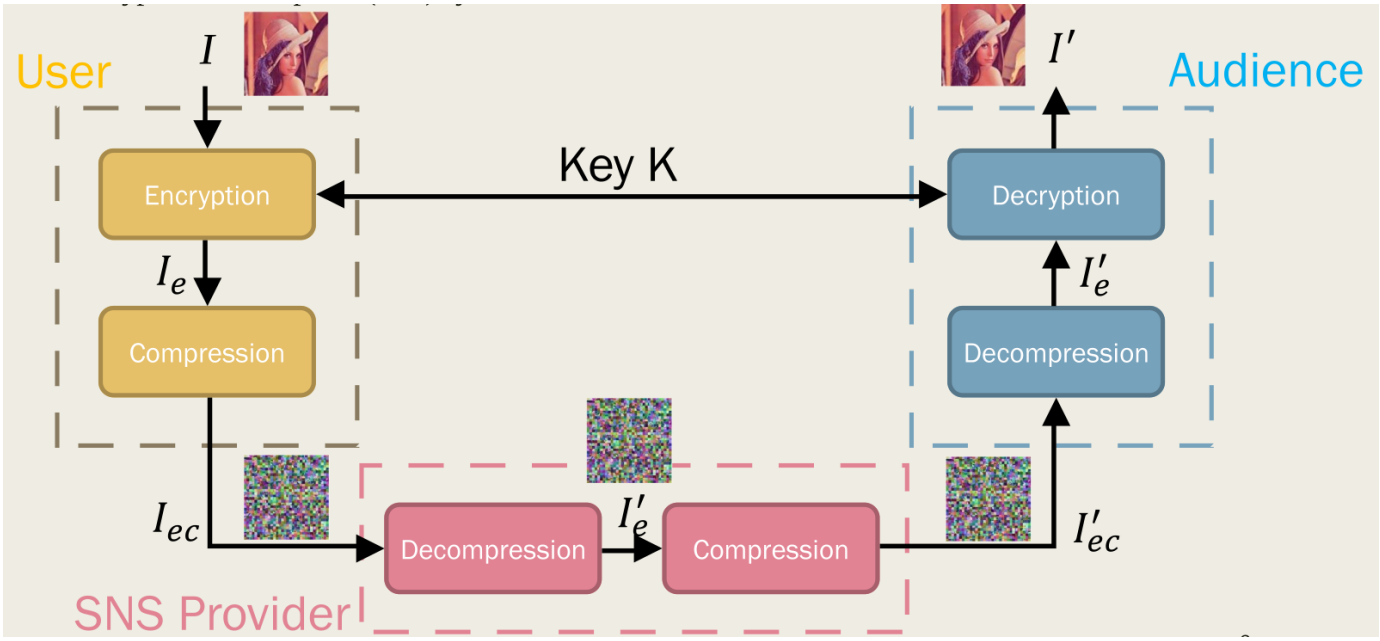
Encryption-then-Compression Systems using Grayscale-based Image Encryption for JPEG Images

Team: B6
Members: 陳宏彥，劉玟慶，劉正仁
Student IDs: R08942066, R08942080, R08942071

Introduction

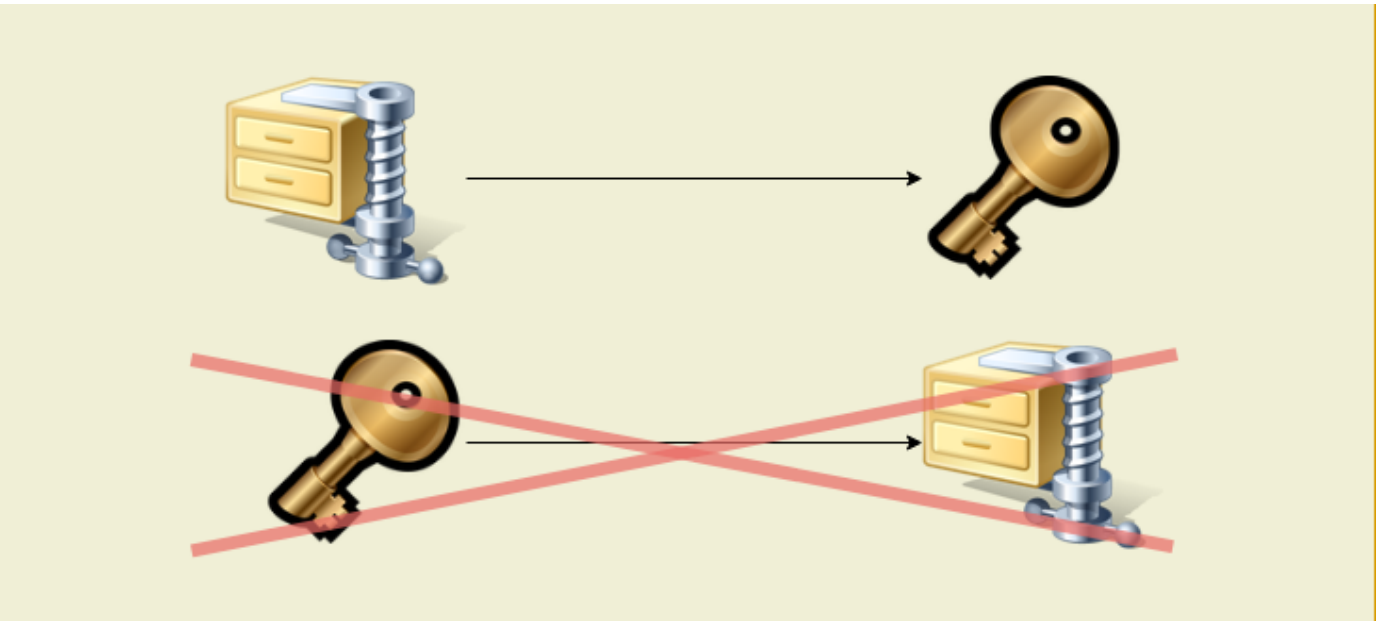
This paper proposed a novel block-scrambling image encryption scheme that enhances the security of EtC systems for JPEG images. Following diagram illustrates the pipeline of encryting and descryting an image in a general EtC system.



