Threshold-based Steganography: A Novel Technique for Improved Payload and SNR

Zakir Khan[1], Mohsin Shah[2], Muhammad Naeem[3], Toqeer Mahmood[4], Shah Khan[5], Noor Ul Amin[6], and Danish Shahzad[7]
[1, 2, 3, 5, 6]Department of Information Technology, Hazara University Mansehra, Pakistan
[4]Department of Computer Engineering, University of Engineering and Technology Taxila, Pakistan
[7]Department of Computer Engineering, Kadir Has University, Turkey

Abstract: *Steganography is the art of hiding user information in various file types including image, audio and video. Security of steganography lies in imperceptibility of secret information in the cover image. Human Visual System (HVS) is not able to detect the changes in low color values of an image. To the best of our knowledge, none of the available steganographic techniques have exploited this weakness of HVS. In this paper, a new LSB technique is presented which hides information in the cover image taking into account the pixel value of color or grey level of every pixel. Our experiments show that the proposed technique has a high payload and low perceptibility of secret information hidden in the cover image as compared to the existing Least Significant Bit (LSB) based algorithms. We have used MATLAB for the implementation of proposed algorithm.*

Keywords: *LSB, cover image, stego image, HVS, data hiding.*

Received April 29, 2014; accepted July 9, 2014; published online August 22, 2015

1. Introduction

The word steganography is the combination of two Greek words steganos means covered and graptos means writing. Steganography is a communication technique that hides the secret information in another information type [14]. This invisible communication decreases the risks of unauthorized access of secret information. In today's modern communication, securing information from unauthorized access is a big challenge. There exist various cryptographic techniques that are used to secure the secret information. Steganography techniques on the other hand hide secret information in a number file formats like image, audio, and text which makes hard for the attackers to suspect information passing before them [21].

There are three components of a steganographic system: The cover file used to hide information; the secret information and the stego-file the resultant file made after information hiding [9].

Embedding secret information in the Least Significant Bits (LSB) of cover image pixels is the common and widely used technique of Steganography. A number of LSB steganographic techniques are available in literature. All the available LSB steganographic techniques have their pros and cons in terms of embedding capacity and Signal to Noise Ratio (SNR) [14, 23].

As motivated in [27], it's hard for the Human Visualization System (HVS) to observe changes in the lower color levels. HVS is very sensitive to light and that's why cannot differentiate between colors in a very dark room or at night. For example, black color has 0 value. A naked eye will not be able to differentiate the black color from 0 to 20. This phenomenon is discussed further below while discussing the difference of images in section 4.

This motivated us to exploit the weakness of HVS to capture the secret information. We scan the cover image for all color levels and secret data is embedded taking into account the threshold of the color levels of cover image. We hide more secret information in low color bits, whereas less information is hidden in high color values. This makes the proposed technique dynamic, in contrast to all available steganographic techniques.

Our results confirm that the proposed technique improves SNR and payload of secret information. All the available LSB steganographic techniques focus on Peak Signal to Noise Ratio (PSNR), payload and bit rate. In the proposed threshold-based LSB steganographic technique, we have calculated ten image quality attributes for the resultant stego image. All of these attributes are suggested by [5, 6, 19] for a steganographic system.

The rest of the paper is arranged as follows: Section 2 elaborates on related approaches, while section 3 discusses proposed algorithm. In sections 4 and 5, we provide experimental results of proposed approach and compare them with the available approaches, respectively. Section 6 concludes the paper.

2. Literature Review

In LSB steganographic techniques, the secret information bits are embedded in the LSBs of the cover file. Thomas [23] has provided a comprehensive survey of image LSB steganographic techniques.

Message embedding in steganographic systems are classified into LSB technique, transform technique, statistical technique and distortion technique [1, 10]. Gupta *et al*. [9] have calculated PSNR, SNR and BER for 1 to 8bit LSB steganographic techniques. They observed that:

1. 2bit and 3bit LSB techniques provide good quality stego images.
2. The capacity of information is decided based on the probability of detection and the false alarm.
3. These parameters put an upper limit on the capacity of information to be hidden in cover image [7]. Discrete cosine transform and discrete wavelet transform are used to embed image in image, audio in audio, audio in image, image in audio [4].

