

# Hiding Image into Another Meaningful Images Using Richardson-Lucy Algorithm with Data Authentication

Ali Sheidaee\*, Leyli Mohammad Khanli

Department of Computer and Electronics Engineering, Tabriz, Iran

**Abstract:** Image steganography is a technique of embedding sensitive information in images. In literature, research articles proposed different image steganography schemes on cover images based on different algorithms. Withal, stego images have less quality in HVS and lower performance. Another topic in image steganography is the quality of extracted data in receiver side that can be affected by transmission channel options or even by the attacks on stego images in transmission channel. In this paper discrete cosine transform (DCT) function and Motion Blur (based on Richardson-Lucy algorithm) is used for secret image transformation and secured hash file of the transformed image generated with RSA cryptosystem therewith. The randomness property of the resultant image reduces the possibility of its detection by HVS and steganalysis techniques. Image data embedding applied with LSBMR substitution algorithm into another significant image. Image deconvolution addressed in recent articles that used different methods such as edge extractions, Richardson-Lucy algorithm, Regularized filters and etc. We apply the Richardson-Lucy deconvolution basics in final secret image extraction to remove the noise. Several experiments and comparative studies are further presented to verify the effectiveness of the proposed algorithm in terms of performance, stego image quality and secret images quality maintenance.

**Keywords:** Steganography; Richardson-Lucy; Motion Blur; Authentication; Human Visual System (HVS)

## 1. Introduction

Steganography is the technique of data hiding in digital media. There has been different research articles in image steganography<sup>[1-7]</sup>. Steganography methods overcome some of the inherent limitations of cryptographic methods such as huge computational complexity and the possibility of detecting the secret data by attackers<sup>[1]</sup>. Image steganography is applicable to a large number of applications such as secure communication between two or more parties, online voting systems and etc.<sup>[2-6]</sup>. Based on Meister article<sup>[8]</sup>, Deconvolution has previously been shown to be a useful statistical technique for unknown density recovery which, in most cases, requires specifying the measurement error

distribution<sup>[9]</sup>. Xiao Feng Dai<sup>[10]</sup> deploy a fully non-parametric algorithm, the RL blind deconvolution method, to decompose firm-specific in efficiencies from their composite errors corrected by the expected inefficiency  $\mu=0$  in productive efficiency analysis.

In this paper, we have presented a new image steganography algorithm, which has used a number of techniques to hide the secret image into selected meaningful cover image to improve our recent work<sup>[3]</sup>. In Ref.<sup>[3]</sup>, we proposed a new steganography method to improve the stego image's quality with transforming the secret images domain by utilizing the DCT function instead of cover image. Data authentication is another important topic in utilizing the steganography methods to obtain reliability in image transmission. In this paper, the

utilized methods are based on Richardson-Lucy (RL) algorithm with Discrete Cosine Transform (DCT) and Data substitution implemented by LSBMR.

RL algorithm has two phase which is divided to the embedding phase and extraction phase (see section 2). Based on RL algorithm, we create Motion blur on secret data image which can be known as watermarking method. After RL algorithms implementation, by employing the DCT function, stego image becomes unrecognizable for Human Visual System (HVS). There is some common domain transform functions which can be utilized in steganography schemes like fast fourier transform (FFT), wavelet transform function and its variants like lifted wavelet transform (LWT), discrete cosine transform (DCT) and etc. we choose DCT function because it is a well-known function for image processing and signal-processing applications and it has a standard for JPEG image format with image quantization and compression. DCT transform function change the image domain from spatial to the frequency domain with better features such as large compression ratio, perfect effect of computational complexity and data integrated capability. After creating the transformed secret image, its hash generates and encrypts by RSA algorithm. We selected the RSA algorithm for its lower complexity but it should be mentioned that the initial values of RSA algorithm should be kept safe and private to forbid others from receiving the data. Finally, the transformed image and its secure hash embedded in the least significant bits of selected cover image.

