ENCRYPTION-THEN-COMPRESSION SYSTEMS USING GRAYSCALE-BASED IMAGE ENCRYPTION FOR JPEG IMAGES

Team: B6

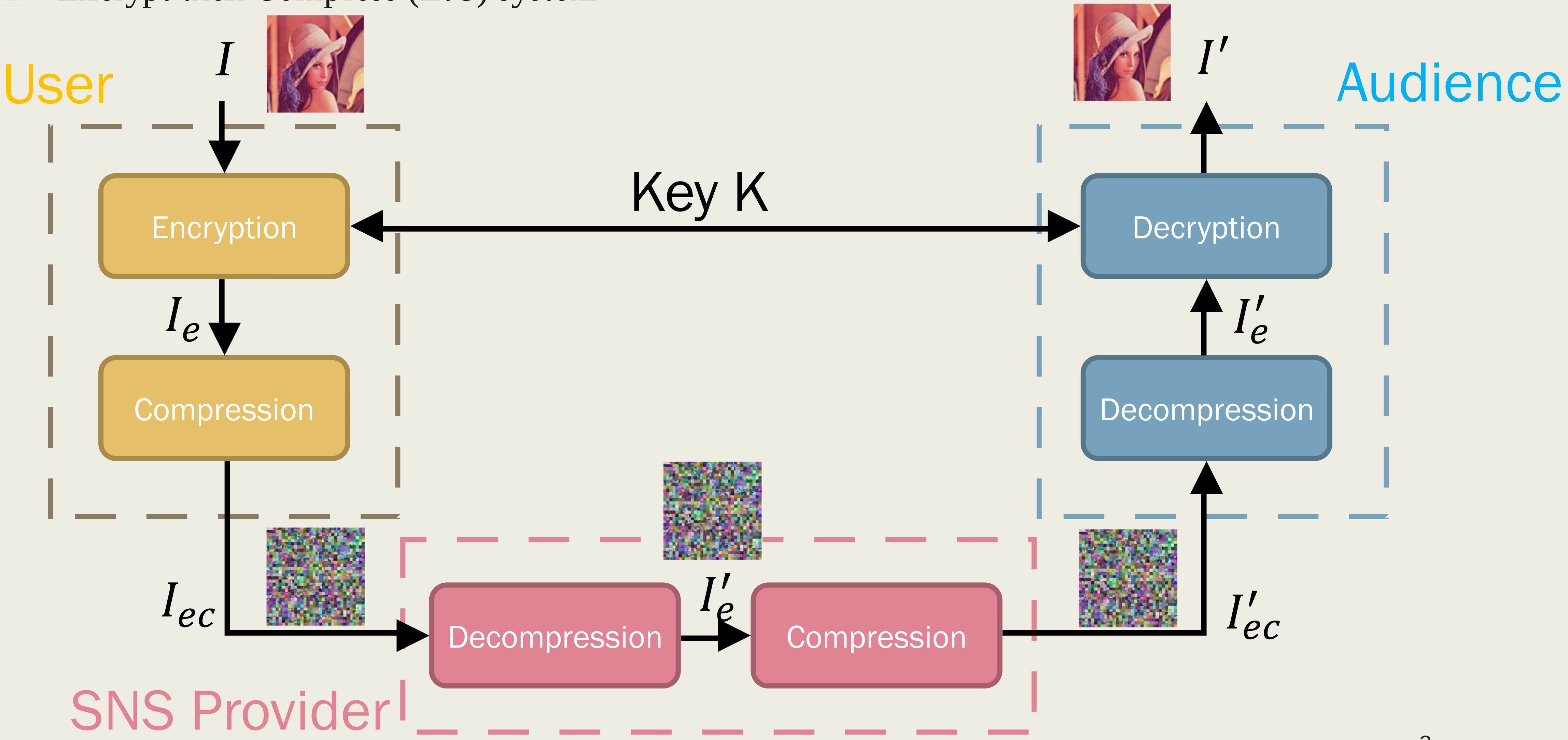
Members: 陳宏彥、劉正仁、劉玟慶

Outline

- Introduction
- Methodology
- Security comparison
- Compression comparison
- Demonstration
- Conclusion

