Criptografía Visual

Erick M.

Escuela Superior de Física y Matemáticas
Instituto Politécnico Nacional

Contenido

Conceptos

Criptología

- Criptografía
- Criptoanálisis

Conceptos

Criptología

- `Criptografía`
- `Criptoanálisis`

Conceptos

- **Mensaje**: Colección de texto.
- **Texto claro**: Es el texto original del mensaje y que se busca cifrar.
- **Criptotexto o texto cifrado**: Texto resultante de cifrar el texto claro.
- **Cifrar/descifrar**: Procedimiento que permite transformar un texto claro en texto cifrado y viceversa.
- **Clave o llave**: Información necesaria para cifrar y/o descifrar un mensaje.
- **Alfabeto**: Colección de símbolos utilizados para escribir el texto, ya sea el texto claro o el criptotexto. El alfabeto del texto claro puede ser diferente al usado en el criptotexto pero generalmente es el mismo.

Conceptos

- **Mensaje**: Colección de texto.
- **Texto claro**: Es el texto original del mensaje y que se busca cifrar.
- **Criptotexto o texto cifrado**: Texto resultante de cifrar el texto claro.
- **Cifrar/descifrar**: Procedimiento que permite transformar un texto claro en texto cifrado y viceversa.
- **Clave o llave**: Información necesaria para cifrar y/o descifrar un mensaje.
- **Alfabeto**: Colección de símbolos utilizados para escribir el texto, ya sea el texto claro o el criptotexto. El alfabeto del texto claro puede ser diferente al usado en el criptotexto pero generalmente es el mismo.

Conceptos

- **Mensaje**: Colección de texto.
- **Texto claro**: Es el texto original del mensaje y que se busca cifrar.
- **Criptotexto o texto cifrado**: Texto resultante de cifrar el texto claro.
- **Cifrar/descifrar**: Procedimiento que permite transformar un texto claro en texto cifrado y viceversa.
- **Clave o llave**: Información necesaria para cifrar y/o descifrar un mensaje.
- **Alfabeto**: Colección de símbolos utilizados para escribir el texto, ya sea el texto claro o el criptotexto. El alfabeto del texto claro puede ser diferente al usado en el criptotexto pero generalmente es el mismo.

Conceptos

- **Mensaje**: Colección de texto.
- **Texto claro**: Es el texto original del mensaje y que se busca cifrar.
- **Criptotexto o texto cifrado**: Texto resultante de cifrar el texto claro.
- **Cifrar/descifrar**: Procedimiento que permite transformar un texto claro en texto cifrado y viceversa.
- **Clave o llave**: Información necesaria para cifrar y/o descifrar un mensaje.
- **Alfabeto**: Colección de símbolos utilizados para escribir el texto, ya sea el texto claro o el criptotexto. El alfabeto del texto claro puede ser diferente al usado en el criptotexto pero generalmente es el mismo.

Conceptos

- **Mensaje**: Colección de texto.
- **Texto claro**: Es el texto original del mensaje y que se busca cifrar.
- **Criptotexto o texto cifrado**: Texto resultante de cifrar el texto claro.
- **Cifrar/descifrar**: Procedimiento que permite transformar un texto claro en texto cifrado y viceversa.
- **Clave o llave**: Información necesaria para cifrar y/o descifrar un mensaje.
- **Alfabeto**: Colección de símbolos utilizados para escribir el texto, ya sea el texto claro o el criptotexto. El alfabeto del texto claro puede ser diferente al usado en el criptotexto pero generalmente es el mismo.

Conceptos

- **Mensaje**: Colección de texto.
- **Texto claro**: Es el texto original del mensaje y que se busca cifrar.
- **Criptotexto o texto cifrado**: Texto resultante de cifrar el texto claro.
- **Cifrar/descifrar**: Procedimiento que permite transformar un texto claro en texto cifrado y viceversa.
- **Clave o llave**: Información necesaria para cifrar y/o descifrar un mensaje.
- **Alfabeto**: Colección de símbolos utilizados para escribir el texto, ya sea el texto claro o el criptotexto. El alfabeto del texto claro puede ser diferente al usado en el criptotexto pero generalmente es el mismo.