The criteria to evaluate the steganography methods is the quality of stego images and extracted secret image's quality on receiver side. To quantify the quality of stego images, two criteria are considered in the literature: Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM). These measures present the differences between the pixels of stego and cover images. Another measurement for images defined with histogram plots. Histogram is the graphical representation of the data distribution. It gives the variation of number of pixels with represent to the intensity of the image. Main application of histogram plots in steganography analysis is checking the variation of the pixel values of different images obtained from steganography methods

implementations.

As shown in the experimental results, our algorithm improves PSNR and SSIM measures and stego image has little changes in comparison with the original cover image. Another important result is the extracted image quality that is near to the original secret image, Therefore image steganography with our proposed method is reasonable in comparison with the previous algorithms. This means that the proposed scheme enhances the visual quality of the stego images, which makes it preferable compared to the existing solutions.

The rest of this paper is organized as follows. In Section II we review the previous works with Richardson-Lucy algorithm. Section III explains the proposed algorithms in details. The effectiveness of the algorithm is investigated in Section IV. Finally, the paper is concluded in Section V.

## 2. Related work

In the following, we briefly review the proposed algorithms in Richardson-Lucy, spatial domain and frequency domain categories<sup>[8-13]</sup>.

### A. Richardson-Lucy algorithm (RL)

This algorithm has two phase that is categorized as 1) Image processing functions: This functions help us to use image tools for creating a noisy image to forbid others from identifying its contents or it can be in form of blurring or even watermarking methods. The most common function in RL implementations is Motion blurring that used in our proposed method. We will use this phase of algorithm in image embedding for motion blur injection on secret image and preparing it to hide into another meaningful image. 2) Image deconvolution: Deconvolution in literature backs to the extracting a noiseless image with calculating the rate of injected noise and denoising it for creating a near extracted image to the original one. Based on Meister article<sup>[8]</sup>, Deconvolution has previously been shown to be a useful statistical technique for unknown density recovery which, in most cases, requires specifying the measurement error distribution<sup>[9]</sup>. Xiao Feng Dai<sup>[10]</sup> deploy a fully non-parametric algorithm, the RL blind deconvolution method, to decompose firm-specific in efficiencies from their composite errors corrected by the

expected inefficiency  $\mu=0$  in productive efficiency analysis. Guangmang Cui *et al.*<sup>[11]</sup> have presented a modified non-blind Richardson–Lucy image deconvolution approach using adaptive reference maps. Taiebeh Askari Javaran *et al.*<sup>[12]</sup> proposed a non-blind deconvolution method for image deblurring. A new image prior, which is based on the difference between a given image and its reblurred version, was introduced. The proposed prior was embedded as a regularization term in a MAP. Since, the minimum of this regularization term corresponds to the true sharp solution, solving the MAP helps to well reconstruct the image details whilst suppressing noise. Hao-Liang Yang *et al.*<sup>[13]</sup> proposed a framework for image deblurring from a single blurred image under the assumption of spatially-invariant blur kernel by using the GARL and BF algorithms.

In our proposed image steganography method both image motion blur noise injection in embedding phase and image deconvolution in extraction process is utilized for creating better Stego image in terms of quality and noiseless secret image extraction in receiver side. This algorithm uses motion blur for noise injection to the target image that help us to create an image with blurred appearance. Another use of Richardson-Lucy algorithm is image deconvolution.

#### B. Image domain- based algorithms

Image domain algorithms are important for implementing different functions on it. Based on utilized methods in steganography, we have to select one of the following domain-based algorithms<sup>[13-16]</sup>.

##### 1) Spatial domain-based algorithms

Most of the spatial domain-based schemes have considered RGB color model, ranging from the simple LSB substitution method to the advanced edge and saliency-based schemes<sup>[13]</sup>. In an attempt to improve the visual quality of the stego images, the authors in<sup>[14, 15]</sup> have presented the LSB matching (LSBM) method, which reduces the asymmetric effects by randomly adding/subtracting one to each pixel of the input image. The problem with this technique is that, if the image is compressed, the secret data may be lost. This difficulty becomes more serious if the secret data contains sensitive information.

