DCC 2022，22-25 March

Compressing Cipher Images by Using Semi-tensor Product Compressed Sensing and Pre-mapping

Bo Zhang*, Di Xiao+, Hui Huang+, and Jia Liang+

*Army Engineering University, + Chongqing University

Bo Zhang(张波)

Army Engineering University

Outline

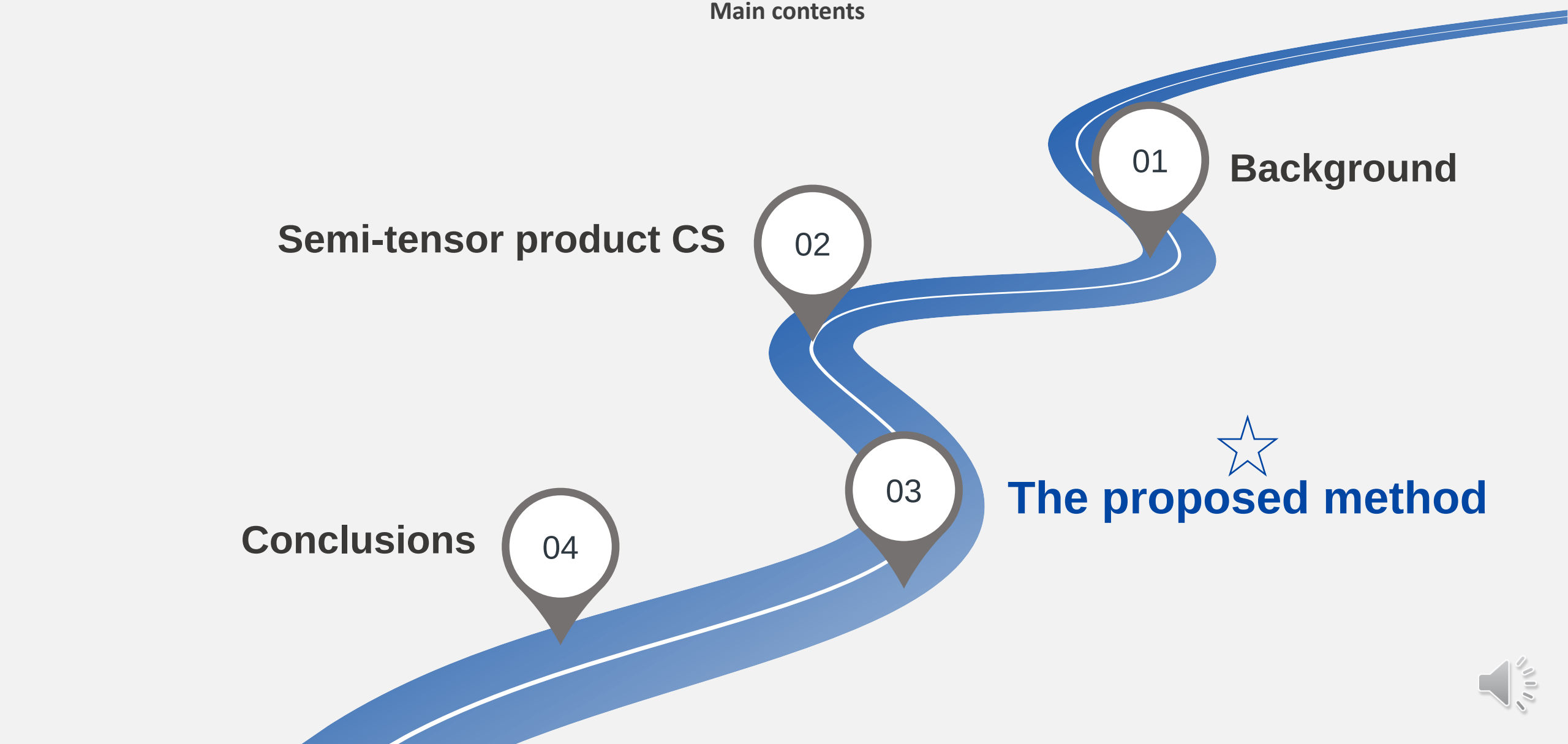