Motivation

Regarding whether data should be compressed first and then encrypted, or data should be first encrypted and then compressed, most of the people adopt compressed-first-then-encrypted scheme. Because most encryption algorithms will transform data into random-like sequence, therefore the correlation between data points would be low. As a consequence, the effect of compression would be bad when applying compression algorithms, such as

arithmetic coding-based approach or singular value decomposition transformation, to random-like sequence.



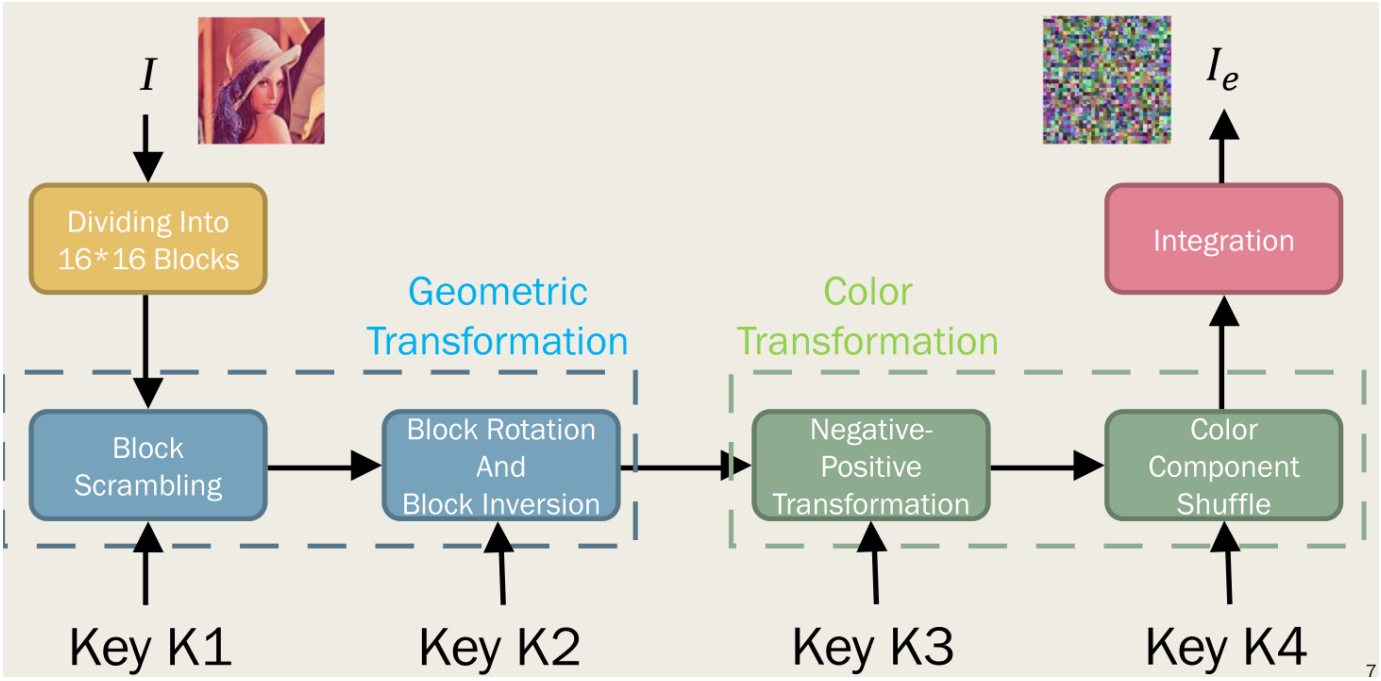
There are two reasons why this paper using block-scrambling encryption scheme. One reason is that image encryption prior to image compression is required in certain practical scenarios such as secure image transmission through an untrusted channel provider. Therefore, this paper use block-scrambling encryption scheme so that the encrypted data is not a good candidate of random-like data. As a consequence, the effect of compression would not so bad. The other reason is that block-scrambling based image encryption schemes are compatible with international compression standards, such as JPEG. Due to the popularity of JPEG formatted images on the Internet, this paper choose block-scrambling based image encryption shceme.

