

Esquema para compartir imágenes secretas con base en retículos

Luis Fernando González Guzmán

Universidad Nacional de Colombia

Facultad de Ciencias

Departamento de Matemáticas

Contenido

1. Compartir un secreto
2. Imágenes digitales
3. Compartir imágenes secretas
4. Retículos
5. Esquema con base en retículos

Compartir un secreto

- Sistema que permite dividir un secreto en distintas piezas que se distribuyen entre varios participantes.
- Según el caso, se requieren todas o algunas de dichas piezas para reconstruir el secreto.
- Cada pieza por separado no tiene ninguna utilidad.

Algunas aplicaciones:

- Dividir un mensaje en varias partes, las cuales se envían por diferentes rutas a cierto destino donde se reconstruye el mensaje.
- Almacenar partes de un documento en diferentes lugares.
- Compartir el mapa de un tesoro entre un grupo de elegidos.

Esquema (k, n)

Definición:¹ Sea \mathcal{S} el secreto a compartir entre n participantes, $2 \leq k \leq n$, un esquema de umbral (k, n) , es alguna forma de distribuir \mathcal{S} en n piezas S_1, S_2, \dots, S_n de tal forma que se cumplan las dos siguientes condiciones:

1. El conocimiento de cualesquiera k piezas S_i permite calcular el valor de \mathcal{S} fácilmente.
2. La información obtenida con menos de k piezas S_i mantiene a \mathcal{S} completamente indeterminado, lo que significa que cualquiera de sus posibles valores es igualmente probable.

¹Shamir (1979), How to Share a Secret

Esquema (k, n) de Shamir

El esquema se basa en interpolación polinomial.²

Teorema

Sea \mathcal{K} un campo, $\{(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k)\}$ un conjunto de k elementos diferentes en \mathcal{K}^2 , existe un único polinomio $f(x)$ de grado $k - 1$, tal que $y_i = f(x_i)$, $1 \leq i \leq k$.

$$f(x) = \sum_{i=1}^k y_i \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)}$$

²Sistema lineal de ecuaciones, matriz de Vandermonde, polinomio de Lagrange

Esquema (k, n) de Shamir

El secreto a compartir debe pertenecer a un conjunto finito en el cual sus elementos se puedan representar mediante números.

Campo finito

El conjunto $\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$, en el cual las operaciones de suma y multiplicación se definen sobre sus elementos mediante aritmética modulo p se convierte en un campo finito si p es primo.

Esquema (k, n) de Shamir

Codificación

1. Representar \mathcal{S} con un número natural
2. Escojer un primo p tal que $p > \mathcal{S}$ y $p > n$
3. Construir $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$
4. Asignar $a_0 = \mathcal{S} \implies \mathcal{S} = f(0)$
5. Asignar valores aleatorios a cada $a_i \in \mathbb{Z}_p$, $0 < i < k$.
6. Generar n diferentes aleatorios $x_j \in \mathbb{Z}_p$, $x_j \neq 0$, $1 \leq j \leq n$
7. Evaluar (mód p) cada $y_j = f(x_j)$, $j = 1, 2, \dots, n$
8. Distribuir las n parejas $\{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$

Esquema (k, n) de Shamir

Codificación

1. Representar \mathcal{S} con un número natural
2. Escojer un primo p tal que $p > \mathcal{S}$ y $p > n$
3. Construir $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$
4. Asignar $a_0 = \mathcal{S} \implies \mathcal{S} = f(0)$
5. Asignar valores aleatorios a cada $a_i \in \mathbb{Z}_p$, $0 < i < k$.
6. Generar n diferentes aleatorios $x_j \in \mathbb{Z}_p$, $x_j \neq 0$, $1 \leq j \leq n$
7. Evaluar (mód p) cada $y_j = f(x_j)$, $j = 1, 2, \dots, n$
8. Distribuir las n parejas $\{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$

Esquema (k, n) de Shamir

Codificación

1. Representar \mathcal{S} con un número natural
2. Escojer un primo p tal que $p > \mathcal{S}$ y $p > n$
3. Construir $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$
4. Asignar $a_0 = \mathcal{S} \implies \mathcal{S} = f(0)$
5. Asignar valores aleatorios a cada $a_i \in \mathbb{Z}_p$, $0 < i < k$.
6. Generar n diferentes aleatorios $x_j \in \mathbb{Z}_p$, $x_j \neq 0$, $1 \leq j \leq n$
7. Evaluar (mód p) cada $y_j = f(x_j)$, $j = 1, 2, \dots, n$
8. Distribuir las n parejas $\{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$