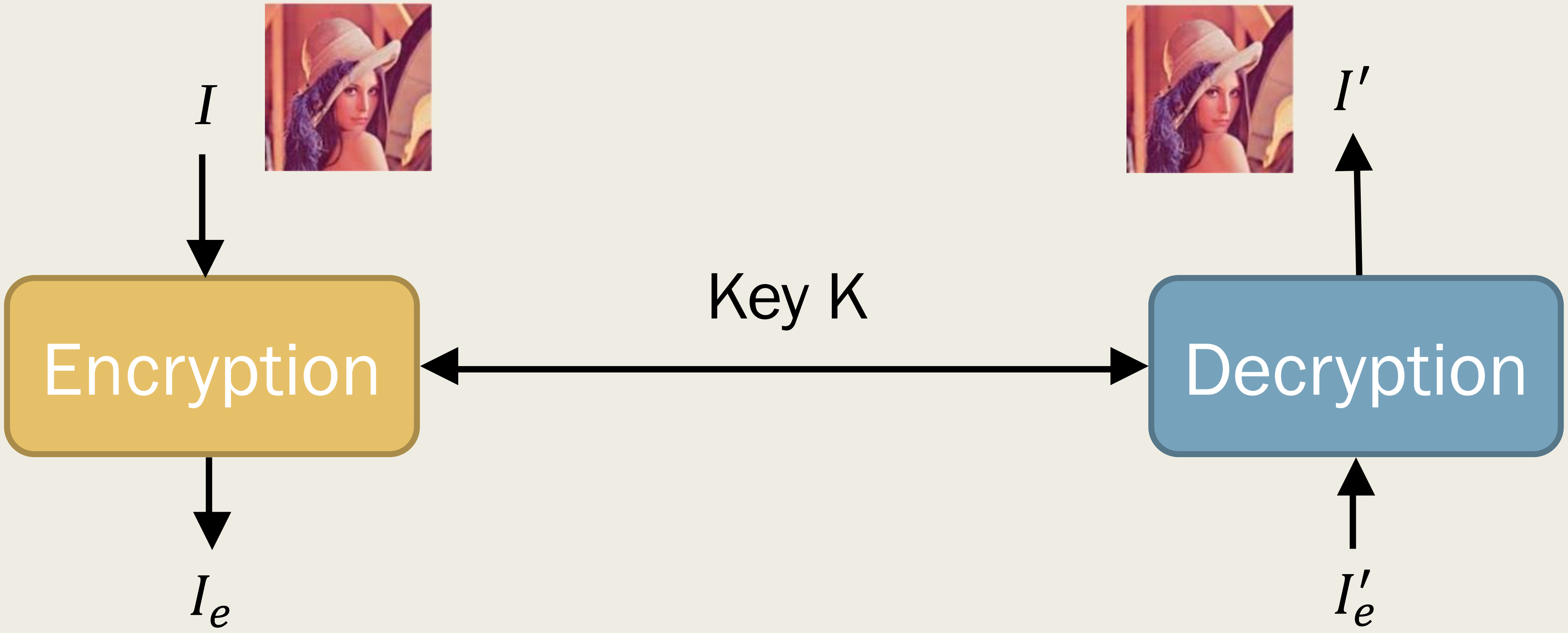
Introduction

- Encrypt then Compress (EtC) system



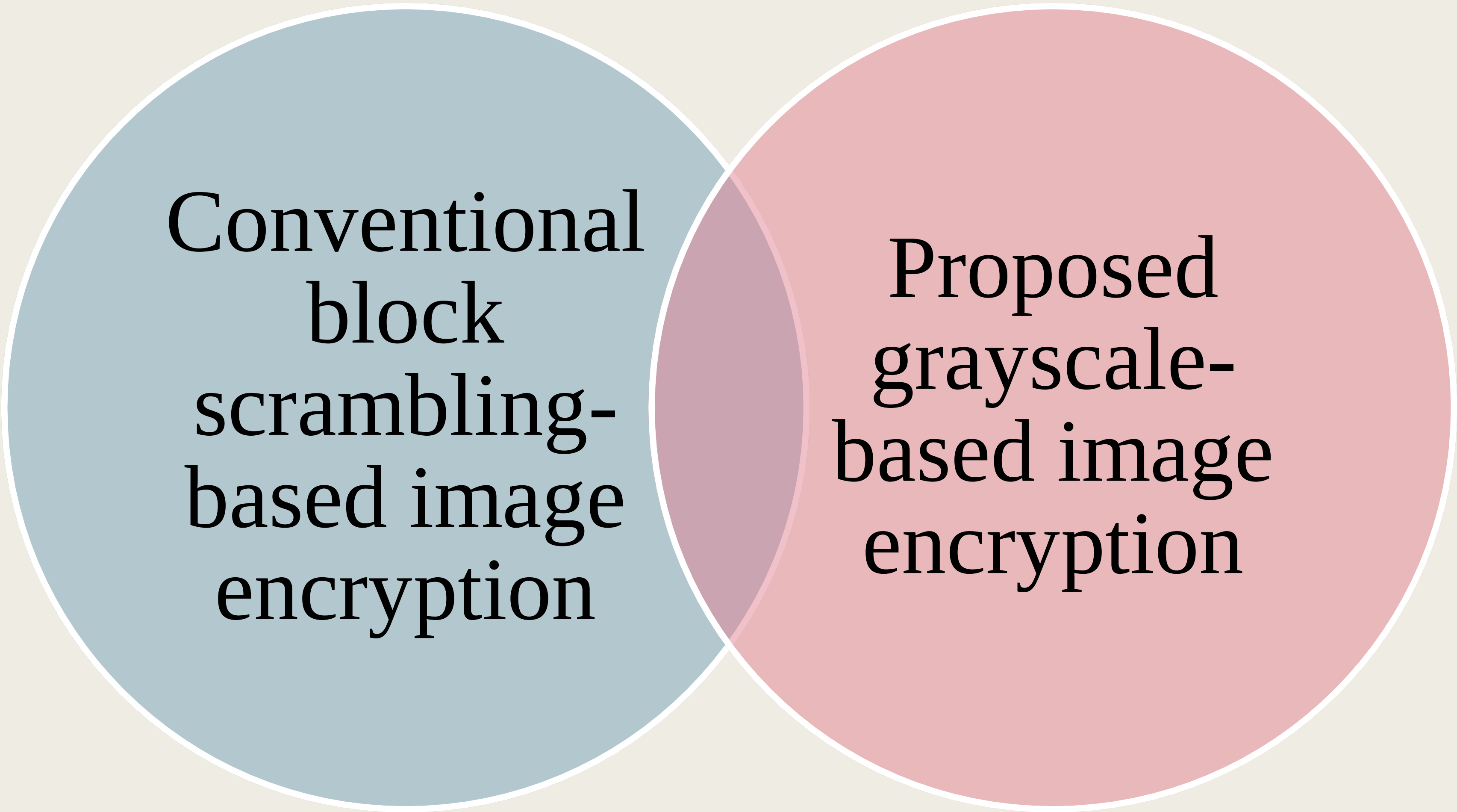
Introduction

- Encrypt then Compress (EtC) system

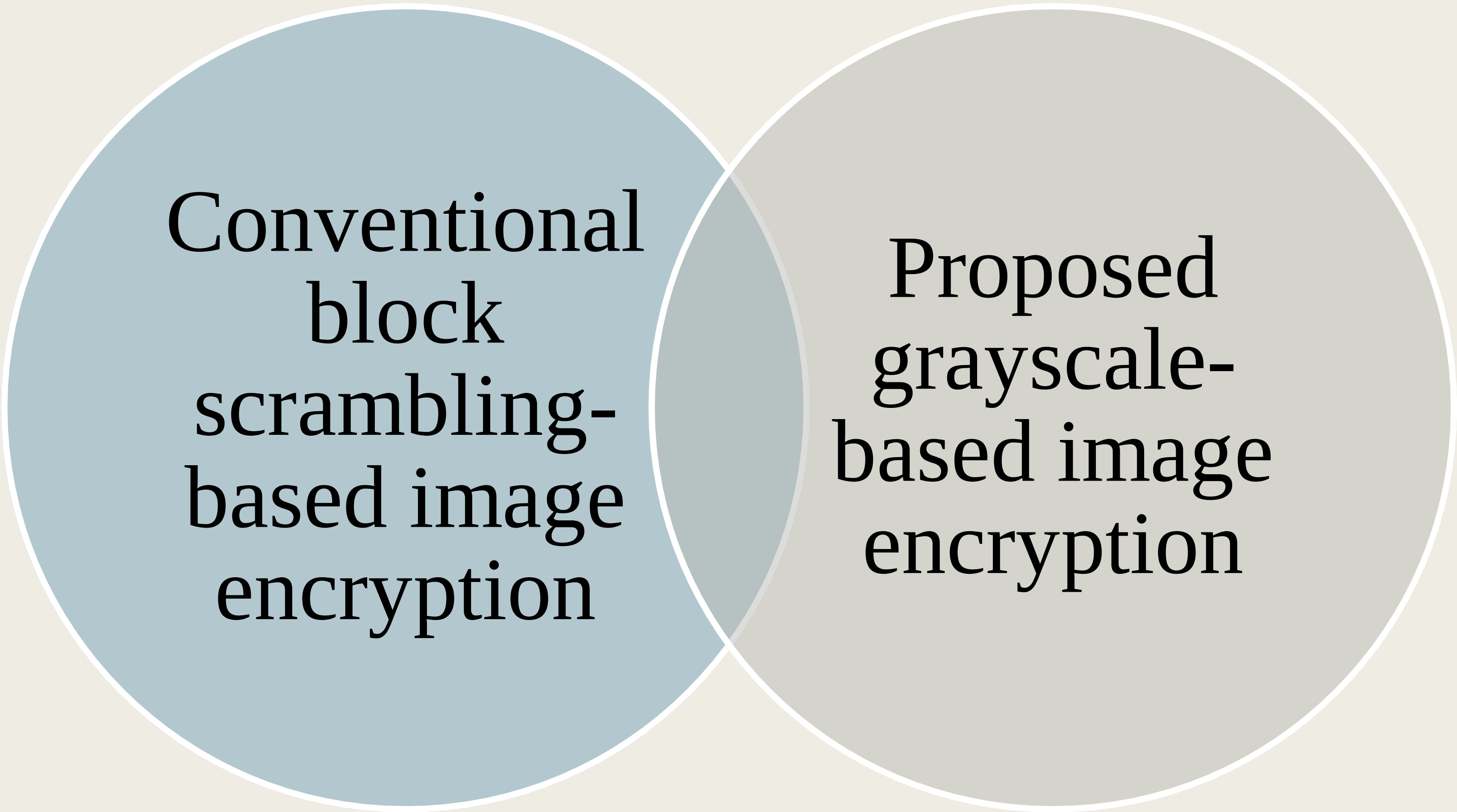


The encryption and decryption algorithm is the main part of the paper

