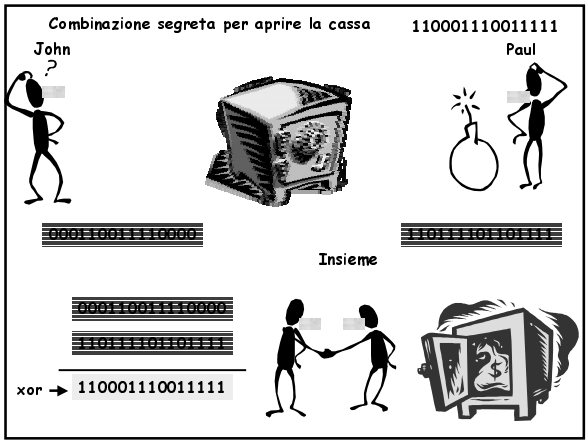
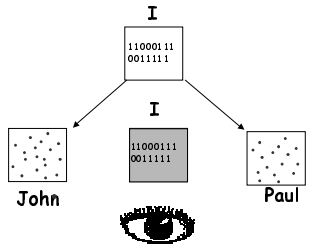
Crittografia Visuale

La Crittografia Visuale

- E' una tecnica crittografica per
  - cifrare immagini
- La proprietà principale è che
  - la decodifica richiede semplicemente l'uso dell'occhio umano





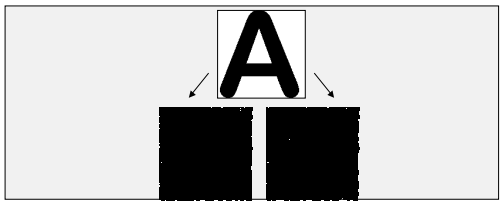
Decodifica effettuata dal sistema visivo umano

[B. Arazi, I. Dinstein, O. Kafri, 1989]

[M. Naor e A. Shamir, 1994]

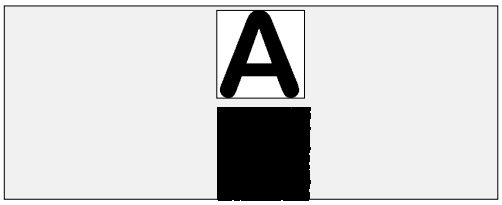
Il modello base

- Per ogni immagine da cifrare vengono prodotte due immagini "oscure"dette share. Ciascuna share non dà alcuna informazione sull'immagine di partenza.

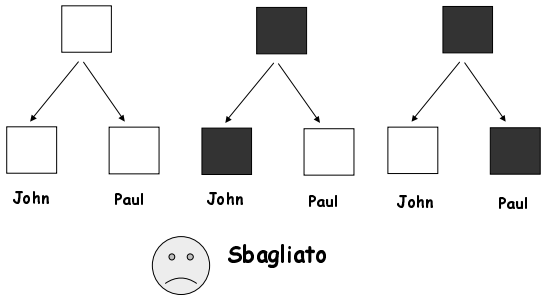


Il modello base

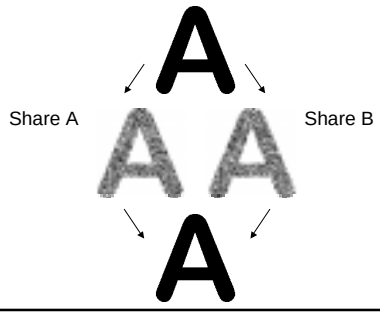
- Le share vengono riportate su dei lucidi la cui sovrapposizione riproduce l'immagine originale



