

A Novel Post-processing Method to Improve the Ability of Reconstruction for Video Leaking Signal

Xuejie Ding, Meng Zhang^(✉), Jun Shi, and Weiqing Huang

Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China
{dingxuejie, zhangmeng, shijun, huangweiqing}@iie.ac.cn

Abstract. The confidential information can be reconstructed by received weak electromagnetic signal from a radiation object, such as a computer display. Usually, the radiation signal is submerged in strong noise and faded in channel, so it is not an easy task to understand the information existed in the signal. In this paper, we propose a new post-processing system to improve the visual quality of reconstruction image in sparse domain. Different from filter and enhancement technologies in image filed, our system focuses on data shrink and repair using the methods in machine learning. It can not only remove the noise interference, but also complement the lost high-frequency and compensate the distortion. Experimental section displays complete procedures and better performance, and it also proves the effectiveness of the novel framework.

Keywords: Electromagnetic radiation · Sparse representation · Data shrink · Data repair

1 Introduction

As the increasing need and wide spread using of information technology equipment (ITE), it has brought a great communication convenience but also the information crisis for human society. One side, people can deal with important information and data easily by ITE, on the other hand, the eavesdroppers can steal the information operated on computer displays by electromagnetic radiation [1–3]. Therefore the information leakage has a strong impact on social and economic activities, and the protection and attack technology for electromagnetic radiation are concerned by military and government of world.

The weak leak signal can be captured and reconstructed to an image or video by eavesdropper's facility [4, 5]. However, understanding this captured data is not an easy job, because the received signal is submerged in strong noise and faded in channel. In order to solve this problem, there are two ways, one is to design a better receiver equipment to improve the received quality, and the other is to add a post-processing part in favor of comprehending the information. Comparing with the first way, adding a post-processing is more flexible. In the past decades, the researchers focused on the post-processing system by means of digital image processing technologies. For example,

the authors in [6] used the adaptive filtering algorithm to improve SNR of the reconstruction images. In report [7], multi-frame average de-noising filter and wavelet transform filter are applied to reconstruct computer video. In order to improve the visual quality of received data, in this paper, we propose a novel post-processing system based on machine learning, which is different from traditional method in image processing filed.

In our framework, the reconstruction image is divided into several blocks, and each block is sparse represented. Then a sparse coefficients set is obtained, which includes the sparse coefficients of each block. We expect to improve the intelligibility of received data by modifying the sparse coefficients set. Firstly, each block is assumed to have a category, and is labeled as background, interference or information. We predict the category for each block using multi-class logistic regression algorithm, then a shrink operation is done on the base of predict result. Secondly, with the purpose of repair the data further, for the blocks labeled as information, the Kernel Density Estimation (KDE) method is imported to estimate their probability density functions, and smooth the sparse coefficients based on the statistical property. It expects to be able to complement the lost high-frequency and compensate the distortion.

The structure of the paper is as follows: the principle of the novel framework is introduced in Sect. 2, and the proposed method is depicted in details in Sect. 3. The experimental results and their analysis are shown in Sect. 4. The conclusion and future work are given at the last part of this paper.

2 The Principle of Novel Method

In this section, we will display the principle of our framework. There are three main parts, they are sparse representation for received data, data processing for sparse coefficients set, and data reconstruction using the new sparse coefficients and original dictionary. The details are shown in Fig. 1.

After the reconstruction image is divided into blocks, each block is sparse represented on the basis of a dictionary which is learned by sparse theory using an abundant training dataset. Then a coefficients set is generated composed by the spare representation of each block.

Then the sparse coefficients set is processed by two steps: (1) Shrink, it means some useless components are removed. It depends on the multi-class predict model trained by logistic regression algorithm, and each block is predicted to a category, such as background, interference or information. According to the shrink criterion, some block coefficients are set to zeros. (2) Repair, it means some non-zeros data are smoothed. It depends on the fit model obtained by Kernel Density Estimation (KDE). For the blocks labeled as information, KDE is used to complement the missing part and compensate the distortion.

At last, the data is reconstructed by the new sparse coefficients set and the dictionary. The process can be seen as an inverse transform of sparse representation.