Antecedentes

- El `cifrado` de texto ha sido ampliamente usado a lo largo de la historia humana.
- Principalmente en el ámbito militar;
- y en aquéllos en los que es necesario enviar mensajes con información confidencial a través de medios no seguros.

Antecedentes

- El `cifrado` de texto ha sido ampliamente usado a lo largo de la historia humana.
- Principalmente en el ámbito militar;
- y en aquéllos en los que es necesario enviar mensajes con información confidencial a través de medios no seguros.

Antecedentes

- El `cifrado` de texto ha sido ampliamente usado a lo largo de la historia humana.
- Principalmente en el ámbito militar;
- y en aquéllos en los que es necesario enviar mensajes con información confidencial a través de medios no seguros.

Antecedentes

Criptografía clásica

- Sistema criptográfico más antiguo conocido se debe a `Julio César`.

Antecedentes

Criptografía clásica

A	B	C	D	E	F	...	X	Y	Z
D	E	F	G	H	I	...	A	B	C

Texto claro ≪CRIPTOGRAFIA VISUAL≫

Texto cifrado ≪FULSWRJUDILD SLVXDO≫

Antecedentes

Criptografía clásica

A	B	C	D	E	F	...	X	Y	Z
D	E	F	G	H	I	...	A	B	C

Texto claro ≪CRIPTOGRAFIA VISUAL≫

Texto cifrado ≪FULSWRJUDILD SLVXDO≫

Antecedentes

Criptografía clásica

A	B	C	D	E	F	...	X	Y	Z
D	E	F	G	H	I	...	A	B	C

Texto claro ≪CRIPTOGRAFIA VISUAL≫

Texto cifrado ≪FULSWRJUDILD SLVXDO≫

Antecedentes

Criptografía Moderna

- AES

Figure: AES

Antecedentes

Criptografía Moderna

- RSA

Figure: Adi Shamir

Criptografía Visual

Criptografía			Criptografía Visual
Mensaje	$\leftrightarrow$	Imagen	Formada por pixeles
Texto claro	$\leftrightarrow$	Imagen clara	Contenido de la imagen a cifrar
Texto cifrado	$\leftrightarrow$	Imagen cifrada	Imagen resultante de cifrar la imagen clara
Alfabeto	$\leftrightarrow$	Pixeles	Generalmente serán claros y negros

Criptografía Visual

Criptografía			Criptografía Visual
Mensaje	$\leftrightarrow$	Imagen	Formada por pixeles
Texto claro	$\leftrightarrow$	Imagen clara	Contenido de la imagen a cifrar
Texto cifrado	$\leftrightarrow$	Imagen cifrada	Imagen resultante de cifrar la imagen clara
Alfabeto	$\leftrightarrow$	Pixeles	Generalmente serán claros y negros

Criptografía Visual

Criptografía			Criptografía Visual
Mensaje	$\leftrightarrow$	Imagen	Formada por pixeles
Texto claro	$\leftrightarrow$	Imagen clara	Contenido de la imagen a cifrar
Texto cifrado	$\leftrightarrow$	Imagen cifrada	Imagen resultante de cifrar la imagen clara
Alfabeto	$\leftrightarrow$	Pixeles	Generalmente serán claros y negros

Criptografía Visual

Criptografía			Criptografía Visual
Mensaje	$\leftrightarrow$	Imagen	Formada por pixeles
Texto claro	$\leftrightarrow$	Imagen clara	Contenido de la imagen a cifrar
Texto cifrado	$\leftrightarrow$	Imagen cifrada	Imagen resultante de cifrar la imagen clara
Alfabeto	$\leftrightarrow$	Pixeles	Generalmente serán claros y negros

Criptografía Visual

Criptografía			Criptografía Visual
Mensaje	$\leftrightarrow$	Imagen	Formada por pixeles
Texto claro	$\leftrightarrow$	Imagen clara	Contenido de la imagen a cifrar
Texto cifrado	$\leftrightarrow$	Imagen cifrada	Imagen resultante de cifrar la imagen clara
Alfabeto	$\leftrightarrow$	Pixeles	Generalmente serán claros y negros

Criptografía Visual

¿Qué es la criptografía visual?

