An improved image steganography technique based on MSB using bit differencing

Conference Paper · August 2016

DOI: 10.1109/INTECH.2016.7845020

CITATIONS
17

READS
1,074

8 authors, including:

Ammad Ul Islam
Institute of Space Technology
3 PUBLICATIONS **17** CITATIONS
SEE PROFILE

Mohsin Shah
Hazara University
23 PUBLICATIONS **172** CITATIONS
SEE PROFILE

Zakir Khan
Hazara University
30 PUBLICATIONS **117** CITATIONS
SEE PROFILE

Toqeer Mahmood
University of Engineering and Technology, Taxila
36 PUBLICATIONS **386** CITATIONS
SEE PROFILE

An Improved Image Steganography Technique based on MSB using Bit Differencing

Ammad Ul Islam[1], Faiza Khalid[2], Mohsin Shah[2], Zakir Khan[2] , Toqeer Mahmood[3], Adnan Khan[2], Usman Ali[2], Muhammad Naeem[4]

[1] Department of Electrical Engineering, Institute of Space Technology Islamabad, Pakistan
Email: ammadulislam92@gmail.com
[2] Department of Information Technology and Telecommunication, Hazara University Mansehra, Pakistan
Email: {syedmohsinshah, zakirk2012}@gmail.com, {engr_faiza, kadnan83, usman930}@yahoo.com
[3] Department of Computer Engineering, University of Engineering and Technology Taxila, Pakistan
Email: toqeer.mahmood@yahoo.com
[4] Department of Information Technology, Abbottabad University of Science and Technology KPK, Pakistan
Email: naeem@aust.edu.pk

***Abstract*—The rapid development of data communication in modern era demands secure exchange of information. Steganography is an established method for hiding data from an unauthorised access. Steganographic techniques hide secret data in different file formats such as: image, text, audio, and video. Invisibility, payload capacity, and security in terms of PSNR and robustness are the key challenges to steganography. In this paper, a novel image stegnography technique based on most significant bits (MSB) of image pixels is proposed. Bit No. 5 is used to store the secret bits based on the difference of bit No. 5 and 6 of cover image. If the difference of bit No. 5 and 6 is different from secret data bit then the value of bit No. 5 is changed. The results state that the proposed technique ensures significant improvements in signal to noise ratio. Usually, the hackers focus on LSB bits for secret data extraction but the proposed technique utilizes the MSB bits that make it more secure from unauthorized access. Furthermore, the presented technique is not only secure, but computationally efficient as well.**

Index Terms*—*Steganography; Cover image; Stego image; Most Significant Bit; Least Significant Bit

I. INTRODUCTION

Information security is necessary for the transmission of confidential data. Steganography and cryprography are the means of securing the confidentiality and secrecy of information. In cryptography secret text is converted into cypher text, while in steganography the secret text remains the same but it is embedded in another format of data. Today, in the presense of powerful communication systems, protecting the secret information from the hackers is a challenging task. Steganograpgy hides the exisance of information and protects secret information from unathorized access [1]. A steganographic system consists of three components, namely: Plain text, Cover file, and Stego file [1]. Secret information to be protected is known as plain text. Cover file can be text, image, audio or video in which data is embedded. Stego file is the output of the steganographic system that contains the hidden information. The three important properties of a steganographic systems are: (1) Security, (2) Payload Capacity, and (3) Robustness.

The rest of the paper is arranged as follows: Section 2 presents a brief literature review in the domain of steganography. In section 3, encoding and decoding procedure of the proposed technique is discussed. Section 4 is dedicated to the experimental results of the proposed technique. The comparison of the proposed technique with the existing methods is presented in Section 5. Finally, the proposed work is concluded in Section 6.

II. LITERATURE REVIEW

Embedding secret information in the least significant bits (LSB) of cover image pixels is a common and widely used technique of steganography. Various techniques have been presented in the domain of LSB steganographic techniques. Each presented technique has it own pros and cons in terms of embedding capacity and signal to noise ratio (SNR) [2, 3]. In LSB steganographic techniques, secret information bits are embedded in the least significant bits of the cover file. In [3], a comprehensive survey of LSB image steganographic techniques is presented. In [4], an LSB array based technique is proposed, in which all the bits of LSB's are taken for data hiding. In this technique, encrypted message block is mapped to the LSB array, where maximum matching is found. In [5], an image steganographic technique based on adaptive LSB substitution is proposed. The presented technique calculates the number of *k-bits* (bits to be hidden) by taking into account the edges, brightness and texture masking of the cover image. The experimental results of this technique shows that the value of *k* is high at non-sensitive image region and it is low at sensitive image regions. Advantage of adaptive based technique is that it can embed high capcity of data, but dataset for experiments is limited; there is not a single image which has many edges with noise region. A combination of stego-key pattern bits and secret bits is used to modify the LSB of cover image pixels [6]. A combination of $M \times N$ block with random key value is used as a pattern. The embedding procedure modifies 2nd LSB bit of the cover image pixel if the pattern matches with the secret data bits. This technique is complex in terms of security but lacks in payload capacity.

