Journal of Industrial Engineering Research, 1(2) March 2015, Pages: 38-44

IWNEST PUBLISHER

Journal of Industrial Engineering Research

(ISSN: 2077-4559)

Journal home page: http://www.iwnest.com/AACE/

Efficient Restoration of Corrupted Images and Data Hiding in Encrypted Images

Lis Sebastian Dr. J. Subash Chandra Bose

ME CSE Associate Professor and Head Department of Computer Science & Engineering, Professional Group of Institutions, Palladam, Trippur, Tamilnadu, India.

ARTICLE INFO

Article history:
Received 22 February 2015
Accepted 20 March 2015

Keywords:
Corrupted Images
Data Hiding
Encrypted Images

ABSTRACT

The distribution of mixed noise, Additive White Gaussian noise (AWGN) coupled with impulse noise (IN), in images does not have a parametric model and has a heavy tail. So the removal of mixed noise from natural images is a difficult task. The proposed method, weighted encoding with sparse nonlocal regularization (WESNR), is used to remove IN and AWGN simultaneously. In WESNR, there is soft impulse pixel detection via weighted encoding is used to deal with IN and AWGN simultaneously. Meanwhile, the image sparsity prior and nonlocal self-similarity prior are integrated into a regularization term and introduced into the variational encoding framework. The Experimental results show that the proposed WESNR method achieves leading mixed noise removal performance in terms of both quantitative measures and visual quality. The denoised image is then used for data hiding by encrypting images. Since data hiding in encrypted images maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. Here we propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. The Implementation has been done by using MATLAB13.

© 2015 IWNEST Publisher All rights reserved.

To Cite This Article: Lis Sebastian,Dr. J. Subash Chandra Bose., Efficient Restoration of Corrupted Images and Data Hiding in Encrypted Images. **J. Ind. Eng. Res.,** ***1(2),*** *38-44, 2015*

INTRODUCTION

Denoising (or noise removal) in image processing, aims to restore the original image from its noise corrupted observation while preserving as much as possible the image edges, textures and fine scale details. Two types of commonly encountered noise are additive white Gaussian noise (AWGN) and impulse noise (IN). An image corrupted by IN will have a portion of its pixels replaced by random noise values with the remaining pixels unchanged. Two types of widely encountered IN are salt-and-pepper impulse noise (SPIN) and random-valued impulse noise (RVIN). An image corrupted by SPIN shows dark pixels in bright regions and bright pixels in dark regions. Weighted Encoding with Sparse Nonlocal Regularization (WESNR) algorithm encode each noise-corrupted patch of an image using a pre-learned dictionary to remove the mixed noise of IN and AWGN simultaneously over a soft impulse pixel detection manner. In WESNR, the mixed noise is removed by weighting the encoding residual gradually so that the final encoding residual will tend to follow Gaussian distribution. The weighted encoding and sparse nonlocal regularization are unified into a framework, which is variational and is easy to minimize. The performance measures in WESNR method with other previous methods can be compared using measures such as PSNR Peak Signal to Noise Ratio and FSIM image perceptual quality index.

The amount of digital images has been increased rapidly for many applications such as confidential transmission, video surveillance, military and medical applications. The solutions for security are encryption and data hiding. There are several methods to encrypt binary images. Major objective of the project is reserving Room before encryption with a traditional RDH algorithm. Reversible data hiding algorithms on encrypted images can be done by first emptying out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data. Remove the embedded data during the decryption step and also decode the cover image. Here also the performance measure is based on PSNR.

Corresponding Author: Lis Sebastian, Dr. J. Subash Chandra Bose, ME CSE, Associate Professor and Head Department of Computer Science & Engineering, Professional Group of Institutions, Palladam, Trippur, Tamilnadu, India.

Journal of Industrial Engineering Research, 1(2) March 2015, Pages: 38-44

II. Related Work:

A. Noise Removal Algorithm with an Impulse Detector:

For identifying noise pixels in images corrupted with impulse noise of random values a local image statistic was introduced. The difference in intensity of the neighbouring pixels are measured by the above statistical values. To remove additive Gaussian noise this statistic may be incorporated into a filter. This method will blur edges of the images significantly. This is not an effective method. This method leaves grainy visually disappointing results.

