Encryption Before Compression Coding Scheme for JPEG Image Compression Standard

Dariusz Puchala, Kamil Stokfiszewski, Mykhaylo Yatsymirskyy

Institute of Information Technology, Technical University of Lodz,
Lodz, Poland

Abstract

In this paper we present a new joint encryption and compression coding scheme of natural images which is intended for the use in conjunction with a popular JPEG image compression standard. The encryption is performed prior to compression step and is carried out using fast, parametrized with a private key, linear transformations which do not alter statistical characteristics of the input image data, what enables JPEG algorithm to maintain its full compression capabilities. The work also includes a mathematical model of the proposed scheme which allows for theoretical analysis of the impact of the image encryption step on the compression process. The presented experimental results indicate that the reconstructed images' qualities at a given compression ratios are comparable to those obtained for the JPEG standard without the encryption step.

Introduction

In our paper we proposed a novel method allowing for image encryption and compression in *encrypt-then-compress* (ETC) scenario. In this scenario the data is encrypted first and then subjected to compression.

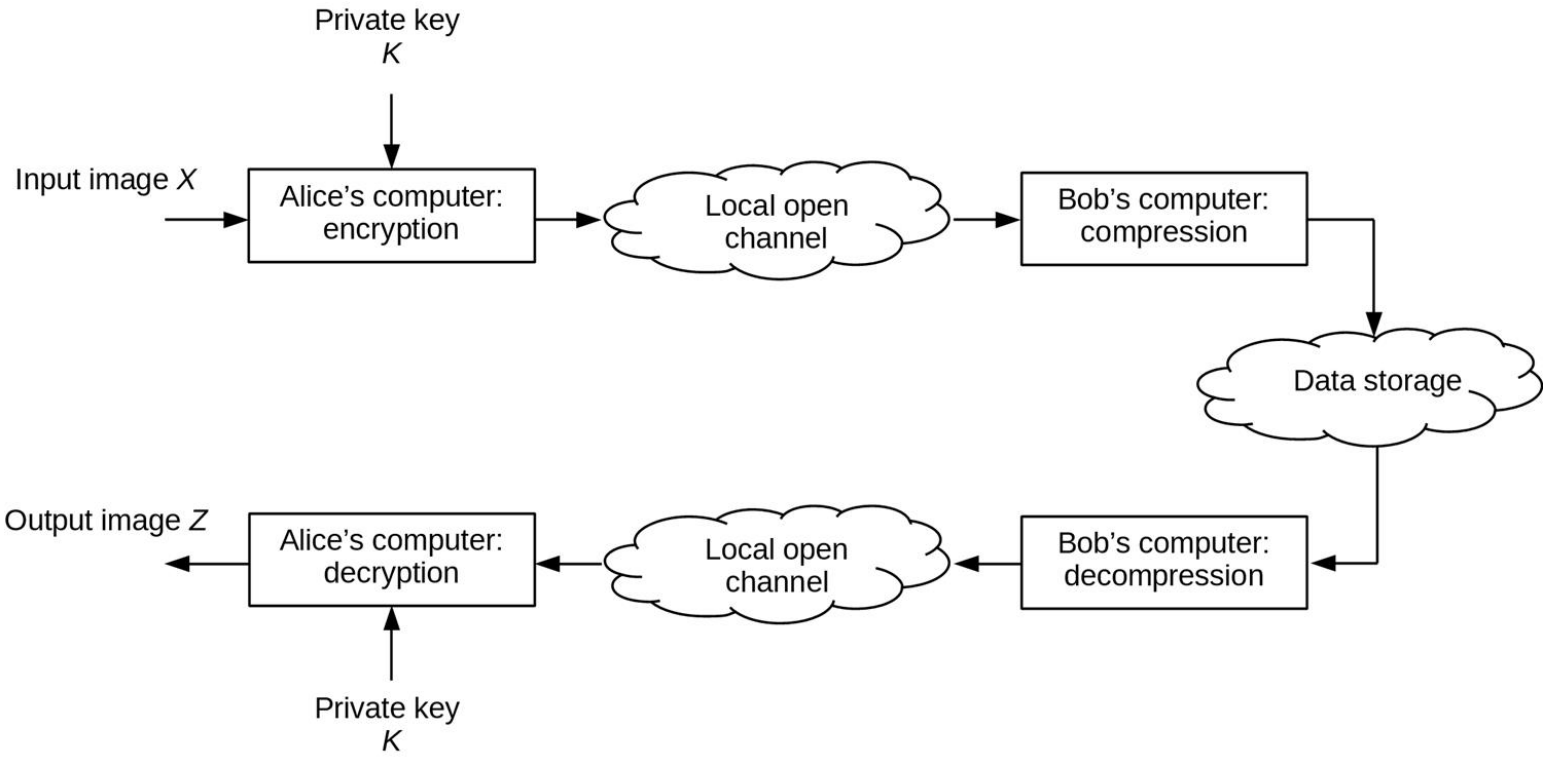


Fig. 1. Data storage scenario

Introduction

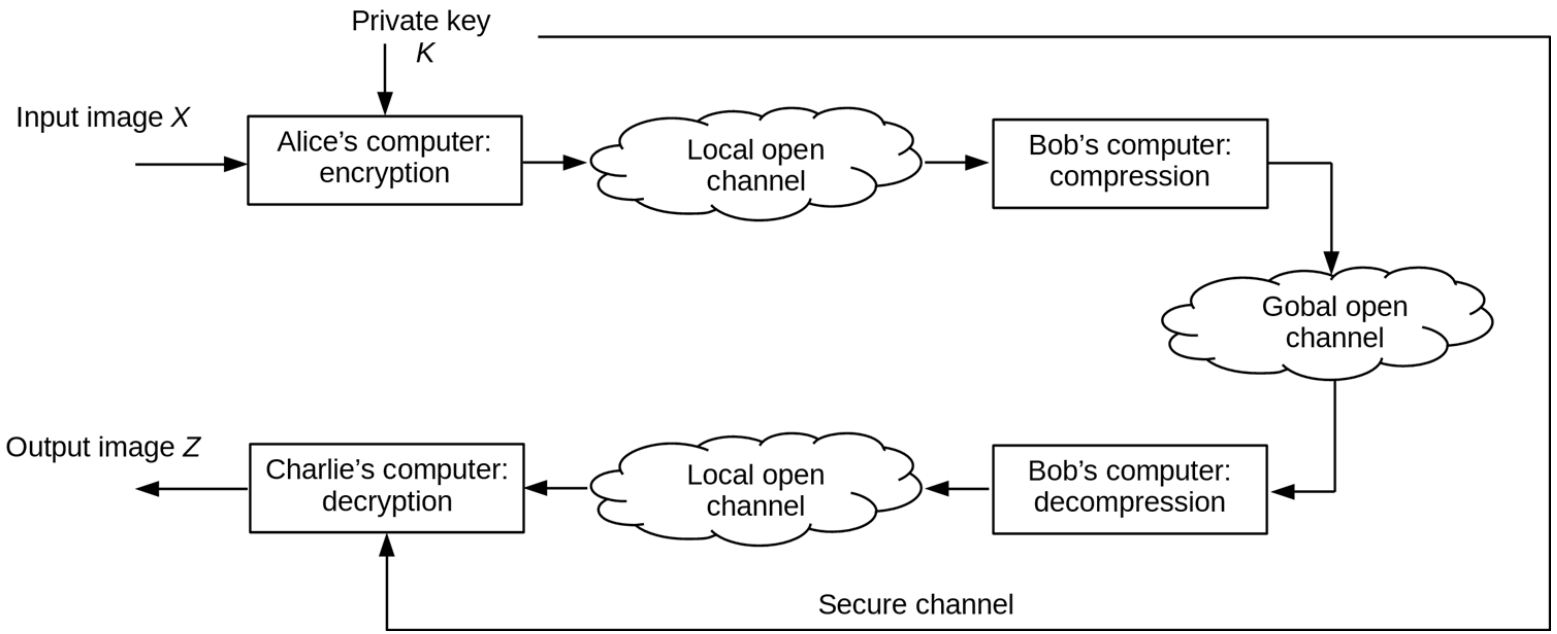


Fig. 2. Scenario for data transmission over global network

The encryption stage takes advantage of linear orthogonal transforms which allows to keep the statistical characteristics of the image. It's crucial from the point of view of the succeeding compression stage.

The proposed coding scheme

The proposed coding scheme can be described in a form of the subsequent steps realized in the order according to the diagram from Fig. 3.