- Técnica de encriptación especial para ocultar información en imágenes.
- Puede ser desencriptada por la visión humana si se usa la imagen clave correcta.
- Utiliza dos imágenes transparentes.

Criptografía Visual

¿Qué es la criptografía visual?

- `Técnica de encriptación` especial para ocultar información en imágenes.
- Puede ser desencriptada por la visión humana si se usa la imagen clave correcta.
- Utiliza dos imágenes transparentes.

Criptografía Visual

¿Qué es la criptografía visual?

- `Técnica de encriptación` especial para ocultar información en imágenes.
- Puede ser desencriptada por la visión humana si se usa la imagen clave correcta.
- Utiliza dos imágenes transparentes.

Criptografía Visual

¿Qué es la criptografía visual?

- `Técnica de encriptación` especial para ocultar información en imágenes.
- Puede ser desencriptada por la visión humana si se usa la imagen clave correcta.
- Utiliza dos imágenes transparentes.

Criptografía Visual

¿Qué es la criptografía visual?

- Una imagen contiene píxeles aleatorios y la otra imagen contiene la información secreta.
- Es imposible recuperar la información secreta de una de las imágenes.
- Se requieren tanto imágenes transparentes como capas para revelar la información.

Criptografía Visual

¿Qué es la criptografía visual?

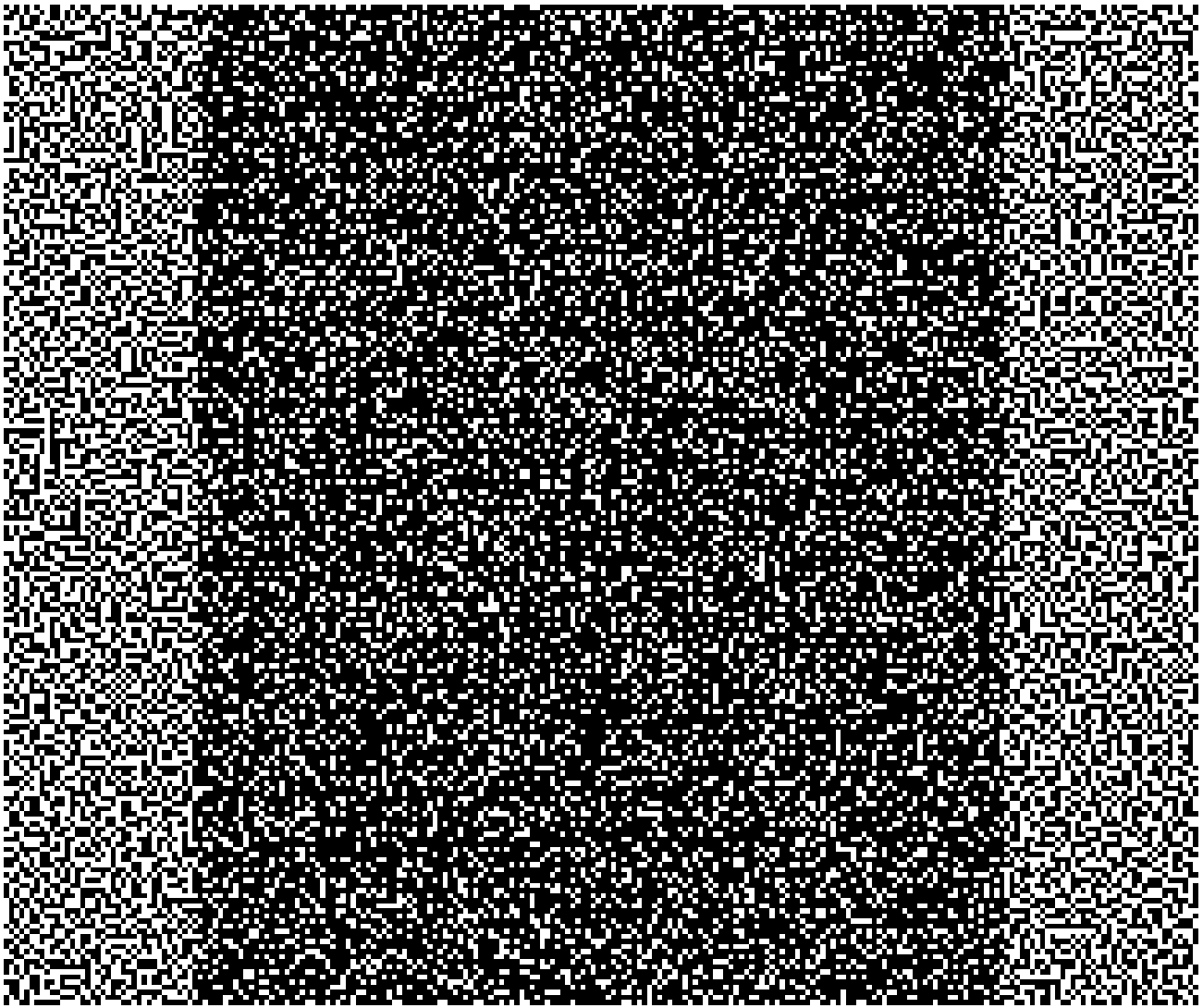
- Una imagen contiene píxeles aleatorios y la otra imagen contiene la información secreta.
- Es imposible recuperar la información secreta de una de las imágenes.
- Se requieren tanto imágenes transparentes como capas para revelar la información.