B. Image Denoising by Sparse 3-D Transform-Domain Collaborative Filtering:

This method proposes an image denoising strategy based on an enhanced sparse representation in transform domain. High computation is necessary in this method.

C. Mixed Gaussian-Impulse Noise Image Restoration Via Total Variation:

For Gaussian and impulse noise here proposes a simple cost functional consisting of a TV regularization term and _2 and _1 data fidelity terms with local regularization parameters selected by an impulse noise Detector. There is poor performance in Impulse Noise. This method removes desirable details. When the noise density is high there is poor performance.

D. Reversible Data Hiding:

Digital watermarking, often referred to as data hiding, has recently been proposed as a promising technique for information assurance. Frequently used watermarking techniques, called quantization index modulation quantization error renders lossy data hiding.

E. Reversible Data Hiding: Principles, Techniques and Recent Studies:

Data hiding are a group of techniques used to put a secure data in a host media with small deterioration in host and the means to extract the secure data afterwards. For example, steganography can be named. Steganography is one such pro security innovation in which secret data is embedded in a cover. But, this paper will get into reversible data hiding. Reversible data hidings insert information bits by modifying the host signal, but enable the exact restoration of the original host signal after extracting the embedded information. Sometimes, expressions like distortion free, invertible, lossless or erasable watermarking are used as synonyms for reversible watermarking. In most applications, the small distortion due to the data embedding is usually tolerable.

III. Proposed Algorithm:

The modified WESNR algorithm is used to overcome the Problem of sequential removal of mixed noise found in the previous methods. WESNR proposes an effective encoding based method for mixed noise removal, encode each noise-corrupted patch over a pre-learned dictionary to remove the IN and AWGN simultaneously in a soft impulse pixel detection manner. Meanwhile, the image sparsity prior and nonlocal self-similarity prior are integrated into a regularization term and introduced into the variational encoding framework.

Mixed Noise Removal algorithm consists of consider two types of mixed noise:

A. The Mixed Noise:

Denote by $\boldsymbol{x}$ an image and by $x_{i,j}$ its pixel at location (i, j). Let $\boldsymbol{y}$ be the noisy observation of $\boldsymbol{x}$. For AWGN, each noisy pixel $y_{i,j}$ in $\boldsymbol{y}$ is modelled as $y_{i,j} = x_{i,j} + v_{i,j}$, where $v_{i,j}$ is i.i.d. noise and follows zero mean Gaussian distribution.

1) AWGN mixed with SPIN
2) AWGN mixed with RVIN and SPIN.

B. The Denoising Model:

Denote by $\boldsymbol{x} \in \mathbb{R}^N$ an image. Let $\boldsymbol{x}_i = \boldsymbol{R}_i\boldsymbol{x} \in \mathbb{R}^n$ be the stretched vector of an image patch of size $\sqrt{n} \times \sqrt{n}$, where $\boldsymbol{R}_i$ is the matrix operator extracting patch $\boldsymbol{x}_i$ from $\boldsymbol{x}$ at location i. There is an over-complete dictionary based on the sparse representation theory $\boldsymbol{\Phi} = [\varphi_1; \varphi_2; \ldots; \varphi_n] \in R^{n\times m}$ to sparsely code $\boldsymbol{x}_i$ where $\varphi_j \in R^n$ is the j th atom of $\boldsymbol{\Phi}$. The representation of $\boldsymbol{x}_i$ over dictionary $\boldsymbol{\Phi}$ can be written as $\boldsymbol{x}_i = \boldsymbol{\Phi}\boldsymbol{\alpha}_i$, where $\boldsymbol{\alpha}_i$ is a sparse coding vector with only a few non-zero entries. The equation for the image is x= $\boldsymbol{\Phi\alpha}$ where α is the set of all coding vectors $\boldsymbol{\alpha}_i$. To encode the noisy observation y over the dictionary $\boldsymbol{\Phi}$ to obtain the desired α. In the case of AWGN, the encoding model can be generally written as $\hat{\alpha} = \arg\min_{\alpha} \|y - \boldsymbol{\Phi}\alpha\|_2^2 + \lambda R(\alpha),$ where $R(\boldsymbol{\alpha})$ is some regularization term imposed on $\boldsymbol{\alpha}$ and λ

Journal of Industrial Engineering Research, 1(2) March 2015, Pages: 38-44

is the regularization parameter. This motivates us to adopt the robust estimation technique to weight the data fitting residual so that its distribution can be more regular.