Main contents

01 Background

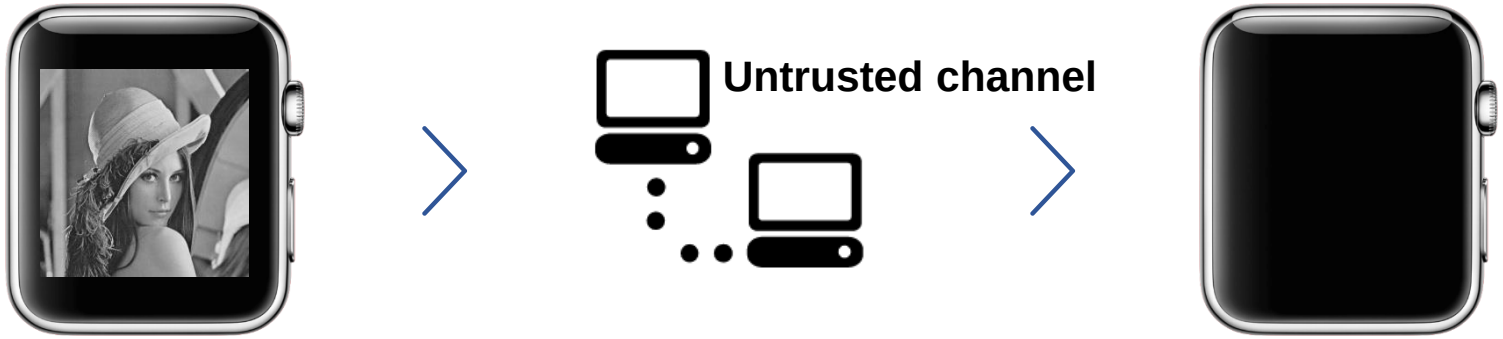
02 Semi-tensor product CS

03 The proposed method

04 Conclusions



- Part 1 **Background Story**



Alice Charlie Bob

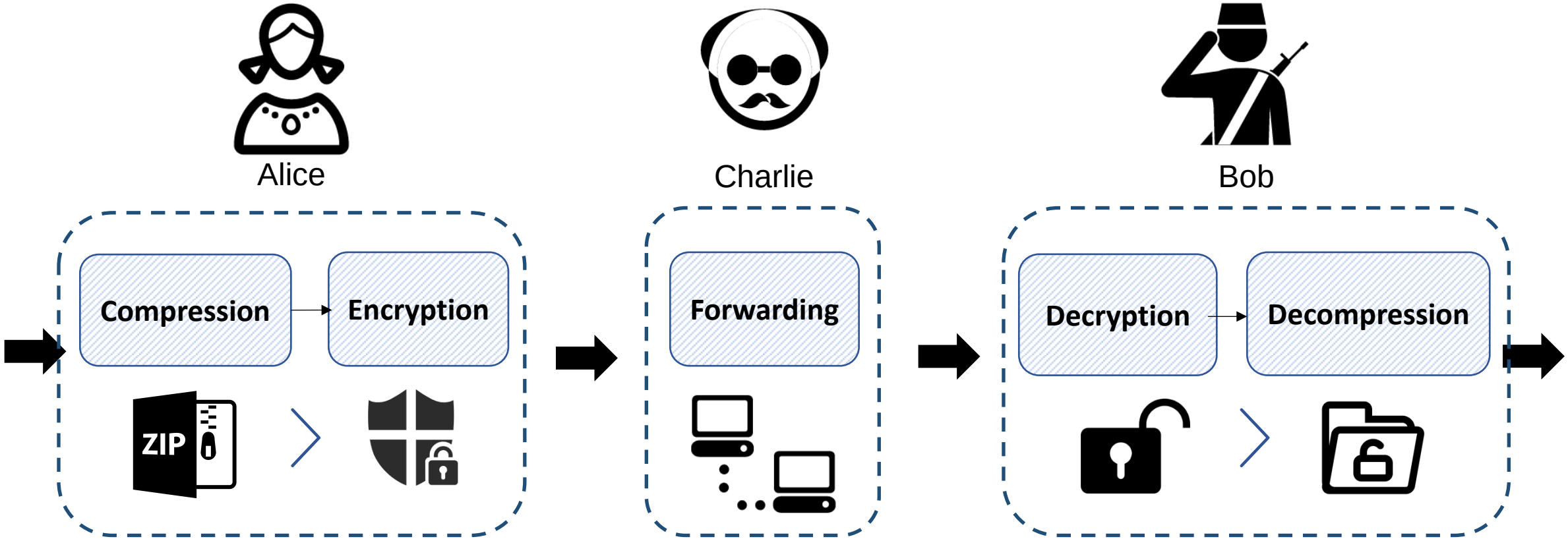
content owner → **Untrusted channel provided by Charlie.** → recipient