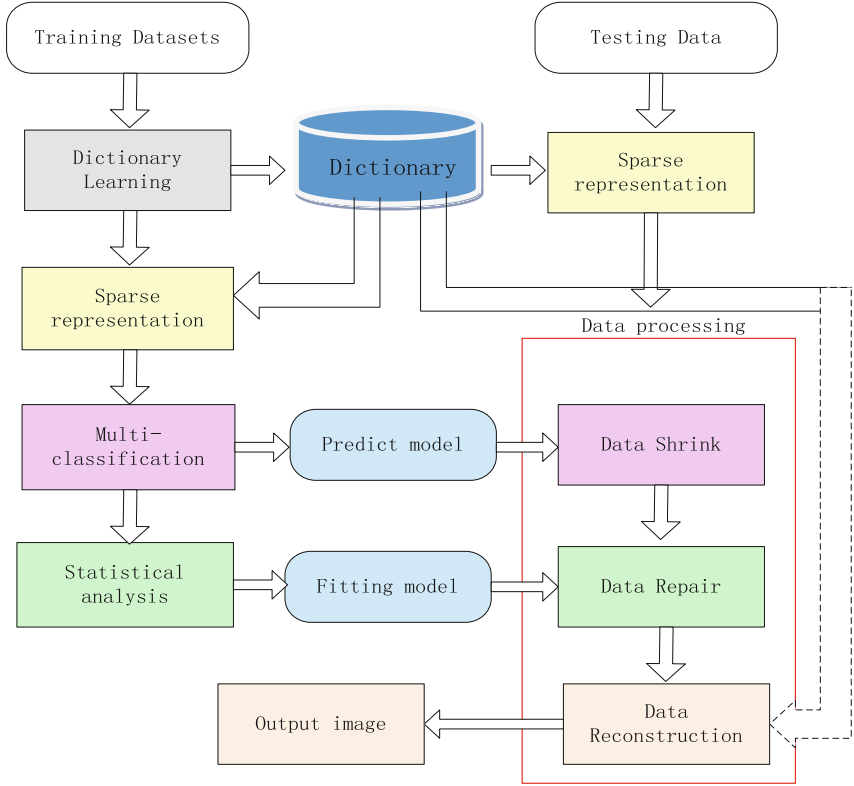


Fig. 1. The principle of our framework

3 The Proposed Method

This section will introduce the details of this novel method. First, the sparse representation theory is presented, it includes the signal decomposition and reconstruction based on this theory. Then the method of shrink is given according to shrink criterion decided by the result of category prediction. At last, KDE is imported to repair the data by smoothing the statistical property.

3.1 Sparse Representation of Received Data

Sparse representation is a powerful decomposition method, it can represent the signal as a linear combination of few elementary components [8]. The sparse representation of a signal is depicted as follows:

$$\mathbf{x} \approx \sum_{t=1}^m \varphi_t \mathbf{d}_t = \mathbf{D} \boldsymbol{\varphi} \boldsymbol{\varphi} \triangleq (\varphi_1, \varphi_2, \dots, \varphi_m) \quad ((1))$$

here the signal \mathbf{x} with size $n \times 1$ is represented approximately as a linear combination of m predefined atoms, and \mathbf{d}_t is the t -th atom (t -th column) of the dictionary \mathbf{D} that is a $n \times m$ matrix. This theory can be transformed as a solution of

$$\hat{\boldsymbol{\varphi}} = \mathbf{arg} \min_{\boldsymbol{\varphi}} \|\boldsymbol{\varphi}\|_0 \text{ subject to } \|\mathbf{D}\boldsymbol{\varphi} - \mathbf{x}\|_2 \leq \varepsilon \quad (2)$$

That is indeed sparse as $\|\hat{\boldsymbol{\varphi}}\|_0 \ll m$. The notation $\|\hat{\boldsymbol{\varphi}}\|_0$ stands for the count of the nonzero entries in $\boldsymbol{\varphi}$. This model should be made more precise by replacing the rough constraint $\mathbf{x} \approx \sum_{t=1}^m \varphi_t \mathbf{d}_t$ with a clear requirement to allow a bounded representation error as $\|\mathbf{D}\boldsymbol{\varphi} - \mathbf{x}\|_2 \leq \varepsilon$.