Methodology

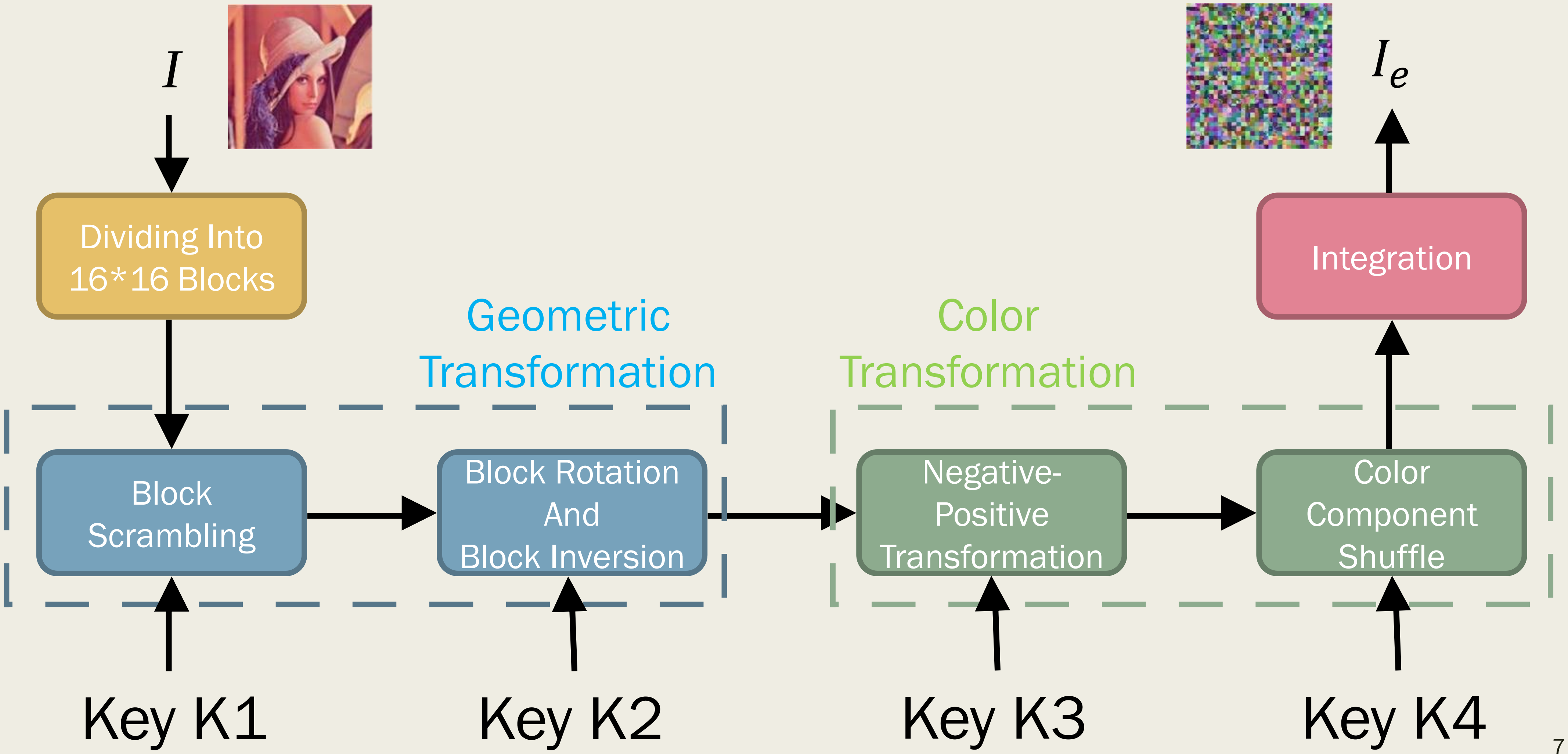


Methodology



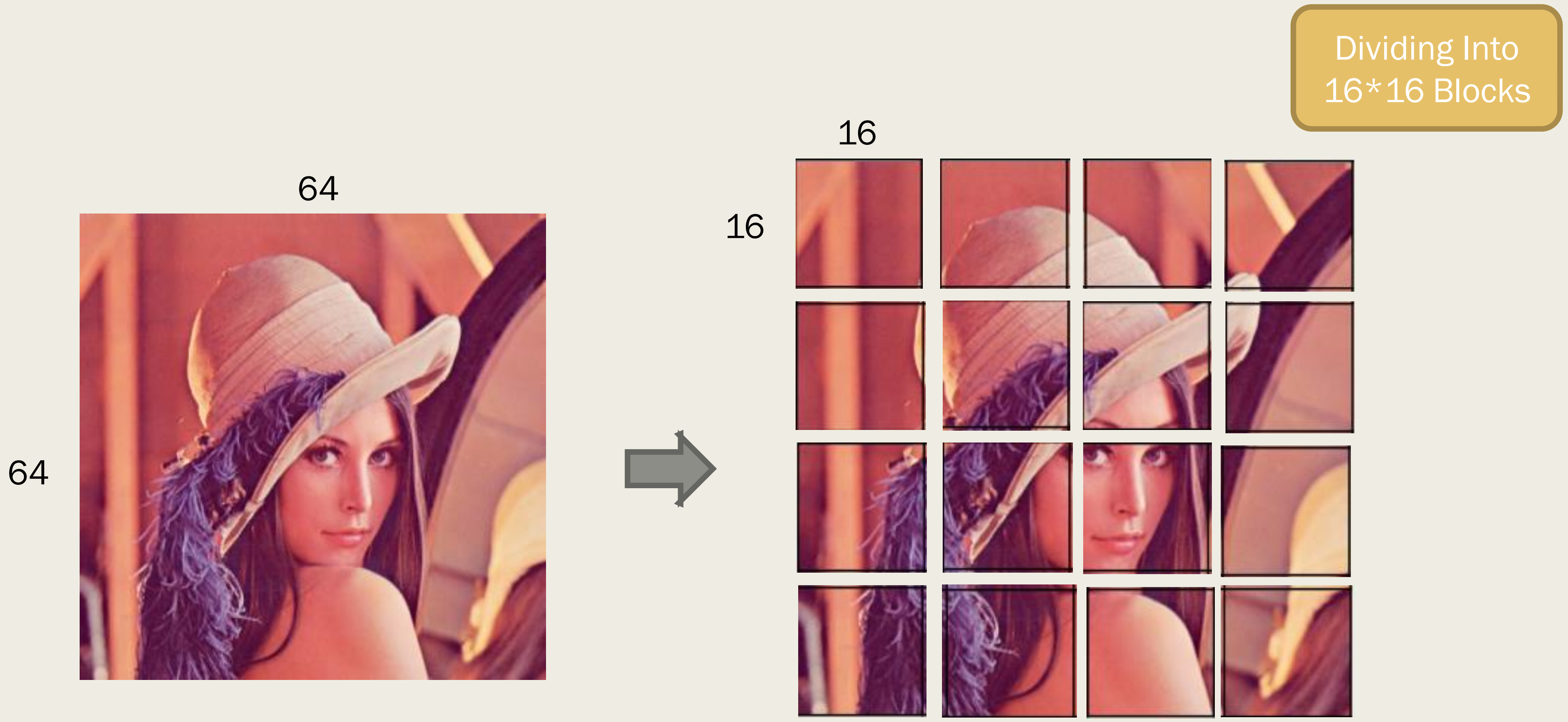
Methodology

- Conventional block scrambling-based image encryption



Methodology

- Conventional block scrambling-based image encryption-Dividing Into 16*16 Blocks

