# नमस्ते

## வணக்கம்

Greetings

# नमस्ते

## வணக்கம்

## Greetings

Arunesh Gour

22MCI0005

Shailesh Goswami

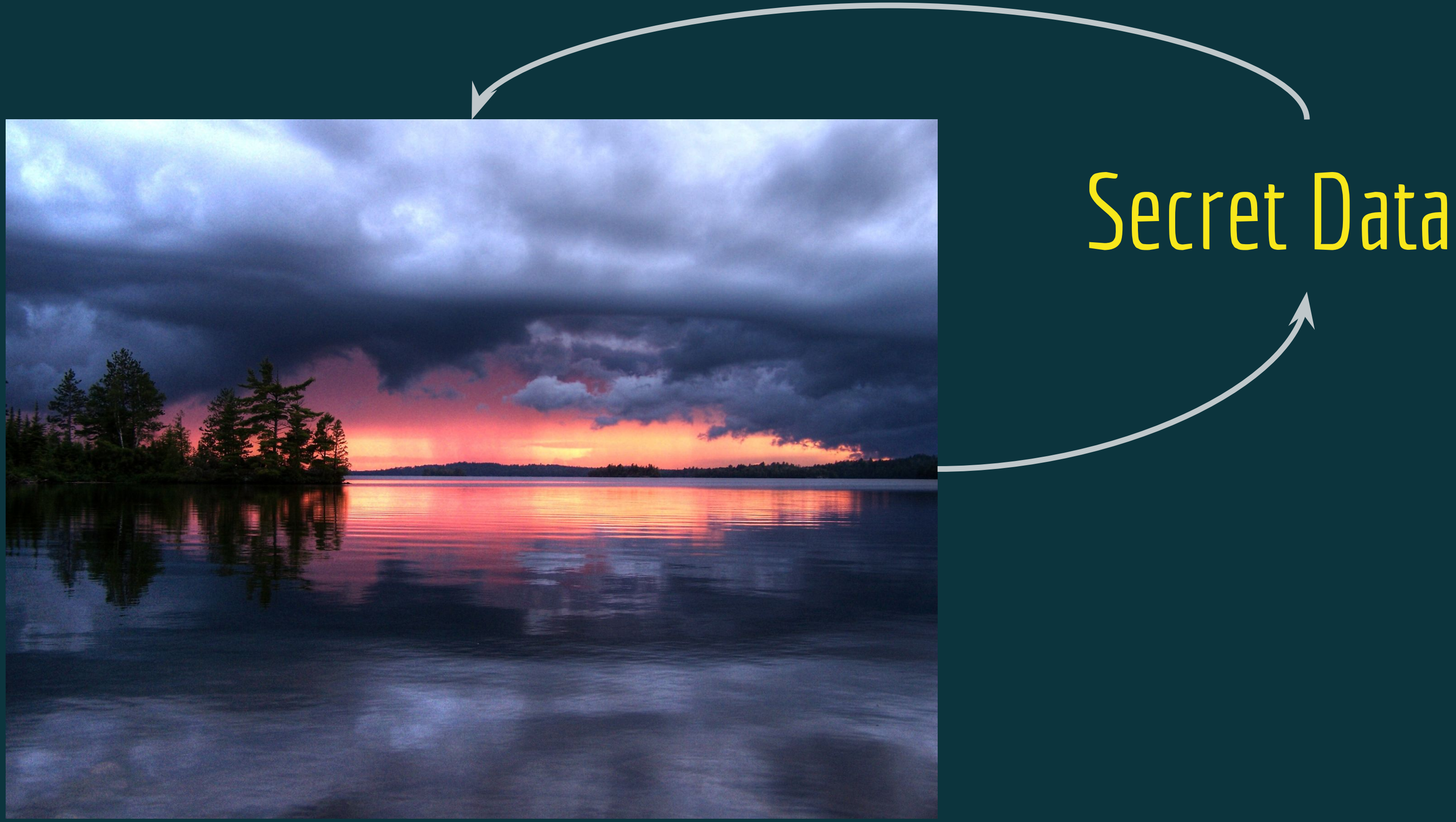
22MCI0007

# Information Security Domain

Steganography

# Steganography:
Reversible Data Hiding

# Steganography



Secret Data

# Secret Data

# Secret_Data

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| S | e | c | r | e | t | _ | D | a | t | a |
| 83 | 101 | 99 | 114 | 101 | 116 | 32 | 68 | 97 | 116 | 97 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ___ | ___ | ___ | ___ | ___ | ___ | ___ | ___ |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

S

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

S

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 83 |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | |

R

G

B

G

0

255

0

255

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ___ | ___ | ___ | ___ | ___ | ___ | ___ | ___ | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | 255 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | |

|  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 255 |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |  |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ___ | ___ | ___ | ___ | ___ | ___ | ___ | ___ |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

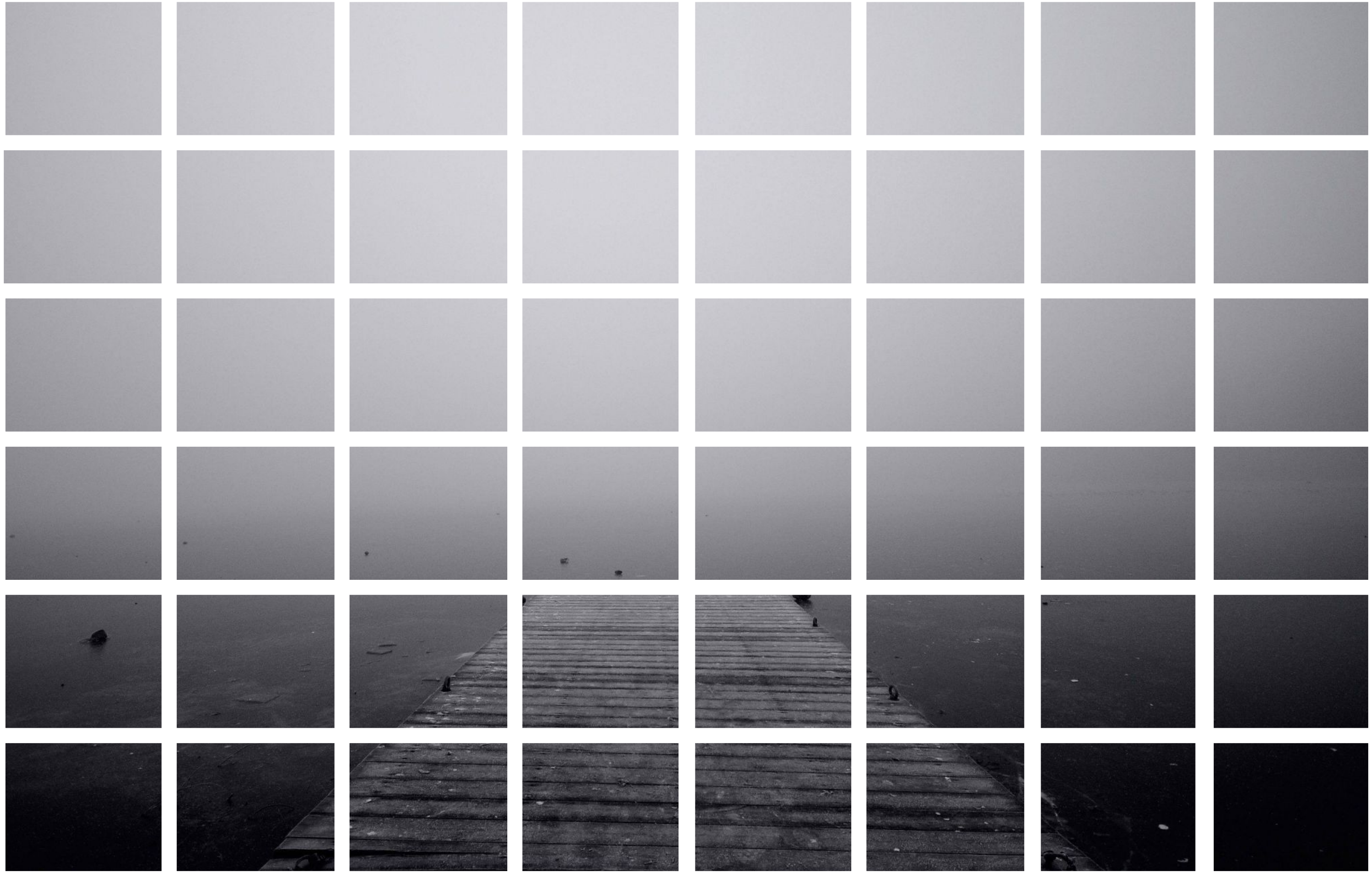
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| _ | _ | _ | _ | _ | _ | X | X |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| _ | _ | _ | _ | X | X | X | X |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

# APDH

## Adjacency Pixel Difference Histogram

X



| | | | | | |
|---|---|---|---|---|---|
| 208 | 209 | 85 | 86 | 183 | 183 |
| 208 | 209 | 86 | 86 | 180 | 180 |
| 187 | 186 | 95 | 98 | 232 | 230 |
| 189 | 186 | 93 | 95 | 230 | 230 |
| 235 | 239 | 127 | 123 | 149 | 144 |
| 239 | 235 | 122 | 124 | 154 | 148 |

2

2

| | | | | | |
|---|---|---|---|---|---|
| 208 | 209 | 85 | 86 | 183 | 183 |
| 208 | 209 | 86 | 86 | 180 | 180 |
| 187 | 186 | 95 | 98 | 232 | 230 |
| 189 | 186 | 93 | 95 | 230 | 230 |
| 235 | 239 | 127 | 123 | 149 | 144 |
| 239 | 235 | 122 | 124 | 154 | 148 |

2

2

| | |
|---|---|
| 208 | 209 |
| 208 | 209 |

| | |
|---|---|
| 85 | 86 |
| 86 | 86 |

| | |
|---|---|
| 183 | 183 |
| 180 | 180 |

| | |
|---|---|
| 187 | 186 |
| 189 | 186 |

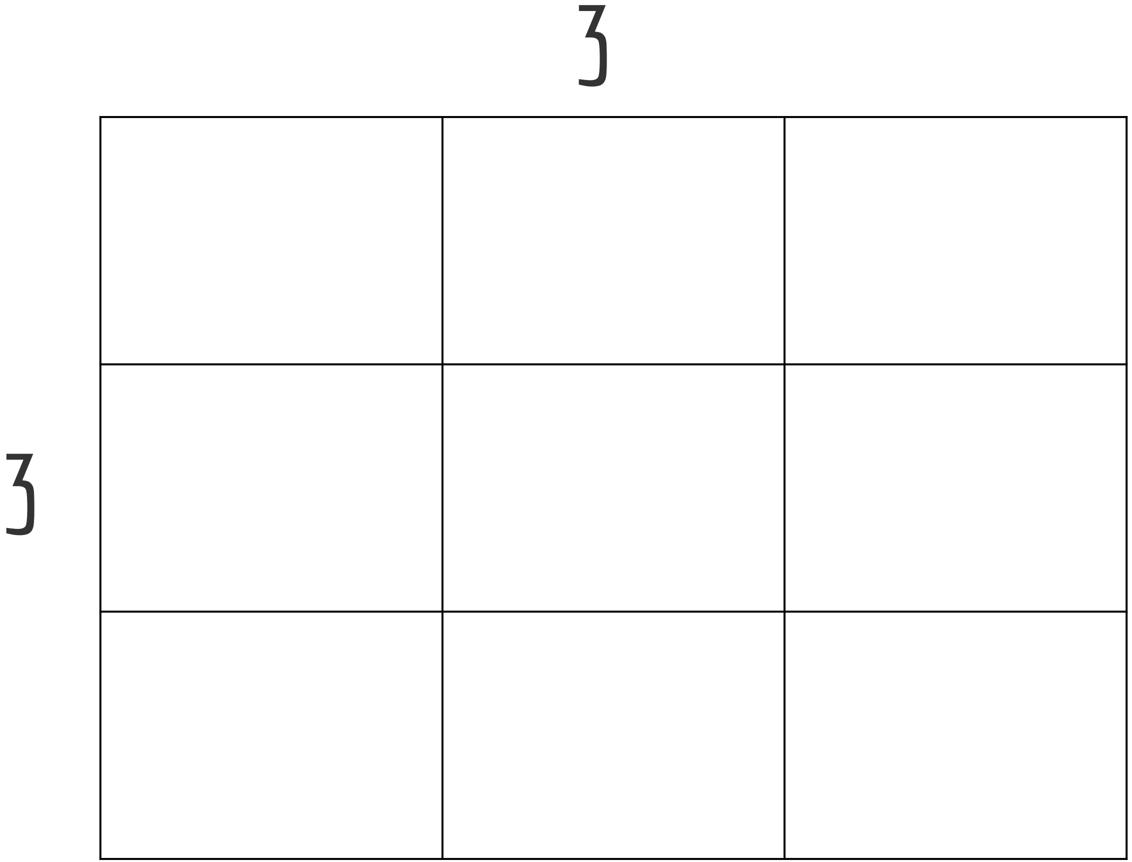
| | |
|---|---|
| 95 | 98 |
| 93 | 95 |

| | |
|---|---|
| 232 | 230 |
| 230 | 230 |

| | |
|---|---|
| 235 | 239 |
| 239 | 235 |

| | |
|---|---|
| 127 | 123 |
| 122 | 124 |

| | |
|---|---|
| 149 | 144 |
| 154 | 148 |


3
3

| | | | | | |
|---|---|---|---|---|---|
| 208 | 209 | 85 | 86 | 183 | 183 |
| 208 | 209 | 86 | 86 | 180 | 180 |
| 187 | 186 | 95 | 98 | 232 | 230 |
| 189 | 186 | 93 | 95 | 230 | 230 |
| 235 | 239 | 127 | 123 | 149 | 144 |
| 239 | 235 | 122 | 124 | 154 | 148 |

|  |  |
|---|---|
| 208 | 209 |
| 208 | 209 |

|  |  |
|---|---|
| 85 | 86 |
| 86 | 86 |

|  |  |
|---|---|
| 183 | 183 |
| 180 | 180 |

|  |  |
|---|---|
| 187 | 186 |
| 189 | 186 |

|  |  |
|---|---|
| 95 | 98 |
| 93 | 95 |

|  |  |
|---|---|
| 232 | 230 |
| 230 | 230 |

|  |  |
|---|---|
| 235 | 239 |
| 239 | 235 |

|  |  |
|---|---|
| 127 | 123 |
| 122 | 124 |

|  |  |
|---|---|
| 149 | 144 |
| 154 | 148 |

132

| | |
|---|---|
| 208 | 209 |
| 208 | 209 |

| | |
|---|---|
| 85 | 86 |
| 86 | 86 |

| | |
|---|---|
| 183 | 183 |
| 180 | 180 |

| | |
|---|---|
| 187 | 186 |
| 189 | 186 |

| | |
|---|---|
| 95 | 98 |
| 93 | 95 |

| | |
|---|---|
| 232 | 230 |
| 230 | 230 |

| | |
|---|---|
| 235 | 239 |
| 239 | 235 |

| | |
|---|---|
| 127 | 123 |
| 122 | 124 |

| | |
|---|---|
| 149 | 144 |
| 154 | 148 |

# 255

| | | | | | |
|---|---|---|---|---|---|
| 208 | 209 | 85 | 86 | 183 | 183 |
| 208 | 209 | 86 | 86 | 180 | 180 |
| 187 | 186 | 95 | 98 | 232 | 230 |
| 189 | 186 | 93 | 95 | 230 | 230 |
| 235 | 239 | 127 | 123 | 149 | 144 |
| 239 | 235 | 122 | 124 | 154 | 148 |