Successful application of sparse decomposition depends on the dictionary used and whether it matches the content of the signal properly. In this paper, the Independent Components Analysis (ICA) theory is applied to learn the dictionary which has been successfully used for unsupervised feature learning [9]. And the ICA is traditionally defined as the following optimization problem:

$$\min_{\mathbf{W}} \sum_{i=1}^m \sum_{j=1}^n g(\mathbf{W}_j x_i) \text{ subject to } \mathbf{W}\mathbf{W}^T = \mathbf{I}, \quad (3)$$

here $\mathbf{W} = \mathbf{D}^{-1}$, g is a nonlinear convex function, and it is $g(\cdot) = \log(\cosh(\cdot))$. The orthogonality constraint $\mathbf{W}\mathbf{W}^T = \mathbf{I}$ is used to prevent the bases in \mathbf{W} from becoming degenerate.

For our work, the sparse coefficients set $\boldsymbol{\varphi}_t$ is main object rather than data itself, we expect to improve the signal equality by modifying the coefficients. After the processing for sparse coefficients set, the new data is reconstructed as

$$\mathbf{x}_{new} = \mathbf{D}\boldsymbol{\varphi}_{new} \quad (4)$$

The process of sparse representation and reconstruction can be seen as a reversible transform.

3.2 Data Shrink

According to their morphology, the sparse representation of each block can be roughly divided into three categories: background component (0 class), noise interference (1 class) and useful information (2 class). In order to extract the useful information, we should remove the noise and interference signal by means of setting their sparse coefficients to zeros. The first step is to predict which category the block is like. In this section, logistic regression algorithm is employed to solve this multi-classifying problem.

The logistic regression model is one of the most useful tools for multi-classifying, and it does so by providing posterior probabilities which will place the data in the appropriate group. It is parameterized by a weight matrix ω and a bias vector \mathbf{b} [10, 11]. Classification is done by projecting an input vector onto a set of hyperplanes, each of which corresponds to a class. The distance from the input to a hyperplane reflects the probability that the input is a member of the corresponding class. Mathematically, the probability of an input vector φ_i which belongs to the class $I \in [0, 1, 2]$, can be written as:

$$P(Y = I|\varphi_i, \omega, \mathbf{b}) = \frac{e^{\omega_I \varphi_i + b_I}}{\sum_j e^{\omega_j \varphi_i + b_j}} \tag{5}$$

where Y is the notation of the class label. The model’s prediction y_{pred} is the class whose probability is maximal, specifically:

$$y_{pred} = \arg \max_I P(Y = I|\varphi_i, \omega, \mathbf{b}) \tag{6}$$

In order to learn the optimal model parameters, we should minimize a loss function. In the case of multi-class logistic regression, it is very common to use the negative log-likelihood as the loss function.

This is equivalent to maximize the likelihood of the data set \mathfrak{X} under the model parameterized by θ . Let us first start by defining the likelihood L and the loss l .

$$L(\theta = \{\omega, \mathbf{b}\}, \mathfrak{X}) = \sum_{i=0}^{|\mathfrak{X}|} \log(P(Y = y^{(i)}|\varphi_t^{(i)}, \omega, \mathbf{b})) \tag{7}$$

$$l(\theta = \{\omega, \mathbf{b}\}, \mathfrak{X}) = -L(\theta = \{\omega, \mathbf{b}\}, \mathfrak{X}) \tag{8}$$

And the gradient descent is applied for minimizing arbitrary non-linear functions. Then we set the sparse coefficients to zeros which belongs to the background and the interference, when the probability of background is larger than useful information’s. And the shrink criterion is depicted as:

$$\varphi_t = \begin{cases} 0 & \text{if } t \in I[0] \\ 0 & \text{if } t \in I[1] \& P_{I[0]} > P_{I[2]} \\ \varphi_t & \text{else} \end{cases} \tag{9}$$

3.3 Data Repair

After the processing of data shrink, we get a more ‘clean’ sparse coefficients set. However, the non-zero coefficient values are not so smooth in samples. Some of them should be pulled up or down to smooth the representations well. Kernel density estimation (KDE) is a non-parametric way to estimate the probability density function and to make the data more smooth [12, 13] KDE differs from the parametric approach in

that kernel density estimation does not force the distribution to take on any pre-defined shape; instead, it lets the data speak for itself.