Following are the most recent LSB steganographic techniques available in literature.

2.1. LSB in GIF Images

Graphic Interchange Format (GIF) is a palette based image where the image colors are stored in alpha channel or a color lookup table. In this technique, data is hidden in the LSBs of GIF images, but this could result in the variation in colors of the image. The main drawbacks of this technique are low payload and open to visual and statistical attacks [2].

2.2. Difference Expansion LSB Technique

LSB embedding based on difference expansion technique explores redundancy in digital content to store 1bit of message in two bits of cover image pixels [24]. This technique embeds less information bits in cover image and also results in low visual quality stego images.

2.3. Hiding Behind The Corners

Hiding behind corners LSB technique takes into account the original information to find the effective hiding areas in cover image and hides message bits in the corners [11]. The main disadvantage of this technique is that its embedding capacity is very low.

2.4. Edge-based LSB Techniques

LSB technique based on hiding information in the edges of an image is another steganographic technique. Here, secret messages are hidden in those areas of image where pixel values differ from their neighbours i.e., edges and corners where the value of derivative is high [22]. The advantage of this technique is that attackers take less notice of data hidden in edges of images. The disadvantage is that it has low embedding capacity.

Another edge based LSB technique is adaptive edge-based hiding technique with spatial LSB domain systems. In this technique, number of message bits to be hidden depends on the difference of two pixel values [31]. This technique hides more bits in edges than in smooth areas of the image. The data embedding capacity of this technique is relatively high, but its security is low.

2.5. Pixel Value Differencing and Modulus LSB Technique

Pixel value differencing and modulus LSB technique is used to hide less data in images. This technique makes use of the pixel difference and modulus function to hide data by modifying the remainder [26].

2.6. Image Interpolation LSB Technique

Image interpolation technique is used to hide data in the interpolation area [17]. This technique hides more bits in complex regions of image than in smooth regions. Major limitation of this technique is insecurity of data. Data hidden behind the file using this technique can easily be obtained [23].

2.7. Edge-Based Technique

Edge-based technique which is also called edge adaptive image steganography based on LSB matching uses a pseudo random number generator to select the data hiding locations in the cover image. The technique exploits sharp region in the cover image to embed more data bits compared to smoother areas [18].

2.8. Neighbourhood Pixel Information Technique

This technique embeds secret information bits in cover file based on the information of neighbouring pixels. Three neighbourhood methods are utilized for embedding four neighbourhood methods, diagonal neighbourhood method and eight neighbourhood methods. Though, this technique guarantees high embedding capacity and high PSNR yet secret information is distorted and its extraction impossible if stego image is changed during transmission [12].

3. Proposed Method

3.1. Embedding Procedure

In proposed approach, we conceal more information bits in lower color levels, whereas less information bits are added in the high color levels of the cover image. The cover image is scanned for all color levels and secret data is embedded based on a threshold of the color levels of cover image. The following figure defines the thresholds of the color levels of cover image and embedded bits of the secret data.

Figure 1 state that 4bits are embedded in the LSBs of the cover image pixel when its cover level falls in the range between 0 and 31. Similarly, 3bits are embedded when the color level range is from 32 to 63 and 2bits and 1bit are added for the color level falling in the ranges 63 to 127 and 128 to 255, respectively.

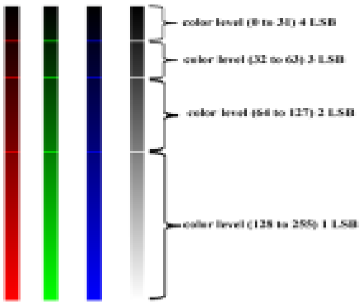

color level (0 to 31) 4 LSB
color level (32 to 63) 3 LSB
color level (64 to 127) 2 LSB
color level (128 to 255) 1 LSB

Figure 1. Color levels of cover image and embedding LSB bits

3.2. Data Encoding

The main concept behind the proposed encoding algorithm is the threshold pixel value. The greater the pixel value in the image the lesser bits used for encoding. For example, if the pixel value is within 128 and 255 then 1bit of secret information is added to the cover image.