##### 2) Frequency domain-based approaches

In these set of algorithms, the transformed

coefficients are used for data embedding, which are generated using various transformation techniques such as DCT, Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT). The main idea of these approaches is to scramble the transformed coefficients. When the frequency domain-based techniques are used for data embedding, the hidden content is spread across the entire image, which provides better resistance against statistical and image processing attacks. The shortcoming of these schemes is that, they are computationally complex, which makes them inappropriate for various real-time applications<sup>[16]</sup>.

### 3. Image Steganography using Richardson-Lucy algorithm with DCT

In this section, we have explained our proposed image steganography. The steps of our proposed scheme are expounded in details.

#### A. The Proposed image embedding Algorithm

Our proposed method generates stego image in a number of phases, including image motion blurring with Richardson-Lucy algorithm, DCT transformation<sup>[13]</sup>, secure hash generation with utilizing RSA algorithm for authentication and applying LSBMR for hiding secret image along with its hash file. These phases are expounded in details in this section. All the mentioned phase are invertible, and we have described the image extraction algorithm at the end of this section.

##### 1) Richardson-lucy algorithm (RL)

The RL algorithm is originally developed for image recovery<sup>[6]</sup> and its blur function helps us in creating a noise-like image, which defined as an image with an injected noise where nobody can identify its contents. The blurred image defined with  $B$  and the clear image is shown as  $I$ , the intensity  $I_p$  at the pixel location  $P$  is computed from the pixel intensities  $B_q$  by:

$$P(I_p) = \sum_q P(I_p|B_q)P(B_q) \quad (1)$$

Where  $p(I_p)$  can be identified as the distribution of  $I_p$  and so forth. Expanding  $P(I_p|B_q)$  by Bayes's rule:

$$P(I_p) = \sum_q \frac{P(B_q|I_p)P(I_p)}{\sum_z P(B_q|I_z)P(I_z)} P(B_q) \quad (2)$$

The best of a bad situation is used to break the dependency of  $P(I_p)$  on both sides, where the current estimation of  $P(I_p)$  is used to approximate  $P(I_p|B_q)$ . Thus:

$$\begin{aligned}
P^{j+1}(I_p) &= \sum_q \frac{P(B_q|I_p)P^j(I_p)}{\sum_z P(B_q|I_z)P^j(I_z)} P(B_q) \\
&= P^j(I_p) \sum_q P(B_q|I_p) \frac{P(B_q)}{\sum_z P(B_q|I_z)P^j(I_z)}
\end{aligned} \tag{3}$$

Where  $j$  is the index of the RL iteration. This algorithm helps us to create a motion blurred image in embedding phase and true colored image extraction for extraction phase where it clears the initial motion blur and any noise that injected in transmission phase.

### 2) Image transform with DCT function

We encrypt the secret image with DCT that is employed in Ref.<sup>[17]</sup>. The encrypted image is pseudo-random and looks like noise. This property preserves the visual quality of stego image, and makes its variations unrecognizable for HVS. As a consequence, it can be transmitted securely over public channels. In this way, the privacy requirement of the secret image is satisfied. In is worth mentioning that the domain

transformation by DCT changes the secret image's structure. This makes the algorithm more robust against steganalysis attacks.

### 3) Applying LSBMR for Image Hidding

LSB and its variant algorithms are the most widely used spatial domain-based steganography technique. In this method, the important parts of the cover image remain unchanged. This property yields high quality stego images that are undistinguishable by the HVS from the cover images. Therefore, we have chosen it for embedding secret image and its secure hash in the cover image.

Algorithm 1 describes the embedding phases of the proposed scheme. In this context,  $IM_{srt}$ ,  $IM_{trans}$ , and  $IM_{cover}$ ,  $IM_{stego}$  stand for secret, DCT transformed, cover, and stego images. As it is shown in this algorithm, the dimensions of the secret and cover images can be different.

---

#### Algorithm 1: Image Embedding.

INPUT:  $IM_{srt}$  with the dimensions of  $K \times L$ ,  $IM_{cover}$  with the dimensions of  $M \times N$ .

OUTPUT:  $IM_{stego}$  with the dimensions of  $M \times N$ .

Add motion blur to the  $IM_{srt}$  based on RL.

If the color mode of  $IM_{srt}$  is RGB then

Change its mode to grayscale.