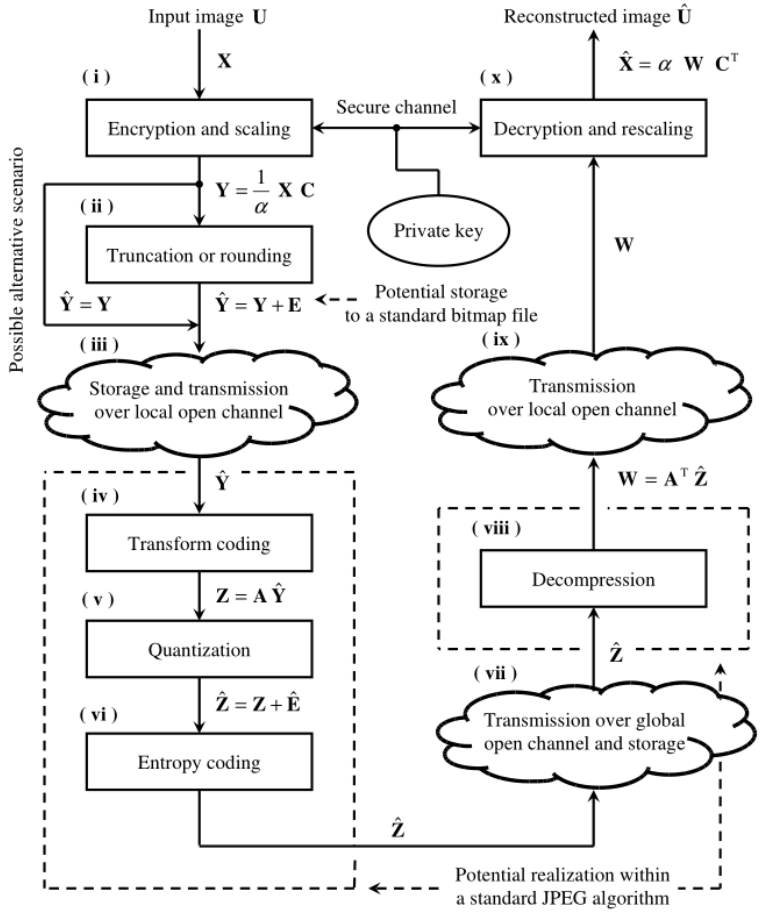


Fig. 3. The diagram showing the following steps of the proposed coding scheme

The proposed coding scheme

Let *U* represent monochromatic input image. To begin encryption it's first necessary to properly arrange input data (image data) into vectors.

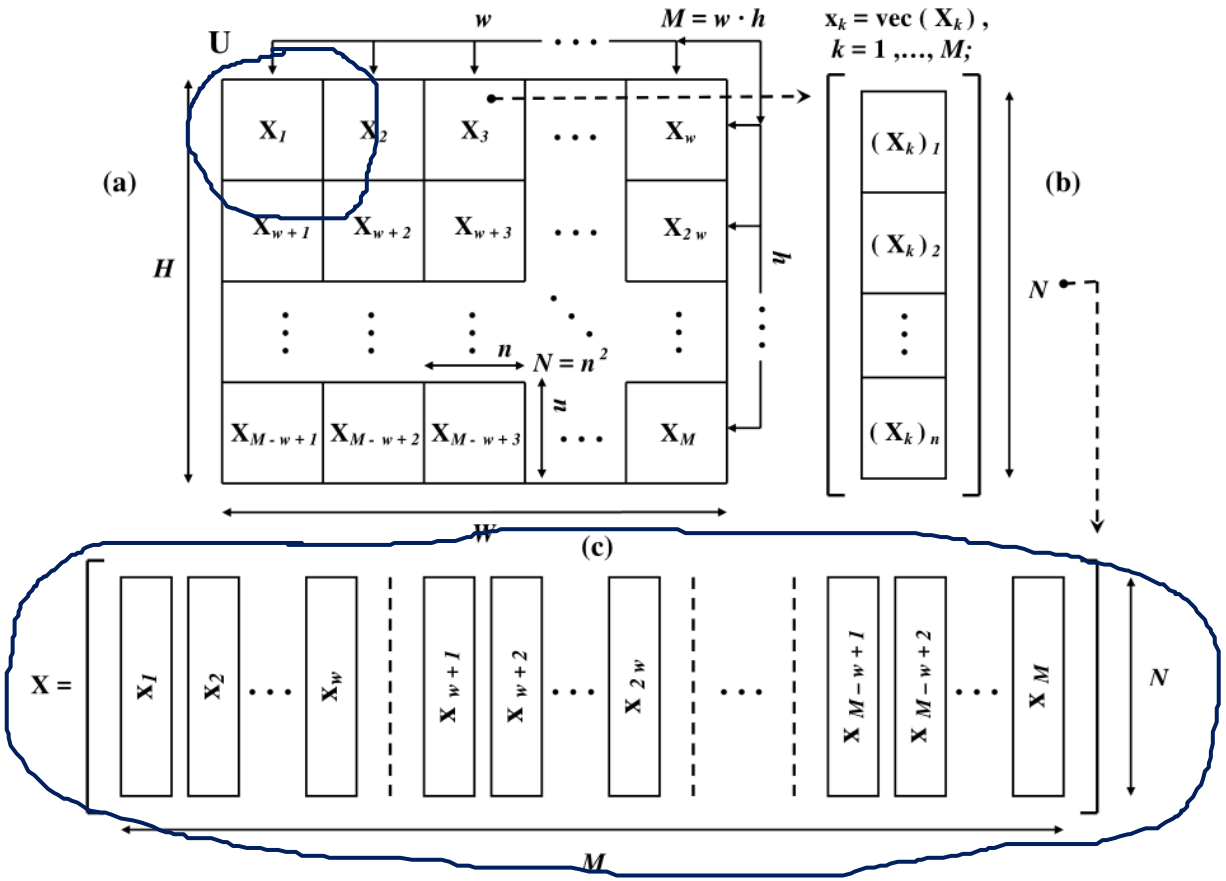
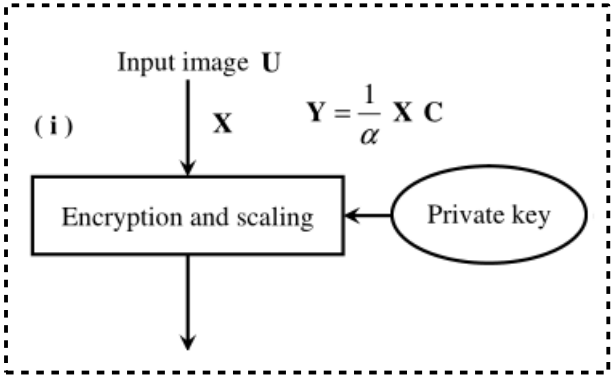