Come cifrare un pixel



Esempio



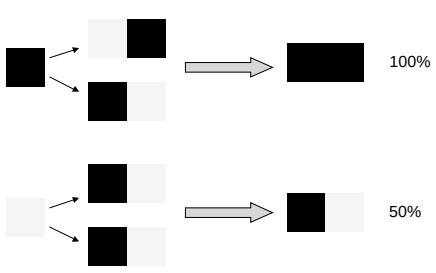
La soluzione

Possibili codifiche per un pixel nero

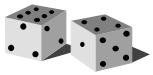
La soluzione

Possibili codifiche per un pixel bianco

La soluzione

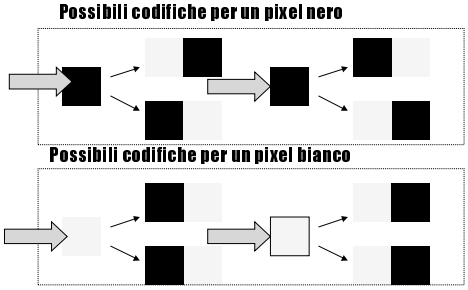


La soluzione



Possibili codifiche per un pixel nero

Possibili codifiche per un pixel bianco

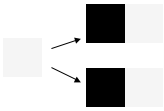


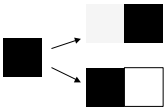
Sicurezza dello schema

Share	Pixel originale	Probabilità
		1/2
		1/2

Share	Pixel originale	Probabilità
		1/2
		1/2

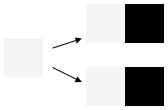
Matrici di base

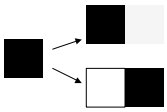




$$S_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \qquad S_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Matrici di base



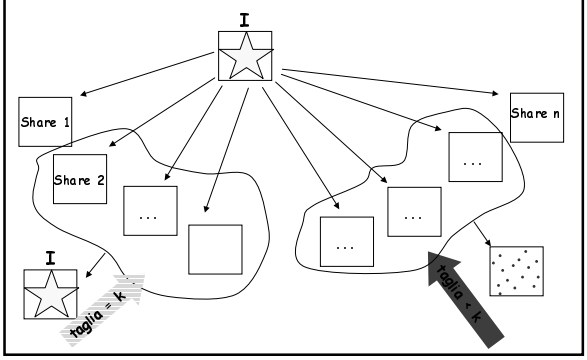


$$S_0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \qquad S_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Schema a soglia (k,n)

- *n* Partecipanti
- Dividere l'immagine segreta in *n* immagini
- L'immagine segreta è visibile sse almeno *k* share vengono sovrapposte
- Non si ottiene alcuna informazione osservando meno di *k* share

Schema a soglia (k,n)



Esempio di schema a soglia (3,3)

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

• Ogni partecipante ottiene una share con 2 sottopixel neri
• Due participanti, se sovrappongono le rispettive share, ottengono una share "composta" con 3 sottopixel neri

Tre partecipanti ricostruiscono l'immagine segreta!

Il bianco viene recuperato al 25 %
Il nero al 100%

Struttura d'accesso

- Specifica esattamente quali sottoinsiemi di partecipanti possono recuperare l'immagine segreta e quali no
- I sottoinsiemi che possono recuperare l'immagine sono detti ***autorizzati***
- I sottoinsiemi non abilitati sono detti ***proibiti***

Schema di Crittografia Visuale

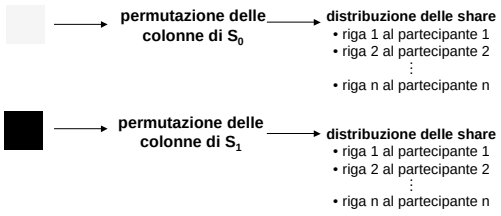
Uno Schema di Crittografia Visuale (VCS) per un insieme P di n partecipanti è un metodo per codificare un'immagine segreta in n immagini, dette share, tale che:

- I partecipanti *autorizzati* possono recuperare visualmente l'immagine sovrapponendo le loro share
- I partecipanti *non autorizzati* non hanno alcuna informazione circa l'immagine segreta

Matrici di base

- VCS in bianco e nero con n partecipanti
- Due matrici $n \times m$ S_0 e S_1
- La riga i della matrice S_0 (S_1) rappresenta la codifica *base* di un pixel bianco (nero) per il partecipante i

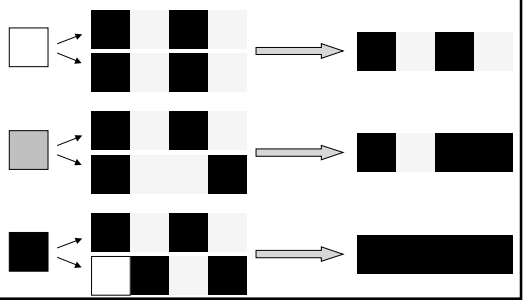
Matrici di Base



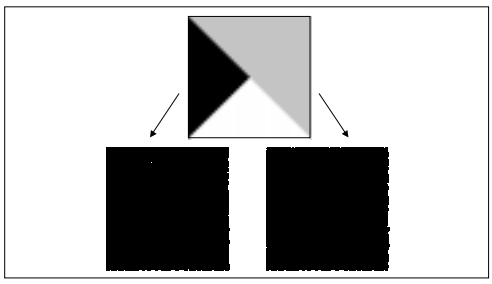
Crittografia Visuale in toni di grigio

- Immagine segreta in toni di grigio
- Share in bianco e nero
- Il tono di grigio ottenuto dipende dal numero di pixel neri che si ottiene sovrapponendo m pixel di A ed m di B