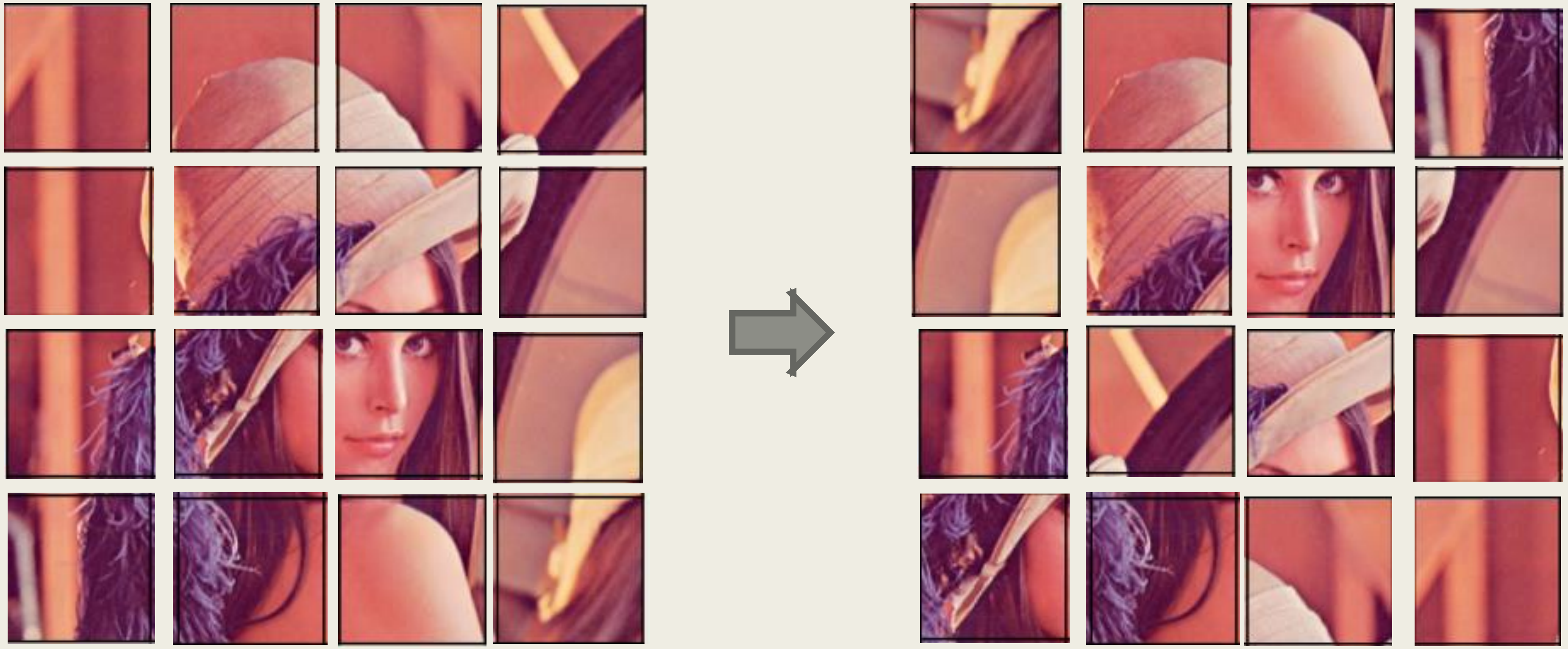


Methodology

- Conventional block scrambling-based image encryption-Block Scrambling

Based on key1 to determine Block Scrambling

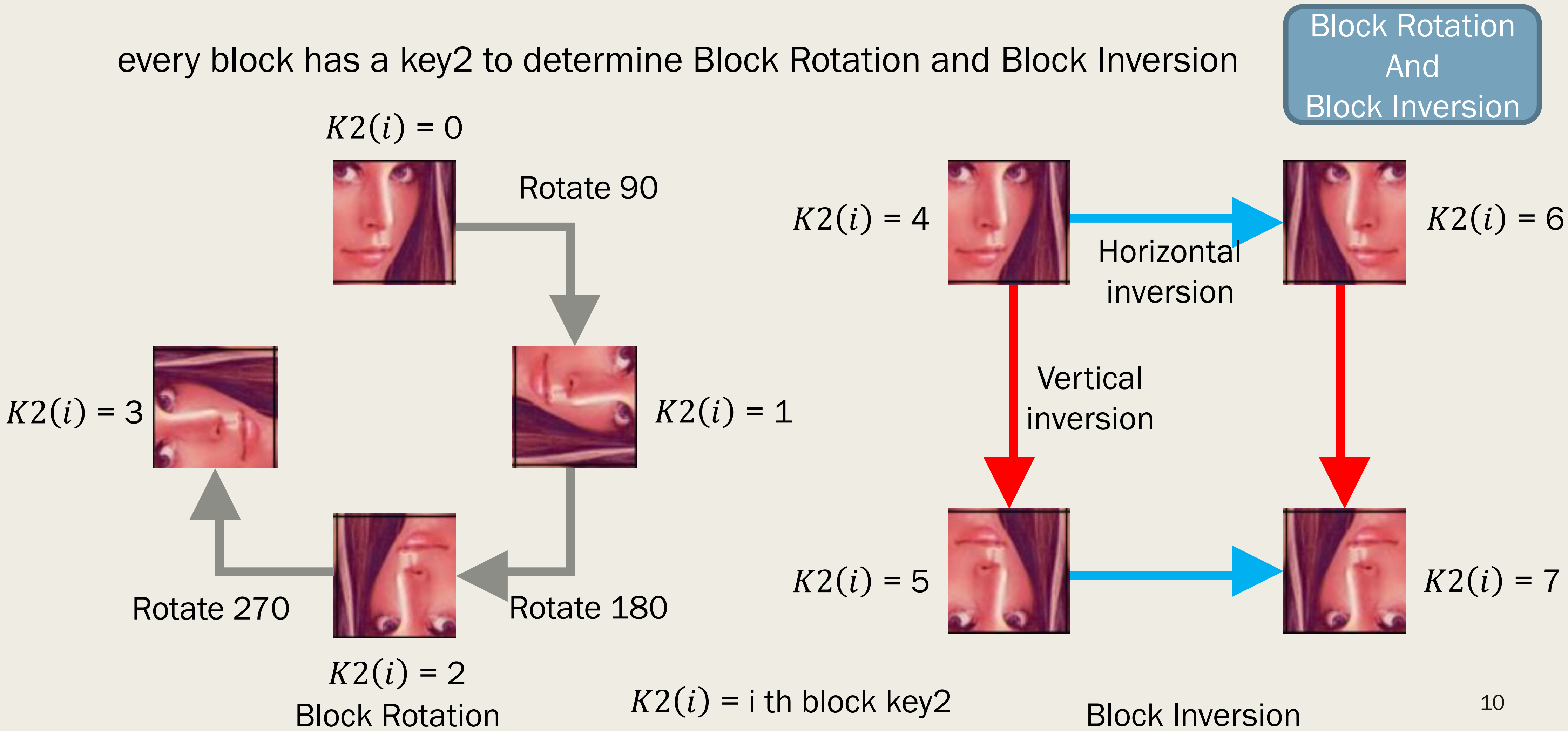
Block Scrambling



Methodology

- Conventional block scrambling-based image encryption-Block Rotation And Block Inversion

every block has a key2 to determine Block Rotation and Block Inversion



$K2(i)$ = i th block key2

Methodology

- Conventional block scrambling-based image encryption-Negative-Positive Transformation

every block has a key3 to determine Negative-Positive Transformation

Negative-Positive Transformation

$$p' \begin{cases} p & if\ K3(i) = 0 \\ p \oplus (2^L - 1) & if\ K3(i) = 1 \end{cases}$$

p' = new pixel value
p = original pixel value
L = how many bits in one pixel
$K3(i)$ = i th block key3