Criptografía Visual

¿Qué es la criptografía visual?

- Una imagen contiene píxeles aleatorios y la otra imagen contiene la información secreta.
- Es imposible recuperar la información secreta de una de las imágenes.
- Se requieren tanto imágenes transparentes como capas para revelar la información.

Criptografía Visual



Criptografía Visual

Compartición de secretos

Compartición de secretos

Nuestro objetivo es dividir un conjunto de datos D (por ejemplo, una clave) en n partes $D_1, ..., D_n$ de manera que:

- El conocimiento de k o más D_i partes hace que D sea fácilmente computable.
- El conocimiento de $k-1$ o menos D_i partes hace que D esté indeterminado, en el sentido de que todos sus valores posibles tienen la misma probabilidad de ser verdaderos.

Criptografía Visual

Compartición de secretos

Compartición de secretos

Nuestro objetivo es dividir un conjunto de datos D (por ejemplo, una clave) en n partes $D_1, ..., D_n$ de manera que:

- El conocimiento de k o más D_i partes hace que D sea fácilmente computable.
- El conocimiento de $k-1$ o menos D_i partes hace que D esté indeterminado, en el sentido de que todos sus valores posibles tienen la misma probabilidad de ser verdaderos.

Criptografía Visual

Compartición de secretos

Compartición de secretos

Nuestro objetivo es dividir un conjunto de datos D (por ejemplo, una clave) en n partes $D_1, ..., D_n$ de manera que:

- El conocimiento de k o más D_i partes hace que D sea fácilmente computable.
- El conocimiento de $k-1$ o menos D_i partes hace que D esté indeterminado, en el sentido de que todos sus valores posibles tienen la misma probabilidad de ser verdaderos.

Criptografía Visual

Compartición de secretos

Compartición de secretos

Esta combinación se denomina combinación o esquema de umbral (k, n)

Si $k = n$ se requiere la concurrencia de todos los participantes para reconstruir el secreto.