The flow chart of the proposed algorithm is shown in Figure 2. As depicted in Figure 2 proposed algorithm first reads the cover image then runs a loop to the length of pixels in the cover image. The proposed algorithm keeps adding secret message bits to the corresponding pixel values of the cover image as long as it finds pixels in the file. Further, these bits are added in the message file in accordance with the constraints defined in Figure 2.

In the case of absence of pixels, the proposed algorithm terminates after generating the stego image. Once the secret message is encoded into the stego image using proposed algorithm and sends to the destination, the next step is to extraction the secret bits from the stego image.

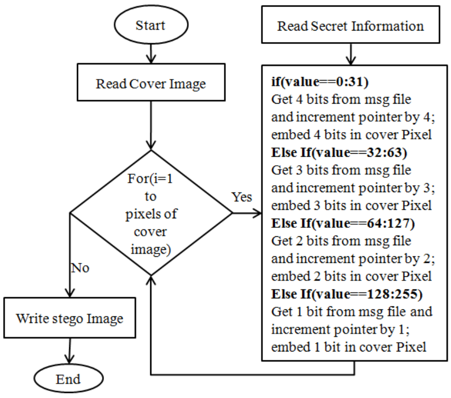

Start
Read Cover Image
For(i=1 to pixels of cover image)
Yes
No
Write stego Image
End
Read Secret Information
if(value==0:31)
Get 4 bits from msg file and increment pointer by 4; embed 4 bits in cover Pixel
Else If(value==32:63)
Get 3 bits from msg file and increment pointer by 3; embed 3 bits in cover Pixel
Else If(value==64:127)
Get 2 bits from msg file and increment pointer by 2; embed 2 bits in cover Pixel
Else If(value==128:255)
Get 1 bit from msg file and increment pointer by 1; embed 1 bit in cover Pixel

Figure 2. Hiding secret information in cover image.

3.3. Data Extraction

In Figure 3, we have shown the flowchart for the algorithm of secret message extraction. The decoding algorithm reads the stego image and decodes the bits according to the threshold of the color level of stego image pixels. The decoded bits are written on another file which contains original embedded message. This procedure gives us back the secret message file from stego image, as shown in Figure 3.

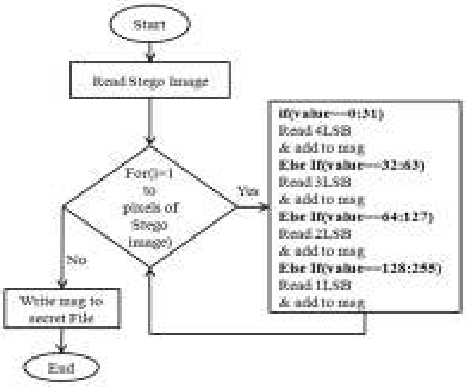
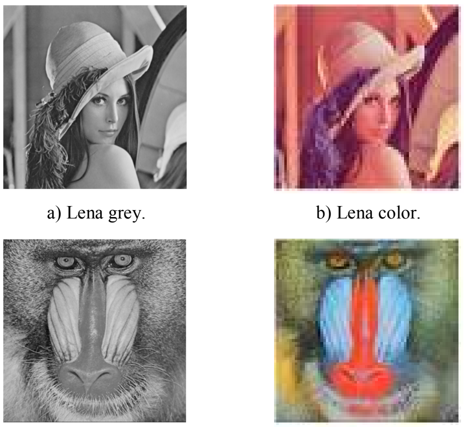


Figure 3. Extracting secret information from stego image.