Key 3

Methodology

- Conventional block scrambling-based image encryption-Negative-Positive Transformation

every block has a key3 to determine Negative-Positive Transformation

Negative-Positive Transformation

25	36	48	23
65	89	102	186
65	6	69	86
0	1	174	169

$K3(i) = 0$

25	36	48	23
65	89	102	186
65	6	69	86
0	1	174	169

$K3(i) = 1$

230	219	207	232
190	166	153	69
190	249	186	169
255	254	81	86

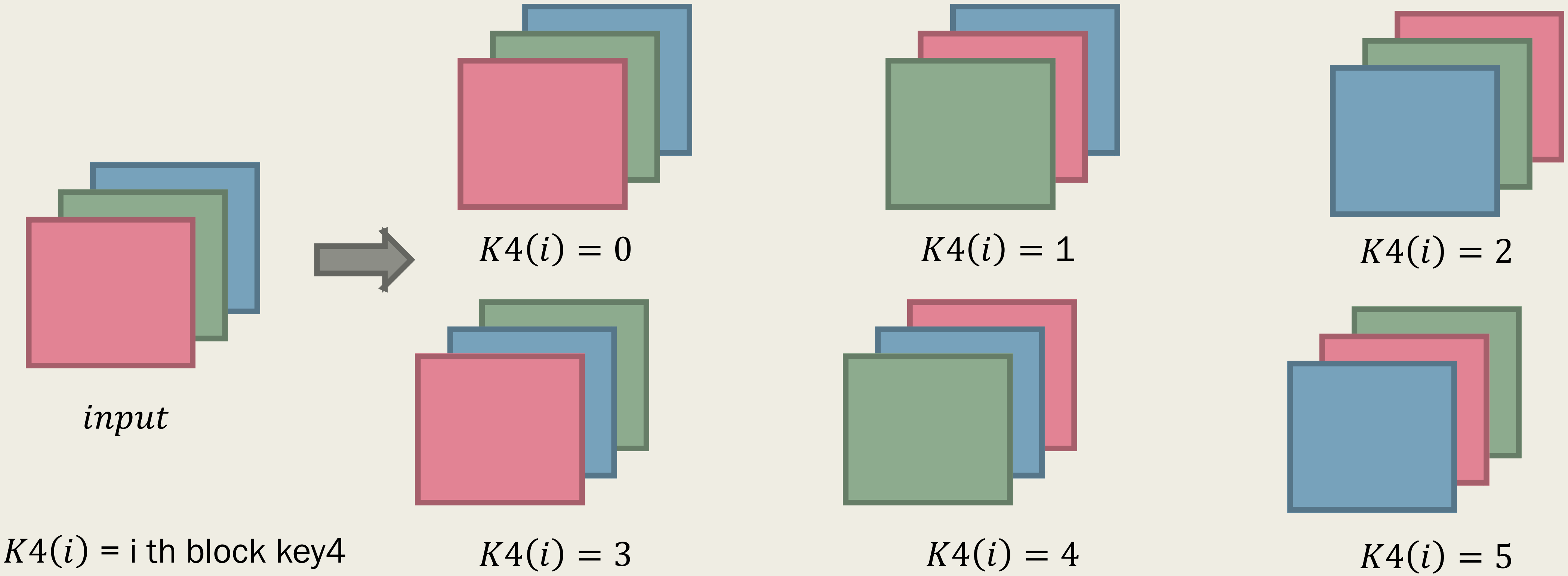
$255 - pixel\ value$

Methodology

- Conventional block scrambling-based image encryption-Color Component Shuffle

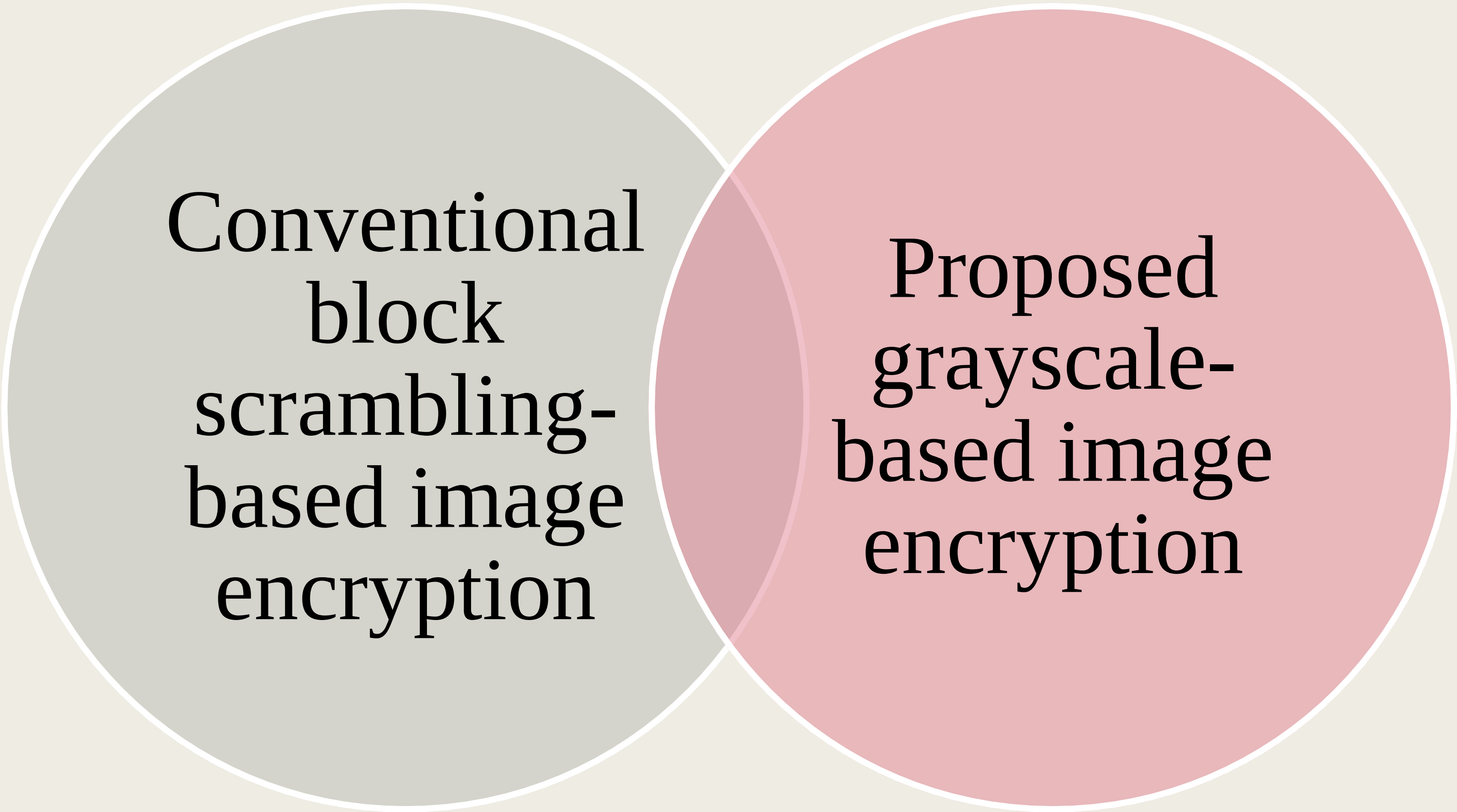
Color Component Shuffle

every block has a key4 to determine Color Component Shuffle



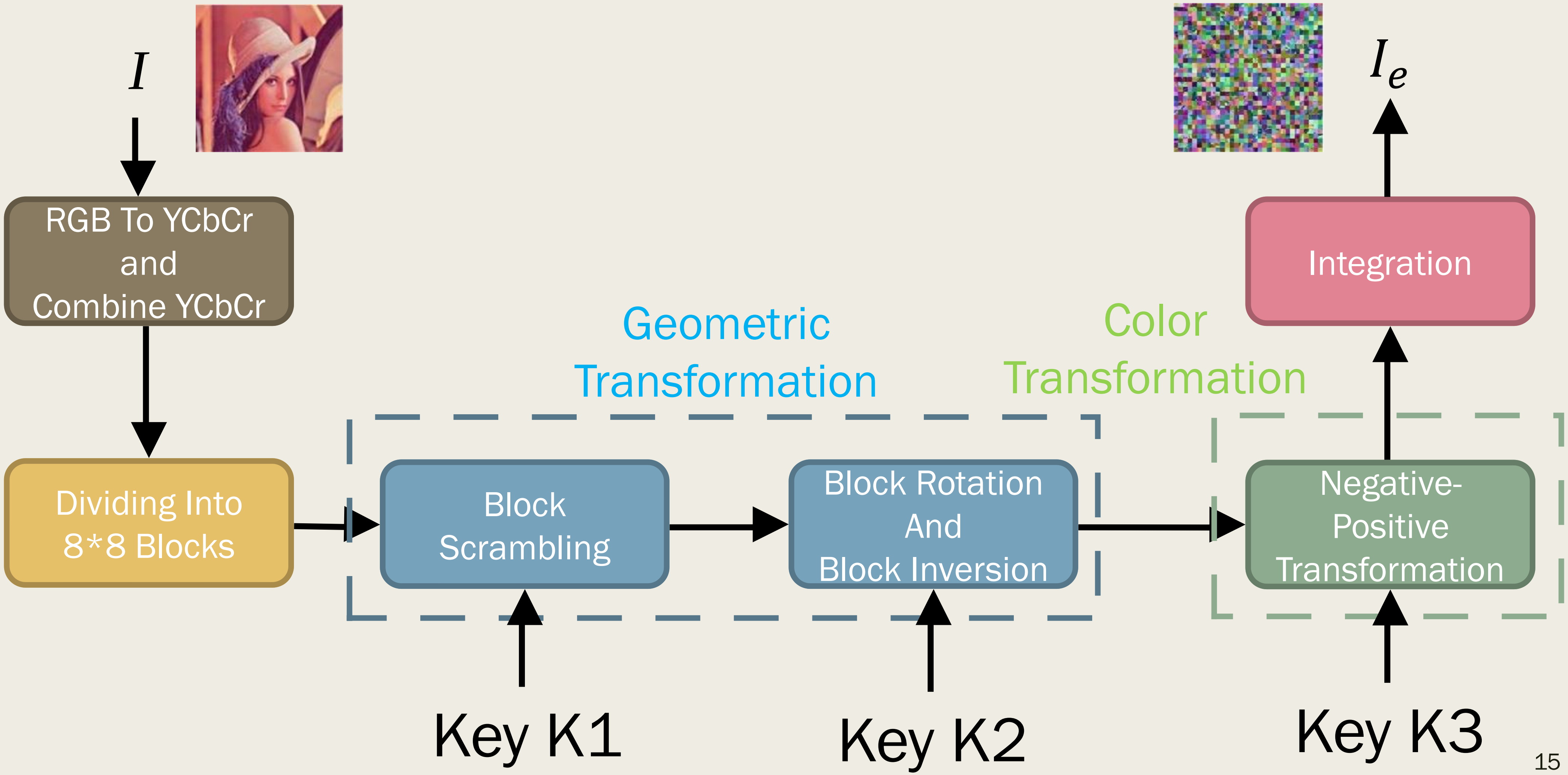
$K4(i)$ = i th block key4

Methodology



Methodology

- Proposed grayscale-based image encryption