Algoritmo

Esquema umbral 2 de 2

Esquema umbral 2 de 2

Se tiene el conjunto de elementos $\{0, 1\}$, forman un campo con las operaciones módulo 2.

$$0 + 0 = 0$$

$$0 + 1 = 1$$

$$1 + 0 = 1$$

$$1 + 1 = 0$$

Algoritmo

Esquema umbral 2 de 2

`Biyección`

- Negro $= 1$
- Blanco $= 0$

Algoritmo

Esquema umbral 2 de 2 (Caso particular)

Construimos dos matrices cuadradas S_1 y S_2 de tamaño mxm.

Construimos y dibujamos nuestro secreto sobre una matriz temporal S_{temp} de tamaño mxm.

Algoritmo

Esquema umbral 2 de 2 (Caso particular)

Construimos dos matrices cuadradas S_1 y S_2 de tamaño mxm.
Construimos y dibujamos nuestro secreto sobre una matriz temporal S_{temp} de tamaño mxm.

Algoritmo

Esquema umbral 2 de 2 (Caso particular)

`Cifrando el mensaje`

- Si $S_{temp}[i][j]$ es negro, pintamos cada cuadro de S_1 de manera aleatoria. S_2 es identico a S_1 tal que $S_1[i][j] \oplus S_2[i][j] = 1$
- Si $S_{temp}[i][j]$ es blanco, S_1 y S_2 se pintan de forma aleatoria tal que $S_1[i][j] = S_2[i][j]$