179

| | | | | | |
|---|---|---|---|---|---|
| 208 | 209 | 85 | 86 | 183 | 183 |
| 208 | 209 | 86 | 86 | 180 | 180 |
| 187 | 186 | 95 | 98 | 232 | 230 |
| 189 | 186 | 93 | 95 | 230 | 230 |
| 235 | 239 | 127 | 123 | 149 | 144 |
| 239 | 235 | 122 | 124 | 154 | 148 |

| | | |
|---|---|---|
| 132 | 255 | 179 |
| 155 | 5 | 128 |
| 111 | 222 | 186 |

| | |
|---|---|
| 132 | 132 |
| 132 | 132 |

| | |
|---|---|
| 255 | 255 |
| 255 | 255 |

| | |
|---|---|
| 179 | 179 |
| 179 | 179 |

| | |
|---|---|
| 155 | 155 |
| 155 | 155 |

| | |
|---|---|
| 5 | 5 |
| 5 | 5 |

| | |
|---|---|
| 128 | 128 |
| 128 | 128 |

| | |
|---|---|
| 111 | 111 |
| 111 | 111 |

| | |
|---|---|
| 222 | 222 |
| 222 | 222 |

| | |
|---|---|
| 186 | 186 |
| 186 | 186 |

○ Blocks

- ○ Blocks
- ○ Random Set

- Blocks
- Random Set
- Cryptographic Key

○ Image Encryption
○ Secret Embedding

## APDH

- Image Encryption

APDH

| | |
|---|---|
| 208 | 209 |
| 208 | 209 |

| | |
|---|---|
| 85 | 86 |
| 86 | 86 |

| | |
|---|---|
| 183 | 183 |
| 180 | 180 |

| | |
|---|---|
| 187 | 186 |
| 189 | 186 |

| | |
|---|---|
| 95 | 98 |
| 93 | 95 |

| | |
|---|---|
| 232 | 230 |
| 230 | 230 |

| | |
|---|---|
| 235 | 239 |
| 239 | 235 |

| | |
|---|---|
| 127 | 123 |
| 122 | 124 |

| | |
|---|---|
| 149 | 144 |
| 154 | 148 |

| | | | | | |
|---|---|---|---|---|---|
| 208 | 209 | 85 | 86 | 183 | 183 |
| 208 | 209 | 86 | 86 | 180 | 180 |
| 187 | 186 | 95 | 98 | 232 | 230 |
| 189 | 186 | 93 | 95 | 230 | 230 |
| 235 | 239 | 127 | 123 | 149 | 144 |
| 239 | 235 | 122 | 124 | 154 | 148 |

| | |
|---|---|
| 208 | 209 |
| 208 | 209 |

| | |
|---|---|
| 132 | 132 |
| 132 | 132 |

| | |
|---|---|
| 255 | 255 |
| 255 | 255 |

| | |
|---|---|
| 179 | 179 |
| 179 | 179 |

| | |
|---|---|
| 155 | 155 |
| 155 | 155 |

| | |
|---|---|
| 5 | 5 |
| 5 | 5 |

| | |
|---|---|
| 128 | 128 |
| 128 | 128 |

| | |
|---|---|
| 111 | 111 |
| 111 | 111 |

| | |
|---|---|
| 222 | 222 |
| 222 | 222 |

| | |
|---|---|
| 186 | 186 |
| 186 | 186 |

| | |
|---|---|
| 132 | 132 |
| 132 | 132 |

| | |
|---|---|
| 255 | 255 |
| 255 | 255 |

| | |
|---|---|
| 179 | 179 |
| 179 | 179 |

| | |
|---|---|
| 155 | 155 |
| 155 | 155 |

| | |
|---|---|
| 5 | 5 |
| 5 | 5 |

| | |
|---|---|
| 128 | 128 |
| 128 | 128 |

| | |
|---|---|
| 111 | 111 |
| 111 | 111 |

| | |
|---|---|
| 222 | 222 |
| 222 | 222 |

| | |
|---|---|
| 186 | 186 |
| 186 | 186 |

| | |
|---|---|
| 208 | 209 |
| 208 | 209 |

Image Block

| | |
|---|---|
| 132 | 132 |
| 132 | 132 |

Random Block

| | |
|---|---|
| 208 | 209 |
| 208 | 209 |

+

| | |
|---|---|
| 176 | 176 |
| 176 | 176 |

Cryptographic
Key

# Operation 1

uint8

|  |  |
|---|---|
| 128 | 128 |
| 128 | 128 |

# Operation 1

uint8

| | |
|---|---|
| 132 | 132 |
| 132 | 132 |

+

| | |
|---|---|
| 176 | 176 |
| 176 | 176 |

Cryptographic Key

Operation 2

uint8

|  |  |
|---|---|
| 52 | 52 |
| 52 | 52 |

# Operation 2

uint8

| | |
|---|---|
| 128 | 128 |
| 128 | 128 |

+

| | |
|---|---|
| 52 | 52 |
| 52 | 52 |

uint8

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

uint8

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 85 | 86 |
| 86 | 86 |

| | |
|---|---|
| 183 | 183 |
| 180 | 180 |

| | |
|---|---|
| 187 | 186 |
| 189 | 186 |

| | |
|---|---|
| 95 | 98 |
| 93 | 95 |

| | |
|---|---|
| 232 | 230 |
| 230 | 230 |

| | |
|---|---|
| 235 | 239 |
| 239 | 235 |

| | |
|---|---|
| 127 | 123 |
| 122 | 124 |

| | |
|---|---|
| 149 | 144 |
| 154 | 148 |

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 183 | 183 |
| 180 | 180 |

| | |
|---|---|
| 187 | 186 |
| 189 | 186 |

| | |
|---|---|
| 95 | 98 |
| 93 | 95 |

| | |
|---|---|
| 232 | 230 |
| 230 | 230 |

| | |
|---|---|
| 235 | 239 |
| 239 | 235 |

| | |
|---|---|
| 127 | 123 |
| 122 | 124 |

| | |
|---|---|
| 149 | 144 |
| 154 | 148 |

| | | | | | |
|---|---|---|---|---|---|
| 180 | 181 | 180 | 181 | 202 | 202 |
| 180 | 181 | 181 | 181 | 199 | 199 |
| 187 | 186 | 95 | 98 | 232 | 230 |
| 189 | 186 | 93 | 95 | 230 | 230 |
| 235 | 239 | 127 | 123 | 149 | 144 |
| 239 | 235 | 122 | 124 | 154 | 148 |

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 199 | 199 |

| | |
|---|---|
| 187 | 186 |
| 189 | 186 |

| | |
|---|---|
| 95 | 98 |
| 93 | 95 |

| | |
|---|---|
| 232 | 230 |
| 230 | 230 |

| | |
|---|---|
| 235 | 239 |
| 239 | 235 |

| | |
|---|---|
| 127 | 123 |
| 122 | 124 |

| | |
|---|---|
| 149 | 144 |
| 154 | 148 |

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 199 | 199 |

| | |
|---|---|
| 182 | 181 |
| 184 | 181 |

| | |
|---|---|
| 196 | 199 |
| 194 | 196 |

| | |
|---|---|
| 200 | 198 |
| 198 | 198 |

| | |
|---|---|
| 186 | 190 |
| 190 | 186 |

| | |
|---|---|
| 189 | 185 |
| 184 | 186 |

| | |
|---|---|
| 175 | 170 |
| 180 | 174 |

- Image Encryption

APDH

○ Secret Embedding

APDH

# Difference Histograms

○ D1

○ D2

○ D3

| | |
|---|---|
| ○ D1 | T1 |
| ○ D2 | T2 |
| ○ D3 | T3 |

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 199 | 199 |

| | |
|---|---|
| 182 | 181 |
| 184 | 181 |

| | |
|---|---|
| 196 | 199 |
| 194 | 196 |

| | |
|---|---|
| 200 | 198 |
| 198 | 198 |

| | |
|---|---|
| 186 | 190 |
| 190 | 186 |

| | |
|---|---|
| 189 | 185 |
| 184 | 186 |

| | |
|---|---|
| 175 | 170 |
| 180 | 174 |

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 199 | 199 |

| | |
|---|---|
| 182 | 181 |
| 184 | 181 |

| | |
|---|---|
| 196 | 199 |
| 194 | 196 |

| | |
|---|---|
| 200 | 198 |
| 198 | 198 |

| | |
|---|---|
| 186 | 190 |
| 190 | 186 |

| | |
|---|---|
| 189 | 185 |
| 184 | 186 |

| | |
|---|---|
| 175 | 170 |
| 180 | 174 |

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

|  |  |
|---|---|
| 1 | 2 |
| 3 | 4 |

|  |  |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 1 | 2 |
| 3 | 4 |

D1 = abs ( 1 - 3 )

| | |
|---|---|
| 1 | 2 |
| 3 | 4 |

D2 = abs ( 2 - 4 )

| | |
|---|---|
| 1 | 2 |
| 3 | 4 |

$$D3 = \mathrm{abs}\ (\ 1 - 2\ )$$

| | |
|---|---|
| 1 | 2 |
| 3 | 4 |

D1 = abs ( 1 - 3 )

D2 = abs ( 2 - 4 )

D3 = abs ( 1 - 2 )

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 199 | 199 |

| | |
|---|---|
| 182 | 181 |
| 184 | 181 |

| | |
|---|---|
| 196 | 199 |
| 194 | 196 |

| | |
|---|---|
| 200 | 198 |
| 198 | 198 |

| | |
|---|---|
| 186 | 190 |
| 190 | 186 |

| | |
|---|---|
| 189 | 185 |
| 184 | 186 |

| | |
|---|---|
| 175 | 170 |
| 180 | 174 |

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

D1 = abs (180 - 180) = 0

D2 = abs (181 - 181) = 0

D3 = abs (180 - 181) = 1

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 199 | 199 |

| | |
|---|---|
| 182 | 181 |
| 184 | 181 |

| | |
|---|---|
| 196 | 199 |
| 194 | 196 |

| | |
|---|---|
| 200 | 198 |
| 198 | 198 |

| | |
|---|---|
| 186 | 190 |
| 190 | 186 |

| | |
|---|---|
| 189 | 185 |
| 184 | 186 |

| | |
|---|---|
| 175 | 170 |
| 180 | 174 |

| | | |
|---|---|---|
| 0 | 1 | 3 |
| 2 | 2 | 2 |
| 4 | 5 | 5 |

D1

D1

| | | |
|---|---|---|
| 0 | 1 | 3 |
| 2 | 2 | 2 |
| 4 | 5 | 5 |

T1 = 2

| | | |
|---|---|---|
| 0 | 0 | 3 |
| 0 | 3 | 0 |
| 4 | 1 | 4 |

D2

| | | |
|---|---|---|
| 0 | 0 | 3 |
| 0 | 3 | 0 |
| 4 | 1 | 4 |

D2

T2 = 0

|   |   |   |
|---|---|---|
| 1 | 1 | 0 |
| 1 | 3 | 2 |
| 4 | 4 | 5 |

D3

|   |   |   |
|---|---|---|
| 1 | 1 | 0 |
| 1 | 3 | 2 |
| 4 | 4 | 5 |

D3

T3 = 1

D1
T1

# Partial Data Embedding

D2
T2

## Partial Data Embedding

D3
T3

→

Partial Data
Embedding

# Partial Data

First n bits of data

n zeros (0) as padding

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 199 | 199 |

| | |
|---|---|
| 182 | 181 |
| 184 | 181 |

| | |
|---|---|
| 196 | 199 |
| 194 | 196 |

| | |
|---|---|
| 200 | 198 |
| 198 | 198 |

| | |
|---|---|
| 186 | 190 |
| 190 | 186 |

| | |
|---|---|
| 189 | 185 |
| 184 | 186 |

| | |
|---|---|
| 175 | 170 |
| 180 | 174 |

# Loop over all blocks

| | |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
Loop over all blocks
    If ($D1 > T1$)
        Histogram shift
```

| | |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
If ($P1 <= P3$):
    $P3 = P3 + (2^n - 1)$

Else:
    $P3 = P3 - (2^n - 1)$
```

```
Loop over all blocks
    Else If (D1 == T1)
        Data Embedding
    End If
End Loop
```

| | |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
If (P1 <= P3):
    P3 = P3 + integer (n bits of data)

Else:
    P3 = P3 - integer (n bits of data)
```

| | |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
    End If
End Loop
```

```
Loop over all blocks
    If (D2 > T2)
        Histogram shift
```

|  |  |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
If (P2 <= P4):
    P4 = P4 + (2^n - 1)