Esquema (k, n) de Shamir

Codificación

1. Representar \mathcal{S} con un número natural
2. Escojer un primo p tal que $p > \mathcal{S}$ y $p > n$
3. Construir $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$
4. Asignar $a_0 = \mathcal{S} \implies \mathcal{S} = f(0)$
5. Asignar valores aleatorios a cada $a_i \in \mathbb{Z}_p$, $0 < i < k$.
6. Generar n diferentes aleatorios $x_j \in \mathbb{Z}_p$, $x_j \neq 0$, $1 \leq j \leq n$
7. Evaluar (mód p) cada $y_j = f(x_j)$, $j = 1, 2, \dots, n$
8. Distribuir las n parejas $\{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$

Esquema (k, n) de Shamir

Codificación

1. Representar \mathcal{S} con un número natural
2. Escojer un primo p tal que $p > \mathcal{S}$ y $p > n$
3. Construir $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$
4. Asignar $a_0 = \mathcal{S} \implies \mathcal{S} = f(0)$
5. Asignar valores aleatorios a cada $a_i \in \mathbb{Z}_p$, $0 < i < k$.
6. Generar n diferentes aleatorios $x_j \in \mathbb{Z}_p$, $x_j \neq 0$, $1 \leq j \leq n$
7. Evaluar (mód p) cada $y_j = f(x_j)$, $j = 1, 2, \dots, n$
8. Distribuir las n parejas $\{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$

Esquema (k, n) de Shamir

Codificación

1. Representar \mathcal{S} con un número natural
2. Escojer un primo p tal que $p > \mathcal{S}$ y $p > n$
3. Construir $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$
4. Asignar $a_0 = \mathcal{S} \implies \mathcal{S} = f(0)$
5. Asignar valores aleatorios a cada $a_i \in \mathbb{Z}_p$, $0 < i < k$.
6. Generar n diferentes aleatorios $x_j \in \mathbb{Z}_p$, $x_j \neq 0$, $1 \leq j \leq n$
7. Evaluar (mód p) cada $y_j = f(x_j)$, $j = 1, 2, \dots, n$
8. Distribuir las n parejas $\{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$

Esquema (k, n) de Shamir

Codificación

1. Representar \mathcal{S} con un número natural
2. Escojer un primo p tal que $p > \mathcal{S}$ y $p > n$
3. Construir $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$
4. Asignar $a_0 = \mathcal{S} \implies \mathcal{S} = f(0)$
5. Asignar valores aleatorios a cada $a_i \in \mathbb{Z}_p$, $0 < i < k$.
6. Generar n diferentes aleatorios $x_j \in \mathbb{Z}_p$, $x_j \neq 0$, $1 \leq j \leq n$
7. Evaluar (mód p) cada $y_j = f(x_j)$, $j = 1, 2, \dots, n$
8. Distribuir las n parejas $\{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$

Esquema (k, n) de Shamir

Codificación

1. Representar \mathcal{S} con un número natural
2. Escojer un primo p tal que $p > \mathcal{S}$ y $p > n$
3. Construir $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$
4. Asignar $a_0 = \mathcal{S} \implies \mathcal{S} = f(0)$
5. Asignar valores aleatorios a cada $a_i \in \mathbb{Z}_p$, $0 < i < k$.
6. Generar n diferentes aleatorios $x_j \in \mathbb{Z}_p$, $x_j \neq 0$, $1 \leq j \leq n$
7. Evaluar (mód p) cada $y_j = f(x_j)$, $j = 1, 2, \dots, n$
8. Distribuir las n parejas $\{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$

Esquema (k, n) de Shamir

Decodificación

1. Reunir un conjunto de cualesquiera k parejas
 $\{(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k)\}$
2. A partir de estos valores, el valor del secreto se calcula evaluando en cero la función de interpolación:

$$\mathcal{S} = f(0) = \sum_{i=1}^k y_i \frac{\prod_{j \neq i} (-x_j)}{\prod_{j \neq i} (x_i - x_j)}$$

¿Qué es una imagen?

- **Imagen:** función bidimensional $f(x, y)$
- La pareja (x, y) define las coordenadas espaciales y el valor de f en cada una de ellas corresponde a la intensidad o nivel de color de la imagen en ese punto.