Let us now discuss the results which we have obtained by the implementation of our algorithm. We have used MATLAB for the implementation of our algorithm.

4. Experimental Results

For the implementation of the proposed algorithm, we have used four images shown in Figure 4. The specifications of these figures are: Grey level Lena 512×512×8, color Lena 512×512×3, grey level baboon 512×512×8 and color baboon 512×512×3. Motivation behind the selection is their wide use among the communities of steganography [9, 14, 21, 23].



a) Lena grey.

b) Lena color.

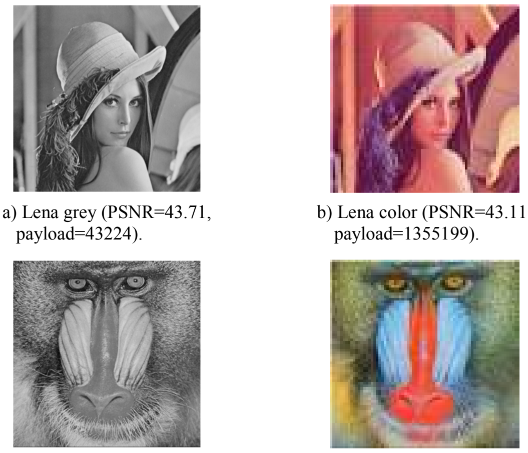
c) Baboon grey.

d) Baboon color.

Figure 4. Cover images.

The secret message for our proposed algorithm is a long bit of stream. MATLAB tool is used to implement the proposed algorithm. After the application of our approach, stego image is produced, as depicted in

Figure 3. The corresponding stego images for the above four cover images produced by the application of our algorithm are shown in Figure 5.



a) Lena grey (PSNR=43.71, payload=43224).

b) Lena color (PSNR=43.11, payload=1355199).

c) Baboon grey PSNR=44.37, payload=410636).

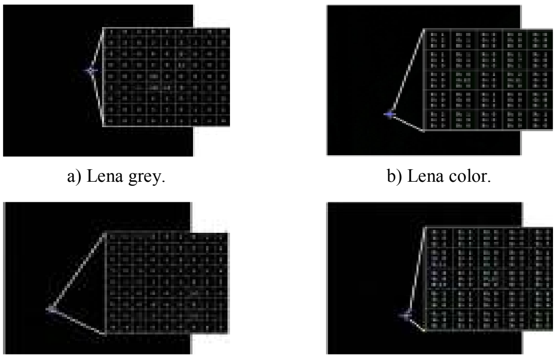
d) Baboon color PSNR=47.10, payload=1329318).

Figure 5. Stego images of the cover images shown in Figure 4.

As motivated earlier, HVS cannot differentiate the colors of low values. Please note that the human eye struggle to find the difference between the cover images as shown in Figure 4 and the stego images as shown in Figure 5. In other words, the produced stego images are of high quality and human eye cannot detect the changes in the stego images. The difference between the cover image and stego image is calculated using the following formula:

$$DiffIPV = Absolute(CoverIPV - StegoIPV)$$

Where *DiffIPV* shows the pixel value of difference image, while *CoverIPV* and *StegoIPV* represent the pixel values of cover image and its corresponding stego image, respectively. The difference is calculated on pixel by pixel basis. Figure 6 shows the difference images for all the four cover images.



a) Lena grey.

b) Lena color.

c) Baboon grey.

d) Baboon color.

Figure 6. Difference of stego images (Figure 5) and cover images figure 4.

Because the pixel values in difference images are either zero or close to zero so all the difference images are black. The difference shows that the change in cover image and stego image is almost un-noticeable. To keep the simplicity of the paper, we have shown the difference of pixel value for a small portion (which is expected to have maximum pixel value) in these images. Please note, the difference of color images is shown by RGB values, while the difference for grey images is shown by a single value. Furthermore, the maximum value in Figure 6 is 14, which also, produces the black color.