Else:
    P4 = P4 - (2^n - 1)
```

# Data Embedding

```
Loop over all blocks
    Else If (D2 == T2)
        If (P2 <= P4):
            P4 = P4 + integer (n bits of data)
        Else:
            P4 = P4 - integer (n bits of data)
    End If
End Loop
```

| | |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
Loop over all blocks
    If (D3 > T3)
        Histogram shift
```

| | |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
If (P1 <= P2):
    P2 = P2 + $(2^n - 1)$

Else:
    P2 = P2 - $(2^n - 1)$
```

# Data Embedding

```
Loop over all blocks
    Else If (D3 == T3)
        If (P1 <= P2):
            P2 = P2 + integer (n bits of data)
        Else:
            P2 = P2 - integer (n bits of data)
    End If
End Loop
```

|  |  |
|---|---|
| P1 | P2 |
| P3 | P4 |

| | |
|---|---|
| 180 | 182 |
| 180 | 184 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 196 | 196 |

| | |
|---|---|
| 182 | 178 |
| 184 | 183 |

| | |
|---|---|
| 196 | 202 |
| 193 | 193 |

| | |
|---|---|
| 200 | 195 |
| 195 | 199 |

| | |
|---|---|
| 186 | 193 |
| 193 | 183 |

| | |
|---|---|
| 189 | 182 |
| 181 | 189 |

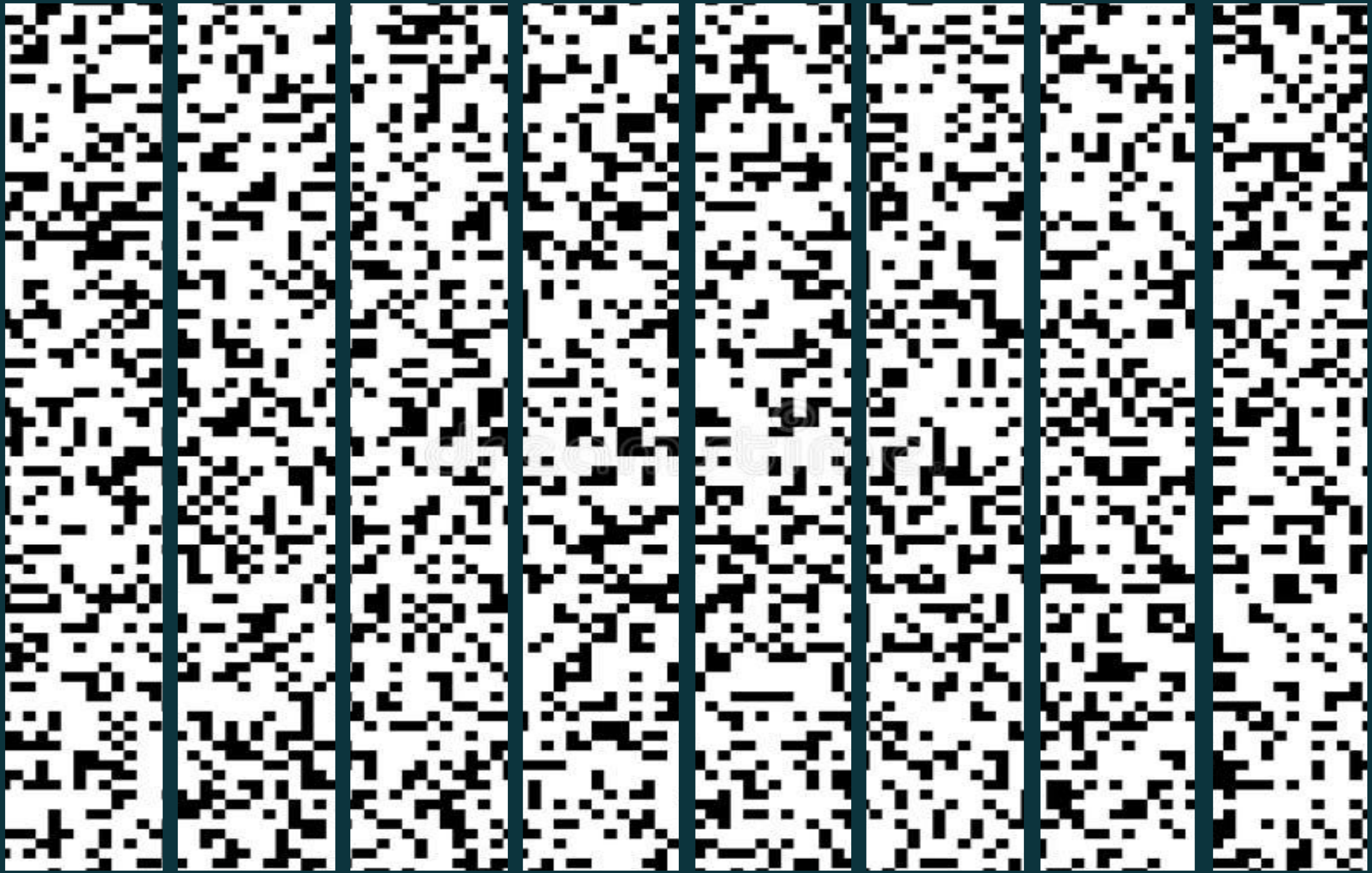
| | |
|---|---|
| 175 | 167 |
| 183 | 177 |

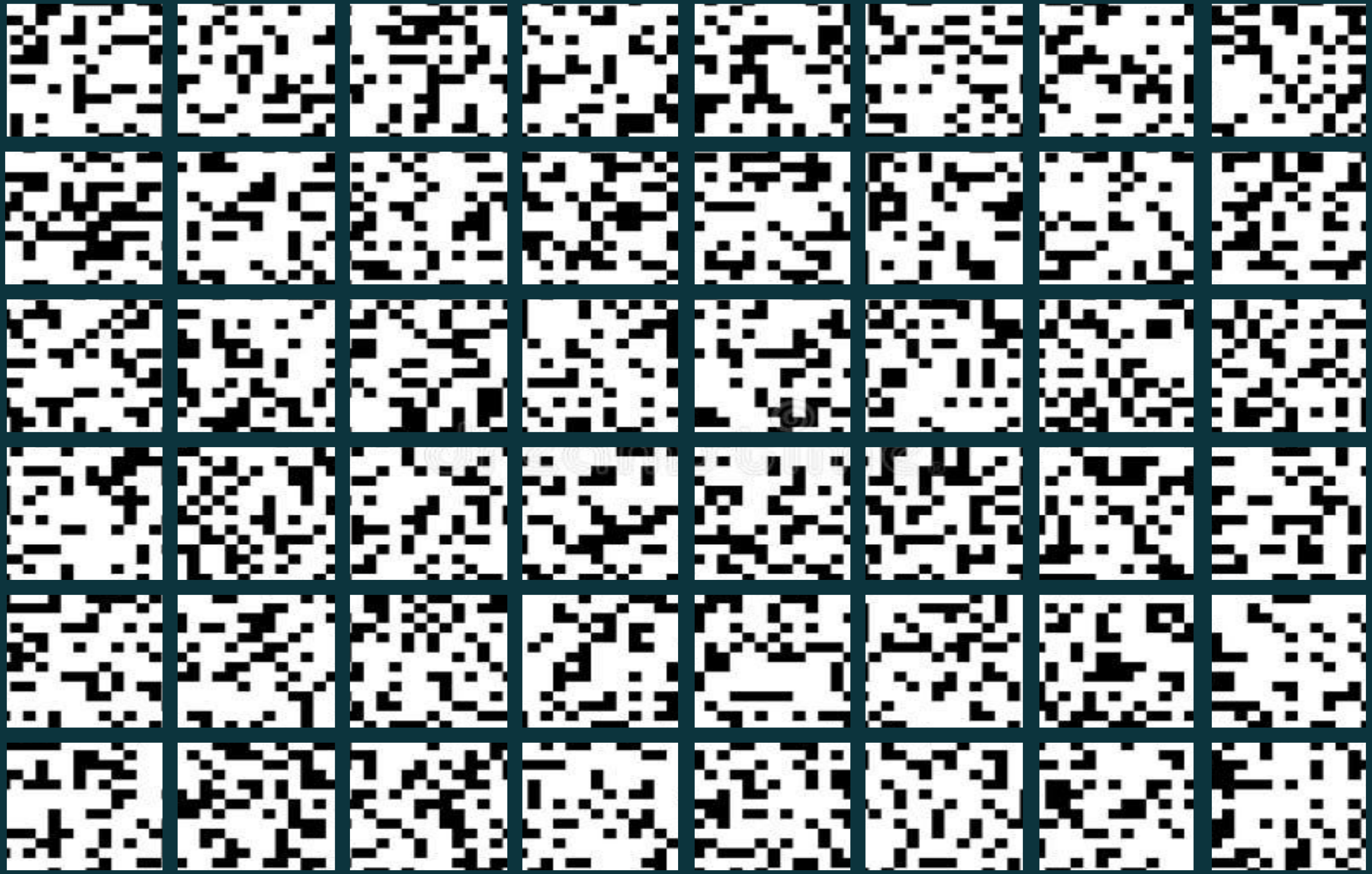
|  |  |  |  |  |  |
|---|---|---|---|---|---|
| 180 | 182 | 180 | 181 | 202 | 202 |
| 180 | 184 | 181 | 181 | 196 | 196 |
| 182 | 178 | 196 | 202 | 200 | 195 |
| 184 | 183 | 193 | 193 | 195 | 199 |
| 186 | 193 | 189 | 182 | 175 | 167 |
| 193 | 183 | 181 | 189 | 183 | 177 |

○ Secret Embedding

APDH

+ Secret Data





| | | | | | |
|---|---|---|---|---|---|
| 180 | 182 | 180 | 181 | 202 | 202 |
| 180 | 184 | 181 | 181 | 196 | 196 |
| 182 | 178 | 196 | 202 | 200 | 195 |
| 184 | 183 | 193 | 193 | 195 | 199 |
| 186 | 193 | 189 | 182 | 175 | 167 |
| 193 | 183 | 181 | 189 | 183 | 177 |

| | |
|---|---|
| 180 | 182 |
| 180 | 184 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 196 | 196 |

| | |
|---|---|
| 182 | 178 |
| 184 | 183 |

| | |
|---|---|
| 196 | 202 |
| 193 | 193 |

| | |
|---|---|
| 200 | 195 |
| 195 | 199 |

| | |
|---|---|
| 186 | 193 |
| 193 | 183 |

| | |
|---|---|
| 189 | 182 |
| 181 | 189 |

| | |
|---|---|
| 175 | 167 |
| 183 | 177 |

# APDH

- Secret Extraction
- Image Decryption

○ Secret Extraction

APDH

# Difference Histograms

| | |
|---|---|
| ○ D1 | T1 |
| ○ D2 | T2 |
| ○ D3 | T3 |

| | |
|---|---|
| 1 | 2 |
| 3 | 4 |

$$D1 = \text{abs}(1 - 3)$$

$$D2 = \text{abs}(2 - 4)$$

$$D3 = \text{abs}(1 - 2)$$

D3
T3

# Partial Data Extraction

D2
T2

# Partial Data Extraction

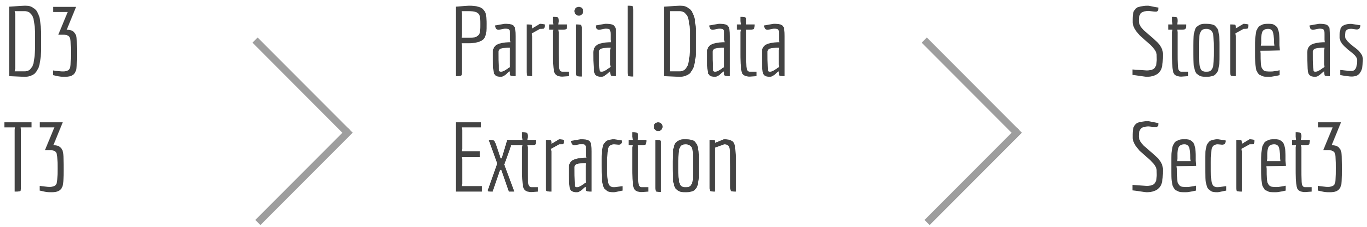
D1
T1

# Partial Data Extraction

# Partial Data

n zeros (0) of padding

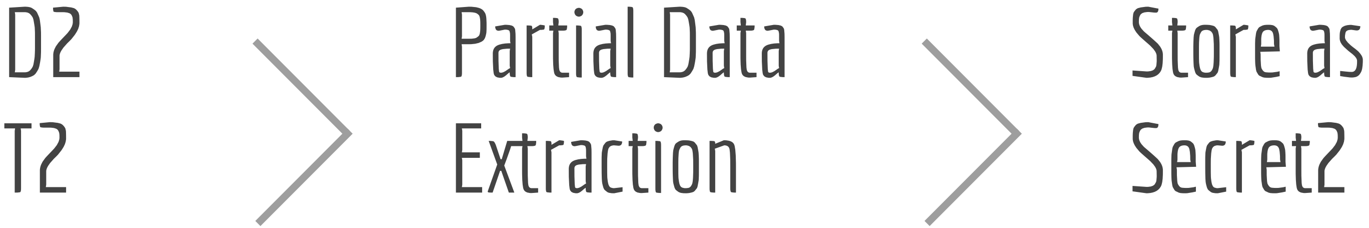
Last (first) n bits of data



D3
T3

Partial Data
Extraction

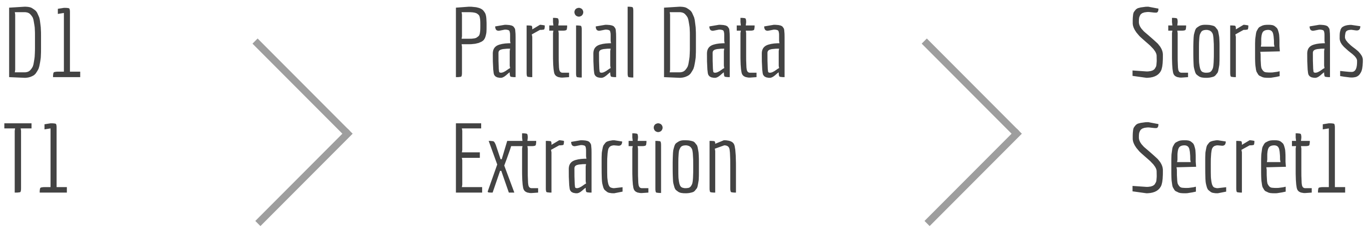
Store as
Secret3



D2
T2

Partial Data
Extraction

Store as
Secret2



D1
T1

Partial Data
Extraction

Store as
Secret1

# Loop over all blocks

| | |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
Loop over all blocks
    If ( T3 <= D3 <= (T3 + (2^n - 1)) )
```