End if

Divide  $IM_{srt}$  into  $8 \times 8$  blocks.

Transform blocks with DCT function.

Quantize each block to generate  $IM_{trans}$ .

Generate hash of  $IM_{trans}$ .

Use RSA for hash encryption ( $RSA_{snt}$ )

Use LSBMR algorithm to hide  $IM_{trans}$  and its

$RSA_{snt}$  in  $IM_{cover}$ . The resultant image is  $IM_{stego}$ .

---

#### Algorithm 2: Image Extraction.

INPUT:  $IM_{stego}$  with the dimensions of  $M \times N$ .

OUTPUT: Authentication result,  $IM_{srt}$  with the dimensions of  $K \times L$ .

Extract the  $RSA_{snt}$ .

Evaluate  $RSA_{rec}$  from received image.

If  $RSA_{snt} == RSA_{rec}$  then

Received image authenticated.

End if

Use inverse function of DCT transform.

Employ Richardson-Lucy image deconvolution.

---

### B. The Proposed image extraction Algorithm

All the phases of the proposed algorithm, including image motion blurring, changing the color mode to grayscale, DCT transformation and LSBMR substitution are invertible. Therefore, the secret image can be extracted with executing the inverse operations in reverse order. The image extraction scheme is given in Algorithm 2. In this algorithm,  $RSA_{snt}$  and  $RSA_{rec}$  denote the generated secure hash by the sender and receiver, respectively. Richardson-Lucy deconvolution algorithm helps us to remove noise from extracted secret image.

Noise can be in form of motion blur, as we inject in embedding phase, gaussian noise and etc. By utilizing Richardson-Lucy algorithm for image deconvolution, extracted secret image has less noise and it is near to the original secret image.

## 4. Experimental Results

In this section, we have presented simulation results to evaluate the effectiveness of our algorithm. The experiments are simulated using MATLAB R2015b, Windows 10 operating system, 2.3 GHz CPU, and 4GB

of RAM. The performed simulations are categorized into two groups. Firstly, the visual quality of the proposed algorithm has been studied. Next, the performance of the algorithm is investigated using PSNR and SSIM criteria.



Figure 1; The utilized cover images.

The set of employed cover images is shown in Figure 1. It comprises Lena with the dimensions of 400×225 pixels, Boat with the dimensions of 256×256 pixels and Peppers with the dimensions of 256×256 pixels. Moreover, the utilized secret images are given in Figure.2. These images are Baboon with the dimensions of 512×512 pixels and Cameraman with the dimensions of 256×256 pixels. All of the mentioned images are derived from globally accepted image dataset<sup>[18]</sup>. In real applications, the most appropriate cover image is chosen according to the visual quality of derived stego images.

Here, cameraman will be embedded in Lena. These images are derived from the globally accepted image dataset<sup>[18]</sup>. Firstly, cameraman is blurred. Next, the resulted blur image domain transforms with DCT and its hash generated and secured with RSA. Finally, the

transformed cameraman and its secure hash are embedded in the Lena image using LSBMR method.

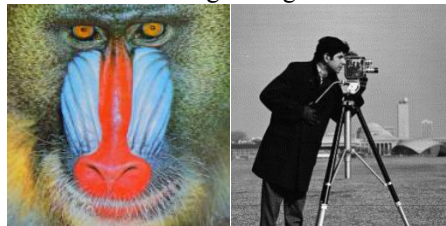


Figure 2; The utilized secret images.

### A. Visual Quality Evaluation

In the proposed scheme, the embedded secret image is like Figure.3.As it is shown in this figure, the embedded image differs significantly from the original one.

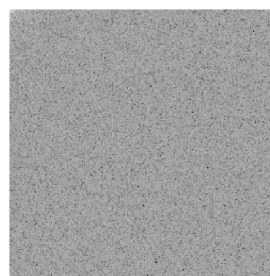


Figure 3; Transformed secret image.