This shows that the proposed technique hides a high capacity of information in the cover image (discussed further below in comparison of results) with very minor changes in the cover image. Let us now compare the results with the available state of art techniques using LSB. We obtain the attributes for our analysis from advises provided by [5, 19].

5. Comparison with Existing Algorithms

The proposed technique is compared with number of techniques available in the literature. The comparison is done on the basis of a number of image performance parameters which are given below. Tables 1, 2, 3 and 4 show the comparison of the proposed technique with the existing techniques. The first column under “Techs” lists the names of techniques. The values for Mean Square Error (MSE), Root Mean Square Error (RMSE), Mean Absolute Error (MAE) and Normalized Absolute Error (NAE) are shown in second, third, sixth and tenth columns, respectively. The values for Universal Image Quality Index (UIQI) are given in fourth column. SNR and PSNR are enlisted in fifth and seventh columns, respectively. Average Difference (AD) and Maximum Difference (MD) values are given in the eighth and ninth columns, respectively. Payload in bits is given in the last column. The value×in each table means that corresponding authors have not considered this attribute in their analysis.

Table 1. Lena stego gray image.

Techniques	MSE	RMSE	UIQI	SNR	MAE	PSNR	AD	MD	NAE	Payload
Ni *et al.* [20]	×	×	×	×	×	48.2	×	×	×	5460
Hwang *et al.* [14]	×	×	×	×	×	48.22	×	×	×	5336
Lin and Hsueh [16]	×	×	×	×	×	46.6	×	×	×	59900
Hu *et al.* [13]	×	×	×	×	×	48.69	×	×	×	60241
Luo *et al.* [17]	×	×	×	×	×	48.82	×	×	×	71674
Wu and Tsai [28]	2.07	×	×	×	×	41.79	×	×	×	50960
Yang *et al.* [31]	×	×	×	×	×	36.28	×	×	×	837332
Vleeschouwer *et al.* [25]	×	×	×	×	×	39	×	×	×	24108
Goljan *et al.* [8]	×	×	×	×	×	30	×	×	×	1024
Xuan *et al.* [29]	×	×	×	×	×	36.6	×	×	×	85507
Celik *et al.* [3]	×	×	×	×	×	38	×	×	×	74600
LSB[1]	40.89	6.39	0.63	7.94	5.21	32.05	0.5	14	0.04	1048756
Proposed	2.79	1.67	0.96	19.61	1.09	43.71	0.1	15	0.009	433224

Table 2. Baboon stego grey image.

Technique	MSE	RMSE	UIQI	SNR	MAE	PSNR	AD	MD	NAE	Payload
Ni *et al.* [20]	×	×	×	×	×	48.2	×	×	×	5421
Hwang *et al.* [14]	×	×	×	×	×	48.2	×	×	×	5208
Lin and Hsueh [16]	×	×	×	×	×	47.61	×	×	×	19130
Hu *et al.* [13]	×	×	×	×	×	48.34	×	×	×	21411
Luo *et al.* [17]	×	×	×	×	×	48.36	×	×	×	22696
Wu and Tsai [28]	3.25	×	×	×	×	37.9	×	×	×	56291
Yang *et al.* [31]	×	×	×	×	×	33.01	×	×	×	916010
Vleeschouwer et al. [25]	×	×	×	×	×	39	×	×	×	2905
Goljan *et al.* [8]	×	×	×	×	×	29	×	×	×	1024
Xuan *et al.* [29]	×	×	×	×	×	32.8	×	×	×	14916
Celik *et al.* [3]	×	×	×	×	×	38	×	×	×	15176
LSB	40.05	6.33	0.9	8.03	5.15	32.14	0	14	0.04	1048576
Proposed	2.4	1.55	0.99	20.3	0.99	44.37	0	15	0.01	410636

[1] LSB refers to Normal 4bit LSB Technique

Table 3. Lena stego color image.