# Data Extraction

| | |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
secret = ( D3 - T3 )

secret3 = secret3 + secret

If (P1 <= P2):
    P2 = P2 - secret

Else:
    P2 = P2 + secret
```

```
Loop over all blocks
    Else If ( $D3 > (T3 + (2^n - 1))$ )
        Histogram re-shift
```

| | |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
        If ($P1 <= P2$):
            $P2 = P2 - (2^n - 1)$

        Else:
            $P2 = P2 + (2^n - 1)$
    End If
End Loop
```

| | |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
    End If
End Loop
```

# Data Extraction

```
Loop over all blocks
    If ( T2 <= D2 <= (T2 + (2^n - 1)) )
        secret = ( D2 - T2 )

        secret2 = secret2 + secret

        If (P2 <= P4):
            P4 = P4 - secret

        Else:
            P4 = P4 + secret
```

| | |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
Loop over all blocks
    Else If ( $D2 > (T2 + (2^n - 1))$ )
```

## Histogram re-shift

|  |  |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
If (P2 <= P4):
    $P4 = P4 - (2^n - 1)$

Else:
    $P4 = P4 + (2^n - 1)$
```

```
    End If
End Loop
```

```
Loop over all blocks
    If ( T1 <= D1 <= (T1 + (2^n - 1)) )
```

# Data Extraction

| | |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
secret = ( D2 - T2 )

secret1 = secret1 + secret

If (P1 <= P3):
   P3 = P3 - secret

Else:
   P3 = P3 + secret
```

```
Loop over all blocks
    Else If ( $D1 > (T1 + (2^n - 1))$ )
        Histogram re-shift
    End If
End Loop
```

|  |  |
|---|---|
| P1 | P2 |
| P3 | P4 |

```
If ($P1 <= P3$):
    $P3 = P3 - (2^n - 1)$

Else:
    $P3 = P3 + (2^n - 1)$
```

Secret = secret1 + secret2 + secret3

CleanUp Steps:

- Remove redundant padded zeros (0’s)
- Format it in 8-bit pairs
- Remove all non-printable characters

Secret = ‘Secret Data’

| | |
|---|---|
| 180 | 182 |
| 180 | 184 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 196 | 196 |

| | |
|---|---|
| 182 | 178 |
| 184 | 183 |

| | |
|---|---|
| 196 | 202 |
| 193 | 193 |

| | |
|---|---|
| 200 | 195 |
| 195 | 199 |

| | |
|---|---|
| 186 | 193 |
| 193 | 183 |

| | |
|---|---|
| 189 | 182 |
| 181 | 189 |

| | |
|---|---|
| 175 | 167 |
| 183 | 177 |

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 199 | 199 |

| | |
|---|---|
| 182 | 181 |
| 184 | 181 |

| | |
|---|---|
| 196 | 199 |
| 194 | 196 |

| | |
|---|---|
| 200 | 198 |
| 198 | 198 |

| | |
|---|---|
| 186 | 190 |
| 190 | 186 |

| | |
|---|---|
| 189 | 185 |
| 184 | 186 |

| | |
|---|---|
| 175 | 170 |
| 180 | 174 |

- Secret Extraction

APDH

○ Image Decryption

APDH

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 199 | 199 |

| | |
|---|---|
| 182 | 181 |
| 184 | 181 |

| | |
|---|---|
| 196 | 199 |
| 194 | 196 |

| | |
|---|---|
| 200 | 198 |
| 198 | 198 |

| | |
|---|---|
| 186 | 190 |
| 190 | 186 |

| | |
|---|---|
| 189 | 185 |
| 184 | 186 |

| | |
|---|---|
| 175 | 170 |
| 180 | 174 |

○ Blocks

- Blocks
- Random Set

- Blocks
- Random Set
- Cryptographic Key

|  |  |  |
|---|---|---|
| 132 | 255 | 179 |
| 155 | 5 | 128 |
| 111 | 222 | 186 |

| | |
|---|---|
| 132 | 132 |
| 132 | 132 |

| | |
|---|---|
| 255 | 255 |
| 255 | 255 |

| | |
|---|---|
| 179 | 179 |
| 179 | 179 |

| | |
|---|---|
| 155 | 155 |
| 155 | 155 |

| | |
|---|---|
| 5 | 5 |
| 5 | 5 |

| | |
|---|---|
| 128 | 128 |
| 128 | 128 |

| | |
|---|---|
| 111 | 111 |
| 111 | 111 |

| | |
|---|---|
| 222 | 222 |
| 222 | 222 |

| | |
|---|---|
| 186 | 186 |
| 186 | 186 |

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 199 | 199 |

| | |
|---|---|
| 182 | 181 |
| 184 | 181 |

| | |
|---|---|
| 196 | 199 |
| 194 | 196 |

| | |
|---|---|
| 200 | 198 |
| 198 | 198 |

| | |
|---|---|
| 186 | 190 |
| 190 | 186 |

| | |
|---|---|
| 189 | 185 |
| 184 | 186 |

| | |
|---|---|
| 175 | 170 |
| 180 | 174 |

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 199 | 199 |

| | |
|---|---|
| 182 | 181 |
| 184 | 181 |

| | |
|---|---|
| 196 | 199 |
| 194 | 196 |

| | |
|---|---|
| 200 | 198 |
| 198 | 198 |

| | |
|---|---|
| 186 | 190 |
| 190 | 186 |

| | |
|---|---|
| 189 | 185 |
| 184 | 186 |

| | |
|---|---|
| 175 | 170 |
| 180 | 174 |

|  |  |
|---|---|
| 180 | 181 |
| 180 | 181 |

Encrypted
Block

|  |  |
|---|---|
| 132 | 132 |
| 132 | 132 |

Random
Block

| | |
|---|---|
| 180 | 181 |
| 180 | 181 |

−

2

*

| | |
|---|---|
| 176 | 176 |
| 176 | 176 |

Cryptographic
Key

Operation 1

uint8

| | |
|---|---|
| 84 | 85 |
| 84 | 85 |

# Operation 1

uint8

## Operation 2

|  |  |
|---|---|
| 84 | 85 |
| 84 | 85 |

−

|  |  |
|---|---|
| 132 | 132 |
| 132 | 132 |

Random
Set

uint8

| | |
|---|---|
| 208 | 209 |
| 208 | 209 |

# Operation 2

uint8

| | |
|---|---|
| 208 | 209 |
| 208 | 209 |

uint8

| | |
|---|---|
| 208 | 209 |
| 208 | 209 |

| | |
|---|---|
| 180 | 181 |
| 181 | 181 |

| | |
|---|---|
| 202 | 202 |
| 199 | 199 |

| | |
|---|---|
| 182 | 181 |
| 184 | 181 |

| | |
|---|---|
| 196 | 199 |
| 194 | 196 |

| | |
|---|---|
| 200 | 198 |
| 198 | 198 |

| | |
|---|---|
| 186 | 190 |
| 190 | 186 |

| | |
|---|---|
| 189 | 185 |
| 184 | 186 |

| | |
|---|---|
| 175 | 170 |
| 180 | 174 |

| | | | | | |
|---|---|---|---|---|---|
| 208 | 209 | **85** | **86** | 202 | 202 |
| 208 | 209 | **86** | **86** | 199 | 199 |
| 182 | 181 | 196 | 199 | 200 | 198 |
| 184 | 181 | 194 | 196 | 198 | 198 |
| 186 | 190 | 189 | 185 | 175 | 170 |
| 190 | 186 | 184 | 186 | 180 | 174 |

| | | | | | |
|---|---|---|---|---|---|
| 208 | 209 | 85 | 86 | 183 | 183 |
| 208 | 209 | 86 | 86 | 180 | 180 |
| 182 | 181 | 196 | 199 | 200 | 198 |
| 184 | 181 | 194 | 196 | 198 | 198 |
| 186 | 190 | 189 | 185 | 175 | 170 |
| 190 | 186 | 184 | 186 | 180 | 174 |

| | |
|---|---|
| 208 | 209 |
| 208 | 209 |

| | |
|---|---|
| 85 | 86 |
| 86 | 86 |

| | |
|---|---|
| 183 | 183 |
| 180 | 180 |

| | |
|---|---|
| 182 | 181 |
| 184 | 181 |

| | |
|---|---|
| 196 | 199 |
| 194 | 196 |

| | |
|---|---|
| 200 | 198 |
| 198 | 198 |

| | |
|---|---|
| 186 | 190 |
| 190 | 186 |

| | |
|---|---|
| 189 | 185 |
| 184 | 186 |

| | |
|---|---|
| 175 | 170 |
| 180 | 174 |

| | |
|---|---|
| 208 | 209 |
| 208 | 209 |

| | |
|---|---|
| 85 | 86 |
| 86 | 86 |

| | |
|---|---|
| 183 | 183 |
| 180 | 180 |

| | |
|---|---|
| 187 | 186 |
| 189 | 186 |

| | |
|---|---|
| 95 | 98 |
| 93 | 95 |

| | |
|---|---|
| 232 | 230 |
| 230 | 230 |

| | |
|---|---|
| 235 | 239 |
| 239 | 235 |

| | |
|---|---|
| 127 | 123 |
| 122 | 124 |

| | |
|---|---|
| 149 | 144 |
| 154 | 148 |

○ Image Decryption

APDH

| | |
|---|---|
| 208 | 209 |
| 208 | 209 |

| | |
|---|---|
| 85 | 86 |
| 86 | 86 |

| | |
|---|---|
| 183 | 183 |
| 180 | 180 |

| | |
|---|---|
| 187 | 186 |
| 189 | 186 |

| | |
|---|---|
| 95 | 98 |
| 93 | 95 |

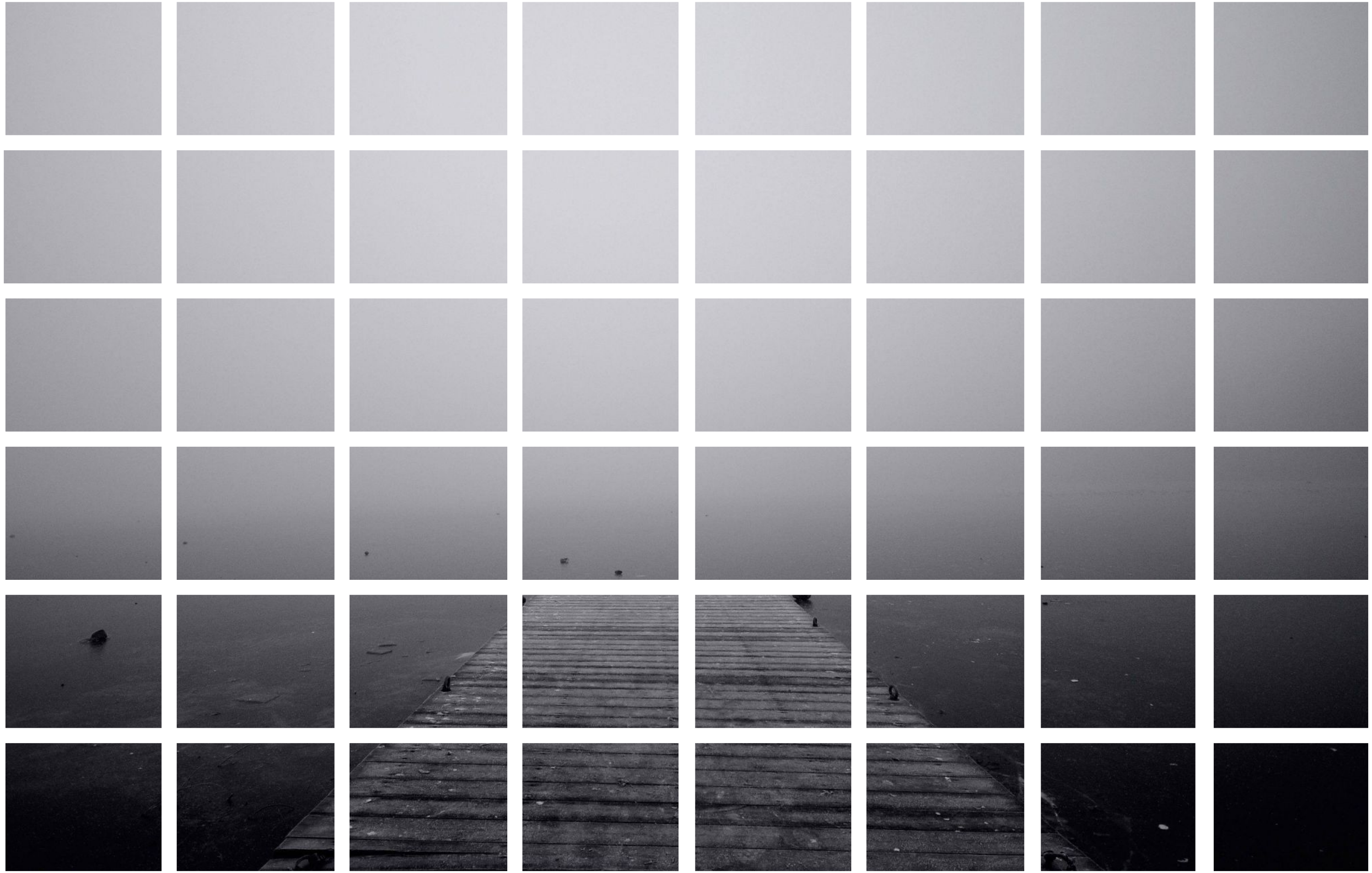
| | |
|---|---|
| 232 | 230 |
| 230 | 230 |