978-1-5090-2000-3/16/$31.00 ©2016 IEEE

Another adaptive LSB technique named pixel value difference (PVD) is presented in [7]. PVD technique uses a simple relationship of pixel difference between two consecutive pixels of cover image to estimate the size of the hidden data bits. This relationship determines adaptive *k-bits* to be hidden in cover image. The experimental results of PVD technique show that it can produce high quality stego images with a decent amount of pay load capacity and high impercibility. However, the PVD technique is complex and computationally cost in-effectrive as it has to calculate pixel value difference for every consective pixel pair of the cover image. Multi-Pixel Differecing (MPD) technique in contrast to PVD uses four pixels to calculate sum of difference value of a four pixel block [8]. It uses the simple LSB embedding method when the difference is low and uses MPD when it is high. MPD is a simple and computationaly efficient technique if the dataset is small otherwise it's a complex way of data hiding. Another PVD technique that takes into account 3 pixels for difference calculation is presented in [9]. The number of *k-bits* are estimated using three pixels near the target pixel. This technique uses optimal pixel adjustment on target pixels to achive high impercibility and high embedding capacity. Experimental results of this technique show that the histograms of cover and stego images are almost the same which proves that this technique can produce high quality stego images. However, dataset for this technique is very small. An image steganographic scheme that is based on edge detection and LSB substitution is presented in [10]. Hybrid edge detection techniques are used to detect edges in cover image and then LSB substitution is used to embed secret data bits in edges of the cover image. This technique can produce stego images with high peak signal to noise ratios (PSNR) but it is weak in terms of security and complexity. In [11], bit complementation based technique is suggested for hiding the data in images. This technique hides 4 bits in every pixel of cover image. Secret information nibbles are compared with the cover image bits from bit No. 2 to bit No. 5 or its complement. Embedding is performed based on a decision whether the secret data nibble matches with the bits from 2 to 5 or its complement. In [12], a novel image steganographic technique which maps pixel bits into alphabetic characters is presented. The main idea is to map 7 bits from pixels of cover image into 26 alphabetic English characters. These mapped English characters are used to write secret messages. The experimental results of this technique show that it does not change the carrier cover image after embedding of secret data. Techniuqe presented in [13] is based on Human Visualization System (HVS) weakness. This technique finds the darkest areas in cover image and utilizes LSB substitution for secret data embedding. A high computational time is required for finding the darkest areas in cover image whick makes this technique computationally in-affective. In [14], a novel technique for secure exchange of secret information between two parties in a communication session is presented. In this technique, the cover image itself works as a secret key. Secret information bits are combined in groups of 8 bits and compared with the cover image pixels color levels. In case of a match with the pixel binary code, the location of that pixel is transmitted. This technique supposed that cover image is securely shared between the two parties of communication.

III. PROPOSED METHOD

In the proposed work, a new technique is presented where most significant bits (MSB) of pixels are taken in order to hide secret data bits. The difference between bit No. 5 and 6 is used for hiding secret information bits. Bit 0 is supposed to be hidden if the difference between bit No. 5 and bit No. 6 is zero and bit 1 hidden if their difference is one. If the incoming secret data bit is not equal to the difference between bit No. 5 and 6 then bit No. 5 is changes to make them equal.