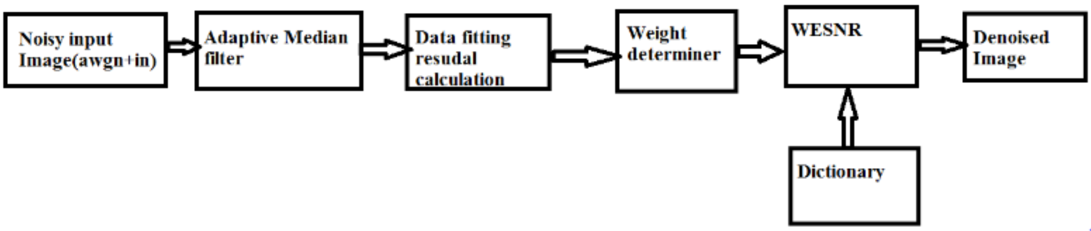
Let $e = [e1, e2, \ldots, eN] = y - \boldsymbol{\Phi}\boldsymbol{\alpha}$ where $ei = (\boldsymbol{y} - \boldsymbol{\Phi\alpha})(i)$. Assume that $e1, e2, \ldots, eN$ are i.i.d. samples. To weaken the effect of the irregularity in mixed noise distribution, we can assign each residual a proper weight, resulting in a weighted residual: $e_i^w = w_i^{1/2} e_i$. There introduced a new model for mixed noise removal: $\hat{\alpha} = \arg\min_{\alpha} \|\boldsymbol{W}^{1/2}(\boldsymbol{y} - \boldsymbol{\Phi\alpha})\|_2^2 + \lambda R(\boldsymbol{\alpha}),$ where $\boldsymbol{W}$ is a diagonal weight matrix with diagonal element $Wii = wi$, some regularization terms $R(\boldsymbol{\alpha})$ can be used to make the above weighted encoding model more effective for mixed noise removal . To make the weighted encoding stable and easy to control, we set $Wii \in [0, 1]$. One simple and appropriate choice of Wii is $Wii = exp(-ae_i)^2$, where a is a positive constant to control the decreasing rate of Wii w.r.t. ei . If a patch and its nonlocal prediction are encoded by a given dictionary $\boldsymbol{\Phi}i$, i.e., $\boldsymbol{x}i = \boldsymbol{\Phi}i\boldsymbol{\alpha}i$ and $\hat{}\boldsymbol{x}i = \boldsymbol{\Phi}i\boldsymbol{\mu}i$, then the coding coefficients $\boldsymbol{\alpha}i$ and $\boldsymbol{\mu}i$ should also be similar. Therefore, we can use $\sum_i \|\boldsymbol{\alpha}_i - \boldsymbol{\mu}_i\|_{l_p}$ as the regularization term to regularize the solution of $\hat{\alpha} = \arg\min_{\alpha} \|W^{1/2}(y - \Phi\alpha)\|_2^2 + \lambda \sum_i \|\alpha_i - \mu_i\|_{l_p},$ where $l\,p$ $(p = 1$ or $2)$ refers to the $l\,p$-norm.

Let $\boldsymbol{V}$ be a diagonal matrix. We first initialize it as an identity matrix, and then in the $(k+1)^{th}$ iteration, each element of $\boldsymbol{V}$ is updated as $V_{ii}^{(k+1)} = \lambda / ((\boldsymbol{\alpha}_i^{(k)} - \mu_i)^2 + \varepsilon^2)^{1/2}$ where ε is a scalar and $\alpha(k)\ i$ is the i^{th} element of coding vector $\boldsymbol{\alpha}$ in the k^{th} iteration.

Then we update $\boldsymbol{\alpha}$ as

$$\hat{\alpha}^{(k+1)} = (\boldsymbol{\Phi}^T \boldsymbol{W\Phi} + \boldsymbol{V}^{(k+1)})^{-1} (\boldsymbol{\Phi}^T \boldsymbol{Wy} - \boldsymbol{\Phi}^T \boldsymbol{W\Phi\mu}) + \boldsymbol{\mu}. \quad (1)$$

By iteratively updating $\boldsymbol{V}$ and $\boldsymbol{\alpha}$, the desired $\boldsymbol{\alpha}$ can be efficiently obtained.