The derived stego images by the proposed algorithm are depicted in Figure 4. From this figure we can conclude that, the visual quality of the derived stego images doesn't decrease equally. The visual quality of the RGB cover images is more distorted by embedding secret images. This is due to that, RGB images have a third dimension of color frequency to define RGB mode. This causes more overhead in size and color intensity after hiding the secret image, which increases the noise. As a result, the quality of color stego images is less than the quality of grayscale ones.



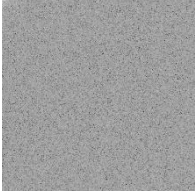



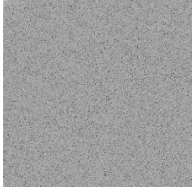

Cover image	Secret image	Encrypted image	Stego image
			
			

Figure 4; The generated Stego images in our proposed method.

### B. Quantitative Analysis

The considered criteria to evaluate the proposed

algorithm are PSNR and SSIM. The PSNR measures the ratio between the maximum power of the signal and the power of the distorting noise that diminishes its quality. The higher the PSNR of a given signal, the more is its quality. In the context of image steganography, the secret image is the corrupting noise which degrades the quality of the stego image. Therefore, higher PSNR indicates the secret image causes less distortion on the cover image. In other words, this criterion measures the differences between cover and stego images. The PSNR of a given image (Here the emphasis is on the stego image.) is calculated as follows:

$$PSNR = 10 \cdot \log_{10} \left( \frac{MAX_I^2}{MSE} \right) \quad (4)$$

In this equation, MSE denotes the mean square error of the stego image in comparison with the cover image. This criterion is formally expressed in Eq.5, in which C and S present the cover and stego images, respectively. In addition, it is assumed that these images are of the dimensions of M×N.

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \| C(i, j) - S(i, j) \|^2 \quad (5)$$

The MAX<sub>I</sub>, which appears in Eq.4, presents the maximum pixel value of the image. In other words, MAX<sub>I</sub> is equal to 2<sup>b</sup> - 1, where b is the number of bits that presents a pixel. For grayscale images, this variable is set to 255, because each pixel is presented by one byte in this setting. For RGB images, which have three color parameters of R, G, and B per pixel, PSNR is defined in a similar manner. The only difference is that, the amount of MSE is further divided by three.

Approach	PSNR				
	The Proposed Algorithm	A.shei daee <i>et al.</i> [3]	LS B [19]	LSB M [14]	LSBM R [19]
Lena	56.31	51.14	42.51	42.61	42.68

**Table 1.** Psnr comparison of the considered algorithms

**Table 1** presents the PSNR of the generate stego images using different algorithms. The proposed algorithm is compared with our latest proposed method<sup>[3]</sup>, LSBM and LSBMR<sup>[14]</sup>, and LSBMR<sup>[19]</sup>. In this experiment, Lena and Cameraman are chosen as cover and secret images, respectively. From the reported results,

we can see that the proposed algorithm improves PSNR by at least 10.1% in comparison with previous schemes. The other criterion to quantify the quality of stego images is SSIM, which presents the similarity between two images. This criterion measures the quality of a given image based on a reference distortion-free image. In the context of image steganography, the examined image is the stego image, and the cover image is considered as the reference image. This criterion is formally stated as follows:

$$SSIM(C, S) = \frac{(2\mu_C\mu_S + C_1)(2\sigma_{CS} + C_2)}{(\mu_C^2 + \mu_S^2 + C_1)(\sigma_C^2 + \sigma_S^2 + C_2)} \quad (6)$$

Where C<sub>1</sub> and C<sub>2</sub> are two variables to stabilize the division with weak denominator. Moreover, μ and σ present the average and covariance of the variables.

The SSIM of resultant stego Lena of considered algorithms are compared in **Table 2**. It is derived from this table that, our algorithm improves SSIM in comparison with LSB method variants. The obtained results in Tables 1. and 2. demonstrate the effectiveness of the proposed algorithm. Finally, Table3 shows the comparison of our proposed method with some of the recent articles in literature.

The SSIM of resultant stego Lena of considered algorithms are compared in Table 2. It is derived from this table that, our algorithm improves SSIM in comparison with LSB method variants. The obtained results in Tables 1.and 2. demonstrate the effectiveness of the proposed algorithm.