División de pixeles

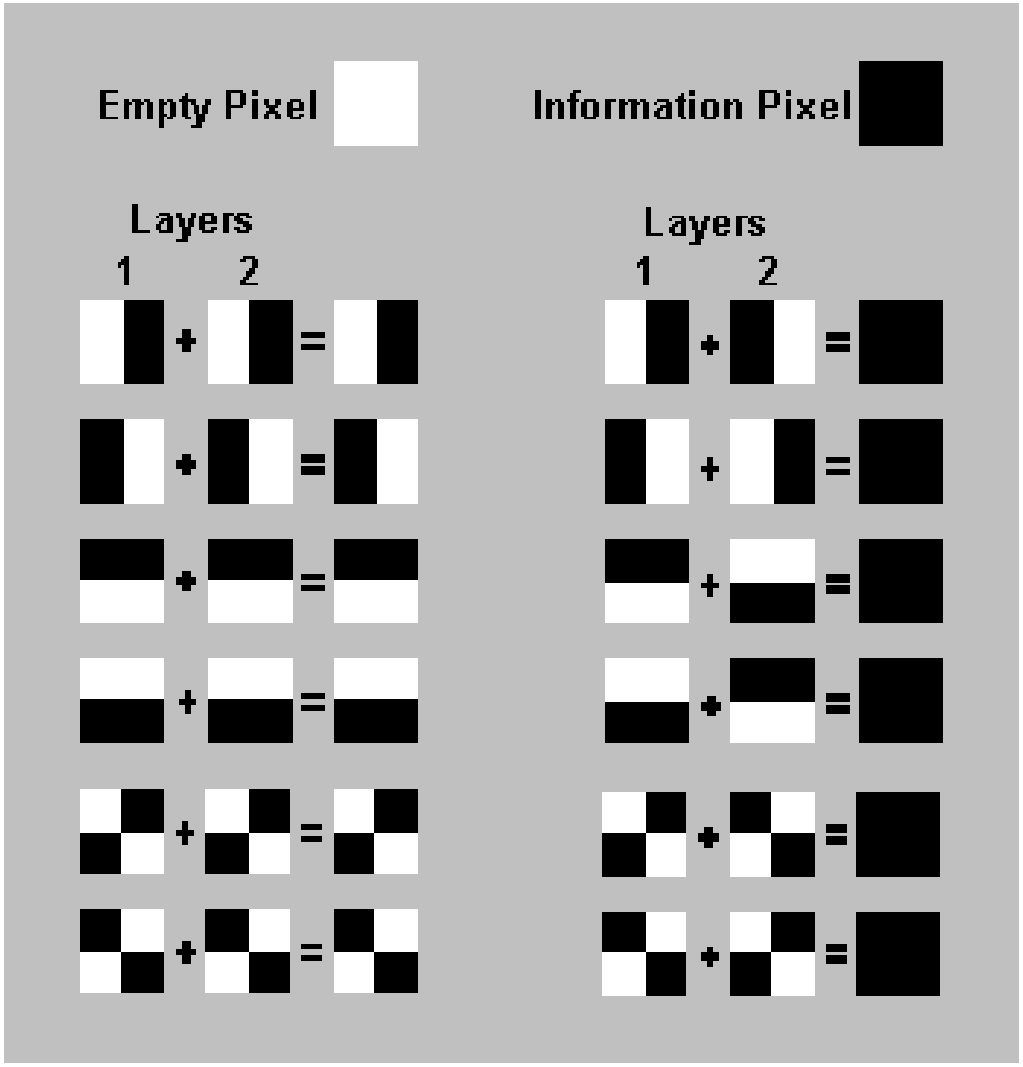


Figure: División de pixeles

Ejecución del programa

