STRENGTHENING WAVELET-BASED IMAGE STEGANOGRAPHY USING THE EFFICIENT IMAGE SCRAMBLING METHOD

Jyoti Khandelwal[1*] and Yash Yadav[2]

Abstract.
Image steganography is the process of hiding secret information behind the cover image. This paper employs the graph wavelet method for image steganography. In the proposed work, the high-quality stego image is provided by the inter-pixel relationship management function of graph wavelet. A scrambling technique based on the pixel intensity of a 2D image is used to raise the secret image's degree of invisibility. Image extraction is the second goal, and it is accomplished using graph signal processing (GSP). Because it saves the neighborhood pixel information, GSP provides an extracted image of higher quality. In the section on experimental results, the value of the blending coefficient is changed to improve the look of both the stego image and the secret image that was extracted from it. For the suggested technique between cover and stego images, the peak signal-to-noise ratio (PSNR) ranges from 44.99 to 37.72 dB for different alpha values. The parameters of the naturalness image quality evaluator (NIQE) is used to analyze the secret image that has been extracted. For the extracted secret image, the NIQE observer score is 3.49. The proposed work tested against a dataset from a previously published paper. The resulting stego's are better and acceptable.

Keywords: Graph Signal Processing, Steganography, Wavelet, NIQE.

[1*]Department of Computer Science & Engineering, University of Engineering & Management Jaipur, India
Email: jyoti.khandelwal19@gmail.com
[2]Department of Computer Science & Engineering, University of Engineering & Management Jaipur, India
Email: yadavyash438@gmail.com

***Corresponding Author:** Jyoti Khandelwal
*****Department of Computer Science & Engineering, University of Engineering & Management Jaipur, India
Email: jyoti.khandelwal19@gmail.com

DOI: - 10.48047/ecb/2023.12.si10.00478

1 Introduction

With the advancements in the field of digital multimedia such as audio, image, text, and video the demand of creating, distributing, and transmitting through the internet is also increase. Therefore, the illegal activity over the information transmitted via the internet increased day by day. For finding the solution for this illegal activity, information system security many approaches are suggested. The most popular approaches are steganography and cryptography, the role of these approaches is to protect data from insecure and harmful activity [1].

Cryptography makes secret data non-readable to the unauthorized party; along with this line it is clear somehow the encryption of data gives an alert about the secret data presence. At the same place, steganography is the secure approach; it is protecting the secret data inside of another digital file which is known as a cover file. Steganography is an arising research field keeping the objective to give the best in the headway of information security [2]. No one should be able to tell the difference visually between the cover image and the stego image if users employ an effective technique of image steganography. In image steganography, the confidential data is represented as data bits and hidden behind the cover image [3]. Image steganography approach broadly classified into two main techniques: spatial domain and transfer domain [4]. Many signal processing strategies are depending on transform techniques, where the input data is represented is addressed in a new premise before investigation or handling. One of the best kinds of transform being used in wavelet analysis [5].

The graph-based data processing approach improved work in the field of technological, biological, social network and for improvement of classical signal processing methods [6]. Graph signal processing (GSP) represents data set information accurately. GSP tools also give the freedom to choose any graph according to the nature of signal. A graph can be denoted as $G = (V, E)$ with vertices (or nodes) in set V and links (or edges) as tuples (i, j) in E, graph future divided in two broad categories named as directed graph and undirected graph [7]. A complete graph can be represented by different topologies like: star graph, line graph, circular graph and mess graph [8].

In recent years, many complex wavelets transform such as tetrolet transform [9], curvelet transform [10], shift-invariant shearlet transform [11] and dual- tree complex wavelet [12] have been proposed. The GSP- based functioning now day follow by many signals, the reason of using graph wavelet – based techniques are (i) the graph wavelet provided better reconstruction because information used to perform reconstruction have localize, temporal and frequency related data [13]. (ii) To manage the multidimensional data graph is more suitable (i.e., image, social network analysis etc.). (iii) The graph wavelet opposes modifying the objective to corrupt or decimate the actual data [12].