Technique	MSE	RMSE	UIQI	SNR	MAE	PSNR	AD	MD	NAE	Payload
Yalman *et al*. [30]	×	×	×	×	×	39.566	×	×	×	1156000
LSB	18.42	4.29	0.75	11.4	3.47	35.48	0.5	14	0.03	3145728
Proposed	3.2	1.79	0.96	19	1.1	43.11	0.2	11	0.01	1355199

Table 4. Baboon stego color image.

Technique	MSE	RMSE	UIQI	SNR	MAE	PSNR	AD	MD	NAE	Payload
Yalman *et al*. [30]	×	×	×	×	×	39.6	×	×	×	1156000
LSB	40	4.29	0.9	8.04	5.15	32.14	0.47	14	0.04	3145728
Proposed	**1.27**	**1.13**	**0.99**	**23**	**0.71**	**47.1**	**0.13**	**13**	**0.01**	**1329318**

Table 1 shows that the proposed technique for Lena grey image is well ahead of the existing techniques in terms of payload except Vleeschouwer *et al.* [25] and normal LSB techniques. The proposed technique has a high PSNR than the Vleeschouwer *et al.* [25] Technique and normal 4bit LSB techniques. MSE, RME, MAE and NAE for normal LSB technique is very high compared to proposed technique, as shown in Table 1. The UIQI of our technique is almost double than the normal LSB technique.

The proposed technique for baboon grey image has a high capacity compared to maximum of the existing techniques. Yang *et al*. [31] and normal LSB technique have high information hiding capacity, but low PSNR compared to our technique, as shown in Table 2. The proposed technique gives better results for MSR, RMSR, UIQI, MAE, SNR, NAE and AD.

To the best of our knowledge, Yalman *et al.* [30] has considered color image in their technique. We have compared our technique with Yalman *et al.* [30] and normal LSB. Please note that the Yalman has also, considered two attributes PSNR and Payload in their technique, but we focus on ten attributes listed in Tables 3 and 4.

The proposed technique for Lena color image is superior in all performance parameters to Yalman *et al.* [30] and normal LSB technique, as shown in Table 3.

Table 4 shows that the proposed technique for baboon color image gives better results than Yalman *et al.* [30] and normal LSB technique.

6. Conclusions

In this paper, a novel steganographic LSB technique is presented. The new LSB technique embeds secret information in the cover image based on its pixel values. The motivation of proposed approach is the weakness of HVS, i.e., HVS is unable to identify changes in low level colors. This idea is used for embedding information in the pixels of cover image. A threshold is set on the pixel values of the cover image and 4bits, 3bits, 2bits and 1bit of the secret information is embedded based on the threshold. The experimental results show that the proposed technique has high payload and PSNR as compared to the existing LSB steganographic techniques.

Furthermore, we have considered ten different attributes in proposed algorithm, whereas none of the available techniques have used more than three attributes during their analysis. The proposed technique also, provides the reverse process of the encoding algorithm. The stego images obtained by the application of proposed technique still have high visual quality and the hidden information is not perceptible to the naked eye in any way.

References

[1] Altaay A., Bin Sahib S., and Zamani M., "An Introduction to Image Steganography Techniques," *in Proceedings of International Conference on Advanced Computer Science Applications and Technologies*, Kuala Lumpur, pp. 122-126, 2013.

[2] Bender W., Gruhl D., Morimoto N., and Lu A., "Techniques for Data Hiding," *IBM Systems Journal*, vol. 35, no. 3, pp. 210-224, 2002.

[3] Celik M., Sharma G., Tekalp A., and Saber E., "Reversible Data Hiding," *in Proceeding of International Conference Image Processing*, pp. 157-160, 2002.

[4] Chadha A., Satam N., Sood R., and Bade D., "An Efficient Method for Image and Audio Steganography using Least Significant Bit Substitution, " *International Journal of Computer Applications*, vol. 77, no. 13, pp. 37-45, 2013.

[5] Chan M., MATLAB Central: Image Error Measurements, available at: http://www.mathworks.com/matlabcentral/fileexchange/29500-image-errormeasurements, last visited 2014.