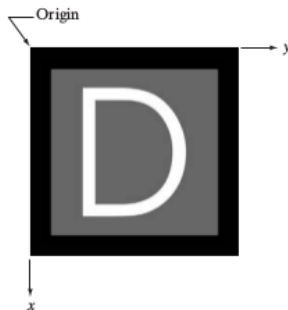
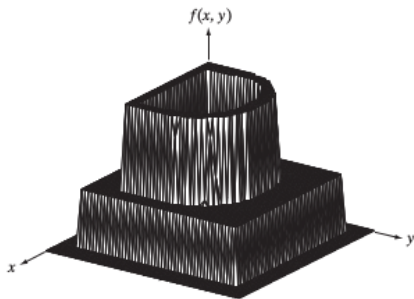


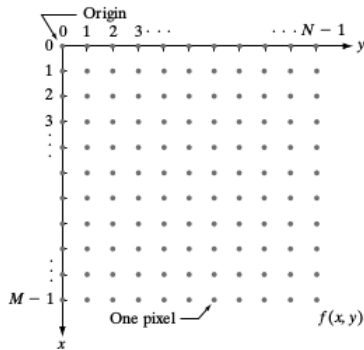
Imagen digital

- Cuando x , y y los valores de f son todas cantidades discretas finitas, $f(x, y)$ representa una imagen digital.
- Una imagen digital de tamaño $M \times N$ se representa en una matriz de M filas y N columnas.

$$f(x, y) = \begin{bmatrix} f(0, 0) & f(0, 1) & \cdots & f(0, N - 1) \\ f(1, 0) & f(1, 1) & \cdots & f(1, N - 1) \\ \vdots & \vdots & & \vdots \\ f(M - 1, 0) & f(M - 1, 1) & \cdots & f(M - 1, N - 1) \end{bmatrix}$$

Imagen digital

Una imagen digital se compone de un numero finito de elementos, cada uno tiene una ubicacion y valor. Cada uno de estos elementos se denomina Pixel.



Pixel
Picture element

$$\mathbf{A} = \begin{bmatrix} a_{0,0} & a_{0,1} & \dots & a_{0,N-1} \\ a_{1,0} & a_{1,1} & \dots & a_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{M-1,0} & a_{M-1,1} & \dots & a_{M-1,N-1} \end{bmatrix}$$

Tipos de imágenes

Imagen binaria

$$f(x, y) \in \{0, 1\}$$

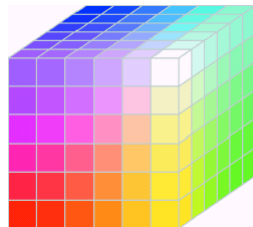
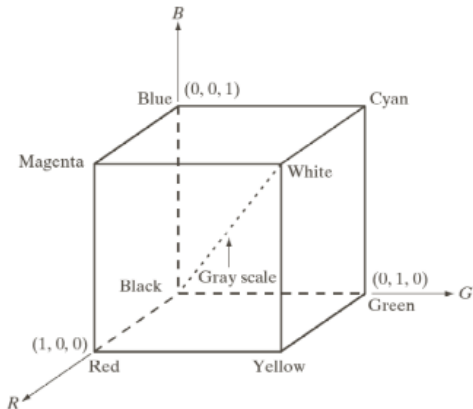
Imagen en escala de grises

$$f(x, y) \in \{0, 1, 2, \dots, L - 1\}^*$$

Imagen a color

$$f(x, y) \in \mathcal{C}, \text{ donde } \mathcal{C} \text{ es un espacio de color.}$$

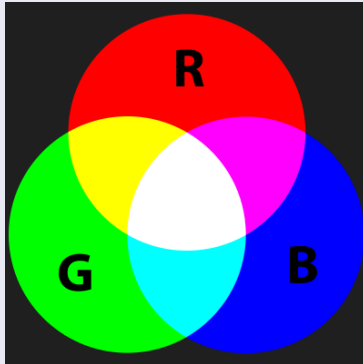
Espacios de colores



$$c = \alpha P_1 + \beta P_2 + \gamma P_3$$

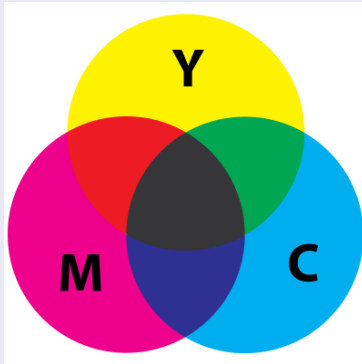
Modelos de Color

RGB



Modelos de Color

CMY-K



Compartir imágenes secretas

- La criptografía visual, introducida por Naor y Shamir en 1994, consiste en ocultar información en imágenes de tal forma que para realizar la decodificación no se utilizan métodos computacionales sino la percepción del sistema visual humano.
- El proceso consiste en generar dos o más imágenes de manera que al imprimirlas en transparencias y apilarlas una sobre otra revelen una imagen secreta.
- El sistema es perfectamente seguro: cada una de las imágenes generadas, analizadas por separado no contienen información acerca de la imagen secreta.