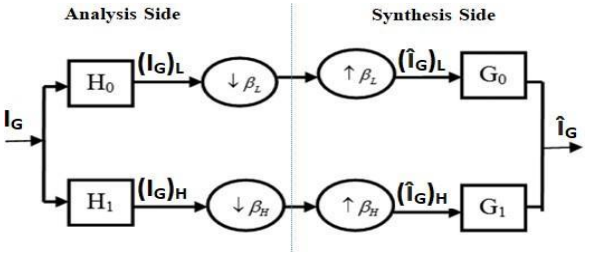


Fig. 1. Representation of analysis and synthesis filter side in graph wavelet.

In Fig.1, graph signal decomposed cover image I, into two-channel by wavelet filter bank. The $H0$ & $G0$ are low pass filter and $H1$ & $G1$ are high pass filter. The analysis side and the synthesis side are the two parts of the low pass and high pass filter, respectively. One side is called the analysis side, and the other is called the synthesis side. In the analysis side ↓ βL and ↓ βH show the down sampling operation for low pass filter, and ↑ βL and ↑ βH show the up-sampling operation for high pass filter [7].

This remaining paper is broken up into seven portions, and the following is a description of each one of them: The review of the connected work is the topic of discussion in Section 2. In the third section, we will discuss the graph as well as the use of graph signals in images. In section 4, we will discuss the graph wavelet steganography technique that has been suggested. The findings and comparative study of the experiments are presented in Section 5. In Section 6, we will discuss the effect that the proposed work will have on the performance analysis parameters. The final step is to make some conclusions.

2 Review of the Related Work

In image steganography safety of secret information, hiding capacity of cover image, and quality of stego image are three important factors. To achieve these three factors, new image steganography techniques have been developed [14]. In literature, many image steganography techniques have been explained for secret data hiding [15] and [16] include steganography algorithms of least significant bit and discrete

wavelet transform in terms of efficiency and capacity of concealing multiple images within a single cover image. Further, involves DWT – IDWT [17] associate with particle swarm improvement (PSO) algorithm, the aim of using PSO to produce effective choice of the pixels to embed the key signal within the image.
The robustness of stego image tested in [18] using different type of attacks. In this, data hide in image using DWT-HD-SVD and the finding is analyzed on invisibility and robustness key factors. Image quality estimation on different parameter presented in [19].

3 Graph

In the field of image feature extraction, now days graph used to represent an image. The natural process of feature extraction and understanding is easy if graph is used for the image. Graph contains nodes and edges in place of neurons and image processing they are responsible to capture the information.

3.1 Fundamental Definition

It is possible to describe a graph as a collection of Vertices (V) and the edges that connect them using the notation G $\subset V \times V$, where × stand for the direct product operation. In two major categories always find in graph named as directed and undirected graph [8].

3.2 Signals On Graphs

In classical signal processing (also known as CSP), the signal is sampled at consecutive time instants that are equally spaced apart. In CSP, the sequence of signal sampling begins with $x(n)$, followed by $x(n-1)$ and $x(n+1)$, which are used as the samples that came before and after $x(n)$, respectively. A number of different graph processing algorithms share a fundamental parameter: the time distance. The sampling instants relationship represented by graph. The sampling instant equally spaced by vertices and ordering of vertex, it is defined by edges when signal is sampled [20].

$$d: v \rightarrow c \quad (1)$$

In eq. (1), d represent dataset with complex scale data, and map as a graph signal. Where, v is set of nodes, and c is a collection of complex numbers.

3.3 Graph- Based Feature Extraction

Image processing is fundamental process in computer vision. In image processing graph signal processing (GSP) used for feature extraction. GSP provide a nice compact format to encode structure within data. Generalization of CSP tools can greatly benefit analysis of such data. The feature extraction using GSP classified as:
(a) Segmentation
(b) Filtering
(c) Classification and clustering

The GSP based segmentation is second step of image processing, first the image consisting of noise is removed by using filtering. Then resultant image is segmented using image segmentation method. The GSP, image segmentation performed by cut- vertex, Bi-partite graph, and minimal spanning tree [21] methods.

4 Proposed Method For Steganography

Encoding, also known as image hiding, and decoding, also known as image extraction, are the two primary processes that are involved in the image steganography scheme that has been suggested. In the process of encoding an image begin with scramble the sensitive secret image by using a technique that is based on the pixel intensity of a 2D image and some basic transformation functions. The image is given a random appearance thanks to this technique, and then a new scrambled secret image matrix is produced. The proposed image scrambling method can be defined as follows:

Algorithm 1: Image Scrambling
Step 1: Covert secret image matrix into single dimension array using row major method.
Step 2: Sort the single dimension array in descending order.
Step 3: Calculate the median intensity pixel and subtract its value from every pixel. Step 4: Convert the resultant single dimension array into matrix according to the secret image original size.
Step 5: Take the transpose of the resultant matrix.