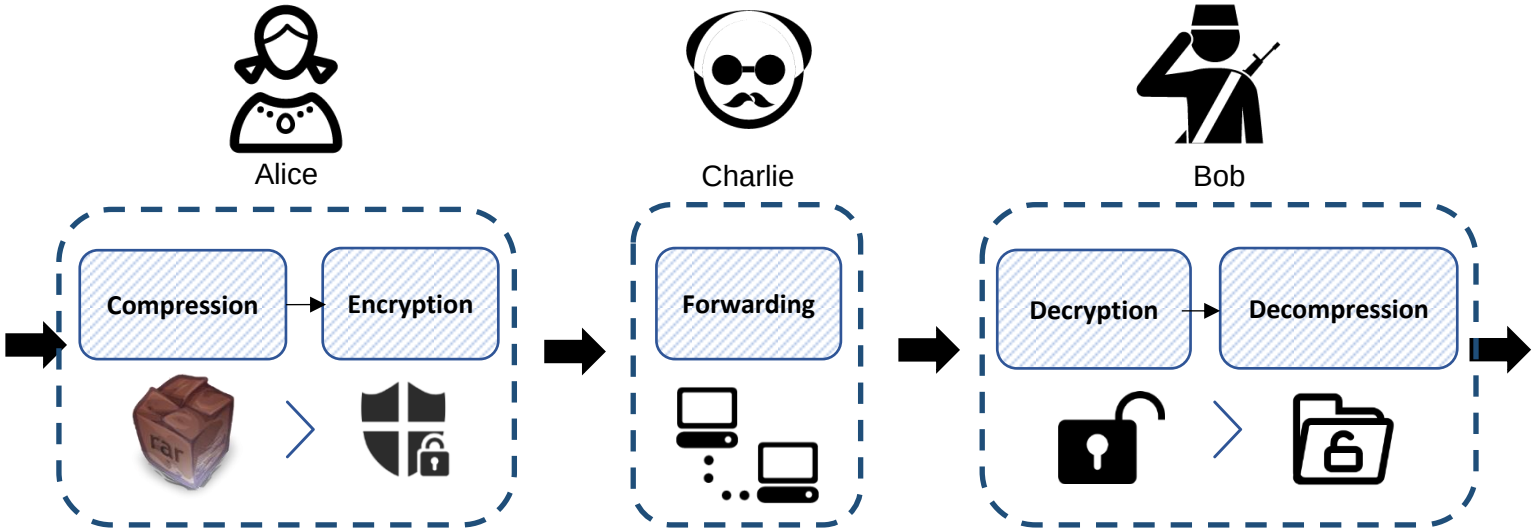
Question:

Can Alice transmit an image via untrusted channel securely and efficiently?

If she can, How?

- **Traditional** Compression-then-Encryption system





Efficient purpose

Compress the image to save channel resource.

Security purpose

Encrypt the compressed image to mask its content.