Methodology

In this section, we review conventional encryption schemes used in EtC systems, and analyze the proposed grayscale-based encryption and its security enhancement.

Conventional block-scrambling based image encryption

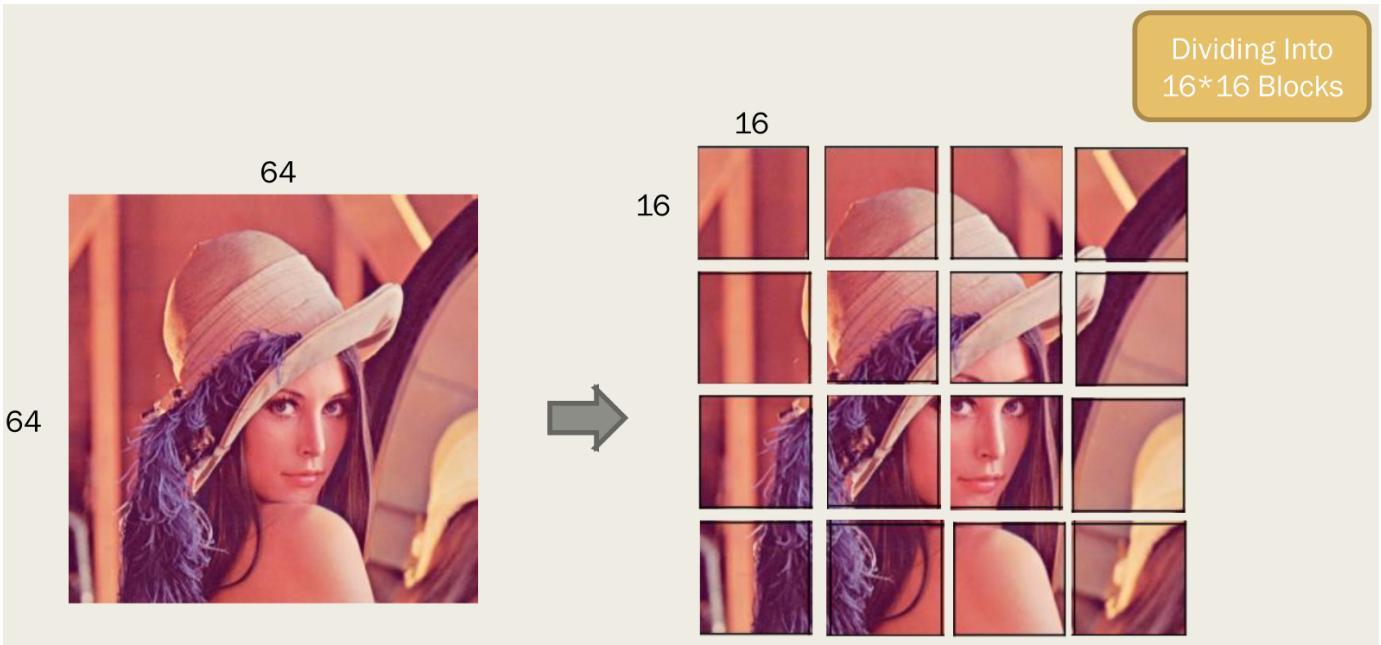
Following diagram is the pipeline of conventional block-scrambling based image encryption