Where, the sorting function used in algorithm step 2 is:
[value, location] =sort (A, 'descend') (2)
The sorting function is also able to return the array indices if the array A is M x N

matrix, then each column of 'location' is a permutation vector of the corresponding column of A, the returned indices preserve the original ordering which is used as a key at the time of secret image extraction. Scrambled secret images provide confidentiality in proposed system; in other words, scrambled secret images provide security and robustness in the system in the proposed image embedding process. The wavelet family always helps to improve the security of the image stereography process. In the proposed work, the graph wavelet is applied to scrambled secret and cover images. Additionally, the mixing of scrambled secret image and cover image is controlled by the alpha blending method, which ends up producing an alpha blending matrix. When the muddled secret image is encoded into the cover image, a process known as "alpha blending" reveals the transparent qualities of the color involved in the process. If the value of alpha is 0%, it indicates that the secret image is very visible; on the other hand, if the value of alpha is 100%, it indicates that the secret image is totally opaque.

When this blending procedure is complete, the stego image is created by applying the inverse of the graph wavelet. The analytic process is referred to as the graph wavelet, and the synthesis process is referred to as the inverse graph wavelet. Simply put, decoding is the process of flipping encoding on its head.

4.1 Secret Image Embedding Framework

The proposed image steganography method embedding framework block diagram show in Fig. 2.

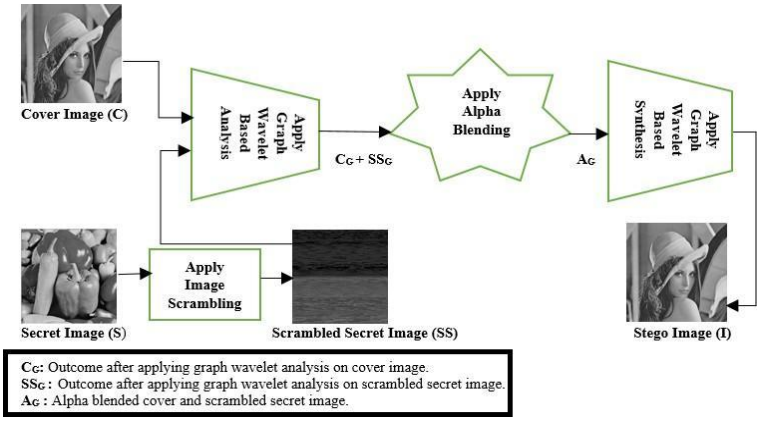


Fig. 2. Secret image embedding framework using proposed image steganography method.

4.2 Secret Image Extraction Framework

Applying graph wavelet to both the stego image and the cover image during the first step of the extraction process is followed by performing a subtraction procedure on both of these images. Second, in order to obtain a scrambled version of the secret picture, the synthesis process, which is the inverse of the graph wavelet, is applied. In the final step, the technique that was suggested to scramble the data should be reversed, and then the image should be rotated, flipped and inverse transpose. The image steganography method extraction framework block diagram that was suggested can be found in Fig. 3.

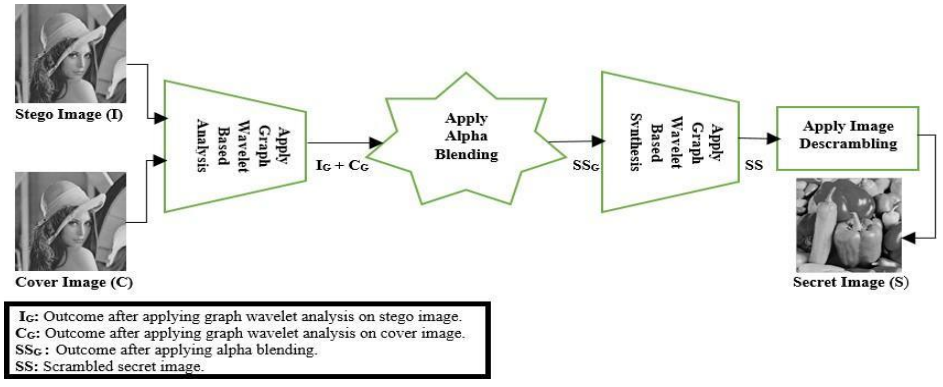


Fig. 3. Secret image extraction framework using inverse method of secret image embedding.