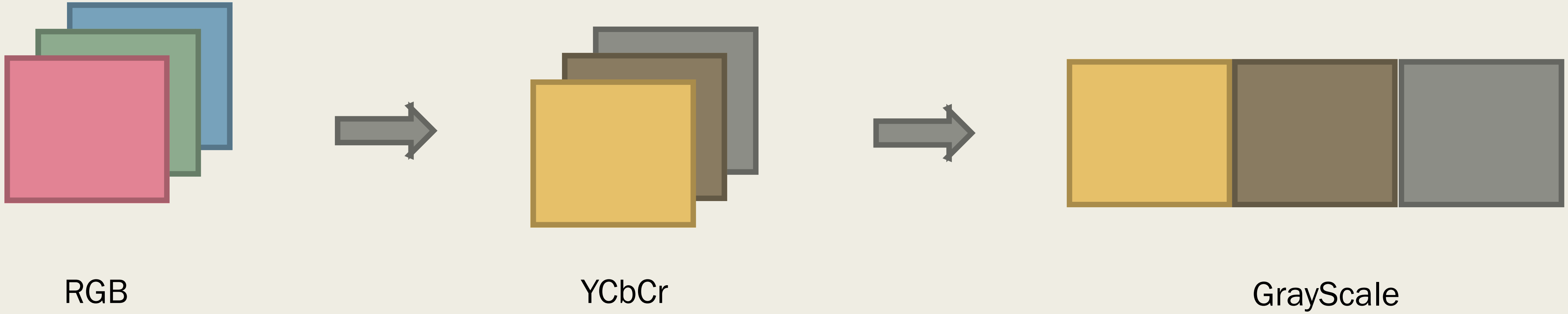


Methodology

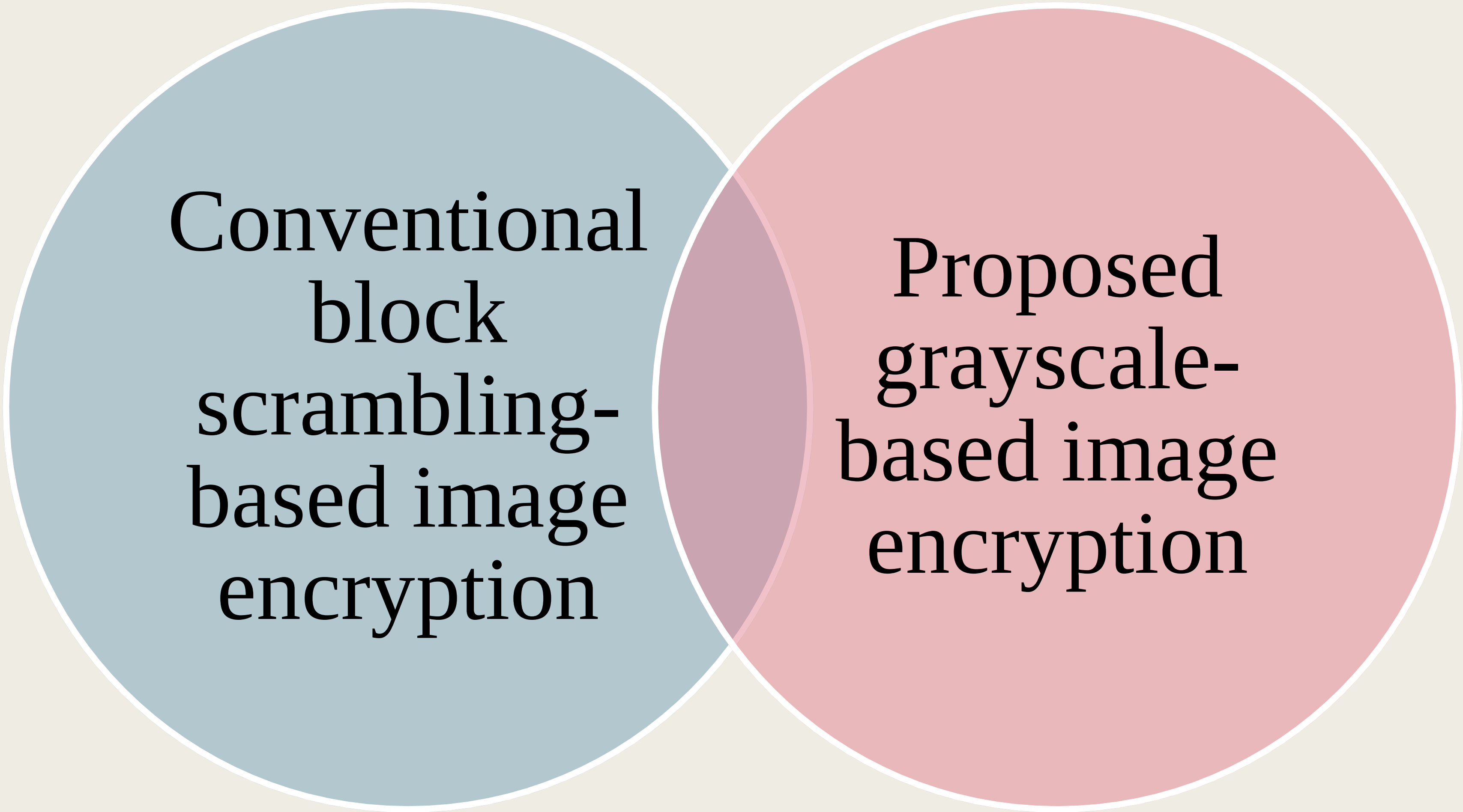
- Proposed grayscale-based image encryption-RGB To YCbCr and Combine YCbCr

RGB To YCbCr
and
Combine YCbCr

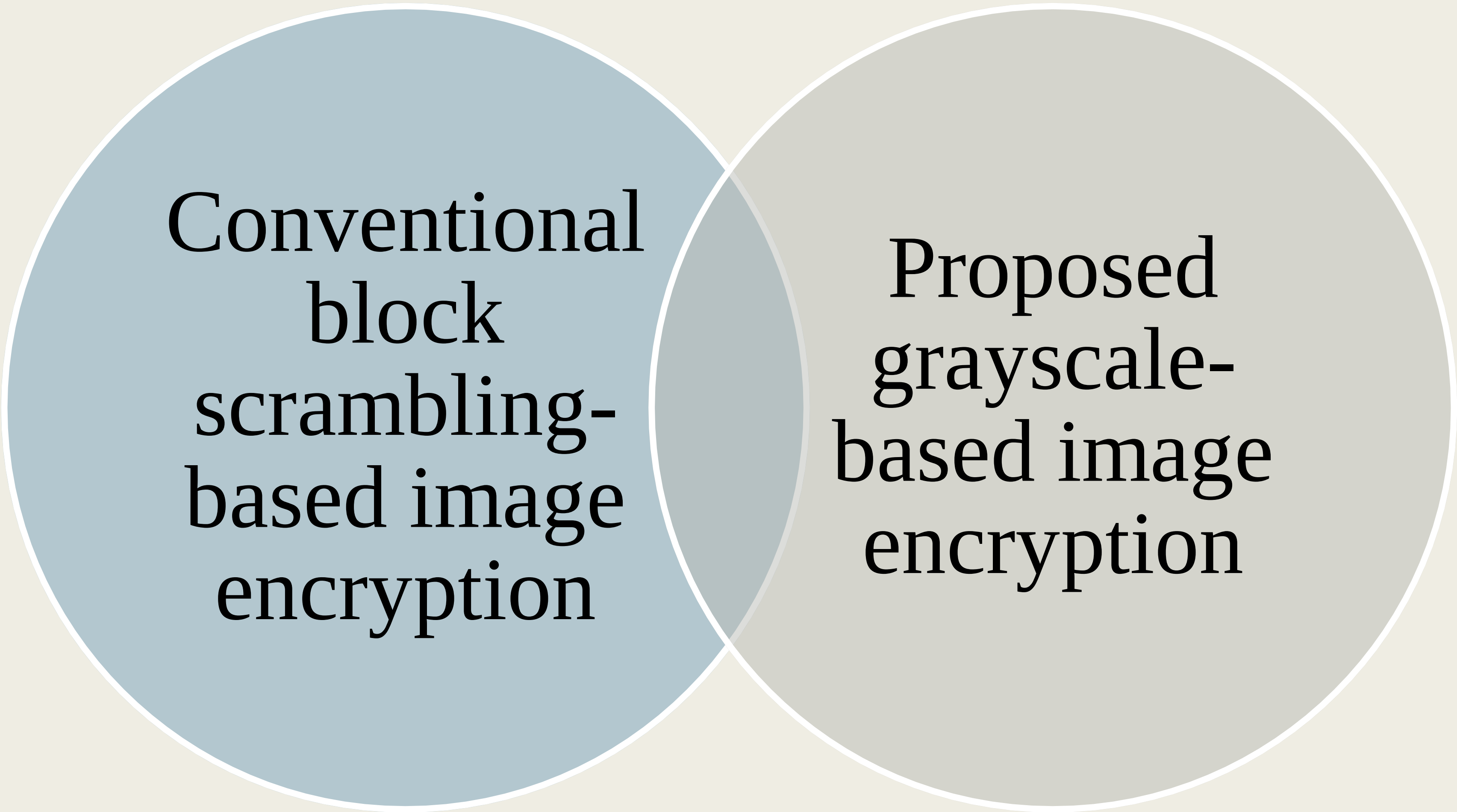
$$
\begin{aligned}
Y &= 0.299 * R + 0.587 * G + 0.114 * B \\
Cb &= -0.1687 * R - 0.3313 * G + 0.5 * B + 128 \\
Cr &= 0.5 * R - 0.4187 * G - 0.0813 * B + 128
\end{aligned}
$$