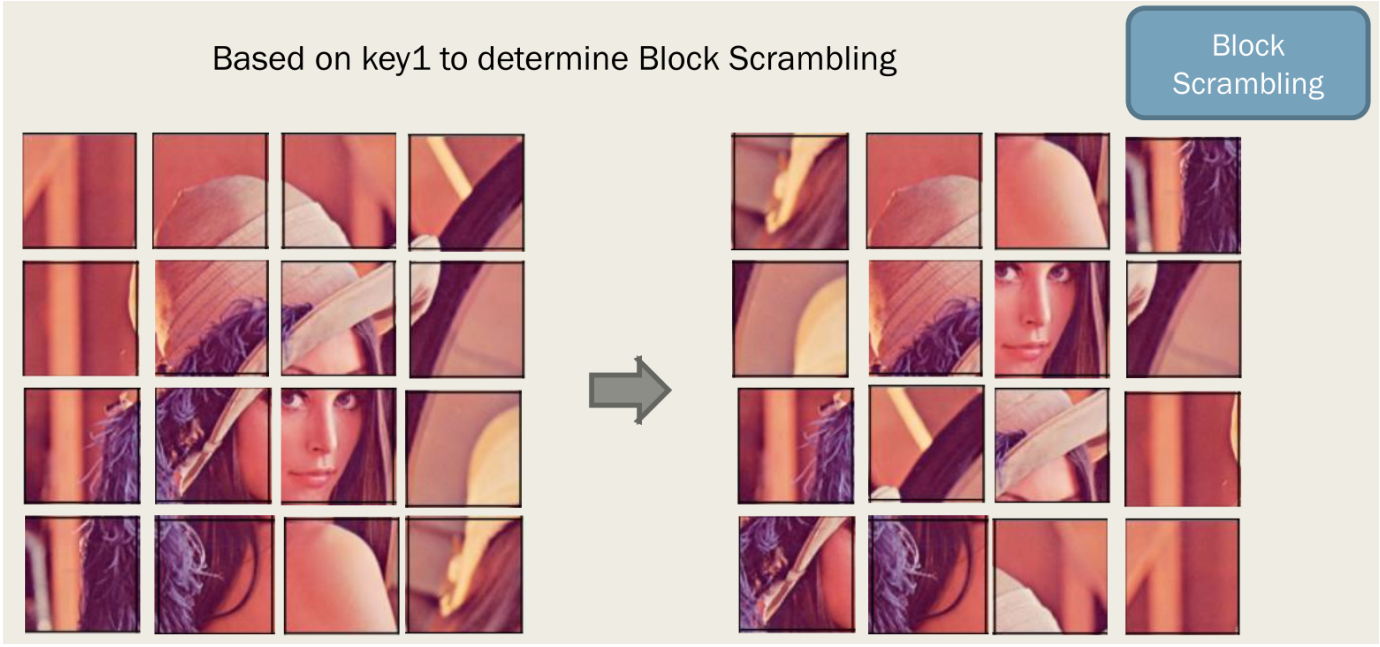
We will explore all the steps one by one with illustration:

1. Dividing into 16x16 blocks
2. Block scrambling
3. Block rotation and block inversion
4. Negative-positive transformation
5. Color component shuffle