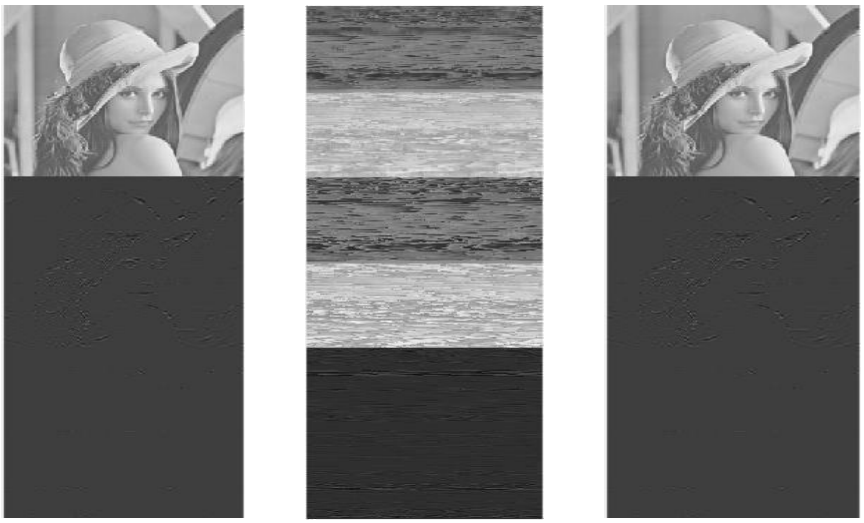
5 Experimental Results

This section includes the outcome of the proposed work. The quality of image steganography method depends upon the stego image and extracted secret image. As we show in Fig. 4(a-b-c); the standard well tested (a) Lenna, and (b) Pepper image taken as a cover and secret image respectively. The size of the both images are 256 x256, before embedding the secret image into cover image it is scrambled by proposed image scrambling method and result show in (c) part of Fig. 4.

(a) (b) (c)

Fig. 4. Image dataset used in proposed method (a) Cover image Lenna (b) Secret image Pepper (c) Scrambled secret image.

The alpha value takes between 0 and 1, here changes in alpha value show the secret image mixing quantity inside the cover image.



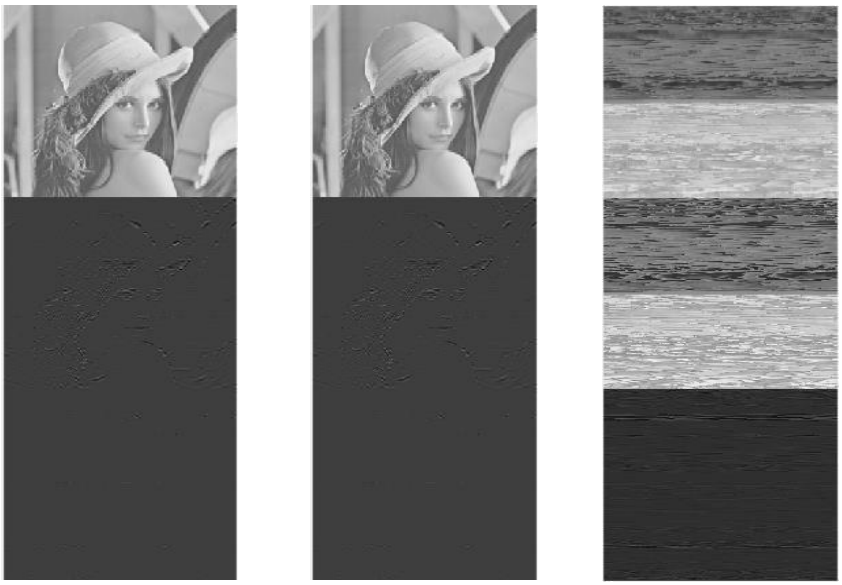
(a) (b) (c)

Fig. 5. Image embedding process
(a)Outcome of cover image, (b) Outcome of scrambled image, (c) Outcome of blended image.