Let $(\varphi_t^1, \varphi_t^2 \dots \varphi_t^n)$ be an independent and identically distributed sample with an unknown density. Its kernel density estimator is

$$\hat{f}(\varphi_t) = \frac{1}{nh} \sum_{i=1}^n K\left(\frac{(\varphi_t - \varphi_t^i)}{h}\right) \quad (10)$$

here K is the kernel function. A range of kernel functions are commonly used: gaussian, Epanechnikov, tophat, exponential and others. And $h > 0$ is a bandwidth parameter which is crucial to dictate the smoothness, controls the tradeoff between bias and variance in the result. A large bandwidth can lead to a very smooth (i.e. high-bias) density distribution, meanwhile, a small bandwidth can lead to an unsmooth (i.e. high-variance) density distribution. However, choosing the optimal bandwidth is not a simple task and is often done by attempting to maximize the asymptotic integrated mean squared error (AMISE).

A simple way to select a bandwidth parameter is to choose a known distribution, such as Gaussian, and assume that its AMISE optimal bandwidth is sufficient for other distributions. The optimal bandwidth for Gaussian kernel is given as

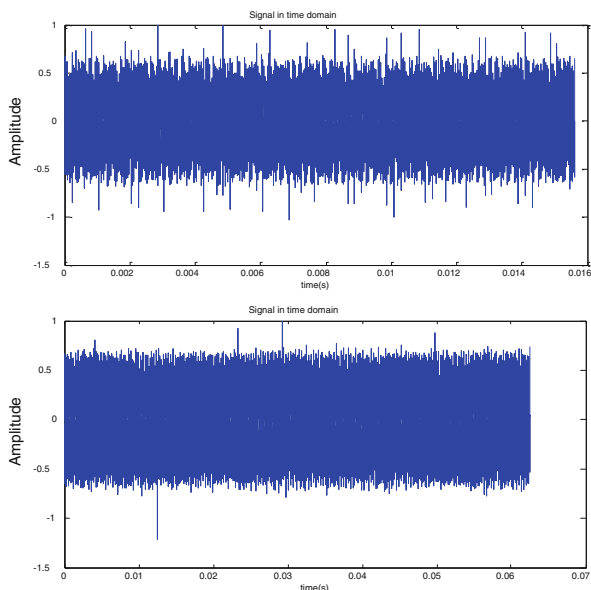
$$h = \left(\frac{4\hat{\sigma}}{3n}\right)^{1/5} \quad (11)$$

And $\hat{\sigma}$ is the standard deviation of the samples.

4 Experimental Results

In this section, to evaluate the performances of our novel system, we conducted the experiments on 1500 data blocks as the training data at the same receiving condition. And the size of block was 20×20 . We used a LCD monitor as a leakage source which resolution is 1024×768 . The signal was received by a frequency spectrometer, and it connected to a transmission line with a current clamp. Then the experimental results are displayed according to the steps in our system, at the same time, a kind of no-reference image quality assessment [14] is applied to evaluate the performance of our framework. The original received signals and their reconstruction images are shown in Fig. 2.

In order to classify the different categories of image blocks, we use multi-classifier to distinguish the signal to three categories, they are background (0 class), interference signal (1 class) and useful information (2 class). And the sparse coefficients of some blocks are set to zeros according to the shrink criterion. The processing results are shown in Fig. 3.



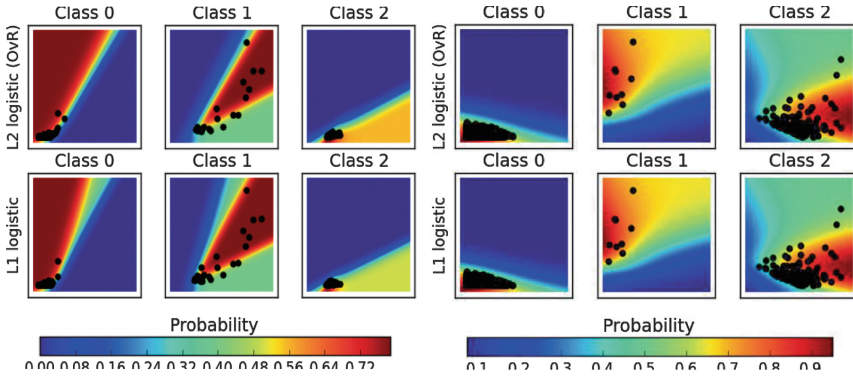
(a) Received one-dimensional signals



(b) Reconstructed display images

Fig. 2. Two received signals and their reconstructed images

The prediction accuracies of data with fewer characters are 89 % and 88.3 % using the two logistic regression methods with L2 and L1 regularizations. And the prediction accuracies of data with more characters are lower as 74.2 % and 74.2 % respectively. It can be found that the error prediction is higher around the edges of character when the character's space is less. According to the principle of our framework, the received signals are repaired further, and the results are shown in Fig. 4.