Fig. 4. The arrangement process of input data

The proposed coding scheme

After the input matrix **X** has been formed, the actual coding process begins, where the first step is encryption and scaling. It can be described as:



$$\mathbf{Y} = (1/\alpha)\mathbf{XC},$$

where **C** is a *M* on *M* element, real valued, orthogonal encryption matrix ($\mathbf{CC}^T=\mathbf{I}$), and α is a scaling factor.

The value of the scaling factor α should be chosen in a way guaranteeing the magnitudes of the elements of cryptogram **Y** are acceptable from the point of view of the subsequent coding steps. The value of this factor is usually greater than 1.

The proposed coding scheme

In practice multiplication by matrix **C** can be implemented in a form a fast parametric transform. Operators $\mathbf{O}_i$ represent plane rotations. The angles of rotations constitute the private key for the encryption algorithm,

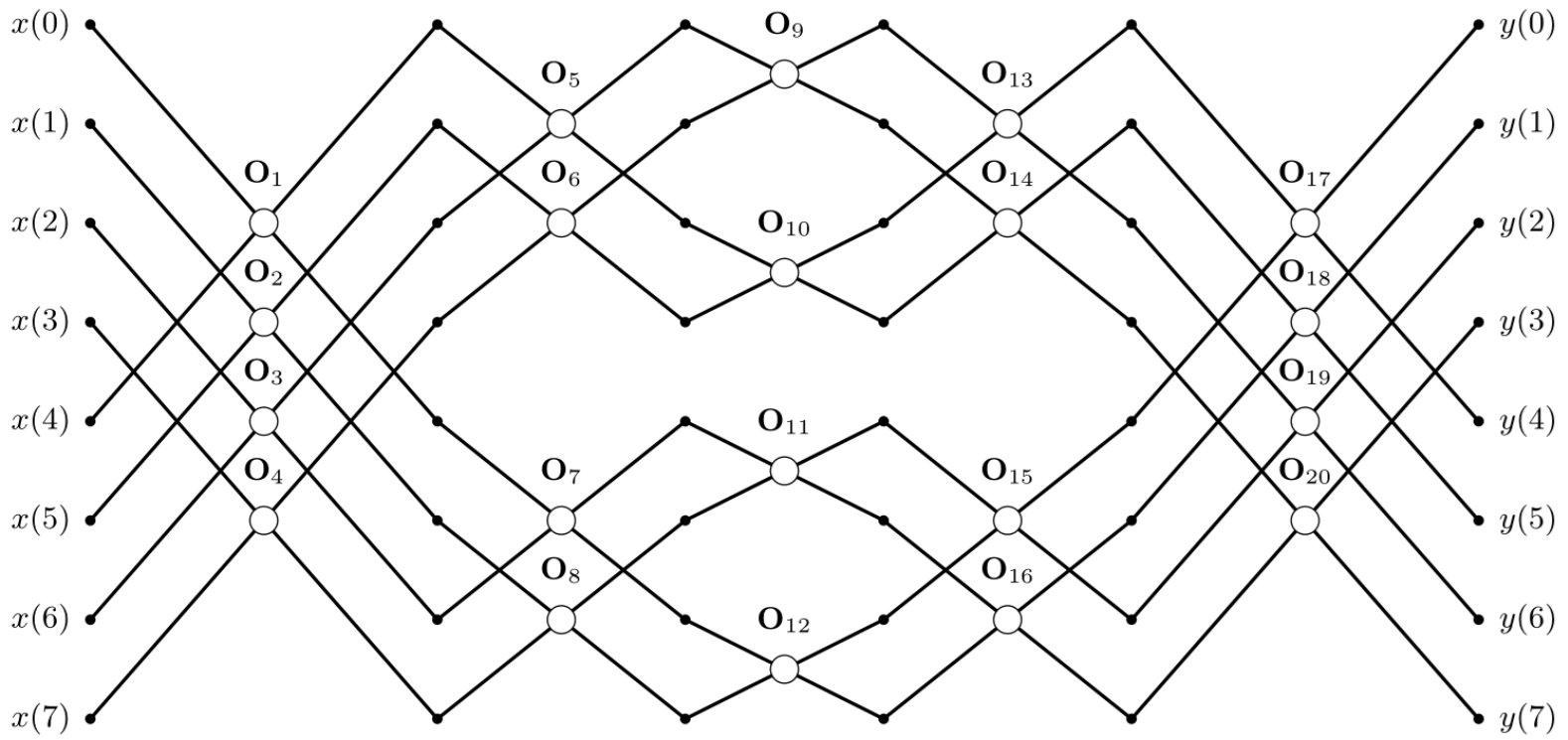