Security comparison



Security comparison



Security comparison

- Brute-force Attack in Conventional block scrambling-based image encryption

If an image with X × Y pixels is divided into blocks with Bx×By pixels, the number of blocks n is given by

$$\mathrm{n} = \frac{X}{B_x} \times \frac{Y}{B_y}$$

The key space of the block scrambling (Step 1) N_s(n) will be

$$N_s(\mathrm{n}) = \mathrm{n}!$$

The key space of the Block Rotation and Block Inversion (Step 2) $N_{R\&I}$(n) will be

$$N_R(\mathrm{n}) = 4^n,\ N_I(\mathrm{n}) = 4^n,\ N_{R\&I}(\mathrm{n}) = 8^n$$

Security comparison

- Brute-force Attack in Conventional block scrambling-based image encryption

The key space of the Negative-Positive Transformation (Step 3) N_N(n) will be

$$N_N(\mathrm{n}) = 2^n$$

The key space of the Color Component Shuffle (Step 4) N_C(n) will be

$$N_C(\mathrm{n}) = 6^n$$

The key space of total N_A(n) will be

$$N_A(\mathrm{n}) = \mathrm{n}! \times 8^n \times 2^n \times 6^n$$

Security comparison

Conventional block scrambling-based image encryption

Proposed grayscale-based image encryption

Security comparison

- Brute-force Attack in Proposed grayscale-based image encryption

If an image with X × Y pixels is divided into blocks with Bx×By pixels, the number of blocks n is given by

$$\mathrm{n} = \frac{X}{B_x} \times \frac{Y}{B_y}$$

The key space of the block scrambling (Step 1) N_s(n) will be

$$N_s(\mathrm{n}) = 3\mathrm{n}!$$

The key space of the Block Rotation and Block Inversion (Step 2) $N_{R\&I}$(n) will be

$$N_R(\mathrm{n}) = 4^{3n},\ N_I(\mathrm{n}) = 4^{3n},\ N_{R\&I}(\mathrm{n}) = 8^{3n}$$

Security comparison

- Brute-force Attack in Proposed grayscale-based image encryption

The key space of the Negative-Positive Transformation (Step 3) N_N(n) will be

$$N_N(\mathrm{n}) = 2^{3n}$$

The key space of total N_B(n) will be

$$N_B(\mathrm{n}) = 3\mathrm{n}! \times 8^{3n} \times 2^{3n}$$

Security comparison

- Brute-force Attack in comparison

The key space of conventional $N_A(n)$ is

$$N_A(\text{n}) = \text{n}! \times 8^n \times 2^n \times 6^n$$
$$= \text{n}! \times 2^{4n} \times 6^n$$

The key space of proposed N_B(n) is

$$N_B(\text{n}) = 3\text{n}! \times 8^{3n} \times 2^{3n}$$
$$= 3\text{n}! \times 2^{9n} \times 9^n$$

$$3\text{n}! \times 2^{9n} \times 9^n \gg \text{n}! \times 2^{4n} \times 6^n$$

$$\text{proposed } N_B(\text{n}) \gg \text{conventional } N_A(n)$$

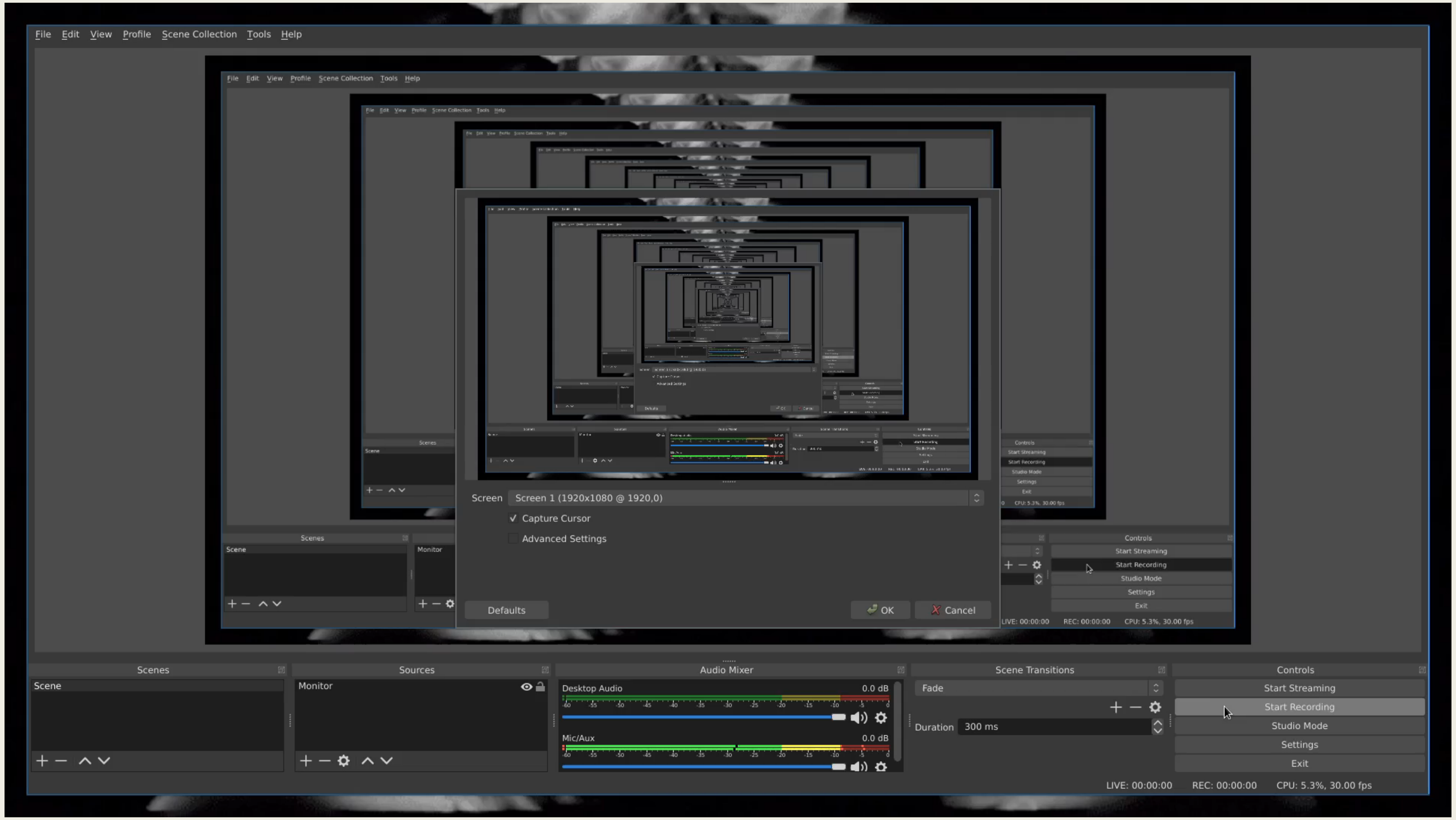
Compression comparison

- PSNR values of non-encrypted and decrypted images after uploading and downloading from Facebook. Boldface indicates highest score per Q_{fu}.

	Uploaded JPEG files		Q_{fu}		
	Sub-sampling ratio	Quantization table	90	95	100
Non-encrypted	4:2:0	Luminance	32.1	32.4	32.4
	4:4:4	Chrominance	32.2	32.3	32.5
Conventional scheme	4:2:0	Luminance	31.0	31.0	31.0
	4:4:4	Chrominance	31.6	31.6	31.7
Proposed scheme	(Grayscale)	Luminance	33.7	**33.8**	**33.8**
		Chrominance	32.6	33.4	**33.8**

Demonstration

- Demonstration



http://140.112.41.71:8000/

Conclusion

- This paper proposed a novel block-scrambling image encryption scheme that enhances the security of EtC systems for JPEG images.
- the proposed scheme enables us to use Bx = By = 8 as a block size, which enhances robustness against ciphertext-only attacks.
- The proposed scheme makes it possible to avoid the effect of the interpolation on social media due to the use of grayscale-based images.
- the proposed scheme has a better performance than the conventional one in terms of the image quality