(a) The probability distributions for multi-class using logistic regression



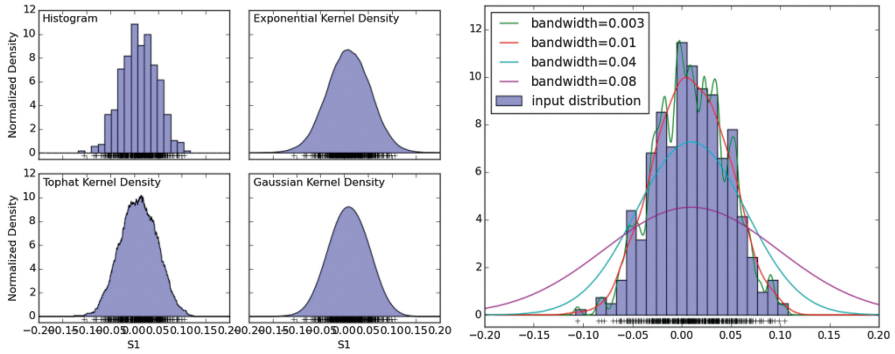
(b) The results after data shrink

Fig. 3. Two kinds logistic regression algorithms are implemented, the two categories (0 class, 1 class) are shrunk by setting sparse coefficients to zeros.

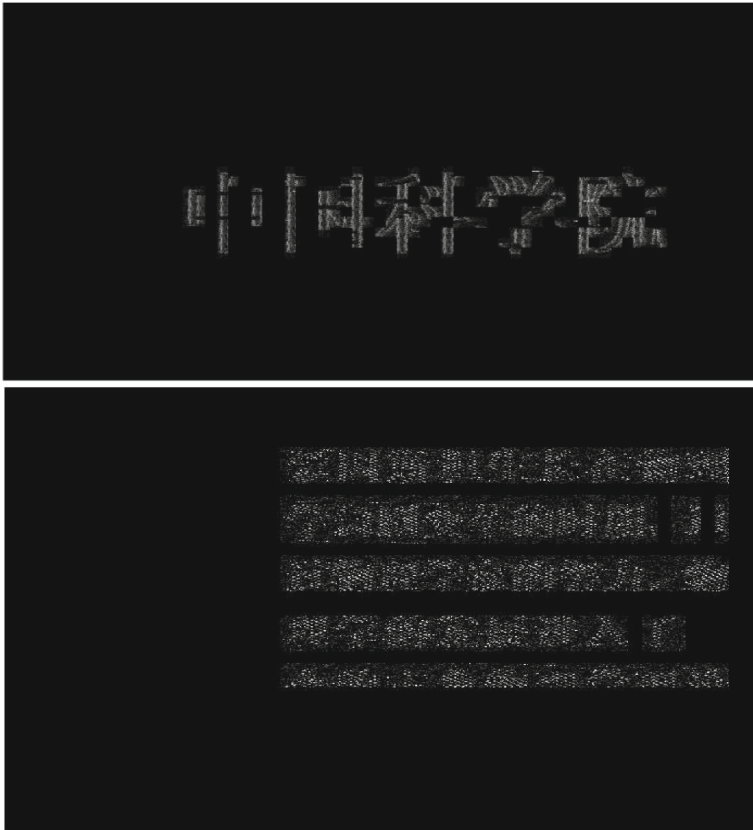
From Fig. 4, it can be seen that visual qualities of reconstructions were improved, and the lost strokes were compensated in some locations. Comparing with the data with more characters, the one with fewer characters had better performance.

In order to measure the effectiveness of our methods objectively, we explored the no-reference evaluation algorithm proposed in [14] to assess the image equality, and the results are given in Table 1.

Table 1 described the non-reference image equality assessment results for the original image and the new image processed by our method respectively. It can be observed that all the scores of new images are great higher than the original ones, such as φ_{data1} , the original score is 17.4439, and the highest score of new image is 63.6877 when the bandwidth is 0.01. This proved that the novel system had a better performance for the weak information recovery.