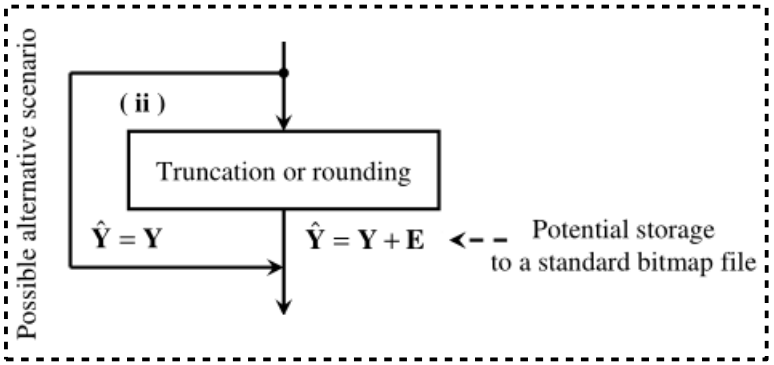


Fig. 5. Data flow diagram of fast parametric transforms for 8 element input vectors

The proposed coding scheme



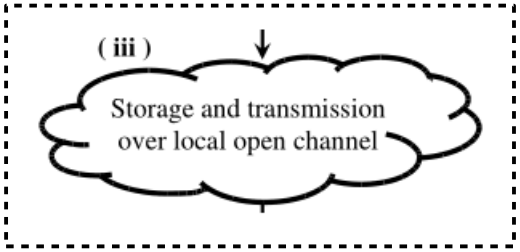
The following possible step is truncation and rounding. It is optional and depends on a specific implementation. At the output of this stage we can obtain scaled and quantized cryptogram possible to be written in the form of a popular BMP file. This process introduces error modeled as:

$$\hat{\mathbf{Y}} = \mathbf{Y} + \mathbf{E},$$

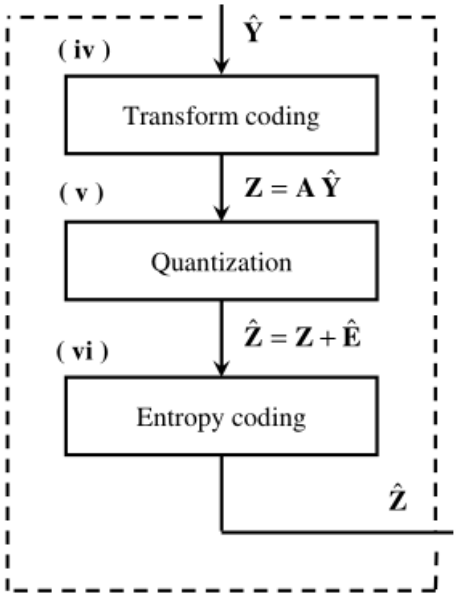
where **E** stands for truncation error matrix.

The proposed coding scheme

The third step is transmission over local open channel.



The following three stages are (iv) transform coding with use of the discrete cosine transform, (v) quantization resulting in error modeled with matrix $\hat{\mathbf{E}}$, (vi) entropy coding, e.g. first order entropy coding with use of Huffman codes.