Block Diagram WESNR

C. The Dictionary:

To make a set of local PCA dictionaries from natural images, We use the same 5 high-quality images . A number of 876,359 patches. (size: 7×7) are extracted from the five images and they are clustered into 200 clusters by using the K-means clustering algorithm. For each cluster, a compact local PCA dictionary is learned. Meanwhile, the centroid of each cluster is calculated. For a given image patch, the Euclidian distance between it and the centroid of each cluster is computed, and the PCA dictionary associated with its closest cluster is chosen to encode the given patch.

D. Algorithm of WESNR:

Step 1: Input dictionary $\boldsymbol{\Phi}$, noisy image y.
Initialize $\boldsymbol{e}, \boldsymbol{W}, \mu = 0$.
Repeat the following step2 - step5 with k =1,2,3,.., K
Step 2: Compute $\boldsymbol{\alpha}^{(k)}$
Step 3: Compute $\boldsymbol{x}^{(k)} = \boldsymbol{\Phi}\,\boldsymbol{\alpha}^{(k)}$ and update the nonlocal coding vector μ
Step 4: Compute the residual $\boldsymbol{e}^{(k)} = \boldsymbol{y} - \boldsymbol{x}^{(k)}$
Step 5: Calculate the weights $\boldsymbol{W}$ ***by*** $\boldsymbol{e}^{(k)}$
Step 6: Output the denoised image $\boldsymbol{x} = \boldsymbol{\Phi}\,\boldsymbol{\alpha}^{(k)}$

The WESNR algorithm is used to remove mixed noise from natural images. The noisy image is given as input. Once the dictionary $\boldsymbol{\Phi}$ is determined for a given patch of the image, the proposed WESNR model can be solved by iteratively updating $\boldsymbol{W}$ and $\boldsymbol{\alpha}$. The updating of $\boldsymbol{W}$ depends on the coding residual $\boldsymbol{e}$.

In AWGN and SPIN , AMF is widely used to detect SPIN. In order to make a fair comparison with them, in the case of mixed noise , AWGN+SPIN noise removal, we apply AMF to $\boldsymbol{y}$ to obtain an initialized image $\boldsymbol{x}^{(0)}$, and then initialize $\boldsymbol{e}$ as: $\boldsymbol{e}^{(0)} = \boldsymbol{y} - \boldsymbol{x}^{(0)}$ **.**

In the case of AWGN+RVIN+SPIN noise removal, AMF cannot be applied to $\boldsymbol{y}$ to initialize $\boldsymbol{x}$. We initialize $\boldsymbol{e}$ as **:** $\boldsymbol{e}^{(0)} = \boldsymbol{y} - \boldsymbol{\mu}_{\boldsymbol{y}.\boldsymbol{1}}$, where μy is the mean value of all pixels in $\boldsymbol{y}$ and **1** is a column vector whose elements are all 1. Ie. the mean value of $\boldsymbol{y}$ to initialize $\boldsymbol{x}$. Then the initial coding residual can be roughly computed. With the

Journal of Industrial Engineering Research, 1(2) March 2015, Pages: 38-44

initialized coding residual $e^{(0)}$, ***W*** can be initialized by $\mathbf{W_{ii = exp(-aei}^2)}$, where *a* is a positive constant to control the decreasing rate of W_{ii} w.r.t. *ei* . the pixels corrupted by IN will be adaptively assigned with lower weights to reduce their impact in the process of encoding. ***W*** is a diagonal weight matrix, and its element W_{ii} is to be automatically determined and assigned to pixel *i* . the coding residual e_i can be used to guide the setting of weight *Wii* , and *Wii* should be inversely proportional to the strength of *ei* . set $W_{ii} \in [0, 1]$.