(a) The fit results of statistical property



(b) The results after data repair

Fig. 4. The fit results using different kernel functions are given in the left of (a), and Gaussian Kernel density is chosen, the fit results using different bandwidths are given in the right of (a). The reconstruct images shown in (b) are attained using the bandwidth as 0.01.

Table 1. The no-reference assessment of image equality

Sparse coefficients	Assessment	KDE	Original	bandwidth				
				0.001	0.003	0.01	0.02	0.1
φ_{data1}	SSEQ	gaussian	17.4439	63.5813	63.5786	63.6205	62.9068	63.5504
		tophat		63.5842	63.5854	63.6877	62.9676	63.5742
gaussian		12.4420	55.9110	55.9018	55.9260	56.0574	56.6080	
tophat			55.9100	55.9038	55.9073	55.9057	55.9182	

5 Conclusion

In this paper, we proposed a novel framework to improve the ability of eavesdropping for electromagnetic leakage by means of making the reconstruction image clearer. Our framework is different from the filter and enhancement technologies in image filed, it improve the visual quality of image by modifying the sparse coefficients based on some machine learning algorithms. It can remove the interference and only reserve the information at the data shrink step. Meanwhile, it can complement the missing part and compensate the distortion at the data repair step. The experimental results had shown that our framework works well. In the future work, we hope to import more methods to process the sparse coefficients and improve the image quality further.

Acknowledgment. This work was supported by the National Natural Science Foundation of China (Grant No.61401460).

References

1. Elibol, F., Sarac, U., Erer, I.: Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system. In: 20th European Signal Processing Conference (EUSIPCO, 2012), pp:1767–1771 (2012)
2. van Eck, W.: Electromagnetic radiation from video display units: an eavesdropping risk? *Comput. Secur.* **4**, 269–286 (1985)
3. Vuagnoux, M., Pasini, S.: An improved technique to discover compromising electromagnetic emanations, Electromagnetic Compatibility (EMC), 2010 In: IEEE International Symposium on Digital object Identifier, pp:121–126 (2010)
4. Tosaka, T., Yamanaka, Y., Fukunaga, K.: Method for determining whether or not information is contained in electromagnetic disturbance radiated from a PC display. *IEEE Trans. Electromagn. Compat.* **53**(2), 318–324 (2011)
5. Kuhn, M.G.: Compromising Emanations of LCD TV Sets. In: IEEE International Symposium on Electromagnetic Compatibility (EMC, 2011), Long Beach, pp. 931–936, 14–19 August 2011
6. Koksaldi, N.E., Olcer, I., Yapanel, U., Sarac, U.: Signal processing applications for information extraction from the radiation of VDUs, National Institute of Electronics & Cryptology, Kocaeli, vol. 41470
7. Tang, Y.: Research on monitoring platform of computer video leaking signal, East China normal university, March 2011

8. Zheng, Z., Yong, X., Jian, Y.: A survey of sparse representation: algorithms and applications. *IEEE Access* **3**, 490–530 (2015)
9. Yanhui, X., Zhengfeng, Z., Yao, Z.: Kernel reconstruction ICA for sparse representation. *IEEE Trans. Networks Learn. Syst.* **26**(6), 1222–1232 (2015)
10. Christopher, M.B.: *Pattern Recognition and Machine Learning*, pp. 205–210. Springer, New York (2006). ISBN: 0-387-31073-8
11. Wenping, Hu, Qian, Yao, et al.: Improved mispronunciation detection with deep neural network trained acoustic models and transfer learning based logistic regression classifiers. *Speech Commun.* **67**, 154–166 (2015)
12. Gonzalez, R. et al.: Process monitoring using kernel density estimation and Bayesian networking with an industrial case study. *ISA Transactions* (2015). <http://dx.doi.org/10.1016/j.isatra.2015.04.001>
13. Silverman, B.W.: *Density Estimation for Statistical and Data Analysis*, p. 48. Chapman & Hall/CRC, London (1998). <http://dx.doi.org/10.1016/j.isatra.2015.04.001>. ISBN: 0-412-24620-1
14. Liu, L., Liu, B., Huang, H., Bovik, A.C.: No-reference image quality assessment based on spatial and spectral entropies. *Sig. Process. Image Commun.* **29**(8), 856–863 (2014)