Approach	SSIM				
	The Proposed Algorithm	A.shei daee <i>et al.</i> [3]	LSB [19]	LSBM [14]	LSB MR [19]
Lena	0.9993	0.9991	0.9920	0.9931	0.9946

**Table 2.** SSIM comparison of the considered algorithms

Algorithm	Secret size	Cover image	PSNR	MSI M
-----------	-------------	-------------	------	-------

S. Subhedar <i>et al.</i> [21]	256×	Lena	49.0	0.9963
	256	Peppers	369	0.9966
			50.1	
Kanso <i>et al.</i> [4]	256×	VMEI-1+ Lena	40.5	0.9987
	256	VMEI-2+ Lena	888	0.9987
		EVMEI+ Lena	40.5	0.9987
			737	
			41.2	
K. Muhammad <i>et al.</i> [19]	8192	Lena	56.1	-
	byte		04	
	s			
K. Muhammad <i>et al.</i> [14]	8192	Lena	42.2	-
	byte		14	
	s			
Xin Liao <i>et al.</i> [22]	7500	AE1+ Lena	50.6	0.9949
	byte	AE2+ Lena	7	0.9952
	s		50.9	
			5	
A. Sheidaee <i>et al.</i> [3]	256×	Lena	51.1	0.9991
	256		4	
Our proposed Method	256×	Lena	56.3	0.9993
	256	Peppers	1	0.9872
			54.0	
		673		

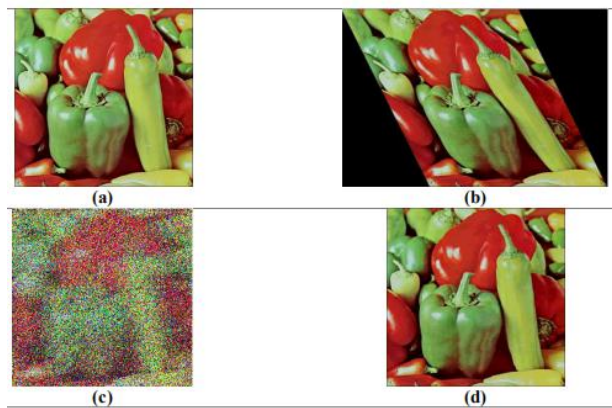
**Table 3.** Comparison of our proposed method with different algorithms

### C. Steganalysis

Steganalysis is the science of attacking steganography. It mimics the already established science of Cryptanalysis. Steganographers can create a steganalysis system merely to test the strength of their algorithm. Steganalysis is achieved through applying different image processing techniques, e.g., image filtering, rotating, cropping, and translating. More deliberately, it can be achieved by coding a program that examines the stego-image structure and measures its statistical properties, e.g., first order statistics (histograms) or second order statistics (correlations between pixels, distance, direction). JPEG double compression and the distribution of DCT (discrete cosine transform) coefficients can give hints on the use of DCT-based image steganography. Passive steganalysis attempts to destroy any trace of secret

communication, without bother to detect the secret data, by using the above mentioned image processing techniques: changing the image format, flipping all LSBs or by under-taking a severe lossy compression, e.g., JPEG. Active steganalysis however, is any specialized algorithm that detects the existence of stego-images [20].

In this paper, steganalysis is not a main subject for evaluation, for this, we tested our proposed steganography method with some known image processing attacks as shown below:



**Figure 5;** Steganalysis attacks on stego image.

In **Figure 5** selected cover image is the Peppers image that has been depicted in **Figure 1** and the embedded secret image is Cameraman from **Figure 2**. In **Figure 5**, (a) depicts the unchanged stego image that carries our secret image via public channel, (b) shows the stego image with shear operation in image processing tools that creates 2D rotation, (c) has a Gaussian noise with 0.3 noise-variance, (d) is the attacked stego image that resized the stego image to 300×300 pixel. An important factor in steganography method analysis against various attacks is the quality of extracted secret data from attacked stego file. The extracted secret data from stego image(**Figure 5** (a)) PSNR equals 38.4319 and MSSIM = 0.8751 but these measures have become worse in image processing attacks:

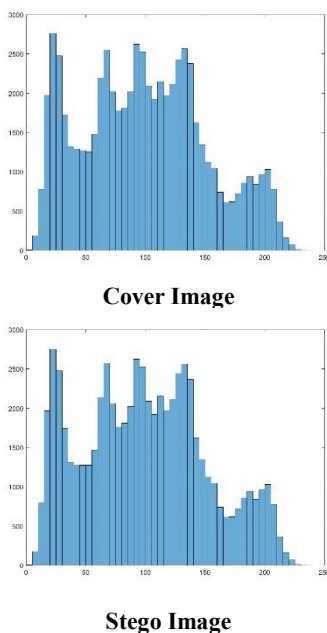
In analysis for image (b) extracted image's PSNR = 19.0752 and MSSIM = 0.5306 where MSSIM = 0.7608 and PSNR = 29.8906 for image (c). (d) Has an extracted image with PSNR = 28.8035 and MSSIM = 0.6852. In comparing with steganography methods, stego image in our proposed method will get some noise in image processing attacks, therefore secure channels will have the best performance in absence of attacks and it validates our method for employing in data transmission

applications.

### A. Histogram Analysis

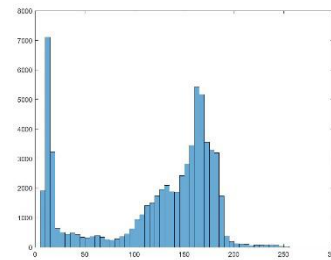
A histogram is an accurate representation of the distribution of numerical data. An image histogram is a type of histogram that acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance.

In the following, we use histogram plots in **Figure 6** to represent the selected cover image and its Stego image histogram. Selected cover image is the Lena image that shown in **Figure 1** and the secret image is Cameraman as depicted in **Figure 2**. As shown in Figure 6, resultant stego image has less modification after embedding the secret image in its original cover image. This comparison shows the efficiency of our proposed method in maintenance of stego image's quality and it can be utilized for transferring secret images or data without attracting others to the existence of hidden data.

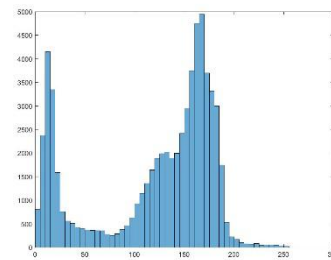


**Figure 6;** Histogram plots of cover and stego images.

In **Figure 7** original secret image and the extracted secret images histogram shown to see its difference at a glance. As shown in Figure 7, extracted secret images histogram shows the lower distribution in comparison with its original secret image. For more details, in horizontal axis the extracted secret image has lower distribution in range of 0 to 50 which means we have changes in final secret image as depicted in **Figure 8**.



**Original Secret Image**



**Extracted secret image**

**Figure 7;** Histogram plots of secret images.



**Figure 8;** Extracted Cameraman from Lena.

## 5. Conclusion

In this paper, image steganography using Richardson-Lucy algorithm with DCT has been addressed. We have proposed an efficient image steganography algorithm, which exploits image motion blurring, DCT and LSBMR methods. In this scheme, firstly the secret image is blurred and transformed by applying DCT on it. Next, the output of this phase is embedded in the cover image. The transformed image looks like noise and therefore, embedding procedure hasn't severe effect on the quality of the cover image. To enable authentication of the message origin, the secured hash of the transformed image, which generated with RSA algorithm, is also embedded in the cover image. The proposed scheme is a spatial domain-based algorithms. Therefore, it suffers from resiliency against different attacks such as cropping and noising.

By utilizing the RSA algorithm for received data



authentication, data replacement, distortion and even its deleting operations can be identified. But steganography methods doesn't concern with reconstructing the cropped or noised images and it is an important issue for future works. In future work, we aim at designing a resistant algorithm against modification attack, which reconstruct modified images efficiently. The other important topics for future works is improving the PSNR and SSIM values of stego images and extracted secret images and utilizing steganalysis methods based on artificial intelligence algorithms for more studies.

## Acknowledgment

The authors thank for anonymous referees whose remarks help us to improve this work.