In the case of AWGN+RVIN+SPIN noise removal, AMF cannot be applied to ***y*** to initialize ***x***. We initialize ***e*** as **:** $\boldsymbol{e^{(0)}=y - \mu_{y.1,}}$ where μy is the mean value of all pixels in ***y*** and **1** is a column vector whose elements are all 1. Ie. the mean value of ***y*** to initialize ***x***. Then the initial coding residual can be roughly computed. With the initialized coding residual $e^{(0)}$, ***W*** can be initialized by $W_{ii = exp(-aei}^2)$, where *a* is a positive constant to control the decreasing rate of W_{ii} w.r.t. *ei* . the pixels corrupted by IN will be adaptively assigned with lower weights to reduce their impact in the process of encoding. ***W*** is a diagonal weight matrix, and its element W_{ii} is to be automatically determined and assigned to pixel *i* . the coding residual e_i can be used to guide the setting of weight *Wii* , and *Wii* should be inversely proportional to the strength of *ei* . set $W_{ii} \in [0, 1]$.

Algorithm 1:

Set $t = \|\boldsymbol{\Phi\alpha}^{(k+1)} - \boldsymbol{\Phi\alpha}^{(k)}\|_2 / \|\boldsymbol{\Phi\alpha}^{(k)}\|_2 < \tau$ as the termination condition. Because of the weighting matrix ***W***, the IN pixels in the image can be well identified and their effect is suppressed in the encoding of ***y***. As a result, both IN and AWGN will be gradually removed in the iteration.

In data hidng scheme in encrypted images , reversible data hiding scheme is replaced by rationale rhombus method. It is the best technique to use in RDH. The algorithm used for rational rhombus method is simple and it provide cover image without any loss. Reserving room before encryption (RRBE). Elaborate a practical method based on this Framework, which primarily consists of four stages: generation of encrypted image, data hiding in encrypted image, data extraction and image recovery. The reserving operation adopt in the proposed method is the modification made in this project. Rationale rhombus method is used to establish the RDH approach. For the secret data hiding the simple method LSB replacement is used.

A. Generation Of Encrypted Image:

To construct the encrypted image, the first stage can be divided into three steps: image partition, self reversible embedding followed by image encryption. At the beginning, image partition step divides original image into two parts A and B; then, the LSBs of A are reversibly embedded into B using rationale rhombus algorithm so that LSBs of A can be used for accommodating messages.

1) Image Partition:

The operator here for reserving room before encryption is a standard RDH technique, so the goal of image partition is to construct a smoother area B, on which rationale rhombus algorithms can achieve better performance. To do that, without loss of generality, assume the original image C is a gray-scale image with its size M x N, it is divided in to two equal sized images. In this the B part has the smoother area to apply the RDH technique. The LSBs of the pixels of A where the data is hiding is stored. Fig. 3 Illustration of image partition and embedding process.

2) Self-Reversible Embeddiing:

The goal of self-reversible embedding is to embed the LSB - planes of A into B by employing rationale rhombus algorithm. Where the datas have to be stored in the LSB – planes of A.

3) Image Encryption:

After self-embedded image and reserving rooms for data hiding the encryption is done with the help of encryption key. The encryption key is an 8 bit word. In this the encryption is done by XORing the image with the key. After all this steps the content owner sends the locations where the data can be embedded along with the encrypted image.

B. Data Hiding In Encrypted Image:

Once the data hider acquires the encrypted image, he can embed some data into it, although he does not get access to the original image. The embedding process starts with locating pixels in which the data can embed in the encrypted version of image. Since the data hider has the locations where the data can be embedded it is effortless for the data hider to read bits information in LSBs of encrypted pixels. After knowing how many bit-planes and rows of pixels he can modify, the data hider simply adopts LSB replacement to substitute the

Journal of Industrial Engineering Research, 1(2) March 2015, Pages: 38-44

available bit-planes with additional data. Finally, the data hider encrypts according to the data hiding key to formulate encrypted image containing data.

C. Data Extraction And Image Recovery:

For data extraction and image recovery both the encryption key and the data hiding key are used to extract the data and then the image . Hence the encrypted image containing data is first decoded using the data hiding key and then the data stored in the LSBs of the pixels in the image are extracted. Then the image once again decoded with the encryption key. Then by applying the rationale rhombus algorithm for data extraction the LSB values are restored and placed it in its own position using LSB replacement algorithm.

A. Rationale Rhombus Method:

Rationale rhombus method used to store the LSB values of the pixel of the A portion of the image. In an image the adjacent pixels have the pixel value in less difference. So while considering a rhombus in the pixels the pixel centered by the four pixels has the average value of the four pixels. This technique is used to develop the rationale rhombus algorithm.