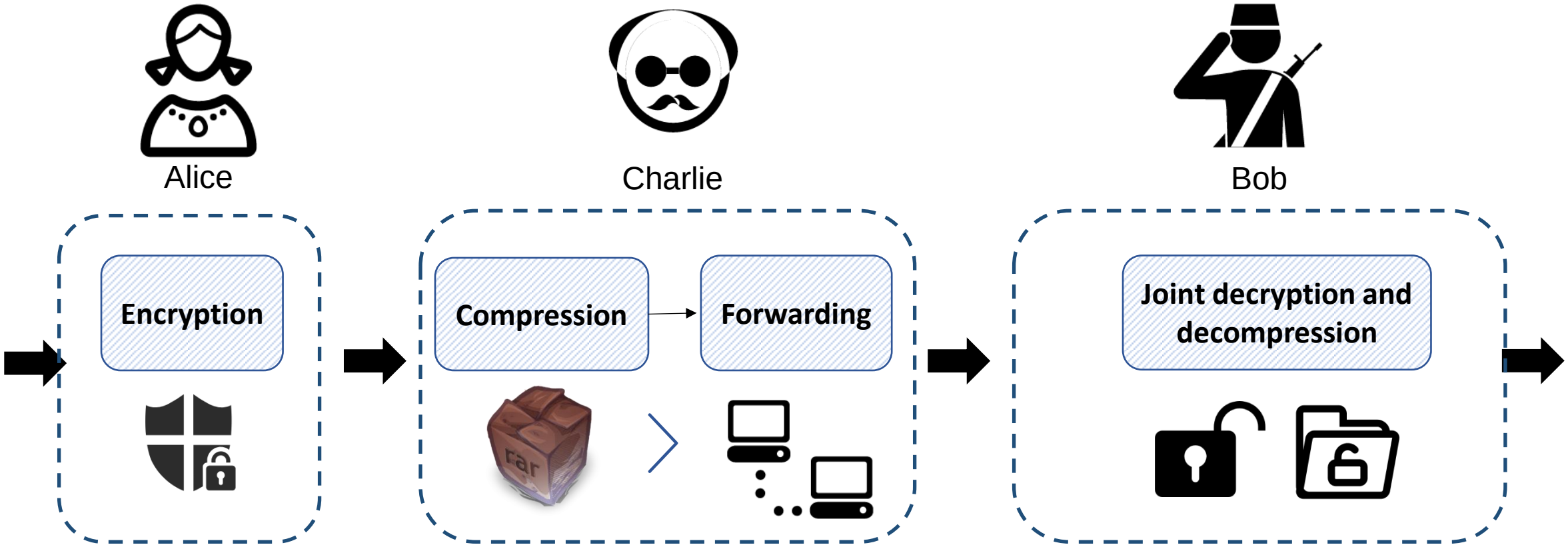
Alice

Compressing is a benefit for Charlie, not for me.

Why I use my limited computing resources to compress the image for Charlie.

This is especially true when I use a resource-deprived mobile device.

- **The Encryption-then-Compression** system



Since an encryption algorithm converts the data from comprehensible to incomprehensible structure, it renders traditional compression algorithms, such as JPEG and JPEG2000, ineffective.

A big challenge:

How can we

compress the cipher image efficiently?

The cipher image can be compressed by using **compressed sensing (CS) effectively.**

CS

However, the previous CS-based schemes are unsatisfactory in terms of compression performance.

Part 2 **Semi-tensor product CS**

2.1 Compressed sensing

$$y = \Phi x$$

$y \in R^M$

The measurement vector.

$\Phi \in R^{M \times N} (M \ll N)$

The measurement matrix

$x \in R^N$

The original signal

However, traditional CS scheme needs massive storage space for the measurement matrix.

2.2 Semi-tensor product CS

$$y = A \ltimes x = (A \otimes I_p)x$$

$y \in R^M$ — The measurement vector

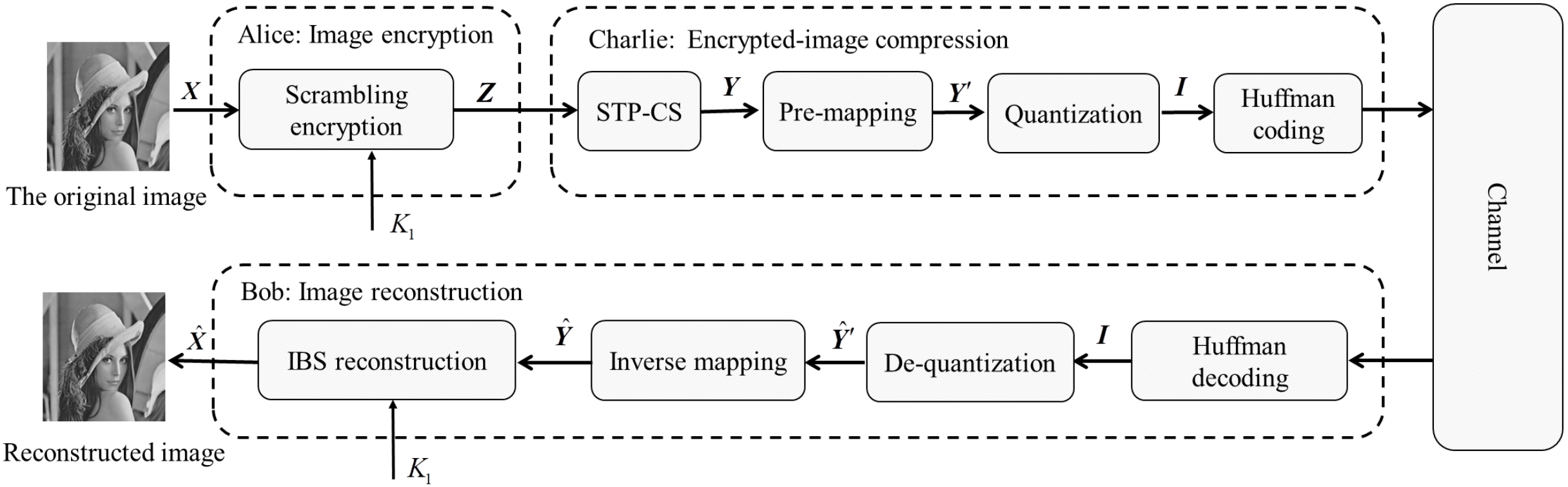
$A \in R^{m \times n} (m \ll n)$ — The measurement matrix