| | |
|---|---|
| 235 | 239 |
| 239 | 235 |

| | |
|---|---|
| 127 | 123 |
| 122 | 124 |

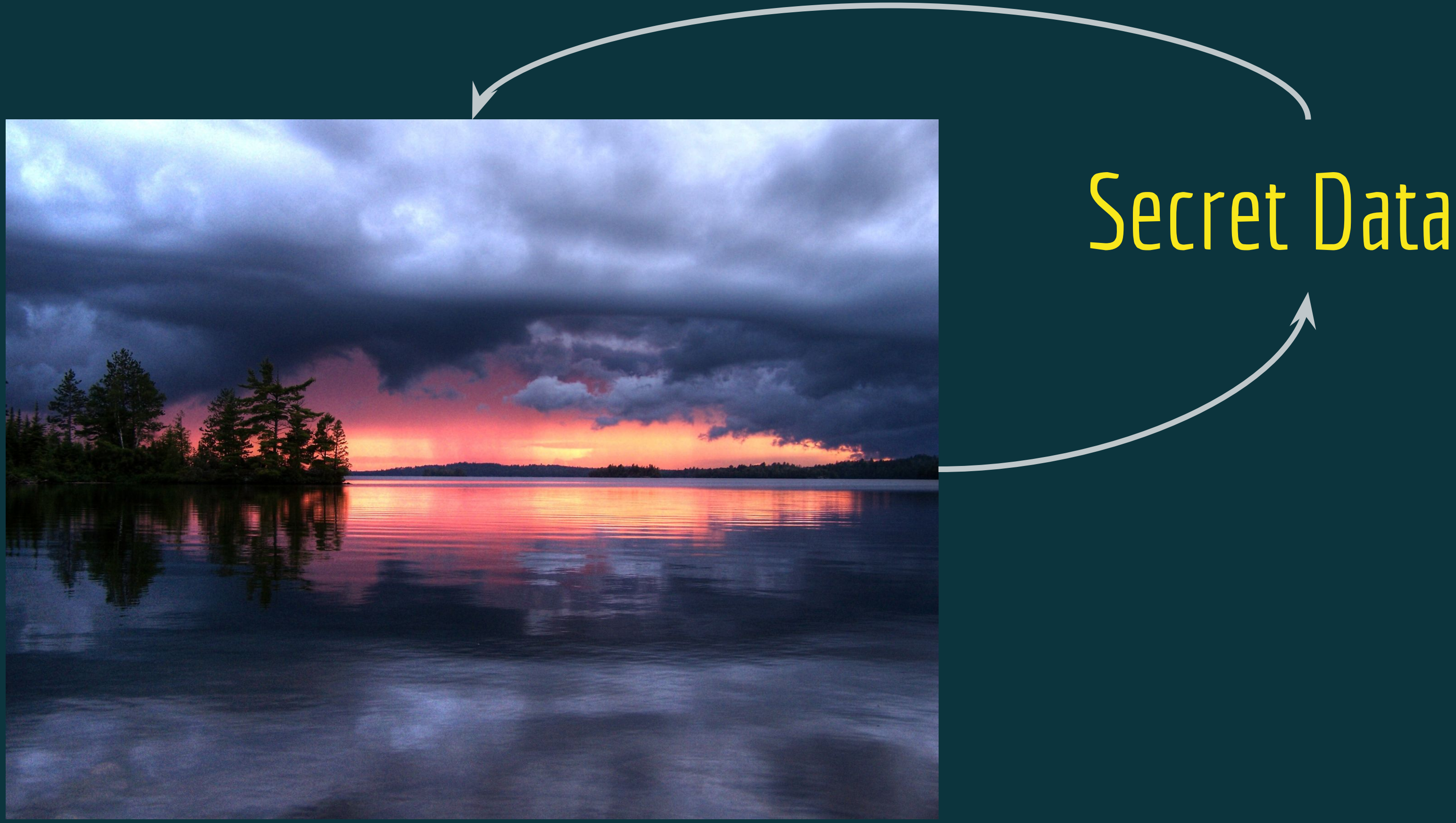
| | |
|---|---|
| 149 | 144 |
| 154 | 148 |

| | | | | | |
|---|---|---|---|---|---|
| 208 | 209 | 85 | 86 | 183 | 183 |
| 208 | 209 | 86 | 86 | 180 | 180 |
| 187 | 186 | 95 | 98 | 232 | 230 |
| 189 | 186 | 93 | 95 | 230 | 230 |
| 235 | 239 | 127 | 123 | 149 | 144 |
| 239 | 235 | 122 | 124 | 154 | 148 |