B. LSB Replacement Algorithm:

In this algorithm embed the each bit of the data in the least significant bits places of the original image. The embedding of the data is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with embedding bits. The extraction of the data is performed by extracting the least significant bit of each of the selected image pixels. If the extracted bits match the inserted bits, then the stored is detected. The extracted bits do not have to exactly match with the inserted bits. A correlation measure of both bit vectors can be calculated. If the correlation of extracted bits and inserted bits is above a certain threshold, then the extraction algorithm can decide that the data is detected.

Step 1. Load the original image.
Step 2. Load the embedding data.
Step 3. Determine the value of the embedding factor (factor that represents how many bits of the datas are embedded in the LSB's of the original image).
Step 4. Call the embedding function to embed the bits in the
least significant bits of the original image.
Step 5. Use the extraction function to extract the watermark.

E. Results:

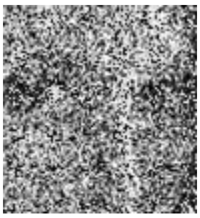



Image corrupted by mixed noise AWGN+SPIN — Output of WESNR

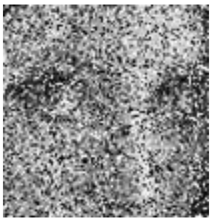



Image corrupted by mixed noise AWGN+RVIN +SPIN — output of WESNR

Journal of Industrial Engineering Research, 1(2) March 2015, Pages: 38-44

Original Image Encrypted Image Containing data Recovered Image

V. Conclusion:

The proposed WESNR algorithm for the mixed noise removal can be implemented successfully on Images which are corrupted by additive white Gaussian noise mixed with impulse noise. This paper adopted the weighted encoding technique to remove Gaussian noise and impulse noise jointly. It encoded the image patches over a set of PCA dictionaries, and weighted the coding residuals to suppress the irregularityof the distribution. The weights were adaptively updated to decide whether a pixel is heavily corrupted by impulse noise or not. Meanwhile, image sparsity prior and nonlocal self-similarity prior were integrated into a single nonlocal sparse regularization term to enhance the stability of weighted encoding. The results clearly demonstrated that WESNR outperforms much other state-of-the-art mixed noise removal methods.

This data hiding method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images. The image is secured during transmission and secret data is also transmitted securely. Confidentiality of image and data is maintained.

Running Time (Second) Comparison on Image Lena With Different Levels of AWGN+RVIN+SPIN

	TF	ROR-NLM	M+BM3D	WESNR
$\sigma = 5, r = 5\%, s = 50\%$	9	317	**4**	103
$\sigma = 10, r = 10\%, s = 40\%$	9	303	**4**	97
$\sigma = 15, r = 15\%, s = 30\%$	9	335	**4**	87

Journal of Industrial Engineering Research, 1(2) March 2015, Pages: 38-44

REFERENCES

[1] Mixed Noise Removal by Weighted Encoding With Sparse Nonlocal Regularization Jielin Jiang, Lei Zhang, *Member, IEEE*, and Jian Yang, *Member, IEEE*.
[2] A Universal Noise Removal Algorithm with an Impulse Detector Roman Garnett, Timothy Huegerich, Charles Chui, Fellow, IEEE, and Wenjie He*, Member, IEEE.
[3] Image Denoising by Sparse 3-D Transform-Domain Collaborative Filtering Kostadin Dabov, Student Member, IEEE , Alessandro Foi, Vladimir Katkovnik, and Karen Egiazarian, Senior Member, IEEE
[4] MIXED GAUSSIAN-IMPULSE NOISE IMAGE RESTORATION VIA TOTAL VARIATION P. Rodr´ıguez, R. Rojas B. Wohlberg fdgh.
[5] K-SVD: An Algorithm for Designing Overcomplete Dictionaries for Sparse Representation. Michal Aharon, Michael Elad, and Alfred Bruckstein.
[6] On the Role of Sparse and Redundant Representations in Image Processing Michael Elad, Senior Member, IEEE, Mario A.T. Figueiredo, Senior Member, IEEE, And Yi Ma, Senior Member, IEEE Invited Paper.