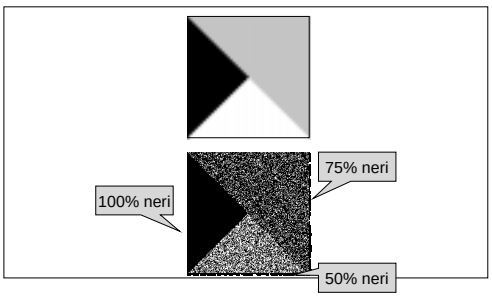
Esempio di VCS a 3 toni di grigio (3-GVCS)



3-GVGS, esempio



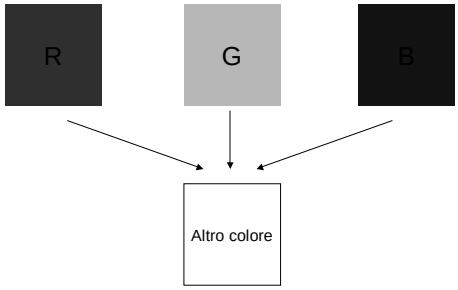
3-GVGS, esempio



Crittografia Visuale a colori

- Immagine segreta a colori
- Share a colori
- Sovrapposizione dei colori
  - composizione RGB

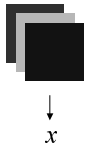
Teoria della tricromia di Maxwell



Composizione RGB

Colori RGB

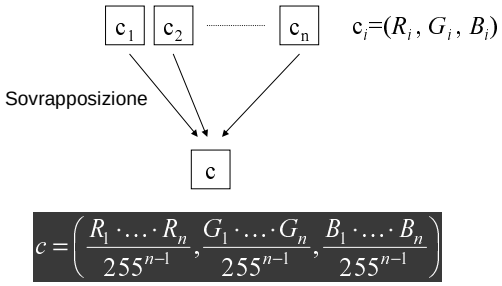
- Colore x = (R,G,B)
  - x è dato dalla composizione dei tre colori Rosso, Verde e Blu (Red, Green, Blu)



Colori RGB, esempio

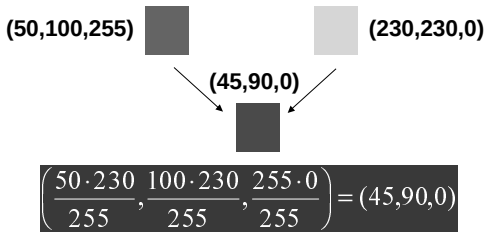
- (0,0,0) la luce è completamente assorbita
  - Nero
- (255,255,255) la luce viene lasciata passare
  - Bianco
- (255,0,0) Il verde ed il blu vengono assorbiti
  - Rosso
- (150,0,0) parte del rosso è assorbito
  - Rosso scuro

Legge di composizione RGB



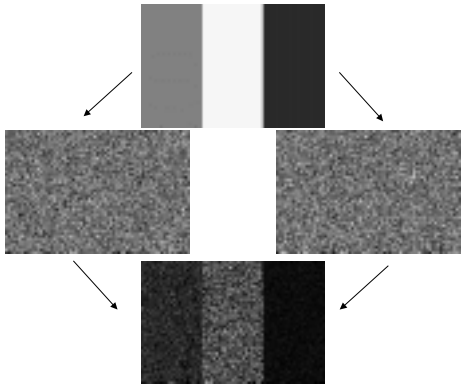
$$c = \left(\frac{R_1 \cdot \ldots \cdot R_n}{255^{n-1}}, \frac{G_1 \cdot \ldots \cdot G_n}{255^{n-1}}, \frac{B_1 \cdot \ldots \cdot B_n}{255^{n-1}} \right)$$

Composizione RGB, esempio



$$\left(\frac{50 \cdot 230}{255}, \frac{100 \cdot 230}{255}, \frac{255 \cdot 0}{255} \right) = (45,90,0)$$

Crittografia Visuale a colori, esempio



Presentazione del VES

Il sito di Crittografia Visuale

Il sito di Crittografia Visuale

- Crittografia Visuale
  - Cos'è
  - Consultare articoli
  - Link a siti correlati
- Visionare esempi
- Interagire con il VES