Steps (iv), (v) and (vi) make up the actual image compression process and are fully compatible with subsequent phases of the image's data processing occurring in the course of operation of the standard JPEG compression algorithm. After this stage we obtain:

$$\hat{\mathbf{Z}} = \mathbf{A}\left((1/\alpha)\mathbf{XC} + \mathbf{E}\right) + \hat{\mathbf{E}}.$$

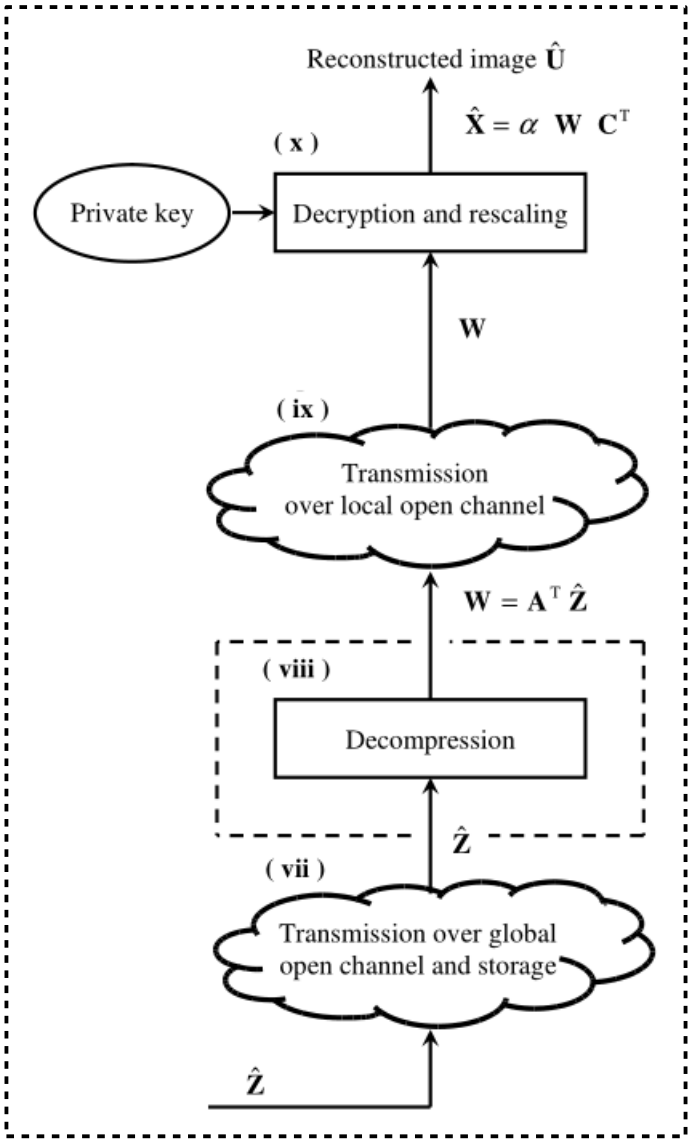
The proposed coding scheme

The resulting matrix $\hat{\mathbf{Z}}$ models the output encrypted and compressed image.

The output image can be stored or transmitted over open global channel according to ETC scenarios.

Before the image gets to the recipient it must go through the steps of decompression (viii), transmission over local channel (ix) and decryption and rescaling (x). The reconstructed image can be described as:

$$\hat{\mathbf{X}} = \alpha \mathbf{A}^T (\mathbf{A}(\alpha^{-1}\mathbf{X}\mathbf{C} + \mathbf{E}) + \hat{\mathbf{E}})\mathbf{C}^T.$$



The proposed coding scheme

Further on in the paper the Authors derive the rate distortion formula describing the proposed coding scheme. It's derived with the following assumptions:

- the variances of truncation error at stage (ii) are identical for all the elements of data vectors and can be described as

$$\sigma_{e_i}^2 = \sigma_e^2 \approx \frac{1}{3}$$

for i=0, 1, … , N-1;

- according to the results in high resolution theory the variances of error values involving rounding towards the nearest integer values, at quantization at stage (v), can be expressed in the following form

$$\sigma_{\hat{e}_i}^2 \approx \frac{\Delta_i^2}{12}$$

for i=0, 1, … , N-1, where Δ_i are the steps of scalar quantizers.

The proposed coding scheme

The resulting formula allowing to evaluate the relationship between the mean squared error *D* and the minimum average bit rate *R* takes the following form:

$$D(R) \approx \frac{\pi e \|\mathbf{\Delta}\|^2}{6N} \left(\prod_{i=1}^{N} \frac{\mathbf{a}_i^T \mathbf{R}_x \mathbf{a}_i + \alpha^2 \sigma_e^2}{\Delta_i^2} \right)^{\frac{1}{N}} 2^{-2R} + \alpha^2 \sigma_e^2,$$

where $\mathbf{a}_i$ stands for a column vector of matrix **A**, and ||**Δ**|| describes a norm of a vector of quantization coefficients Δ_i.