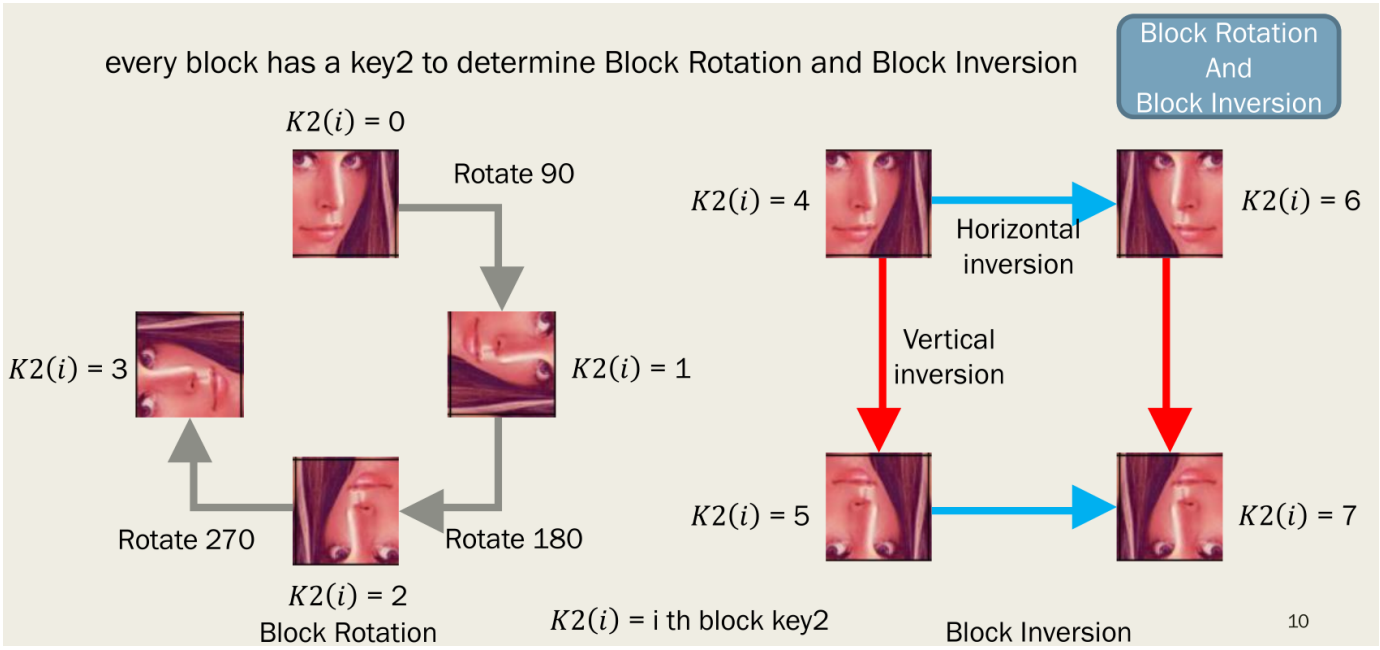
Dividing into 16x16 blocks



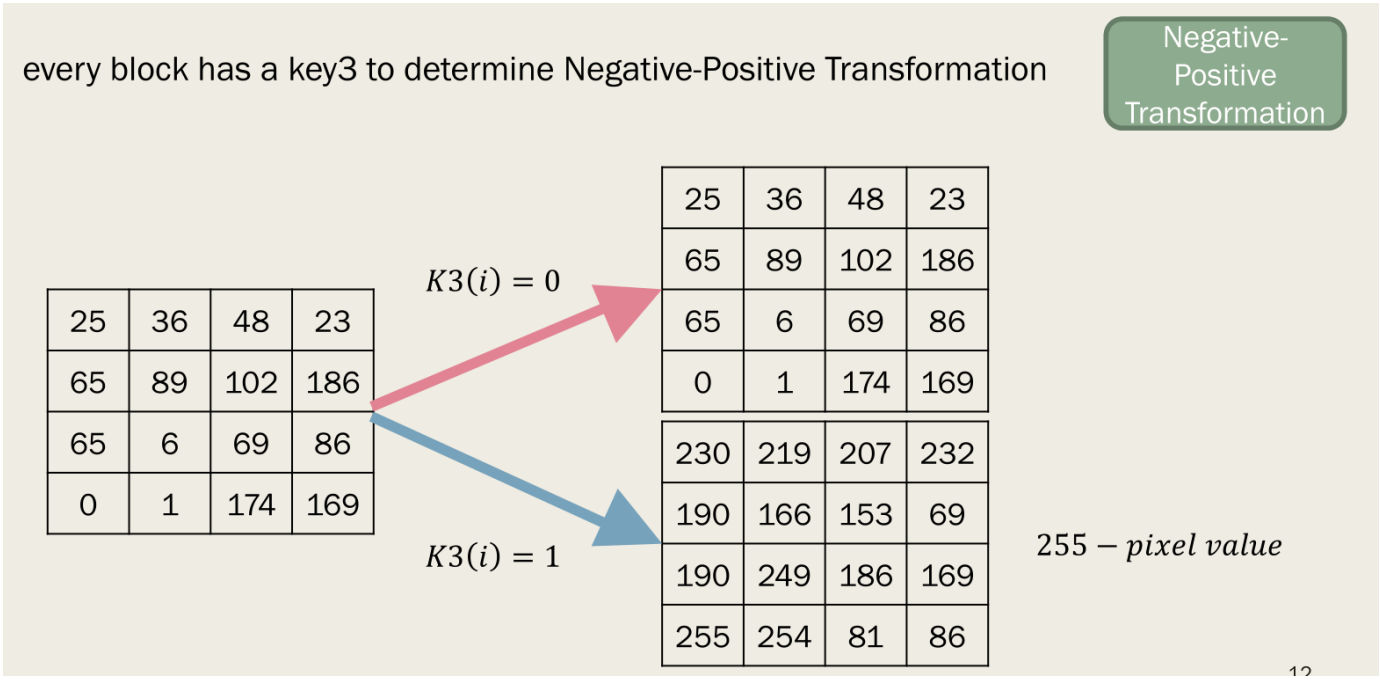
Block scrambling



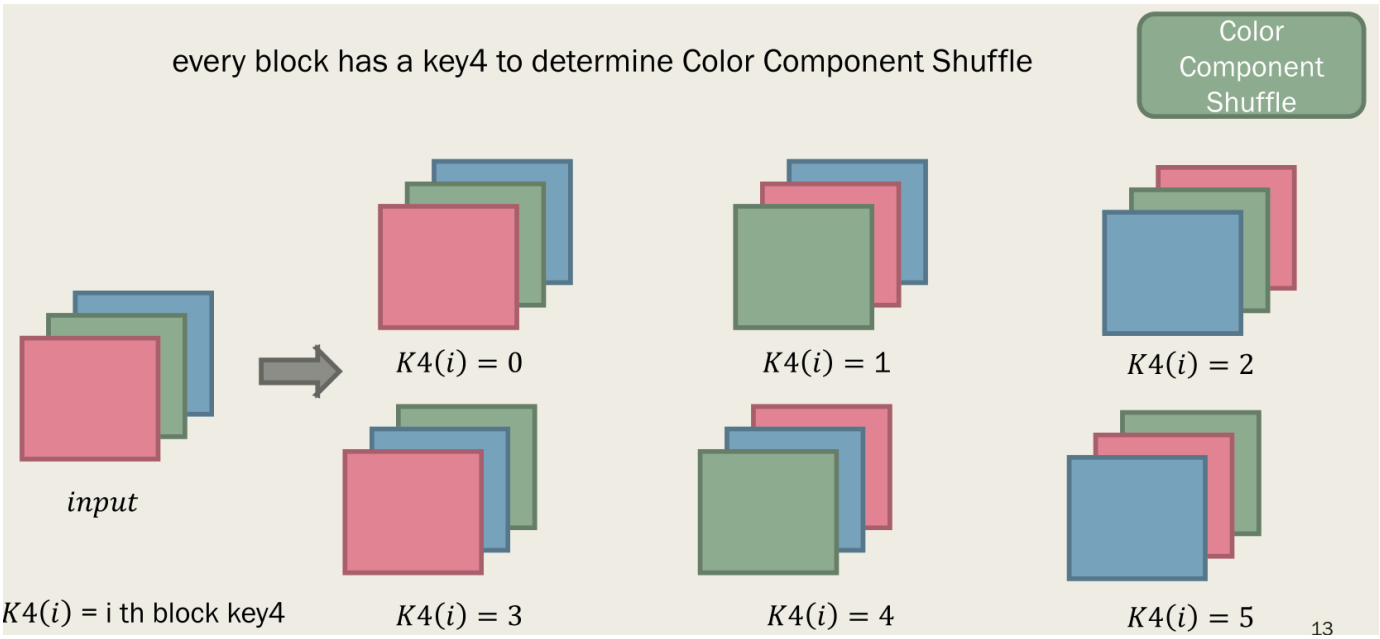
Block rotation and block inversion



Negative-positive transformation

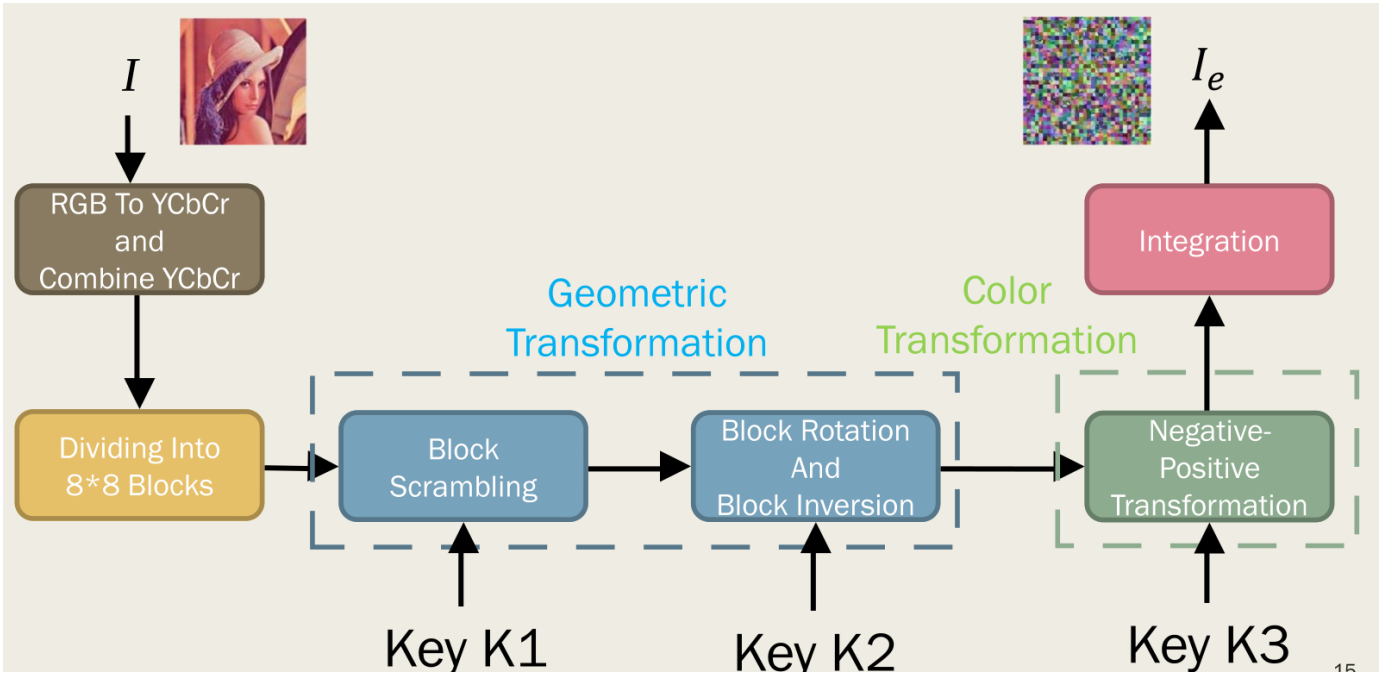


Color component shuffle

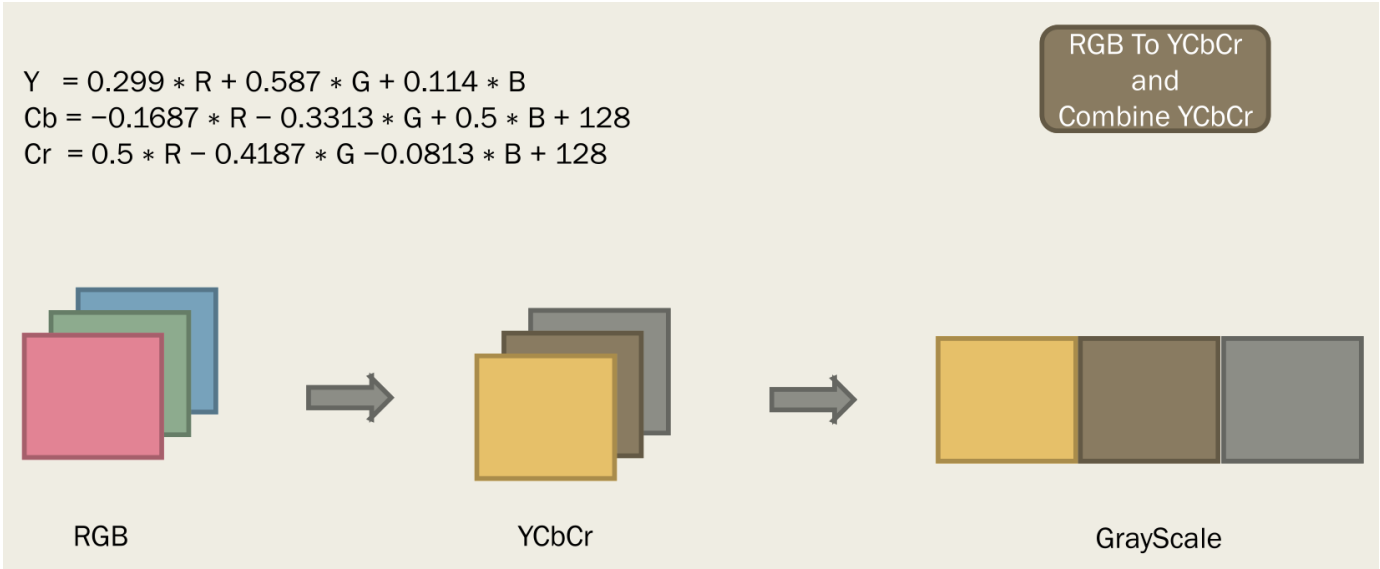


Proposed grayscale-based image encryption