In Fig. 5, Outcome images after applying graph- based analysis process in secret image embedding process shown.

Fig. 6. Outcome of embedding process: Stego image (I).

The graph-based synthesis process or we can say inverse of graph wavelet performed on the blended image represent in Fig. 5(c) and generate stego image (I) shown in Fig.
6. Outcome images after applying graph- based analysis process in secret image extraction process show in Fig. 7.



(a) (b) (c)

Fig. 7. Image extraction process (a) Outcome of Cover image, (b) Outcome of Stego image, (c) Outcome of blended image.

Fig. 8. Final outcome of proposed method: Extracted secret image (S).

After applying the extraction process to the stego image (I), the secret image (S) is extracted as a result (see Fig. 8). Following an examination of the data presented in Fig. 6 and 8, we are able to reach the conclusion that the quality of the stego and extracted secret image acceptable by the human visual system (HVS) and proposed method is improved.

6 Performance Analysis

The numerical assessment of proposed work outcome discusses in this section. The peak signal to noise ratio (PSNR) and mean square error (MSE) [19] are the basic parameter to analyze the quality of the image. The comparative study of quality between cover and stego image shown in Table 1.

Table 1. PSNR based comparison between cover image and stego image.

Alpha Value	PSNR (dB)	MSE
0.01	44.99	1.06
0.02	41.47	2.00
0.03	38.97	4.39
0.04	37.04	8.02
0.05	37.72	12.00

According to the Table 1, PSNR and MSE calculate over the different value of alpha. The value of alpha decided the mixing ratio of two images. The extracted secret image quality checked over naturalness image quality evaluator (NIQE) [22]. The lesser value of NIQE represent the acceptance of image in HVS. The initial and extracted secret images are represented by the NIQE of 3.52 and 3.49, respectively.
The comparison performs on [10], by using cover

and secret image dataset. According to the [10], image steganography performed using curvelet and genetic algorithm.

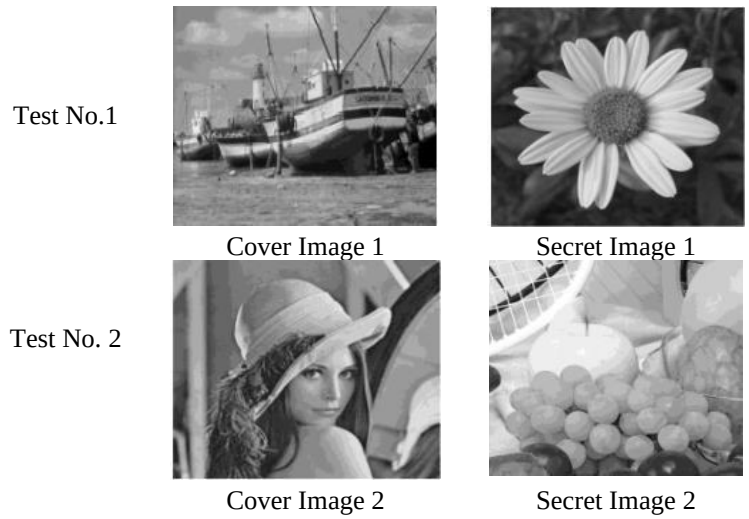


Fig. 9. Database of Cover and Secret Images Used in [10].

Fig. 9, show the collection of cover image and secret image used in [10], and Table 2 represent the outcome of the comparative stego result based on PSNR value.

Table 2. PSNR based stego image comparison between [10] and proposed method.

Test No.	PSNR (dB) [10]	PSNR(dB) Proposed Work
1	40.02	41.89
2	40.09	42.05

7 Conclusion & Future Scope

The graph wavelet-based image steganography method is strengthened in the proposed work. The proposed work uses a grayscale cover and a secret image. The scrambling technique based on the pixel intensity of a 2D image is used to provide the imperceptibility of the stego image. The quality of the stego image and the extracted secret image is analyzed by the PSNR, MSE, and NIQE parameters. The outcomes demonstrate the effectiveness of the suggested approach, which added high-quality stego and extracted a covert image. Also proposed work performed on reference [10] dataset, the stego generated by the comparative study are better from the previous work done by reference [10]. In the future, experiments can be performed using the image smoothening method based on deep learning.