[6] Chan M., "Wavelet Polynomial Threshold based Filter for High Resolution Microscopy," http://gradworks.umi.com/14/92/1492064.html, last visited 2011.

[7] Chandramouli R. and Memon N., "Analysis of LSB based Image Steganography Techniques," *in Proceedings of International Conference on Image Processing*, Thessaloniki, pp. 1019-1022, 2001.

[8] Goljan M., Fridrich J., and Du R., "Distortion-Free Data Embedding," *in Proceedings of the 4th Information Hiding Workshop*, Pittsburgh, pp. 27-41, 2001.

[9] Gupta H., Kumar R., and Changlani S., "Enhanced Data Hiding Capacity using LSB based Image Steganography Method," available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.413.8492&rep=rep1&type=pdf, last visited 2013.

[10] Gupta S., Goyal A., and Bushan B., "Information Hiding using Least Signifcant Bit Steganography and Cryptography," *International Journal of Modern Education and Computer Sciences*, vol. 6, pp. 27-34, 2012.

[11] Hempstalk K., "Hiding Behind Corners: Using Edges in Images for Better Steganography,"

available at: http://diit.sourceforge.net/files/HidingBehindCorners.pdf, last visited 2006.

[12] Hossain M., Al Haque S., and Sharmin F., "Variable Rate Steganography in Gray Scale Digital Images using Neighbourhood Pixel Information," *the International Arab Journal of Information Technology*, vol. 7, no. 1, pp. 34-38, 2010.

[13] Hu Y., Lee H., and Li J., "De-based Reversible Data Hiding With Improved Overflow Location Map," *IEEE Transactions on Circuits Systems and Video Technolog*y, vol. 19, no. 2, pp. 250-260, 2009.

[14] Hussain M. and Hussain M., "A Survey of Image Steganography Techniques," *the International Journal of Advanced Science and Technology*, vol. 54, pp. 113-124, 2013.

[15] Hwang J., Kim J., and Choi J., "A Reversible Watermarking based on Histogram Shifting," *in Proceedings of the 5th International Workshop on Digital Watermarking*, Jeju Island, Korea, pp. 348-361, 2006.

[16] Lin C., and Hsueh N., "A Lossless Data Hiding Scheme based on Three-Pixel Block Differences," *Pattern Recognition*, vol. 41, no. 4, pp. 1415-1425, 2008.

[17] Luo L., Chen Z., Chen M., Zeng X., and Xiong Z., "Reversible Image Water Marking Using Interpolation Technique," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 187-193, 2010.

[18] Luo W., Huang F., and Huang J., "Edge Adaptive Image Steganography based on LSB Matching Revisited," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 201-214, 2010.

[19] Narayanan S., "MATLAB Central: image quality measures," available at: http://www.mathworks.com/matlabcentral/fileexchange/25005-image-quality-measures, last visited 2014.

[20] Ni Z., Shi Y., Ansari N., and Wei S., "Reversible Data Hiding," *IEEE Transactions on Circuits Systems and Video Technology*, vol. 16, no. 3, pp. 354-362, 2006.

[21] Nosrati M., Karimi R., and Hariri M., "An Introduction to Steganography Methodes," *World Applied Programming*, vol. 1, no. 3, pp. 191-195, 2011.

[22] Singh K., Singh L., Singh A., and Devi K., "Hiding Secret Message in Edges of the Image," *in Proceedings of International Conference on Information and Communication Technology*, Dhaka, pp. 238-241, 2007.

[23] Thomas P., "Literature Survey on Modern Image Steganographic Techniques," available at: http://iieng.org/images/proceedings_pdf/8221E1114029.pdf, last visited 2013.

[24] Tian J., "Reversible Data Embedding using a Difference Expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, 2013.

[25] Vleeschouwer C., Delaigle J., and Macq B., "Circular Interpretation on Histogram for Reversible Watermarking," *in Proceedings of the 4th IEEE International Workshop on Multimedia Signal Processing*, Cannes, pp. 345-350, 2001.