Compartir imágenes secretas

Codificación

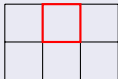
1. Generar varias transparencias a partir de la imagen secreta.
2. Expandir cada pixel de la imagen en una región de subpíxeles.
3. De acuerdo al color del pixel se asigna al azar un patrón de expansión adecuado en cada una de las transparencias.

Decodificación

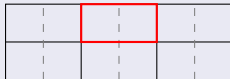
- El secreto se revela al apilar, según se requiera, todas o algunas de las transparencias correctamente alineadas.

Expansión de pixel

$$m = 2$$

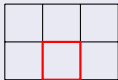


$$2 \times 3 = 6 \text{ pix}$$

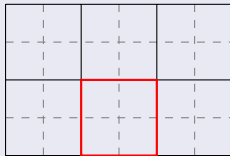


$$2 \times 6 = 12 \text{ pix}$$

$$m = 4$$

















$$2 \times 3 = 6 \text{ pix}$$



$$4 \times 6 = 24 \text{ pix}$$

Esquema Básico (2, 2)

Expansión de pixel: $m = 2$

Pixel				
Probabilidad	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
T_1				
T_2				
$T_1 \oplus T_2$				

Expansión de pixel: $m = 4$



$[0, 0, 1, 1]$



$[1, 1, 0, 0]$



$[0, 1, 0, 1]$



$[1, 0, 1, 0]$



$[0, 1, 1, 0]$



$[1, 0, 0, 1]$

$$S_w = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad S_b = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

$C_w = \{\text{matrices obtenidas permutando las columnas de } S_w\}$

$C_b = \{\text{matrices obtenidas permutando las columnas de } S_b\}$

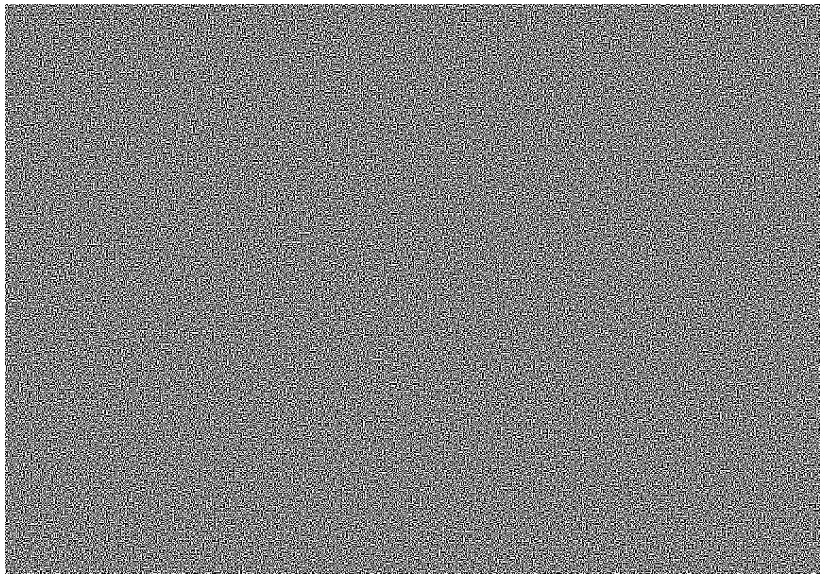
Para cada pixel de la imagen: Seleccionar al azar una matriz de la colección C_w si dicho pixel es blanco (C_b si el pixel es negro) y asignar a cada transparencia T_i la expansión de pixel dada por el vector fila i de la matriz seleccionada.