## References

1. L. Bin, T. Shunquan, W. Ming and H. Jiwu. (2014). Investigation on cost assignment in spatial image steganography. *IEEE Trans. Inf. Forensics Secur* 9 (2014). 1264-1277.
2. G. Linjie, N. Jiangqun and S. Yun Qing. (2014). Uniform embedding for efficient JPEG steganography. *IEEE Trans. Inf. Forensics Secur* 9 (2014). 814-825.
3. Ali Sheidaee and L. Farzinvas. (2017). A novel image steganography method based on DCT and LSB. 9th international conference on information and knowledge technology (ikt2017). IEEE - Amirkabir University of technology, Iran, Oct. 18-19, 2017.
4. A. Kanso and M. Ghebleh. (2017). an algorithm for encryption of secret images into meaningful images. *Optics and lasers in engineering* 90 (2017). 196-208.
5. K. Qazanfari and R. Safabakhsh. (2014). a new steganography method which preserves histogram: Generalization of LSB. *Inform* 277 (2014). 91-101.
6. W. Zhang, X. Zhang and S. Wang. (2007). a double layered "plus-minus one" data embedding scheme". *IEEE Signal Process* 14 (2007). 848-851.
7. S. Sun. (2016). A novel edge based image steganography with  $2^k$  correction and Huffman encoding. *Information Processing Letters* 116 (2016). 93-99.
8. Meister. (2006). A Density estimation with normal measurement error with unknown variance. *Statistica Sinica* 16 (2006). 195-211.
9. Stefanski and Carroll. (1990). Deconvolving kernel density estimators. *Statistics* 21 (1990). 169-184.
10. Xiaofeng Dai. (2016). Non-parametric efficiency estimation using Richardson-Lucy blind deconvolution. *European Journal of Operational Research* 248 (2016). 731-739.
11. Guangmang Cui, Huajun Feng, Zhihai Xu and Li, Yueting Chen. (2014). A modified Richardson-Lucy algorithm for single image with adaptive reference maps. *Optics & Laser Technology* 58 (2014). 100-109.
12. Taiebeh Askari Javaran, Hamid Hassanpour and Vahid Abolghasemi. (2017). Non-blind image deconvolution using a regularization based on re-blurring process. *Computer Vision and Image Understanding* 154 (2017). 16-34.
13. Hao-Liang Yang, Po-Hao Huang and Shang-Hong Lai. (2014). A novel gradient attenuation Richardson-Lucy algorithm for image motion deblurring. *Signal Processing* 103 (2014) 399-414.
14. K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad and S.W. Baik. (2015). A secure method for color image steganography using gray-level modification and multi-level encryption. *KSII Trans. Internet Inf. Syst* 9 (2015) 1938-1962.
15. W. Luo, F. Huang and J. Huang. (2010). Edge adaptive image steganography based on LSB matching revisited. *IEEE Trans. Inf. Forensics Secur* 5 (2010). 201-214.
16. Y. Luo, M. Du and J. Liu. (2015). A symmetrical image encryption scheme in wavelet and time domain. *Common Nonlinear Sci. Numer. Simul* 20 (2015). 447-460.
17. Jianhua Wu, Mengxia Zhang and Nanrun Zhou. (2016). Image encryption scheme based on random fractional discrete cosine transform and dependent scrambling and diffusion. *Journal of Modern Optics* (2016).
18. J. Laaksonen, M. Koskela, S. Laakso and E. Oja. (2000). PicSOM-content-based image retrieval with self-organizing maps. *Pattern Recognit. Lett* 21 (2000). 1199-1207.
19. K. Muhammad, M. Sajjad, I. Mehmood, S. Rho and S.W. Baik. (2016). Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems* (2016).
20. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevit. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing* 90 (2010). 727-752.
21. Mansi S. Subhedar, Vijay H. Mankar, Image steganography using redundant discrete wavelet transform and QR factorization, *Computer and Electrical Engineering* 54, 406-422, 2016.
22. Xin Liao, Zheng Qin, Liping Ding, Data embedding in digital images using critical functions, *Signal Processing: Image Communication* 58, 146-156, 2017.