It should be noted that the effectiveness of the compression process does not depend in any way on the choice of the encryption matrix **C**. We have (**Y**=**CX**):

$$\mathbf{R}_y = \frac{1}{M}\mathbf{Y}\mathbf{Y}^T = \frac{1}{\alpha^2 M}\mathbf{X}\mathbf{C}\mathbf{C}^T\mathbf{X}^T = \frac{1}{\alpha^2 M}\mathbf{X}\mathbf{X}^T = \frac{1}{\alpha^2}\mathbf{R}_x.$$

Effectiveness of encryption

For encryption we've used block-orthogonal coding matrix, with block size K=8, with a fast parametric two-stage structure. In Fig. 6 we have two examples of images together with their forms obtained after decryption with an invalid private key. Visual inspection of the obtained results indicates lack of similarity between the input and the encrypted images. Moreover the probability distributions of pixel luminances in images obtained after encryption have Gaussian noise characteristics. Hence, taking into account both, the results from Fig. 6 and high combinatorial complexity of the presented encryption scheme, where for a block size K=8 the private key was 184320 bits long, we conclude the encryption process can be considered to be efficient.

Effectiveness of encryption

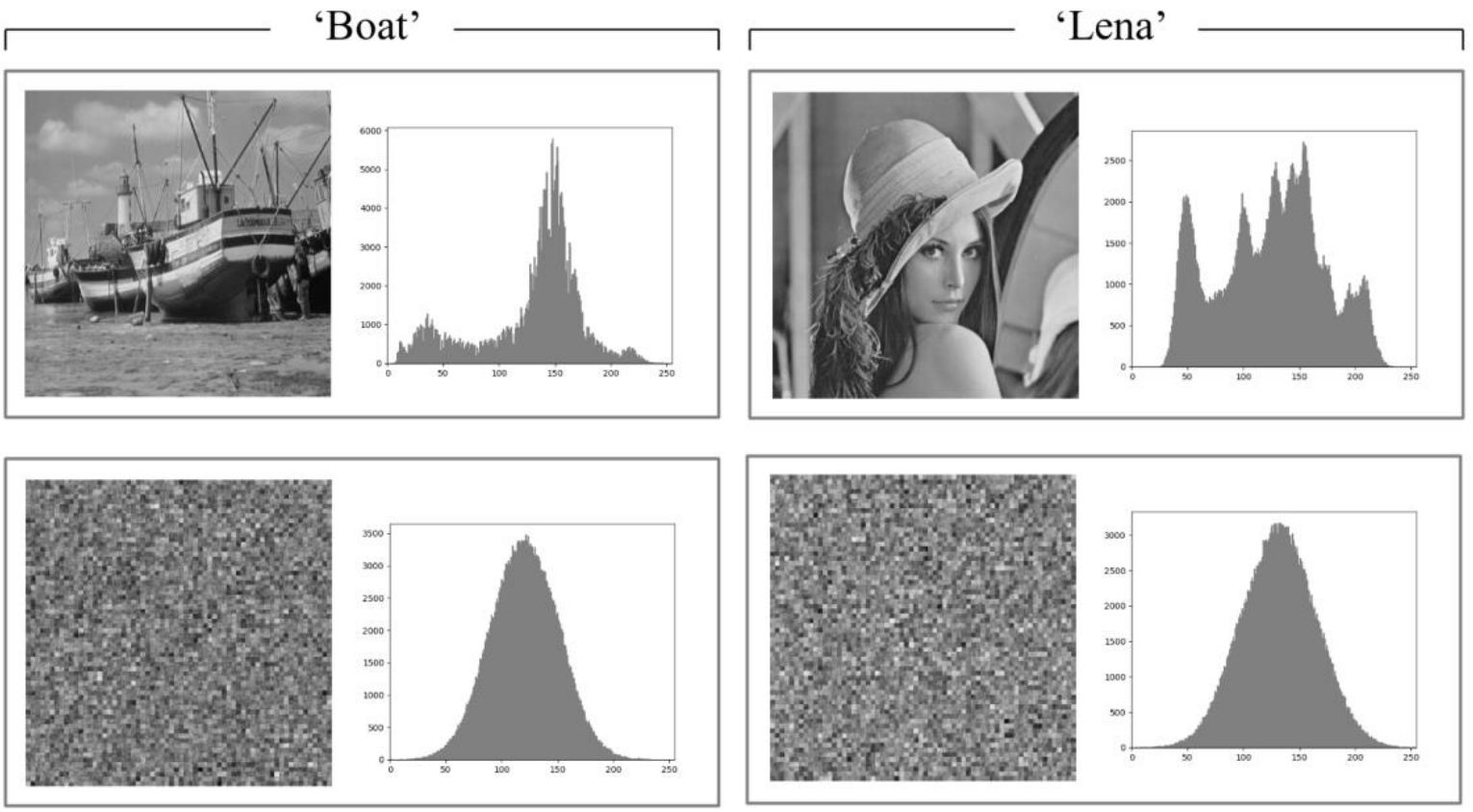


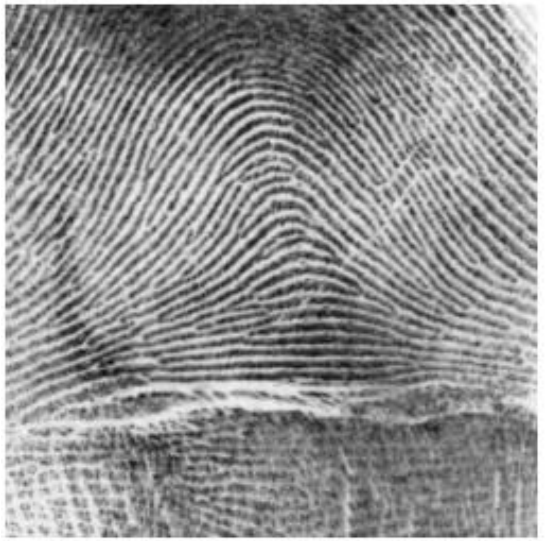
Fig. 6. Exemplary images and their histograms before and after encryption

Experimental results

In order to verify practically the effectiveness of the compression and encryption processes present within the proposed scheme a number of tests were carried out using natural images with different statistical characteristics. All of the images used during experiments were 8–bit grayscale ones with resolutions of 512 × 512 pixels each.

Lena

Boat



Fingerprint

Fig. 7. Exemplary images used during the experiments

Experimental results

To check the influence of the block size *K* of the block-orthogonal encryption matrix **C**, on the proposed scheme's compression efficiency, the compression process quality was tested for three mentioned block sizes, namely for *K* = 8, 16 and 32. It's worth mentioning that the block size value regulates oppositely the cryptogram's strength on one hand and the compression effectiveness on the other. For that second case, the bigger the block size is, the greater the value of the scaling factor α might be, worsening potentially the effectiveness of the compression process. Tab. 1 shows the results of the conducted experiments of image compression effectiveness comparisons between the standard JPEG method and the proposed scheme for different compression ratios and three selected encryption matrix block sizes.