Imagen binaria $m = 4$

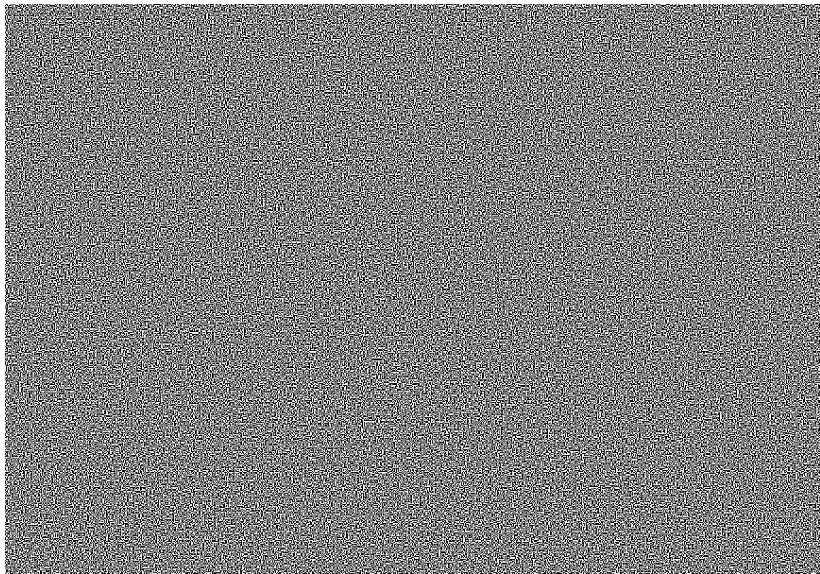
Imagen secreta



$$T_1$$



$$T_2$$



$$T_1 \oplus T_2$$



Posets

Una relación binaria \preceq en un conjunto no vacío \mathcal{P} es un orden parcial en \mathcal{P} si para todo $x, y, z \in \mathcal{P}$ se cumplen las siguientes tres propiedades (reflexiva, antisimétrica y transitiva):

1. $x \preceq x$
2. $x \preceq y, \quad y \preceq x \implies x = y$
3. $x \preceq y, \quad y \preceq z \implies x \preceq z$

Un poset (conjunto parcialmente ordenado) es una pareja (\mathcal{P}, \preceq)

Sea (\mathcal{P}, \preceq) un poset y $x_1, x_2, y \in \mathcal{P}$

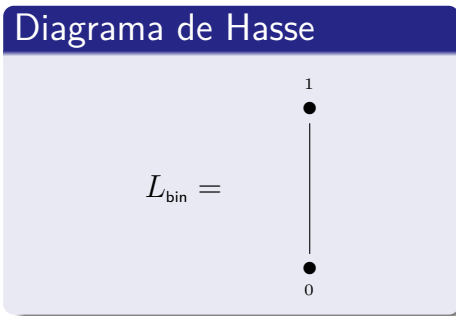
- y es una cota superior de x_1, x_2 si $x_1 \preceq y$ y $x_2 \preceq y$.
- y es el supremo de x_1, x_2 si y es una cota superior de x_1, x_2 y $y \preceq z$ para todo z que sea cota superior de x_1, x_2 .
- El supremo de x_1, x_2 se denota $\sup(x_1, x_2)$
- y es una cota inferior de x_1, x_2 si $x_1 \succeq y$ y $x_2 \succeq y$.
- y es el ínfimo de x_1, x_2 si y es una cota inferior de x_1, x_2 y $y \succeq z$ para todo z que sea cota inferior de x_1, x_2 .
- El ínfimo de x_1, x_2 se denota $\inf(x_1, x_2)$

¿Qué es un retículo?

Un retículo es un poset en el cual para toda pareja de elementos existe tanto el supremo como el ínfimo.

Un ejemplo de retículo finito es el conjunto de los divisores de algún número natural con la relación de divisibilidad. En dicho retículo para cualquier pareja de elementos, el supremo corresponde al mínimo común múltiplo y el ínfimo al máximo común divisor.

Retículos



$$a \cup b = \sup(a, b)$$

\cup	0	1
0	0	1
1	1	1

$$a \cap b = \inf(a, b)$$

\cap	0	1
0	0	0
1	0	1

Producto cartesiano de un retículo

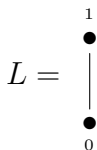
- El m -ésimo producto cartesiano de un retículo finito L es también un retículo finito L^m
- Los operadores \cup_{L^m} y \cap_{L^m} se inducen en L^m
- \cup_L y \cap_L denotan los operadores definidos en L

$$\forall (a_1, a_2, \dots, a_m), (b_1, b_2, \dots, b_m) \in L^m$$

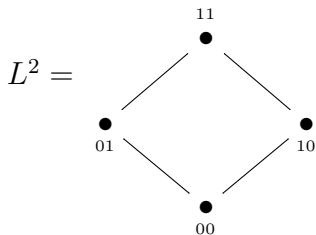
$$(a_1, \dots, a_m) \cup_{L^m} (b_1, \dots, b_m) = (a_1 \cup_L b_1, \dots, a_m \cup_L b_m)$$

$$(a_1, \dots, a_m) \cap_{L^m} (b_1, \dots, b_m) = (a_1 \cap_L b_1, \dots, a_m \cap_L b_m)$$