[26] Wang C., Wu N., Tsi C., and Hwang M., "High Quality Steganographic Method with Pixel Value Differencing and Modulus Function," *Journal of Systems and Software*, vol. 81, no. 1, pp. 150-158, 2007.

[27] Woods J., "Multidimensional Signal, Image and Video Processing and Coding," available at: http://books.google.com.pk/books?id=fIdsYOwIhOoC, last visited 2014.

[28] Wu D. and Tsai W., "A Steganographic Method for Images by Pixel-Value Differencing," *Pattern Recognition Letters*, vol. 24, no. 9, pp. 1613-1626, 2003.

[29] Xuan G., Zhu J., Chen J., Shi Y., Ni Z., and Su W., "Distortionless Data Hiding based on Integer Wavelet Transform," *IEEE Letters*, vol. 38, no. 25, pp. 646-1648, 2002.

[30] Yalman Y., Akar F., and Erturk I., "An Image Interpolation based Reversible Data Hiding Method Using R-Weighted Coding," *in Proceedings of the 13th International Conference on Computational Science and Engineering*, Hong Kong, pp. 346-350, 2010.

[31] Yang C., Weng C., Wang S., and Sun H., "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems," *IEEE Transaction on Information Forensics Security*, vol. 3, no. 3, pp. 488-497, 2008.

Zakir Khan has done his Bachelor of Computer Science from Hazara University Mansehra, Pakistan in 2011 and is currently enrolled for his Master in Computer Science at the Department of Information Technology Hazara University, Pakistan. He is a skilled programmer and his research interests include image and signal processing, optical fiber communication, network security and computer networks.

Mohsin Shah is currently serving as lecturer at the Department of Information Technology Hazara University Mansehra, Pakistan. He has done his BSc Telecommunication Engineering from University of Engineering and Technology Peshawar, Pakistan in 2007 and M.Sc. Telecommunication Engineering from University of Engineering and Technology Taxila, Pakistan in 2012. He has 2 years of diversified experience in the field of cellular mobile communication systems. His research interests include image processing, optics and photonics and data security.

Muhammad Naeem is serving as Lecturer at the Department of Information Technology Hazara University Mansehra, Pakistan. He got his PhD from University of Leicester, UK in 2012. His research interests include software product lines, requirements engineering, steganography and computational mathematics. He is also, interested in formal framework like linear logic and proportional logic.

Toqeer Mahmood is currently serving as Programmer at University of Engineering and Technology Taxila, Pakistan. He completed his MS Computer Engineering in 2010 from Center for Advanced Studies in Engineering (CASE) Islamabad, Pakistan. He is currently pursuing his PhD in Image Forensics from University of Engineering and Technology Taxila, Pakistan. His research interests include image processing, computer vision, computer networks and numerical techniques.

Shah Khan has been serving as lecturer at the Department of Information Technology Hazara University Mansehra, Pakistan. He has done his BSc Telecommunication Engineering from University of Engineering and Technology Peshawar, Pakistan in 2008 and pursuing his MSc Telecommunication Engineering from University of Engineering and Technology Taxila, Pakistan. His research interests include image processing and data communication.

Noor Ul Amin is currently serving as Assistant Professor and Head of Department of Information Technology Hazara University Mansehra, Pakistan. He completed his MS Computer Engineering in 2010 from International Islamic University, Pakistan. Currently, he is pursuing his PhD in Computer Science from Hazara University Mansehra, Pakistan. His research interests include network security, senser network and image and signals processing.

Danish Shehzad is Research Assistant at Department of Computer Engineering, Kadir Has University Istanbul, Turkey. He has done MS in Computer Science from Hazara University Mansehra, Pakistan in 2014. His BS (Hons) is in Telecommunication and Networks from Comsats Institute of Information Technology, Abbottabad Pakistan, 2010. His areas of research interest are hybrid programming, network security and image and signal processing.