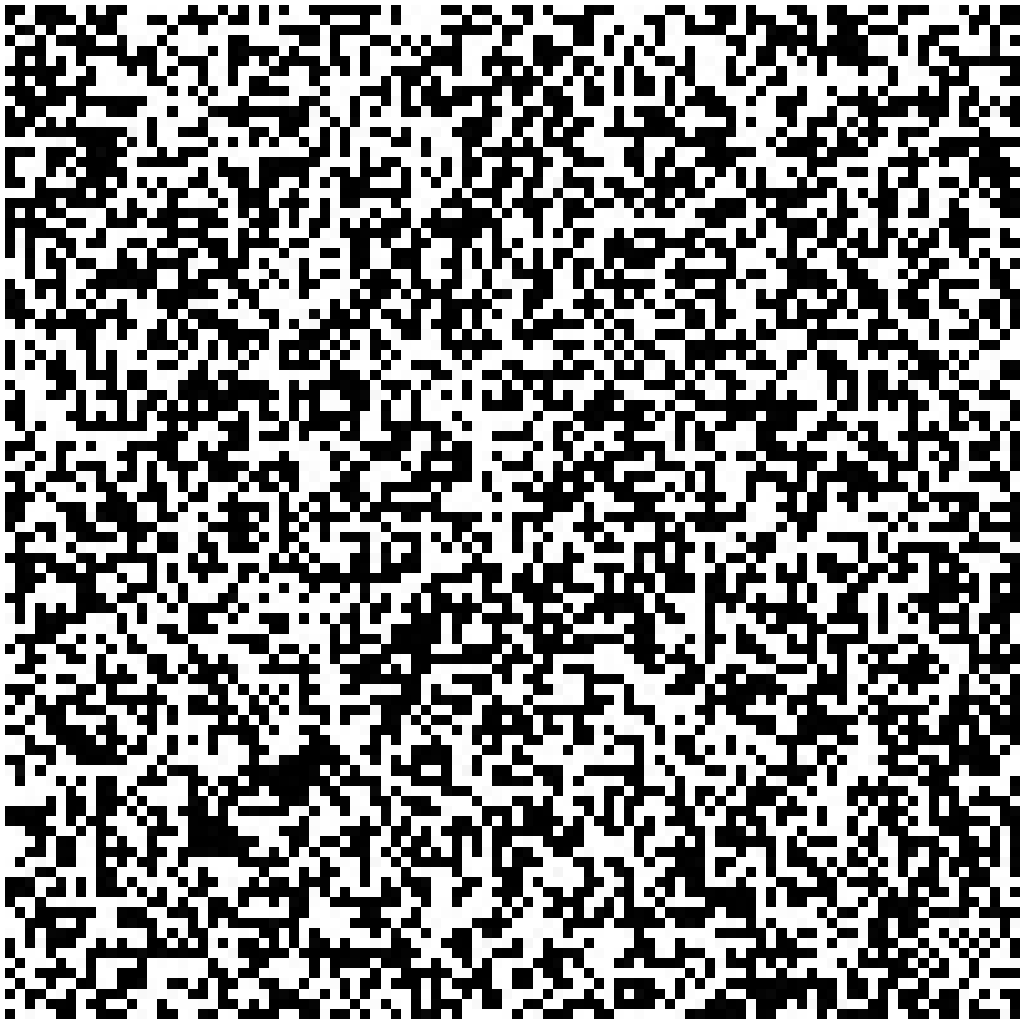


Figure: S_1

Ejecución del programa

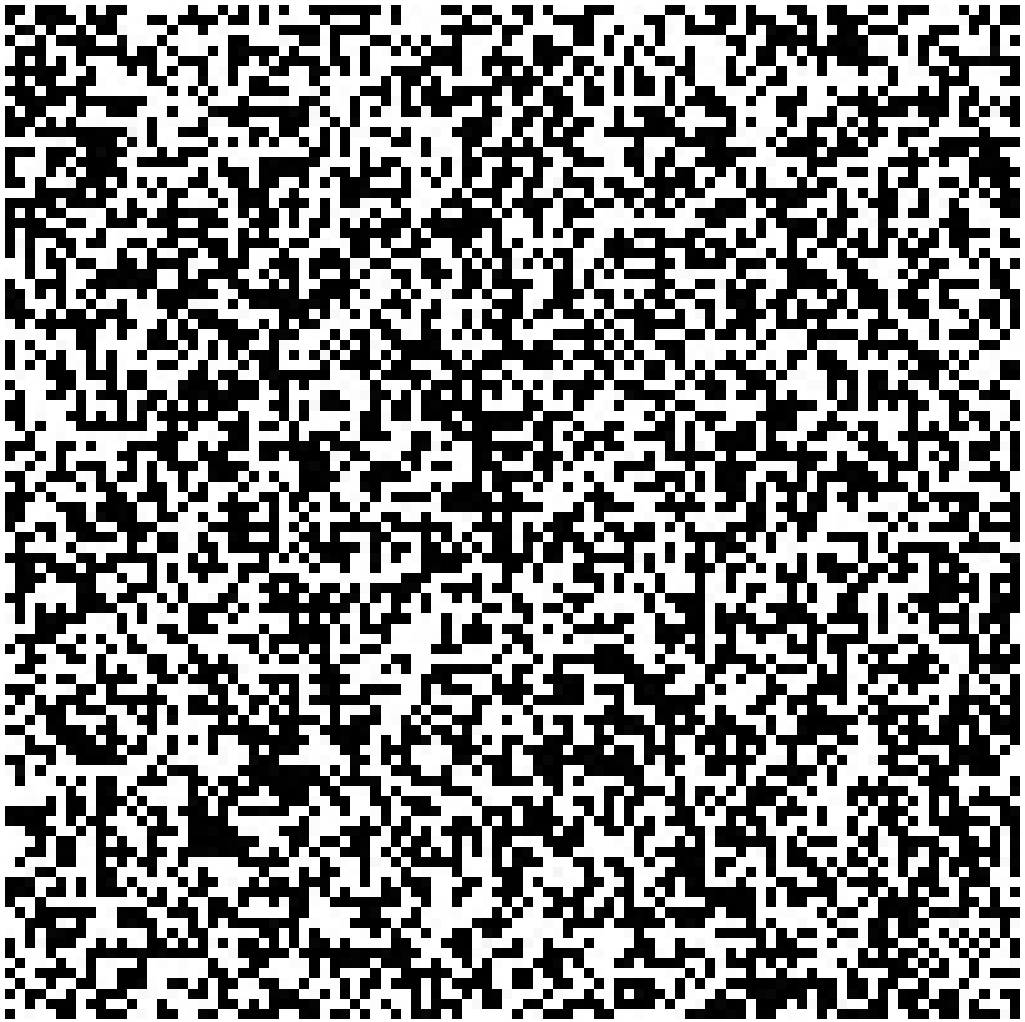