Producto cartesiano de un retículo

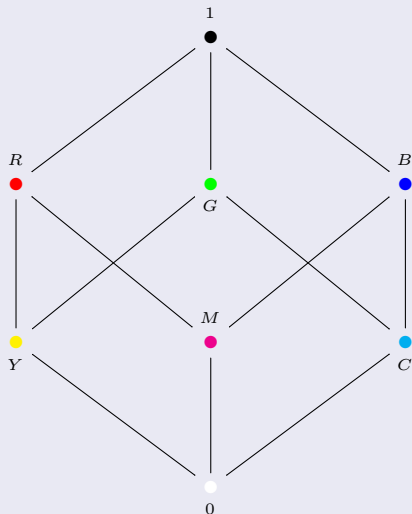


\cap_{L^2}	00	01	10	11
00	00	00	00	00
01	00	01	00	01
10	00	00	10	10
11	00	01	10	11



\cup_{L^2}	00	01	10	11
00	00	01	10	11
01	01	01	11	11
10	10	11	10	11
11	11	11	11	11

Diagrama de Hasse de L_{col}



$$Y \cup M = R$$

$$M \cup C = B$$

$$R \cup 1 = 1$$

$$B \cup 0 = B$$

$$Y \cup Y = Y$$

Esquema (k, n) con base en retículos

Definición:³ Sea L un retículo finito y $m > 0$. Para todo q y diferentes $\{i_1, i_2, \dots, i_q\} \subseteq \{1, 2, \dots, n\}$, tal que $1 \leq q \leq k$

$$h^{(i_1, i_2, \dots, i_q)} : (L^m)^n \longrightarrow (L^m)$$
$$h^{(i_1, i_2, \dots, i_q)}(x) = x_{i_1} \cup x_{i_2} \cup \dots \cup x_{i_q}$$

$$x = (x_1, x_2, \dots, x_n) \in (L^m)^n$$

$$a \cup b = \sup(a, b); \quad a, b \in L^m$$

³Operación al apilar transparencias.

Esquema (k, n) con base en retículos

Sea L un retículo finito, $m > 0$, $\mathcal{C} = \{c_1, c_2, \dots, c_J\} \subseteq L$

Si existe

$$\{(\mathcal{X}_{c_j}, \mathcal{Y}_{c_j})\}_{j=1}^J, \quad \mathcal{X}_{c_j} \subseteq (L^m)^n, \quad \mathcal{Y}_{c_j} \subseteq L^m$$

$\{(\mathcal{X}_{c_j}, \mathcal{Y}_{c_j})\}_{j=1}^J$ se denomina el esquema (k, n) basado en retículos con colores \mathcal{C} , si cumple las tres siguientes propiedades.

Propiedades Esquema (k, n)

1. $\forall j = 1, 2, \dots, J; \{i_1, i_2, \dots, i_k\} \subseteq \{1, 2, \dots, n\}; x \in \mathcal{X}_{c_j}$

$$h^{(i_1, i_2, \dots, i_k)}(x) \in \mathcal{Y}_{c_j}$$

2. Para todo $q < k$ y $\{i_1, i_2, \dots, i_q\} \subseteq \{1, 2, \dots, n\}$ se define

$$\mathcal{X}_{c_j}^{(i_1, i_2, \dots, i_q)} = \{(x_{i_1}, x_{i_2}, \dots, x_{i_q}) : (x_1, x_2, \dots, x_n) \in \mathcal{X}_{c_j}\}$$

Entonces, $\mathcal{X}_{c_j}^{(i_1, i_2, \dots, i_q)}, j = 1, 2, \dots, J$ son indistinguibles⁴.

3. Para todo $c_j \in \mathcal{C}$

- Si $c_j \neq 1$, todos los elementos en \mathcal{Y}_{c_j} se componen de 1's y al menos un c_j .
- Si $c_j = 1$, \mathcal{Y}_{c_j} tiene un único elemento compuesto de m 1's.

⁴Contienen los mismos elementos con las mismas frecuencias.

Propiedades Esquema (k, n)

1. $\forall j = 1, 2, \dots, J; \{i_1, i_2, \dots, i_k\} \subseteq \{1, 2, \dots, n\}; x \in \mathcal{X}_{c_j}$

$$h^{(i_1, i_2, \dots, i_k)}(x) \in \mathcal{Y}_{c_j}$$

2. Para todo $q < k$ y $\{i_1, i_2, \dots, i_q\} \subseteq \{1, 2, \dots, n\}$ se define

$$\mathcal{X}_{c_j}^{(i_1, i_2, \dots, i_q)} = \{(x_{i_1}, x_{i_2}, \dots, x_{i_q}) : (x_1, x_2, \dots, x_n) \in \mathcal{X}_{c_j}\}$$

Entonces, $\mathcal{X}_{c_j}^{(i_1, i_2, \dots, i_q)}, j = 1, 2, \dots, J$ son indistinguibles⁴.