References

1. Zaidan, F. K.: Digital Image Steganography scheme based on DWT and SVD. Diyala Journal of Engineering Sciences, 13(4), 10–17 (2020).
2. Tyagi, S., Saxena, A. K., & Dwivedi, R. K.: High capacity steganography protected using Shamir's threshold scheme and permutation framework. International Journal of Innovative Technology and Exploring Engineering, 8(9S), 784–795 (2019).
3. Ansari, A. S., Mohammadi, M. S., & Parvez, M. T.: A multiple-format steganography algorithm for color images. IEEE Access, 8, 83926–83939 (2020).
4. Kaur, M., & Kumar, V.: A comprehensive review on Image Encryption Techniques. Archives of Computational Methods in Engineering, 27(1), 15–43 (2018).
5. Hammond, D. K., Vandergheynst, P., & Gribonval, R.: Wavelets on graphs via spectral graph theory. Applied and Computational Harmonic Analysis, 30(2), 129–150 (2011).
6. Ortega, A., Frossard, P., Kovacevic, J., Moura, J. M., & Vandergheynst, P.: Graph Signal Processing: Overview, challenges, and applications. Proceedings of the IEEE, 106(5), 808– 828 (2018).
7. Narang, S. K., & Ortega, A.: Perfect reconstruction Two-channel wavelet filter banks for graph structured data. IEEE Transactions on Signal Processing, 60(6), 2786–2799 (2012).
8. Stanković, L., Daković, M., & Sejdić, E.: Introduction to graph signal processing. Signals and Communication Technology, 3–108 (2018).
9. Sarath, D., & Sucharitha, M.: A study on image retrieval based on Tetrolet transform. International Journal of Engineering & Technology, 7(3.27), 321 (2018).
10. Mostafa, H., Fouad, A., & Sami, G.: A hybrid curvelet transform and genetic algorithm for

Image Steganography. International Journal of Advanced Computer Science and Applications, 8(8), (2017).
11. Wang-Q Lim.: The discrete shearlet transform: A new directional transform and compactly supported Shearlet frames. IEEE Transactions on Image Processing, 19(5), 1166–1180 (2010).
12. Hamidi, H., Chehel Amirani, M., & Rahimzadeh Arashloo, S.: Local selected features of dual-tree complex wavelet transform for single sample face recognition. IET Image Processing, 9(8), 716–723 (2015).
13. Rustamov, R. M., & Guibas, L. J.: Wavelets on graphs via deep learning. Signals and Communication Technology, 207–222 (2018).
14. Gulve, A. K., & Joshi, M. S.: An image steganography method hiding secret data into coefficients of integer wavelet transform using pixel value differencing approach. Mathematical Problems in Engineering, 1–11 (2015).
15. Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A.: Image steganography: A review of the recent advances. IEEE Access, 9, 23409–23423 (2021).
16. Gutub, A., & Al-Shaarani, F.: Efficient implementation of multi-image secret hiding based on LSB and DWT Steganography Comparisons. Arabian Journal for Science and Engineering, 45(4), 2631–2644 (2020).
17. Nipanikar, S. I., Hima Deepthi, V., & Kulkarni, N.: A sparse representation based image steganography using particle swarm optimization and wavelet transform. Alexandria Engineering Journal, 57(4), 2343–2356 (2018).
18. Liu, J., Huang, J., Luo, Y., Cao, L., Yang, S., Wei, D., & Zhou, R.: An optimized image watermarking method based on HD and SVD in DWT domain. IEEE Access, 7, 80849– 80860 (2019).
19. Pradhan, A., Sahu, A. K., Swain, G., & Sekhar, K. R.: Performance evaluation parameters of image steganography techniques. In: 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), Bangalore, India (2016).
20. Sonti, N., & Reddy V. P.: A Systematic Review of Graph Signal Processing. International Journal of Advanced Science and Technology, 29(5), 862 – 868 (2020).
21. Basavaprasad , B., & Hegadi, R. S.: A Systematic Study on Applications of Graph Theory in Image Processing With a Focus on Image Segmentation. International Journal of Scientific & Engineering Research, 7(5), 74–76 (2016).
22. Mittal, A., Soundararajan, R., & Bovik, A. C.: Making a “completely blind” Image quality analyzer. IEEE Signal Processing Letters, 20(3), 209–212 (2013).