Figure: S_2

Ejecución del programa

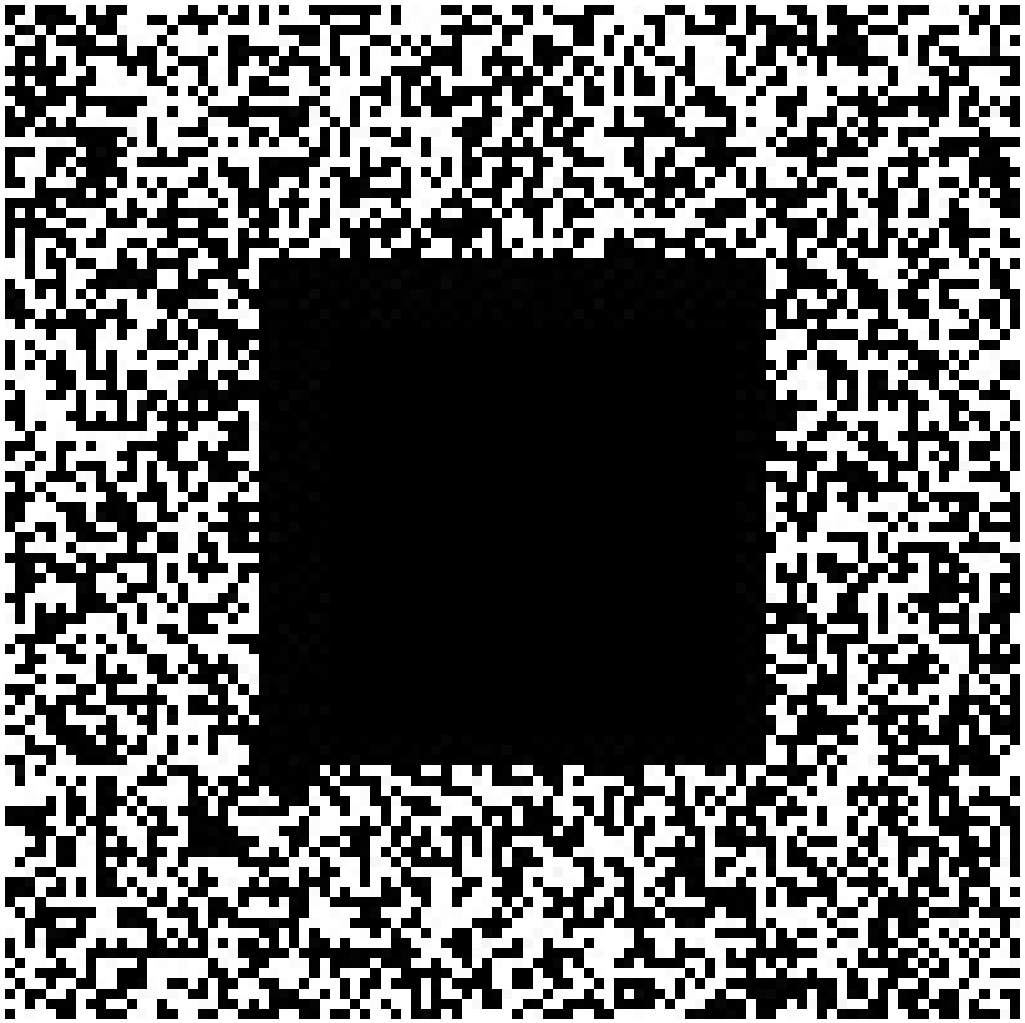


Figure: *Mensaje*