The difference between the proposed method and the conventional one is that the proposed method divides image into more blocks, and it transforms the original RGB 3-channels image to a YCbCr 1-channel image, which is grayscale.



RGB to YCbCr transformation



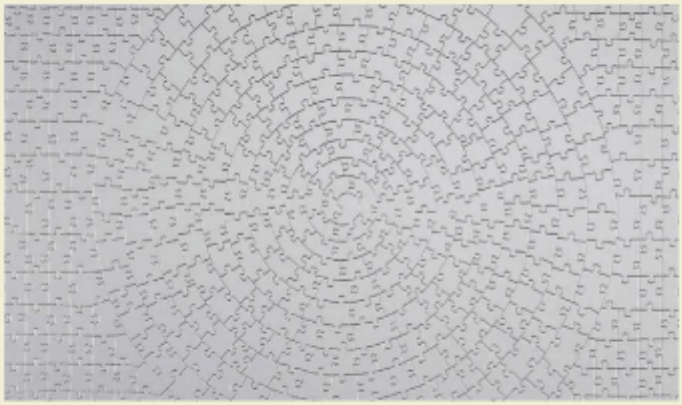
Security Comparison

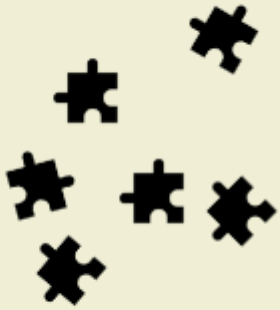
Before talking about the security of these two methods, we need to know how would a malicious one trying to attack the system. There are two ways someone can adopt to attack the system:

1. Brute-force attack
2. Jigsaw puzzle attack

As the malicious party already knew the encryption and decryption algorithm, it will adopt brute-force attack to try to find the possible key from the key space. Therefore, the key space should be large enough so that the system is computationally unbreakable.