$I_p \in R^{p \times p}$ — An identity matrix

$x \in R^N$ — The original signal

- Part3 **The proposed method**

3.1 Overview



STP-CS：Semi-tensor product Compressed sensing

IBS：iterative bivariate shrinkage

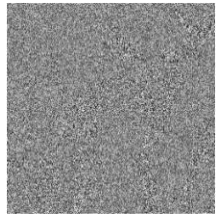
3.2 Image encryption

Original image

X

Scrambling

Z



The cipher image

$$Z = \mathrm{E}(X)$$

$Z \in R^{N \times N}$

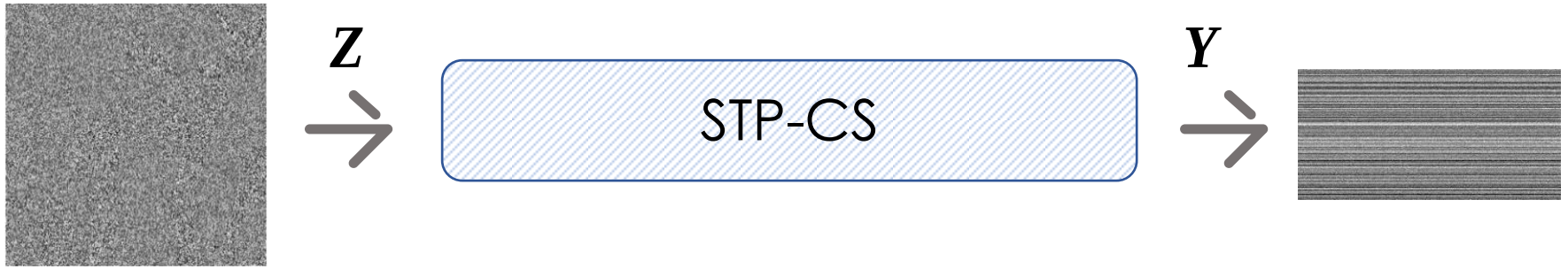
The cipher image

$\mathrm{E}(\bullet)$

The scrambling encryption operation

3.3 Cipher-image Compression

Step 1: Compress the cipher image by using STP-CS.



The cipher image

The CS samples

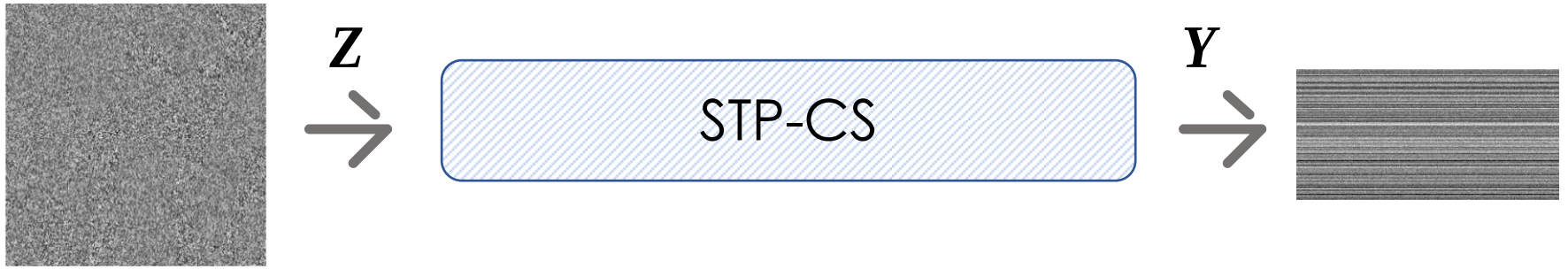
$$\boldsymbol{Y} = \boldsymbol{A} \measuredangle \boldsymbol{Z}$$

$$\boldsymbol{Y} \in R^{M \times N}$$

The CS samples

3.3 Cipher-image Compression

Step 1: Compress the cipher image by using STP-CS.



