorati) può essere utilizzata per una identificazione, e con ***c*** il numero totale di colori che S può usare per generare l'immagine.
Un nemico P può, quindi, interagire con U spacciandosi per S al più ***l*** volte ottenendo i colori di **d·*l*** quadrati. Affinché P riesca a farsi identificare come U da S, dovrà rispondere al lucido di S con i **d** colori esatti.
Si supponga che S chieda a P il colore di un quadrato per volta: la probabilità che P lo conosca è **d·*l*/N**; se P non lo conosce, ha comunque probabilità **1/c** di indovinare quello esatto. Poiché la probabilità che S chieda a P un quadrato che questi non conosce è **(N-d·*l*)/N**,

Probabilità che **P** risponda ad **S** comunicando il colore corretto è al più:

$$\frac{d \cdot l}{N} + \frac{1}{c} \cdot \frac{N - d \cdot l}{N} = \frac{1}{c} + \frac{(c-1) \cdot d \cdot l}{c \cdot N}$$

Probabilità che **P** riesca a spacciarsi per **U** é al più: $\left(\frac{1}{c} + \frac{(c-1) \cdot d \cdot l}{c \cdot N} \right)^d$

Scelto il valore di **l** : $l = \frac{N}{(c-1) \cdot d}$

La probabilità che **P** non riesca nel suo intento è: $1 - \left(\frac{2}{c} \right)^d$

Questo sistema ha posto le basi per una forma molto più avanzata di identificazione visuale la scansione della retina dove l'immagine di riferimento è la scansione dell'utente i il sistema può creare lucidi a partire dall'immagine di partenza e fare le sfide su un immagine momentanea fornita dall'utente che risponde alle sfide del sistema.