After applying these two block-scrambling based encryption methods, recovering the encrypted image to its original one is like a jigsaw puzzle game. Therefore, the more the puzzle pieces, the harder it is to break the jigsaw puzzle game. Moreover, the less color information the puzzle piece reveals, the harder it is to place the pieces to the right place in the jigsaw.





Key space analysis

Conventional block scrambling-based image encryption

If an image with $X \times Y$ pixels is divided into blocks with $B_x \times B_y$ pixels, the number of blocks n is given by:

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

The key space of the block scrambling (Step1) $N_s(n)$ will be:

$$N_s(n) = n!$$

The key space of the block rotation and block inversion (Step2) $N_{R\&I}(n)$ will be:

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

The key space of the Negative-Positive transformation (Step3) $N_N(n)$ will be:

$$N_N(n) = 2^n$$

The key space of the color component shuffle (Step4) $N_C(n)$ will be

$$N_C(n) = 6^n$$

The key space of total $N_A(n)$ will be

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

Proposed grayscale-based image encryption

If an image with $X \times Y$ pixels is divided into blocks with $B_x \times B_y$ pixels, the number of blocks n is given by:

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

The key space of the block scrambling (Step1) $N_s(n)$ will be:

$$N_s(n) = 3n!$$

The key space of the block rotation and block inversion (Step2) $N_{R\&I}(n)$ will be:

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

The key space of the Negative-Positive transformation (Step3) $N_N(n)$ will be:

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

The key space of total $N_A(n)$ will be

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

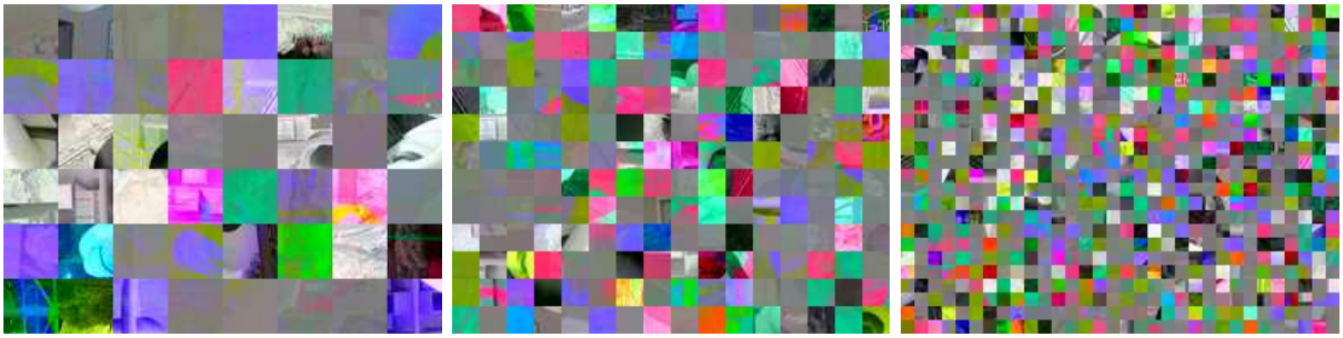
Jigsaw puzzle analysis

In conventional scheme, the malicious one can assemble the encrypted image to original one based on the color information of each block. You can see from the diagram bellow, as the proposed method transform RGB image to a YCbCr grayscale image, the assembled

image is not recovered well.

(a) Original image ($X \times Y = 256 \times 192$)
(b) Assembled image (Conventional scheme, $B_x = B_y = 16$,
(c) Assembled image (Grayscale, $B_x = B_y = 16$,

It is trivial that if there are more puzzle pieces, the malicious one will more difficult to deal with the jigsaw puzzle. In contrary to the conventional block-scrambling encryption method, the proposed one can divide the image into more blocks, which means more puzzle pieces. Therefore, it is more difficult to solve the jigsaw in the proposed encryption method.



(a) Assembled image (Proposed, $B_x = B_y = 32$,
(b) Assembled image (Proposed, $B_x = B_y = 16$,
(c) Assembled image (Proposed, $B_x = B_y = 8$,

Compression Comparison

PSNR values of non-encrpted and descrypted images after uploading and downloading form 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**

Conclusion

- This paper proposed a novel block-scrambling image encrpytion scheme that enhances the enhances that security EtC systems for JPEG images.
- The proposed scheme enables us to use smaller 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.