3. Para todo $c_j \in \mathcal{C}$

- Si $c_j \neq 1$, todos los elementos en \mathcal{Y}_{c_j} se componen de 1's y al menos un c_j .
- Si $c_j = 1$, \mathcal{Y}_{c_j} tiene un único elemento compuesto de m 1's.

⁴Contienen los mismos elementos con las mismas frecuencias.

Propiedades Esquema (k, n)

1. $\forall j = 1, 2, \dots, J; \{i_1, i_2, \dots, i_k\} \subseteq \{1, 2, \dots, n\}; x \in \mathcal{X}_{c_j}$

$$h^{(i_1, i_2, \dots, i_k)}(x) \in \mathcal{Y}_{c_j}$$

2. Para todo $q < k$ y $\{i_1, i_2, \dots, i_q\} \subseteq \{1, 2, \dots, n\}$ se define

$$\mathcal{X}_{c_j}^{(i_1, i_2, \dots, i_q)} = \{(x_{i_1}, x_{i_2}, \dots, x_{i_q}) : (x_1, x_2, \dots, x_n) \in \mathcal{X}_{c_j}\}$$

Entonces, $\mathcal{X}_{c_j}^{(i_1, i_2, \dots, i_q)}, j = 1, 2, \dots, J$ son indistinguibles⁴.

3. Para todo $c_j \in \mathcal{C}$

- Si $c_j \neq 1$, todos los elementos en \mathcal{Y}_{c_j} se componen de 1's y al menos un c_j .
- Si $c_j = 1$, \mathcal{Y}_{c_j} tiene un único elemento compuesto de m 1's.

⁴Contienen los mismos elementos con las mismas frecuencias.

Ejemplo 1. Esquema (2, 2)

$$L = \begin{array}{c} 1 \\ \bullet \\ | \\ \bullet \\ 0 \end{array}$$

$$m = 2$$

$$\mathcal{C} = \{0, 1\}$$

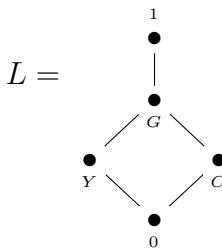
$$\mathcal{X}_0 = \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}, \quad \mathcal{Y}_0 = \{01, 10\}$$

$$\mathcal{X}_1 = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}, \quad \mathcal{Y}_1 = \{11\}$$

Ejemplo 2. Esquema (2, 2)

$$m = 4$$

$$\mathcal{C} = \{Y, C, G\}$$

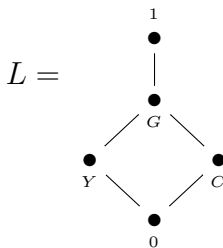


	Y				C				G			
y	Y	Y	1	1	C	C	1	1	G	G	1	1
x	Y		1		C		1					1
		Y		1		C		1				1
x	Y		1	C	C		1	Y	Y	C		1
		Y	C	1		C	Y	1	C	Y	1	
x	Y	0	1	C	C	0	1	Y	Y	C	0	1
	0	Y	C	1	0	C	Y	1	C	Y	1	0

Ejemplo 2. Esquema (2, 2)

$$m = 4$$

$$\mathcal{C} = \{Y, C, G\}$$

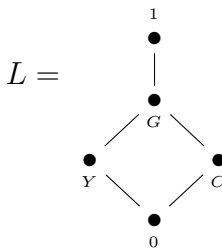


	Y				C				G			
y	Y	Y	1	1	C	C	1	1	G	G	1	1
x	Y		1		C		1					1
		Y		1		C		1				1
x	Y		1	C	C		1	Y	Y	C		1
		Y	C	1		C	Y	1	C	Y	1	
x	Y	0	1	C	C	0	1	Y	Y	C	0	1
	0	Y	C	1	0	C	Y	1	C	Y	1	0

Ejemplo 2. Esquema (2, 2)

$$m = 4$$

$$\mathcal{C} = \{Y, C, G\}$$

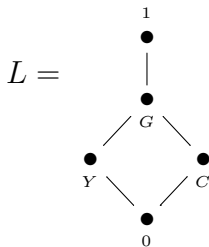


	Y				C				G			
y	Y	Y	1	1	C	C	1	1	G	G	1	1
x	Y		1		C		1					1
		Y		1		C		1				1
x	Y		1	C	C		1	Y	Y	C		1
		Y	C	1		C	Y	1	C	Y	1	
x	Y	0	1	C	C	0	1	Y	Y	C	0	1
	0	Y	C	1	0	C	Y	1	C	Y	1	0