Il sito di Crittografia Visuale

- Crittografia Visuale
- Visionare esempi
  - Galleria di immagini e relative share
- Interagire con il VES

Il sito di Crittografia Visuale

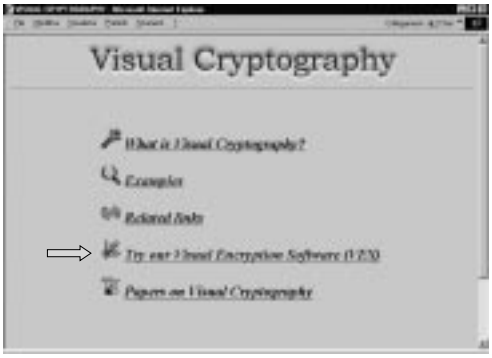
- Reperire documenti circa la Crittografia Visuale
- Visionare esempi
- Interagire con il VES
  - Generare le share
    - uno strumento innovativo
    - altri siti non lo consentono

Visual Encryption Software

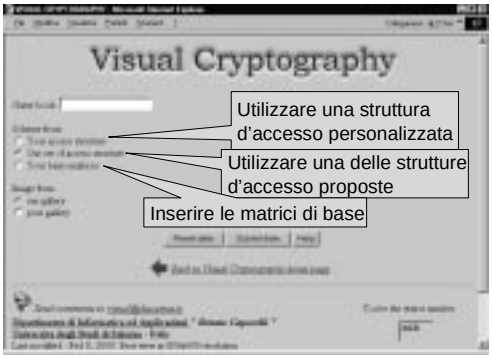
E' un sistema software

- Generazione Schemi di Crittografia Visale
  - in bianco e nero
  - in toni di grigio
- Generazione di share per immagini
  - in bianco e nero
  - in toni di grigio
  - a colori
- Verifica delle share
  - animazione interattiva
  - sovrapposizione digitale

Home page del sito di CV



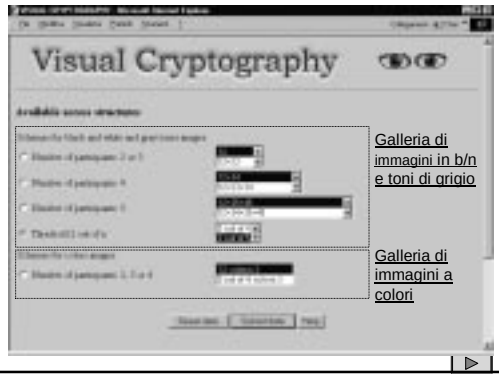
Home page del VES



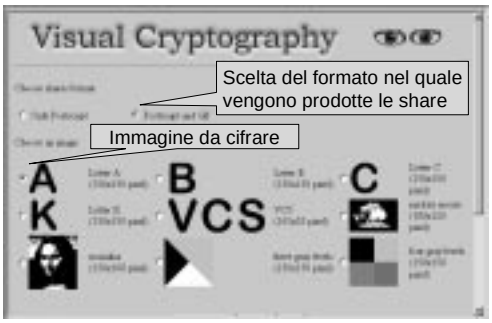
Home page del VES

Home page del VES

Strutture d'accesso proposte



Galleria delle immagini in b/n e in toni di grigio



Galleria delle immagini a colori

Verifica e download delle share

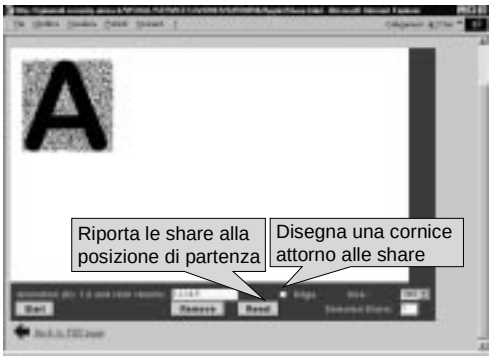
Animazione interattiva delle share

Permette all'utente di sovrapporre le share

- manualmente
- mediante un'animazione

Animazione delle share

Animazione delle share



Animazione delle share

Animazione delle share

Animazione delle share

La piattaforma

- Sistema
  - Linux
- Linguaggi utilizzati
  - C e JAVA
- Ambiente
  - CGI
- Web Server
  - Apache