APDH

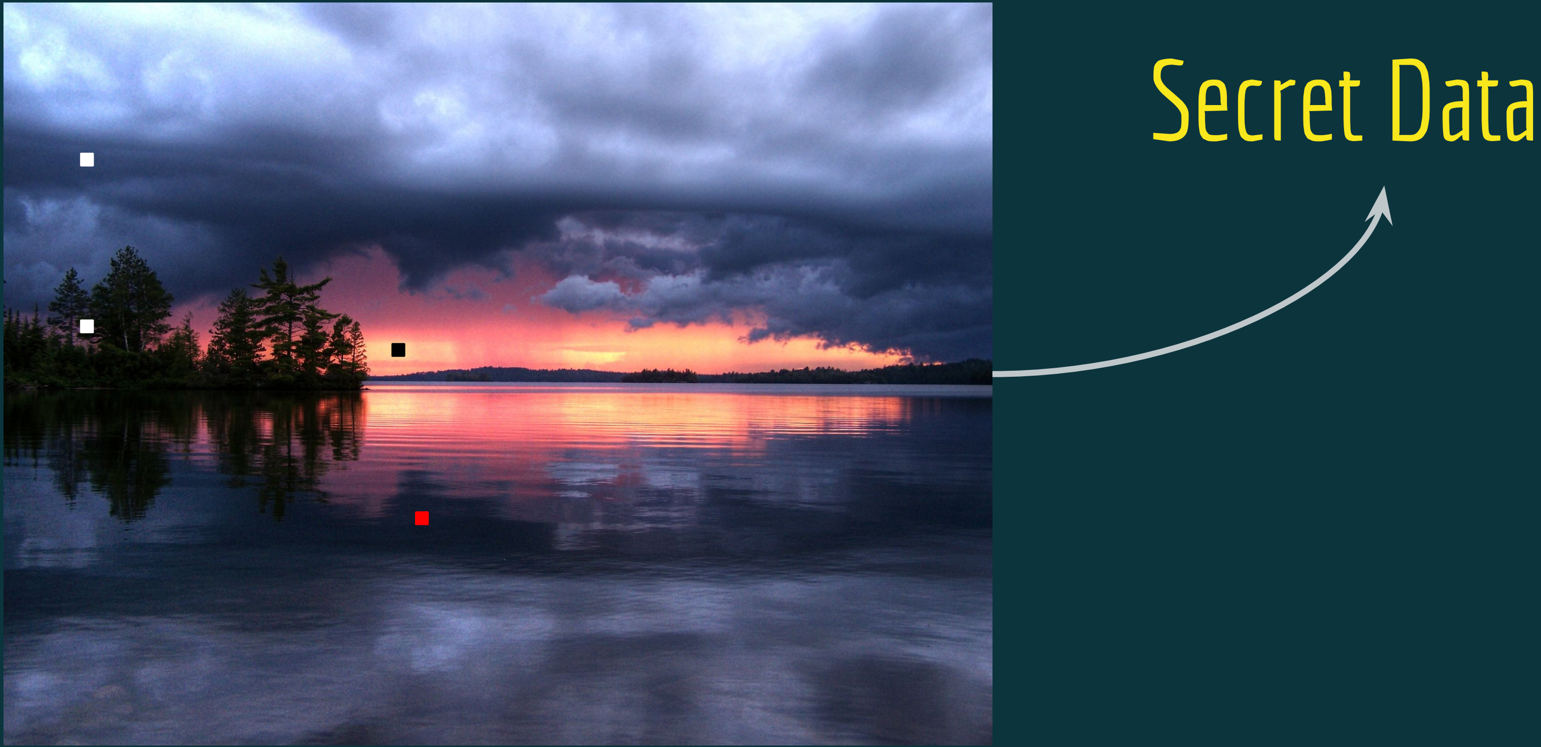
# Reversible Data Hiding



Secret Data

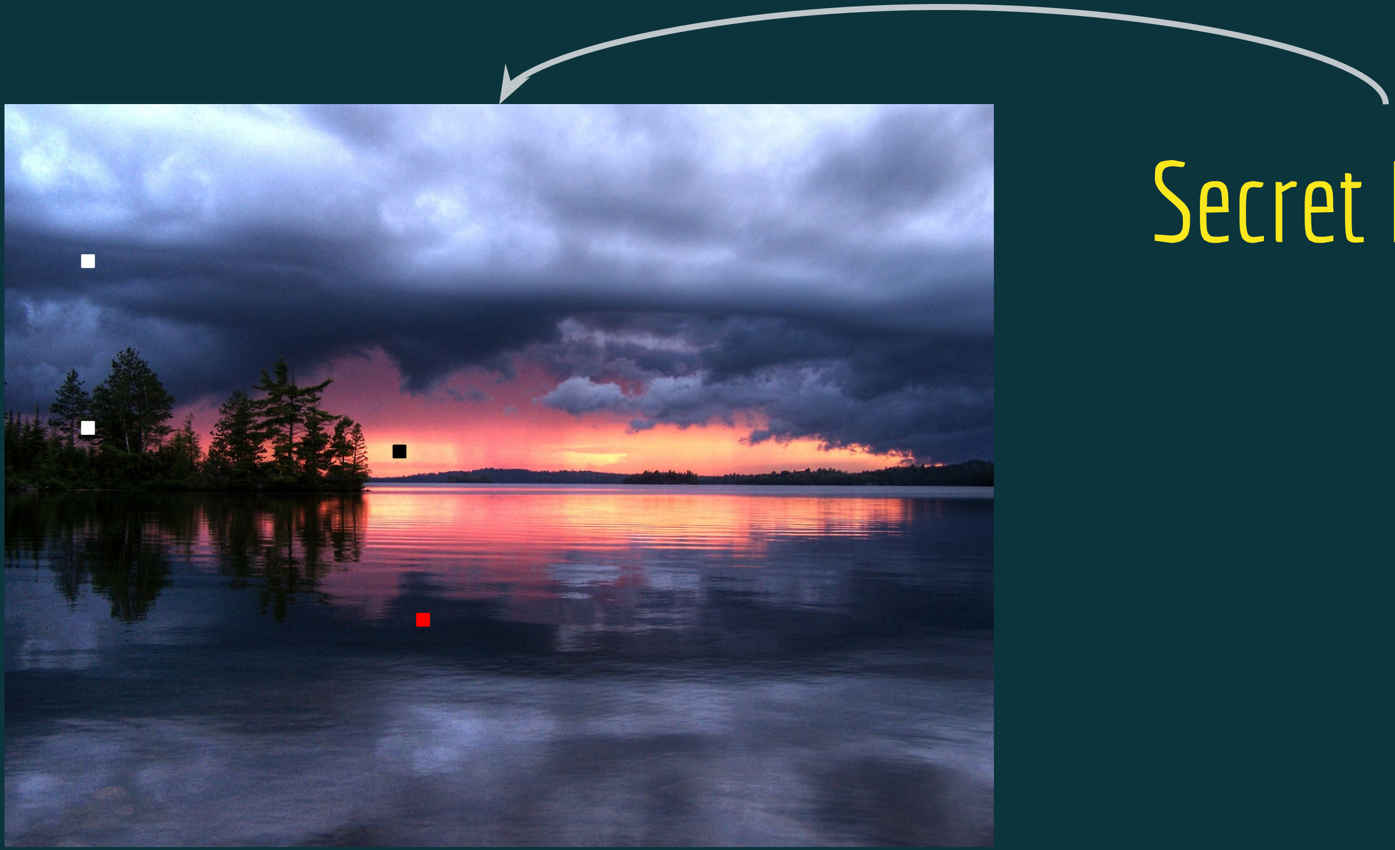
# Secret Data

Secret Data

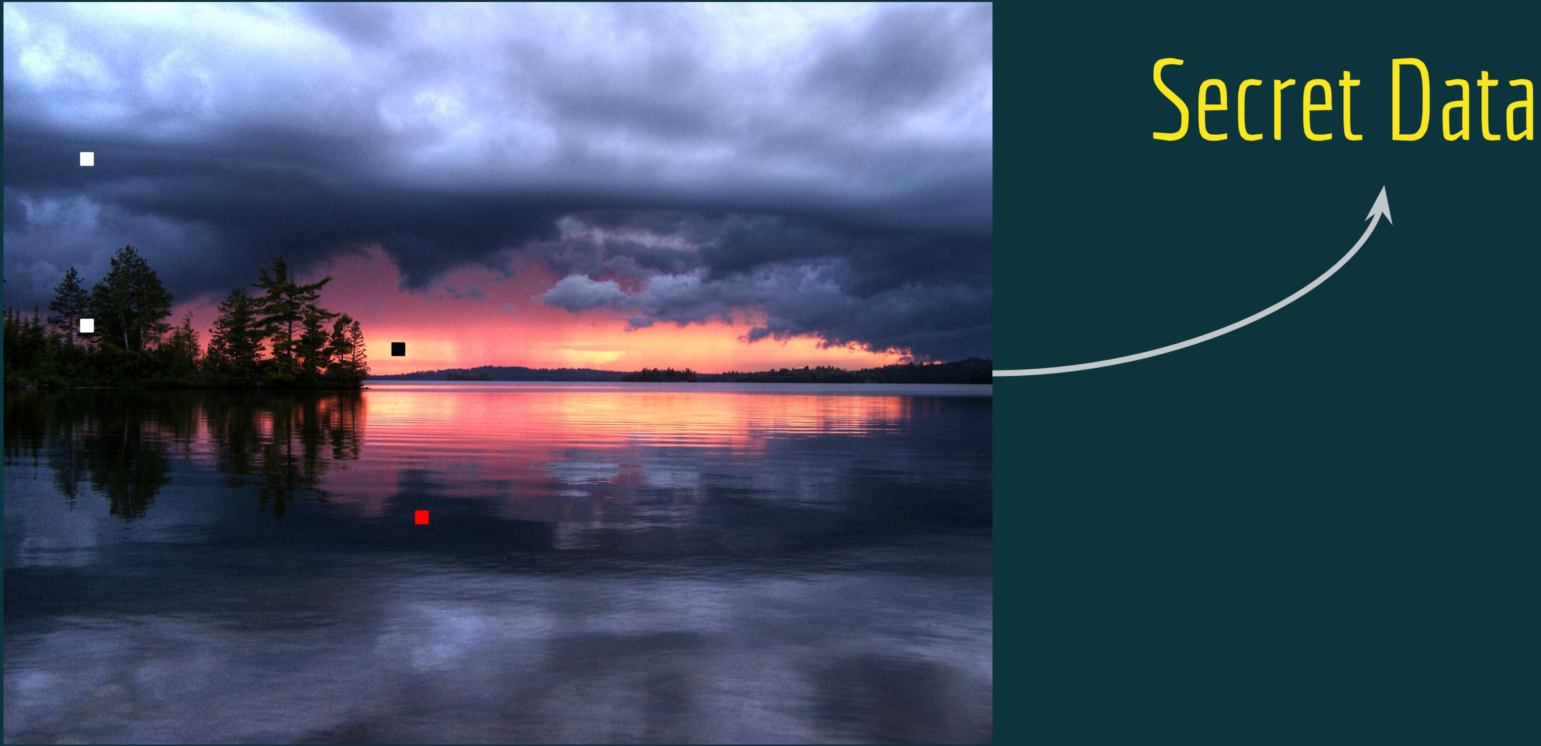


Secret Data

# Secret Data



Secret Data



Secret Data

Secret Data

# Secret Data

# Reversible Data Hiding

- Untapped potential

- Hardly any services

- Hardly any services: Open Platforms

- Hardly any services: Public Platforms

# Fueled with:

- Potential use case(s)

Fueled with:

- Potential use case(s)
- Our desire to work on

# Fueled with:

- Potential use case(s)
- Our desire to work on:
  - Cryptography related

Fueled with:

- Potential use case(s)
- Our desire to work on:
  - Cryptography related
  - Mathematically challenging

# What if

Service

○ On-demand cryptography

## Service

○ Secure image hosting services

Service

- Easy-to-use API calls

# Service

○ Integrate with existing platforms & services

Idea !

# A Revolutionary Idea !

What we call it as . . .

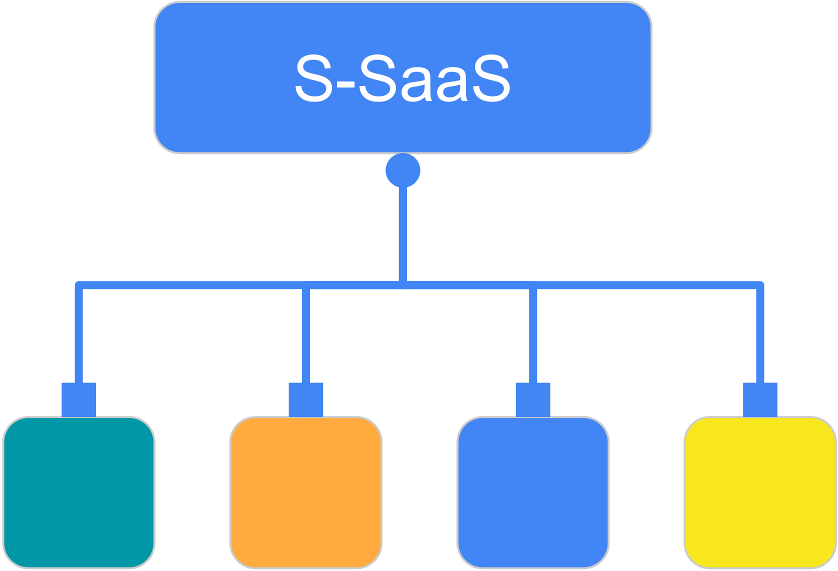
# S-SaaS

# S-SaaS

Secure - Steganography as a Service

S-SaaS

- Cloud service



- Multi-user access

# Seamless APIs

# S-SaaS

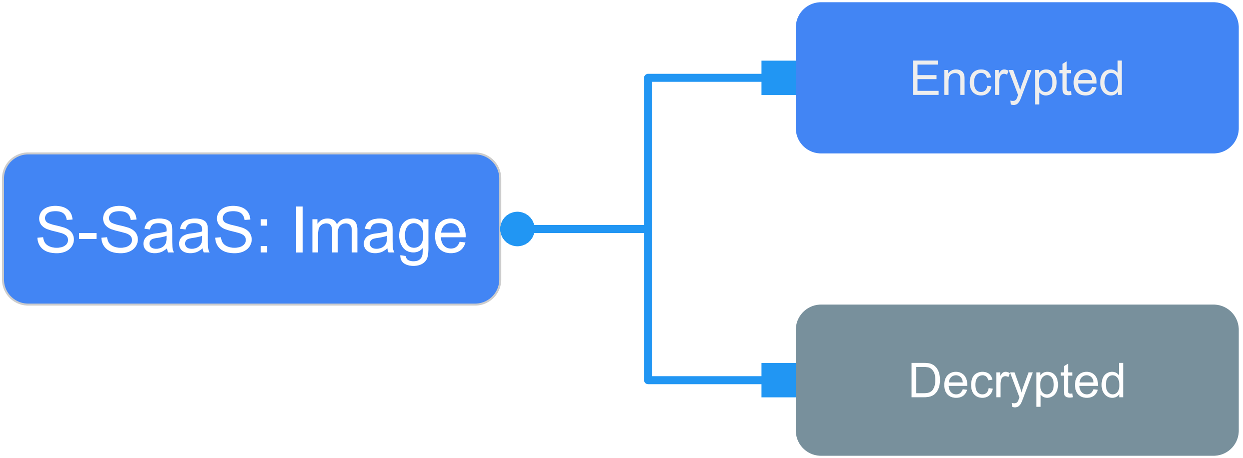
# On-demand Secure Image Cryptography Service