The cipher image

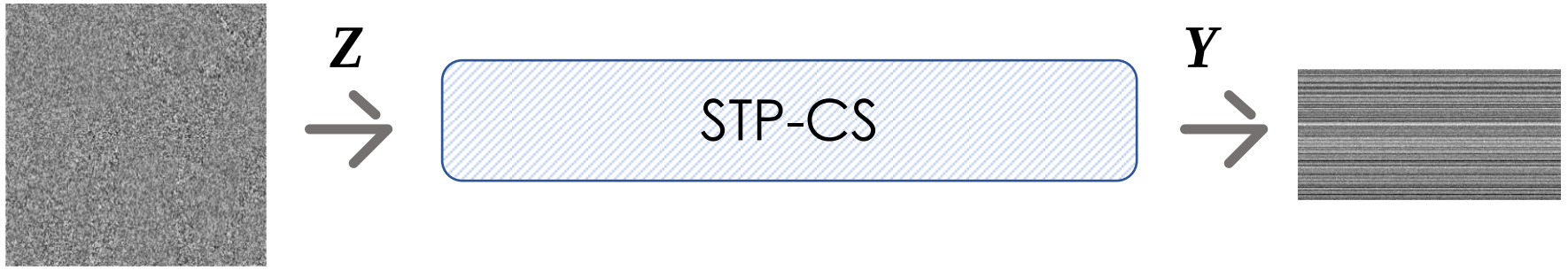
The CS samples

After CS encoding, the CS samples can be quantized and entropy coding into bits directly.

According to classical quantization theory, the more centralized the source symbols distribute, the smaller the quantization distortion is.

3.3 Cipher-image Compression

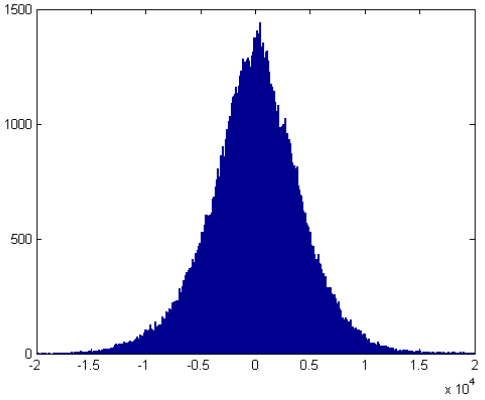
Step 1: Compress the cipher image by using STP-CS.



The cipher image

The CS samples

Unfortunately, the distribution of CS samples is usually decentralized, which means the bit size required for encoding each CS sample is large. As a result, the compression performance of CS-based image coding is unattractive.



Question:

Can we find a strategy to make the distribution of CS samples more centralized?

If can, How?

3.3 Cipher-image Compression

Step 2: Process the CS samples by using pre-mapping operation

The CS samples

The mapped CS samples

$$Y' = Y - A \times \mu$$

$Y' \in R^{M \times N}$

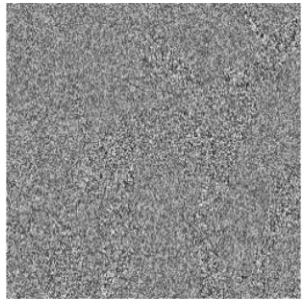
The mapped CS samples

$\mu \in R^{N \times N}$

The mean value matrix

3.3 Cipher-image Compression

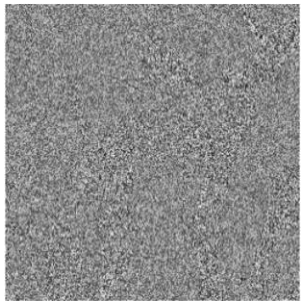
Step 2: Process the CS samples by using pre-mapping operation



Y

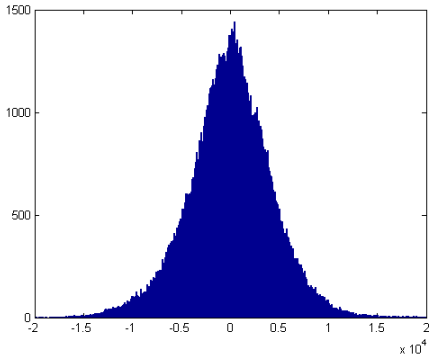
Pre-mapping operation

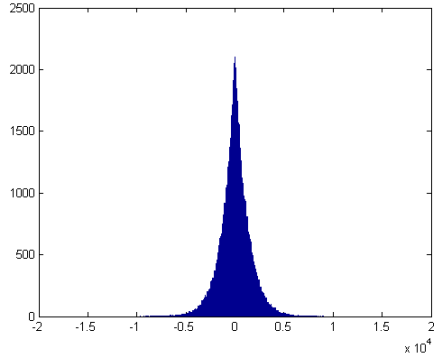
Y'



The CS samples

The mapped CS samples

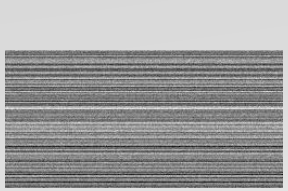




Since pre-mapping operation can make the probability distribution of CS samples more centralized, this operation helps to improve the compression performance.