Ejemplo 2. Esquema (2, 2)

$$m = 4$$

$$\mathcal{C} = \{Y, C, G\}$$



$$\mathfrak{X}_Y = \Pi \left\{ \begin{bmatrix} Y & 0 & 1 & C \\ 0 & Y & C & 1 \end{bmatrix} \right\}$$

$$\mathfrak{Y}_Y = \Pi \{ Y \ Y \ 1 \ 1 \}$$

$$\mathfrak{X}_C = \Pi \left\{ \begin{bmatrix} C & 0 & 1 & Y \\ 0 & C & Y & 1 \end{bmatrix} \right\}$$

$$\mathfrak{Y}_C = \Pi \{ C \ C \ 1 \ 1 \}$$

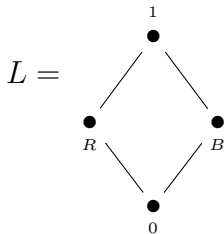
$$\mathfrak{X}_G = \Pi \left\{ \begin{bmatrix} Y & C & 0 & 1 \\ C & Y & 1 & 0 \end{bmatrix} \right\}$$

$$\mathfrak{Y}_G = \Pi \{ G \ G \ 1 \ 1 \}$$

Ejemplo 3. Esquema (2, 3)

$$m = 6$$

$$\mathcal{C} = \{R, B\}$$



$$\mathcal{X}_R = \Pi \left\{ \begin{bmatrix} R & 1 & 0 & B & 1 & 1 \\ 0 & R & 1 & 1 & B & 1 \\ 1 & 0 & R & 1 & 1 & B \end{bmatrix} \right\}$$

$$\mathcal{Y}_R = \Pi \{ R \ 1 \ 1 \ 1 \ 1 \ 1 \}$$

$$\mathcal{X}_B = \Pi \left\{ \begin{bmatrix} B & 1 & 0 & R & 1 & 1 \\ 0 & B & 1 & 1 & R & 1 \\ 1 & 0 & B & 1 & 1 & R \end{bmatrix} \right\}$$

$$\mathcal{Y}_B = \Pi \{ B \ 1 \ 1 \ 1 \ 1 \ 1 \}$$

$$h^{(1,3)}(\mathcal{X}_R) = 11R111 \in \mathcal{Y}_R$$

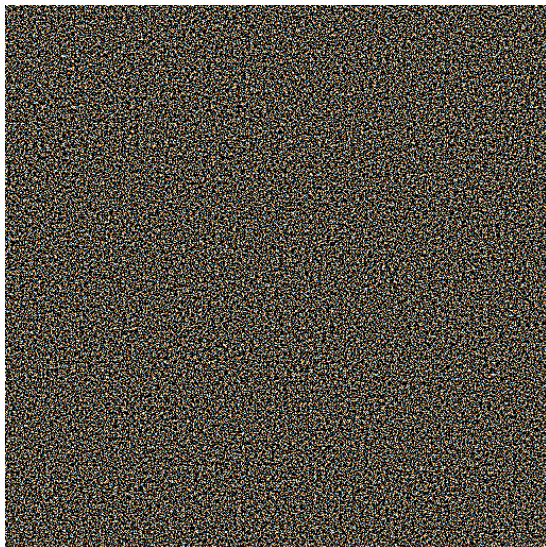
$$h^{(2,3)}(\mathcal{X}_B) = 1B1111 \in \mathcal{Y}_B$$

Imagen 8 colores $m = 16$

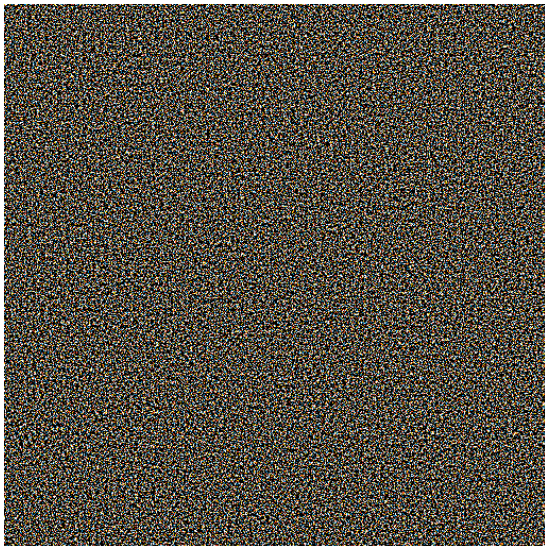
Imagen secreta (128×128)



$$T_1$$



$$T_2$$



$$T_1 \oplus T_2$$