# S-SaaS

Dynamic
Image
Hosting

# S-SaaS

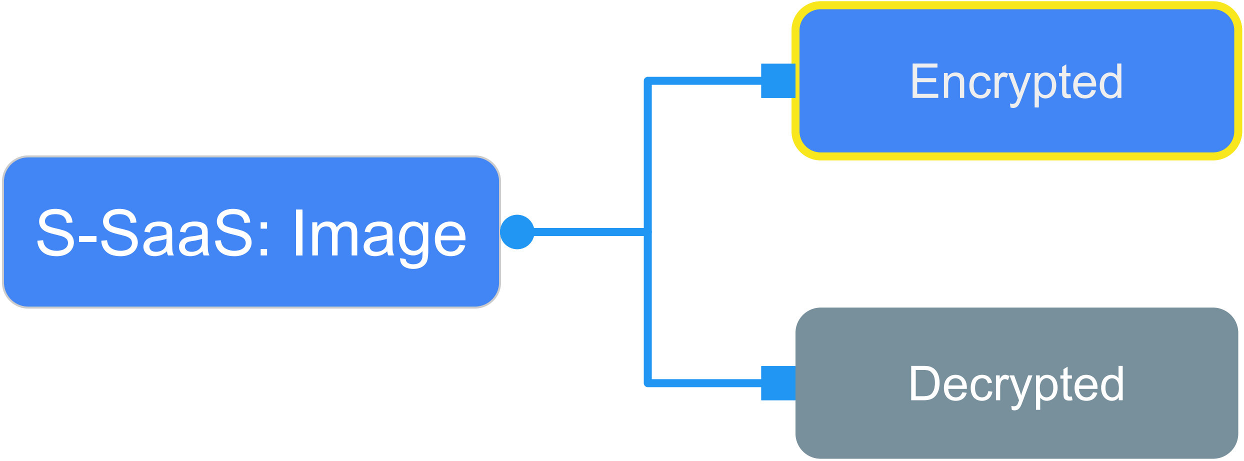
## On-demand dynamic state switching



S-SaaS: Image

Encrypted

Decrypted



S-SaaS: Image

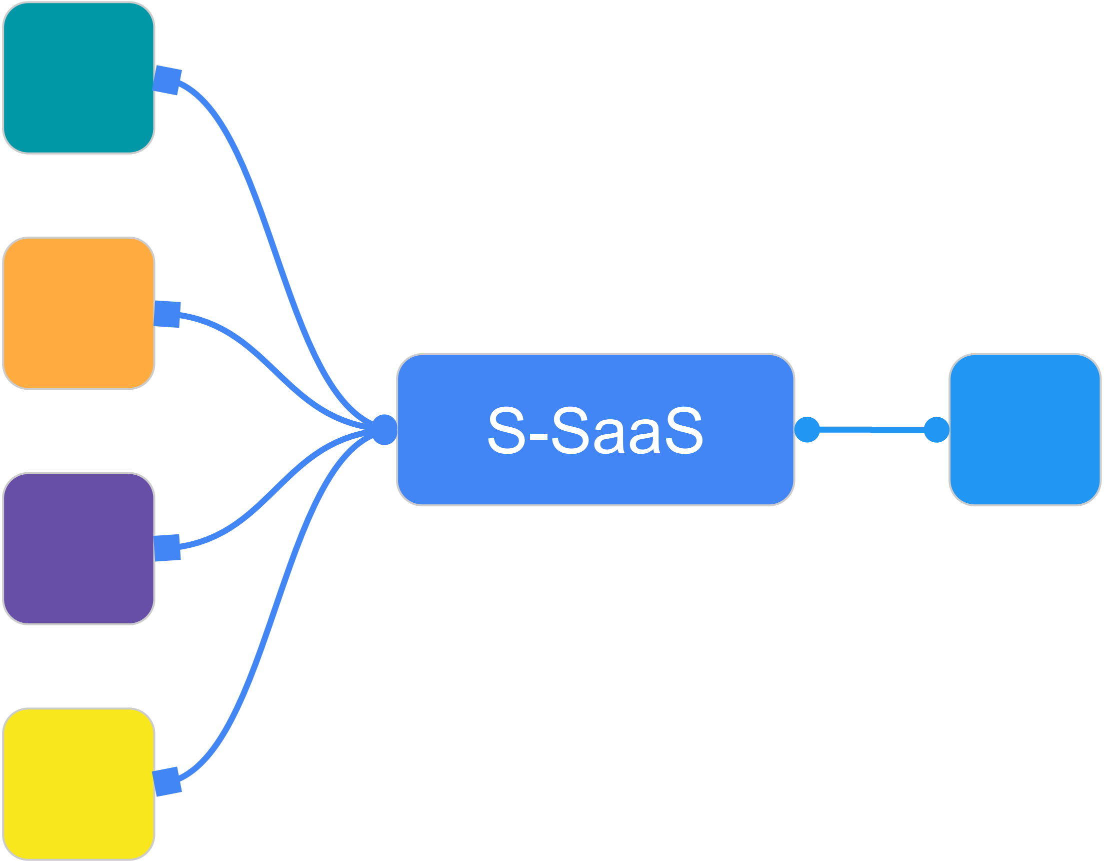
Encrypted

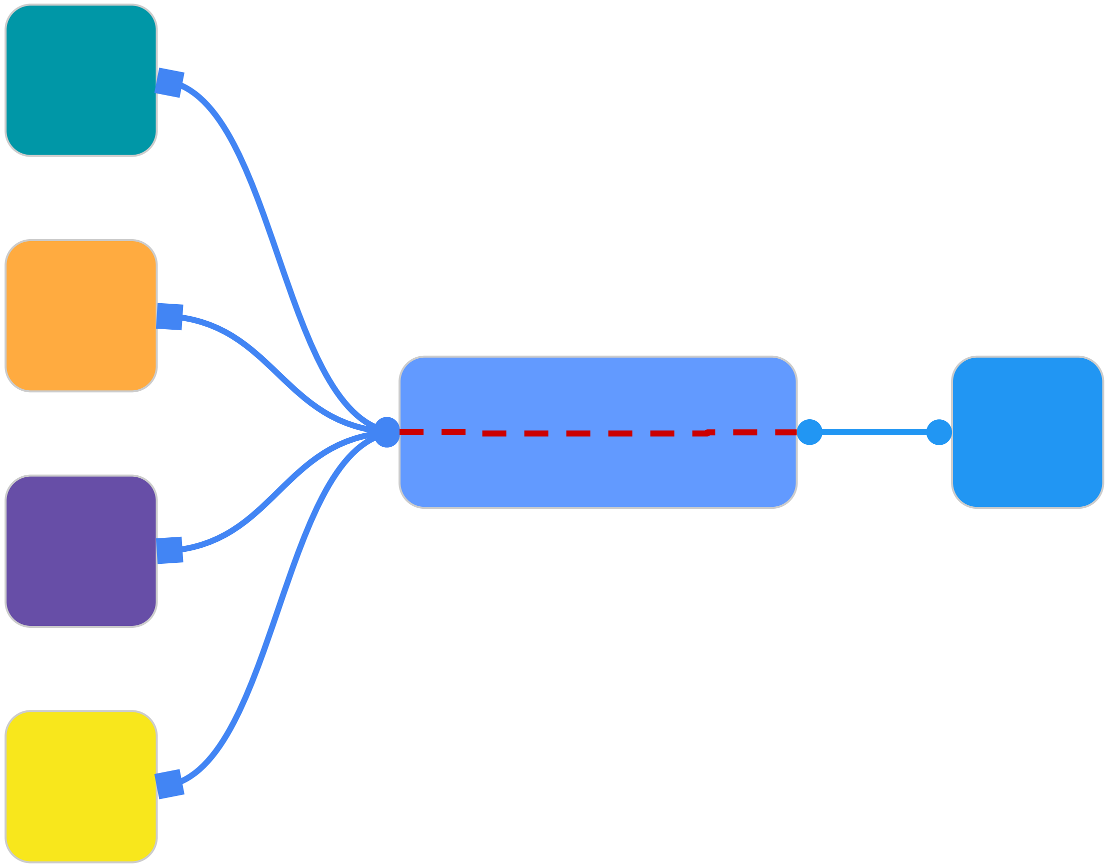
Decrypted

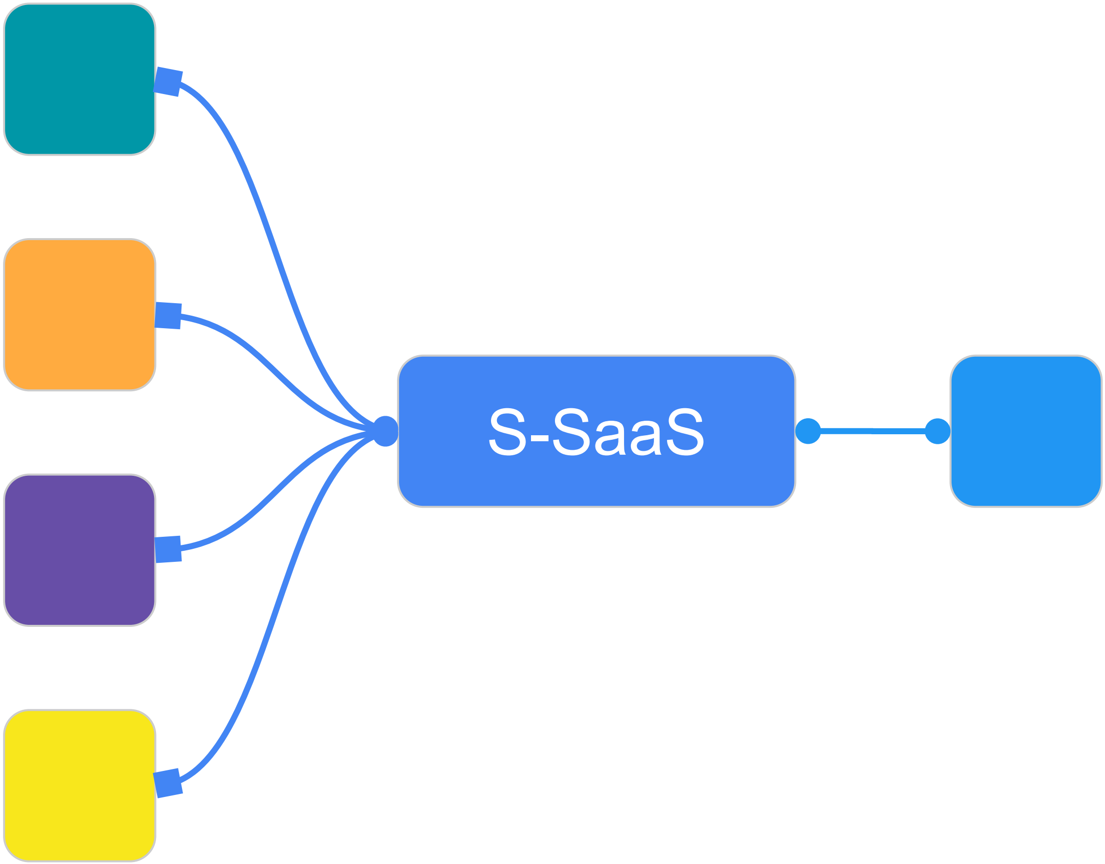
- Fail-secure

# S-SaaS

# Tokenized Dynamic Access Links


S-SaaS




S-SaaS

Now, that . . .

We may want

We need !

We’ve Developed

# A First of its Kind

Truly Remarkable

INTRODUCING

# CIS

Cloud Image Storage / Service

# CIS

# S-SaaS

CIS

# S-SaaS

Fully compliant with S-SaaS v0.1 Standards

- On-demand secure image cryptography
- Dynamic image hosting

- CIS

- Seamless APIs
- On-demand dynamic state switching

& more . . .

- CIS

- SSaaS: CIS

Back-end

Database

Front-end

Storage

- Modules

Security

Functionality

Router

- Backend

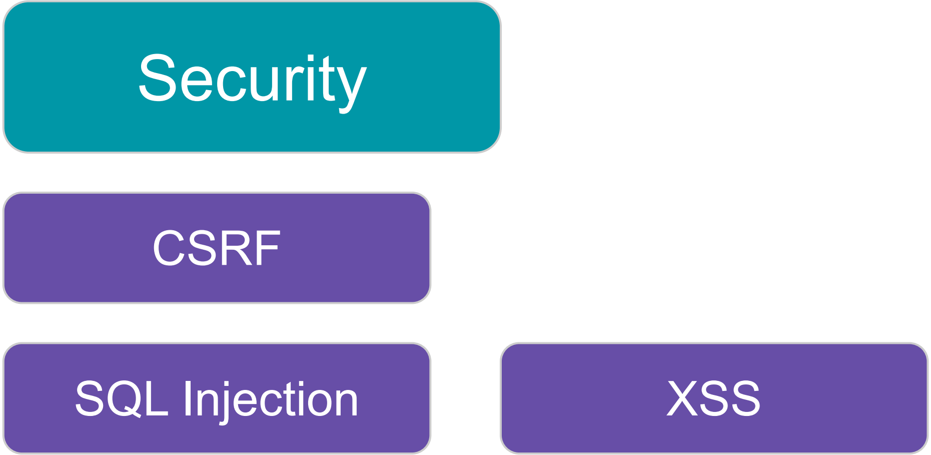
Routing

Web Hosting

Page Bindings

End-points

- Backend



Security

CSRF

SQL Injection

XSS

- Backend

## Security

Secure keygen

Password hasher

16-digit tokens

- Backend

## Functionality

Centralized User Authentication

APDH APIs

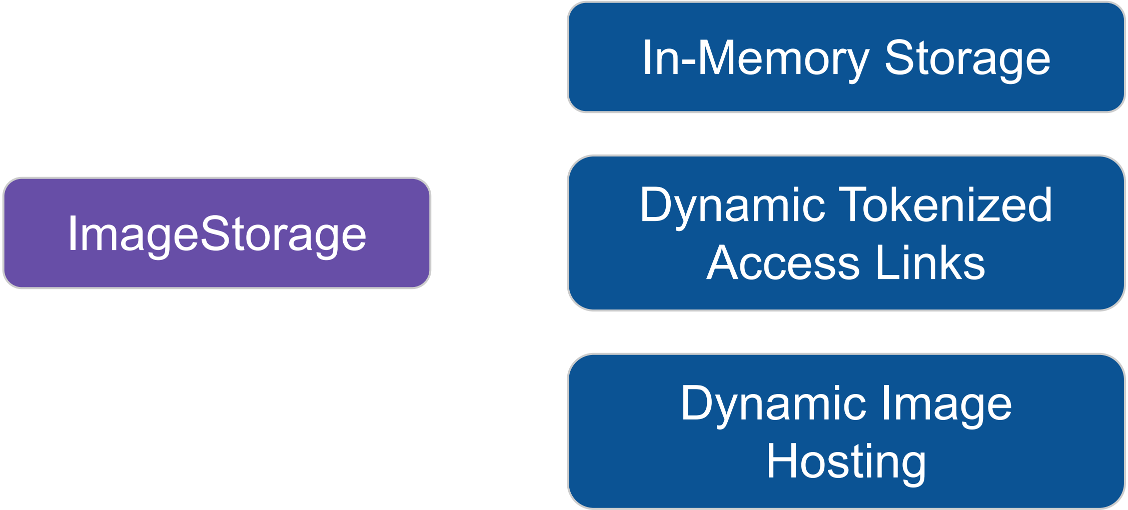
- Backend

Functionality

SSaaS Cryptographic APIs & Bindings

ImageStorage

- Backend



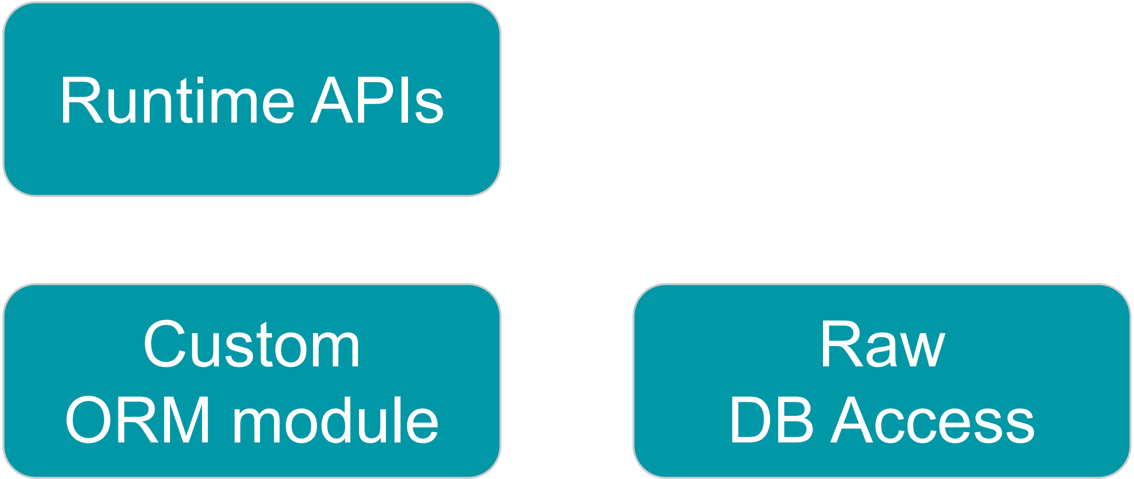
ImageStorage

In-Memory Storage

Dynamic Tokenized Access Links

Dynamic Image Hosting

- Backend



Runtime APIs

Custom ORM module

Raw DB Access

- Database

- Runtime Database API calls

- Database

- ○ Custom ORM (built over sqlite3)