3.3 Cipher-image Compression

Step 3: Scalar quantization and Huffman coding.



Y'

SQ

I

Huffman coding

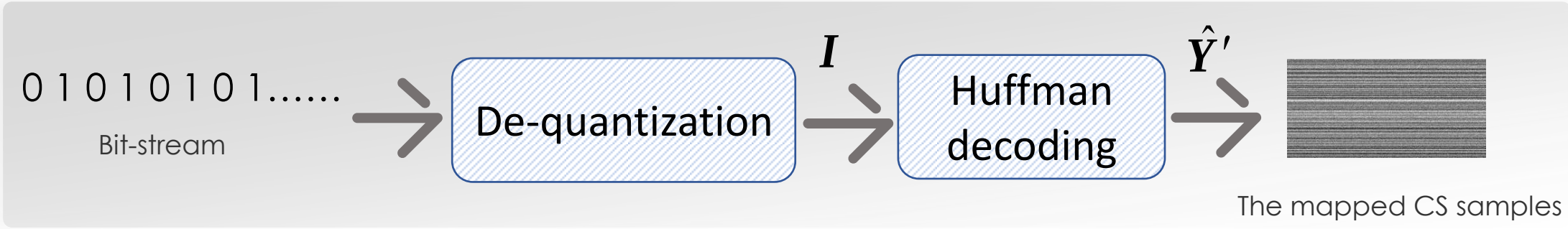
0 1 0 1 0 1 0 1……

The mapped CS samples

Bit-stream

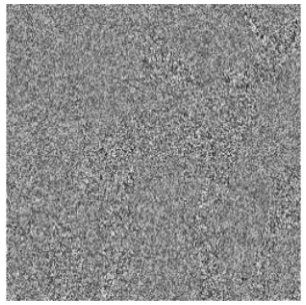
3.4 Decoding steps

Step 1: De-quantization and Huffman decoding.



3.4 Decoding steps

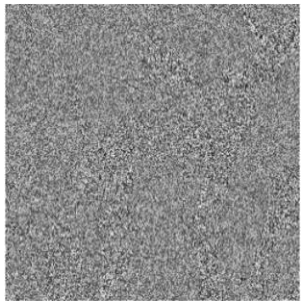
Step 2: Inverse mapping operation



$\hat{Y}'$

Inverse mapping operation

$\hat{Y}$



The mapped CS samples

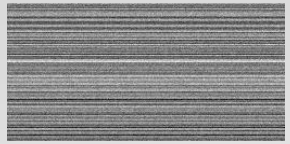
The CS samples

$$\hat{Y} = \hat{Y}' + A \times \mu$$

3.4 Decoding steps

Step 3: Image reconstruction

$\hat{Y}$



The CS samples

Image reconstruction

$\hat{X}$

Reconstructed image

A big challenge is encountered:
how can we recover the original image effectively.

3.4 Decoding steps

Step 3: Image reconstruction

By taking the encryption into consideration,
the joint image reconstruction can be achieved by using this equation

$$\hat{\boldsymbol{X}} = \arg\min_{\boldsymbol{X}} \left\| \boldsymbol{\Psi X \Psi}^{\mathrm{T}} \right\|_1 \ \text{s.t.}\ \hat{\boldsymbol{Y}} = \boldsymbol{A} \prec \mathrm{E}(\boldsymbol{X})$$