Experimental results

Compression ratios	PSNR values [dB]							
	'Lena' image				'Fingerprint' image			
	Standard method	Proposed method			Standard method	Proposed method		
		K=8	K=16	K=32		K=8	K=16	K=32
2.455	48.839	44.589	43.935	43.288	40.130	40.110	39.481	39.344
3.232	43.020	41.488	40.934	40.377	36.955	37.028	36.817	36.513
4.009	41.240	39.810	39.205	38.687	34.688	34.814	34.600	34.453
4.787	39.967	38.597	37.883	37.404	32.960	33.045	32.883	32.742
5.564	38.989	37.676	36.971	36.371	31.587	31.637	31.515	31.423
6.341	38.271	36.953	36.128	35.421	30.457	30.498	30.400	30.331
7.118	37.660	36.293	35.353	34.648	29.477	29.484	29.401	29.341
7.896	37.104	35.641	34.756	33.956	28.681	28.686	28.635	28.545
8.673	36.595	35.116	34.230	33.393	27.984	28.010	27.910	27.844
9.450	36.201	34.642	33.723	32.921	27.324	27.376	27.310	27.183

Tab. 1. The effectiveness of the proposed scheme in the sense of compression in scenarios without (standard) and with encryption

Conclusions

The paper proposes a new joint encryption and compression coding scheme of natural images which is intended for the use in conjunction with a popular JPEG image compression standard. Due to utilization of fast parametric linear transforms at the encryption stage, not only the presented scheme is efficient computationally but, what's most important, does not change the statistical characteristics of the images being compressed, what is in turn crucial for the effectiveness of the scheme's compression process. The proposed scheme's mathematical model is also presented, which agrees with the obtained experimental results and allows for theoretical analysis of the proposed scheme's performance for different practical scenarios. Experimental results along with the presented theoretical analysis reveal that the scheme is highly efficient both in terms of its encryption capabilities and compression quality, as well as in terms of ease of application as a JPEG standard extension.

Thank you for your attention