- Database

- Modular data access

- Database

Persistent File Storage

DataBases

Encrypted Images

- Storage

- ○ Persistent File Storage

- ● Storage

○ Store
Encrypted Images

- Storage

- ○ Database Files Storage

- ● Storage

○ Web-UI

● Front-end

○ Web-UI

- User Signup
- User Login / Logout
- Account deletion
- Image storage

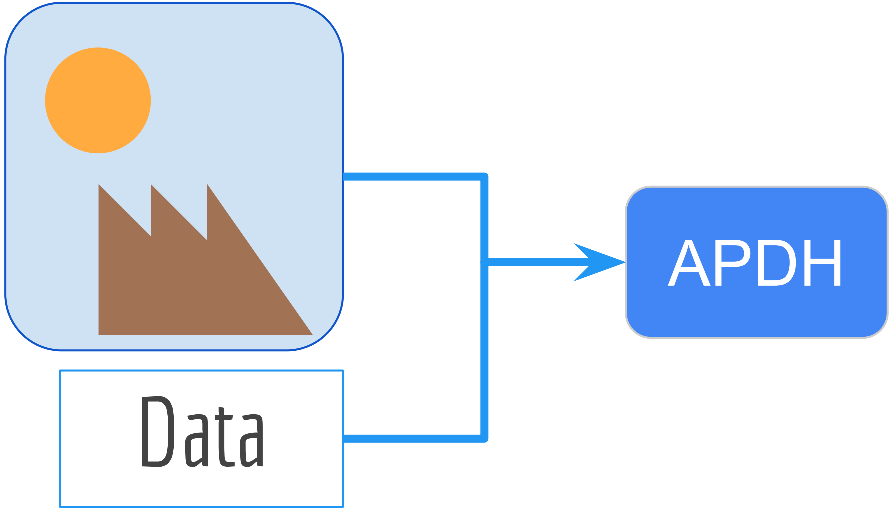
- Front-end

- Web-UI

- Data Embedding
- Data Extraction
- Image Cryptography
- Access Controls

- Front-end

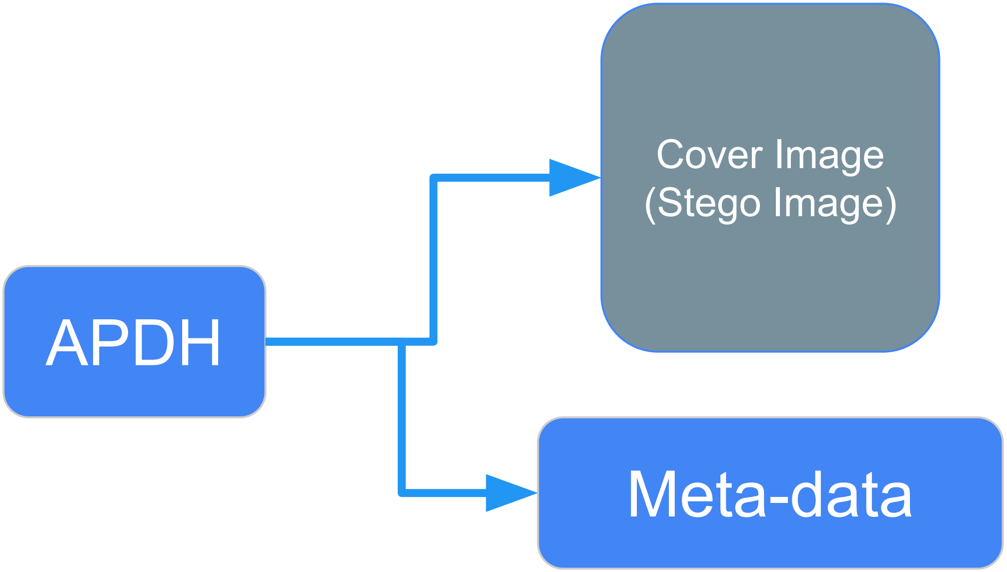
# Working



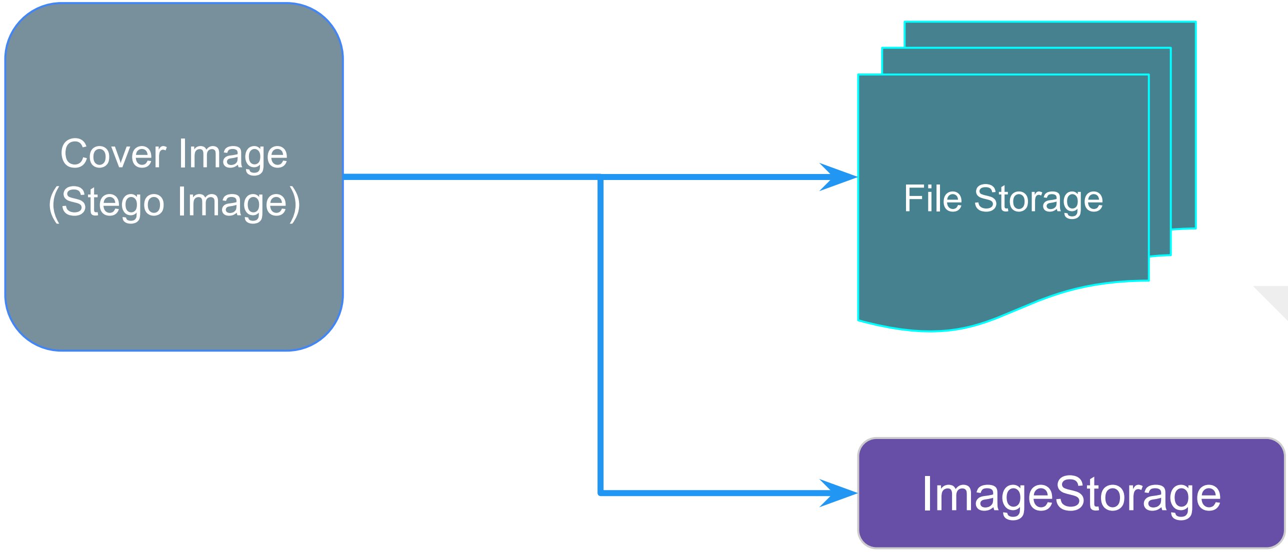
Data

APDH

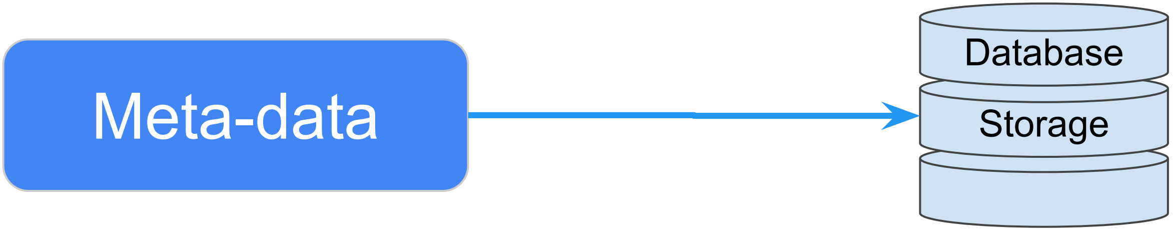
- Encryption



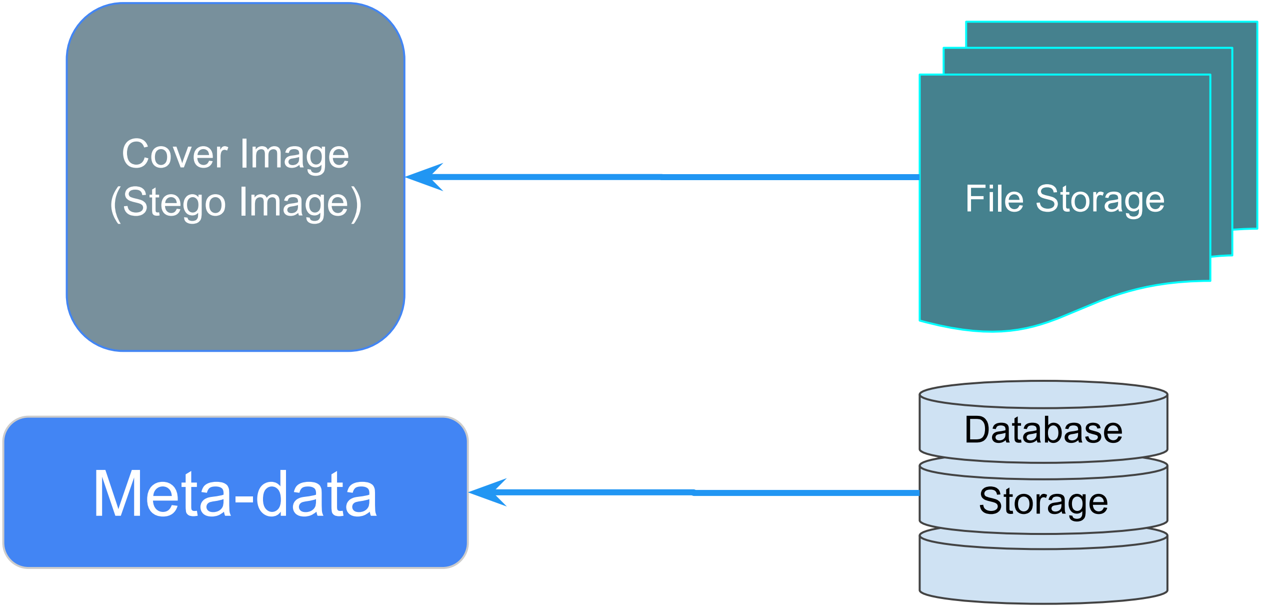
- Encryption



- Encryption



- Encryption



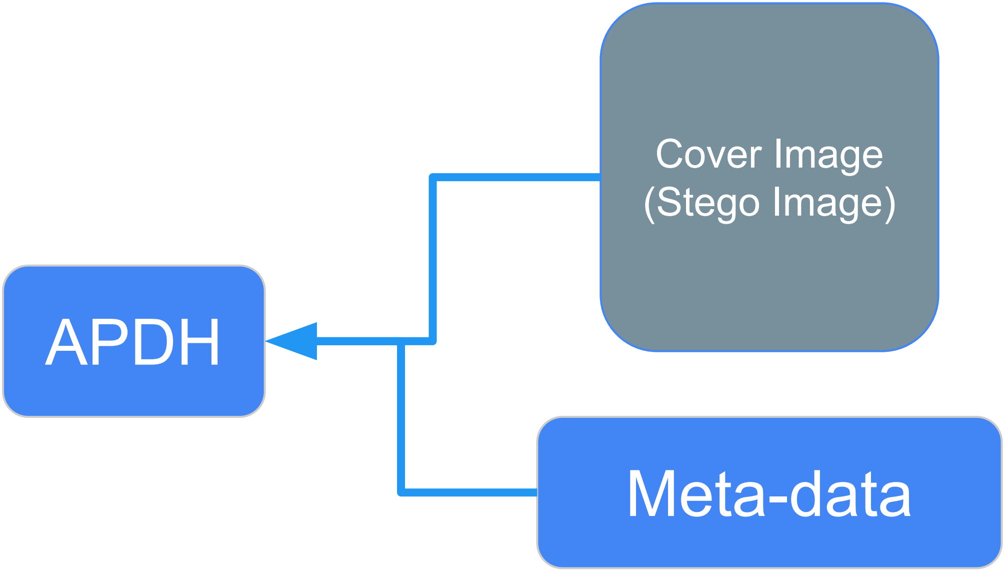
Cover Image
(Stego Image)

File Storage

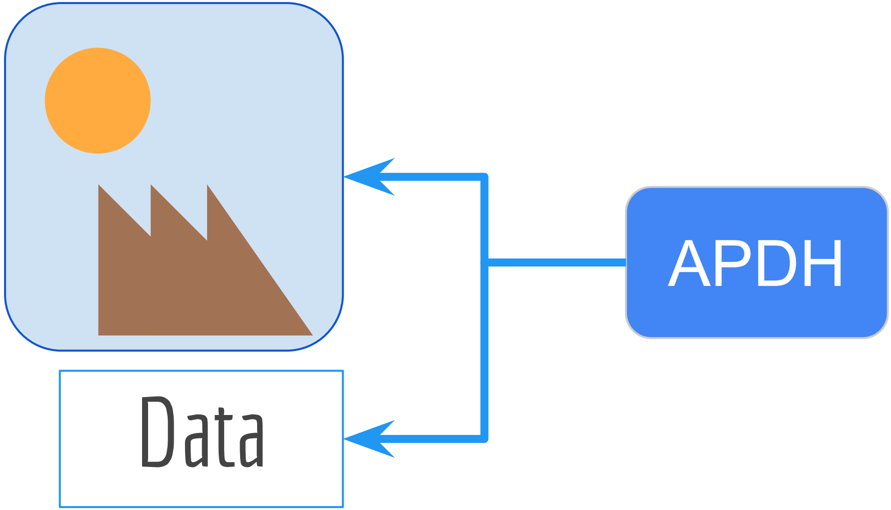
Meta-data

Database
Storage

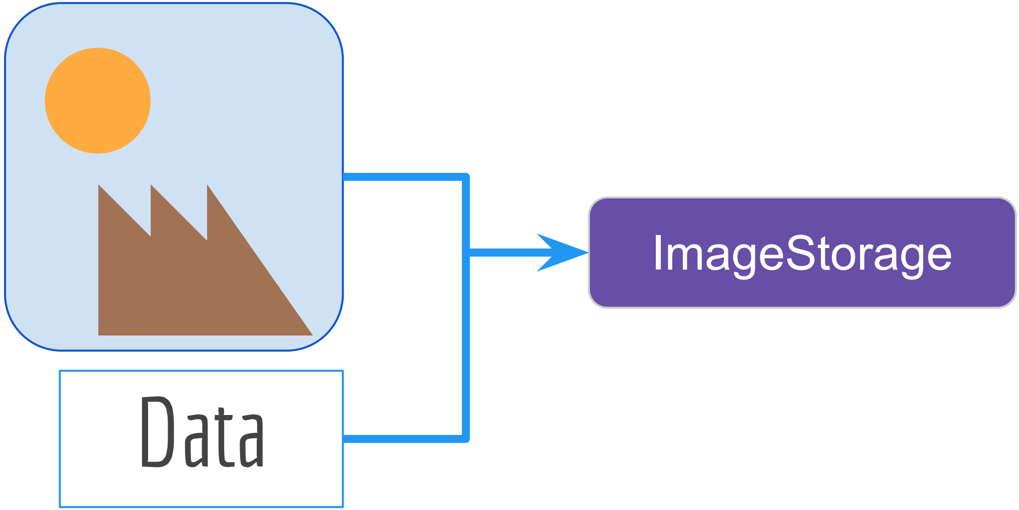
- Decryption



- Decryption



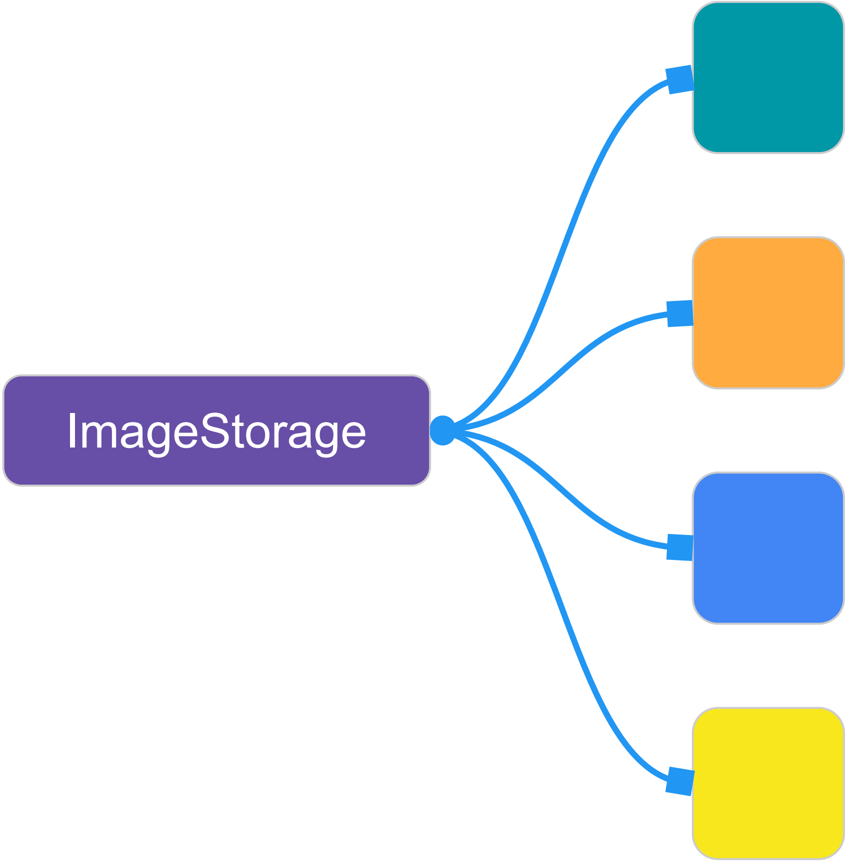
- Decryption



Data

ImageStorage

- Hosting



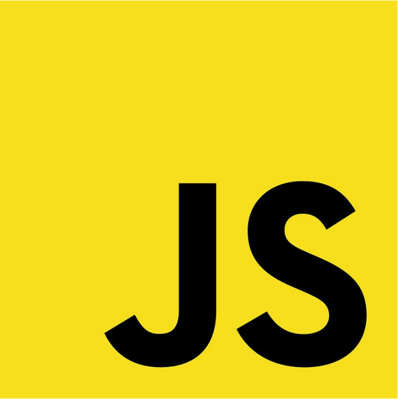
- Hosting

# Built using

- Python 3.8.x+

- Python-Flask 2.3.x

- Jinja2 3.1.x
- HTML 5



- JavaScript
- CSS 3

- Bootstrap 5

- jQuery v3.6

# CIS

Cloud Image Storage / Service

CIS

S-SaaS

# S-SaaS

Secure - Steganography as a Service

S-SaaS

# Thank You