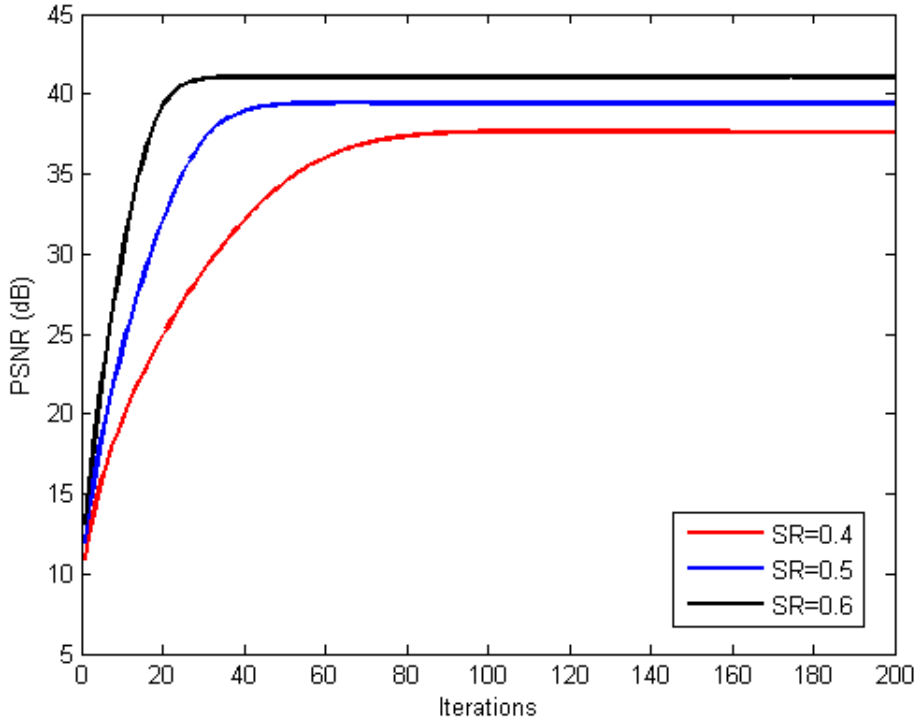
$$\boldsymbol{\Psi} \in R^{N \times N}$$

a wavelet basis matrix

An iterative bivariate shrinkage (IBS) algorithm is proposed,
where the image is recovered in an iterative manner.

3.5 Simulations results

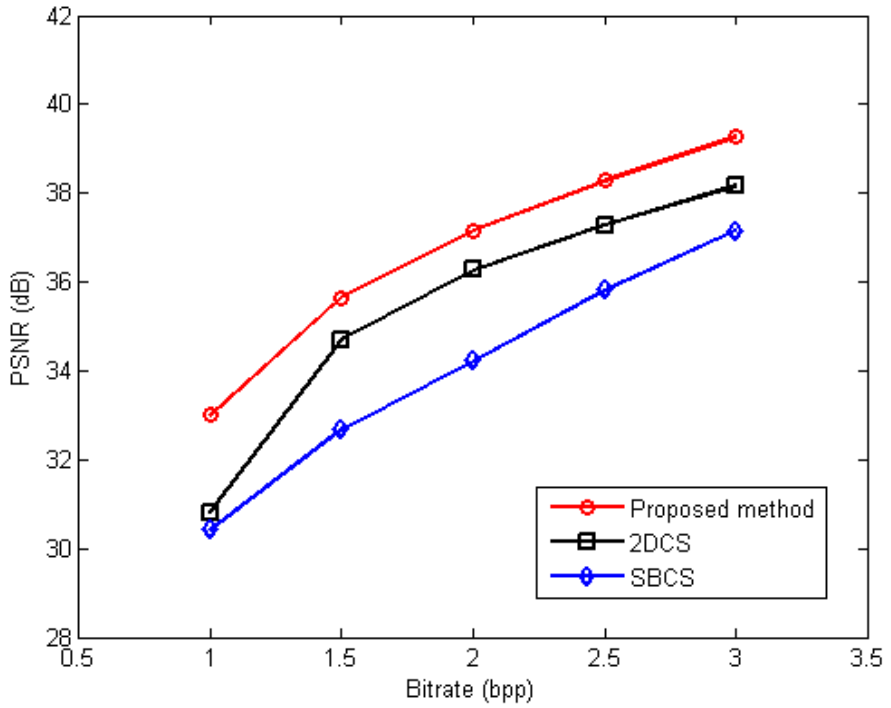
The convergence of IBS algorithm.



The PSNR of the reconstructed Lena image with respect to the number of iterations for the proposed IBS algorithm.

3.5 Simulations results

Compression performance evaluation



The proposed scheme has better compression performance than the previous schemes.

- Part4 **Conclusions**

4.1 Conclusion

In this paper,
an image encryption-then-compression (ETC) scheme by using semi-tensor product CS (STP-CS) and pre-mapping is proposed.

4.1 Conclusion

In summary, the contributions of this work are as follows:

- **An image ETC scheme by using STP-CS and pre-mapping operation is proposed. Compared with the existing CS-based image ETC schemes, the proposed scheme has better *compression* performance.**

- **An iterative bivariate shrinkage (IBS) algorithm is proposed, which can be used to reconstruct the original image effectively.**

Thank you !