A. Encoding Algorithm

The data encoding procedure of the proposed technique is shown in Fig. 1. The steps for encoding the secret information in cover image are given as under:

i. Read the secret information bits
ii. Read the cover image
iii. For every pixel of cover Image
   a. Read bit No. 5 and 6
   b. Compute the difference
   c. Compare the difference with secret information bit, If data bit is not equal to the difference then transverse bit No. 5
iv. Write the stego image

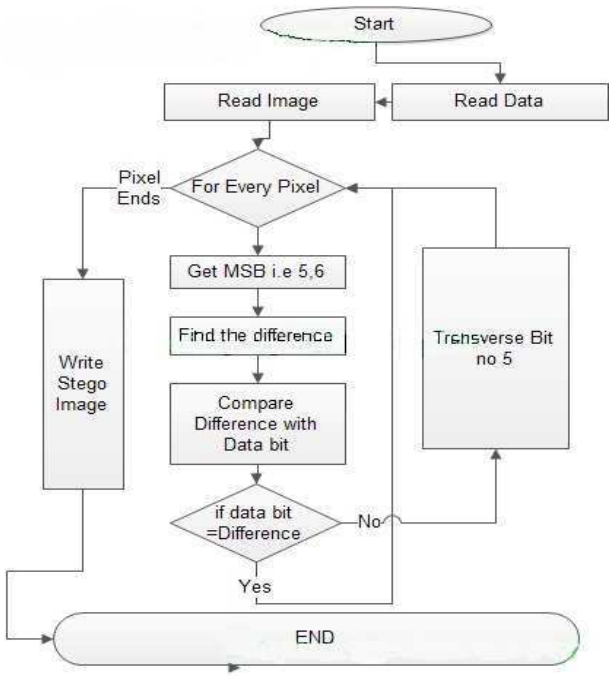


Fig. 1. Data Encoding

B. Decoding Algorithm

The following steps are required to extract the secret information bits from the stego image.

i. Read the stego image
ii. For every pixel of stego image
   a. Compte the difference between 5^{th} and 6^{th} bits: data bit = difference
iii. write the secret data to file

In above algorithm, after reading every pixel of stego image, we take the difference between 5^{th} and 6^{th} bit. The result of difference will be the value of data bit. The data decoding procedure of the proposed algorithm is given in Fig. 2.

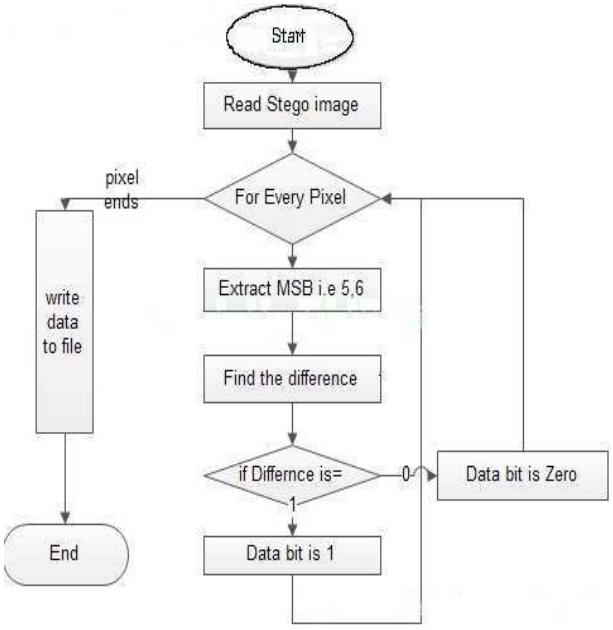


Fig. 2. Data Decoding

The example of encoding and decoding procedure of the proposed algorithm is demonstrated in Table 1 which is self explanatory.

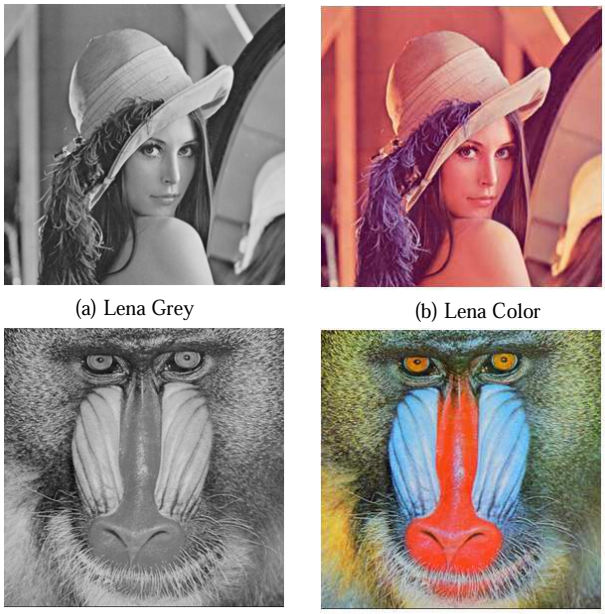
TABLE I. AN EXAMPLE OF ENCODING AND DECODING PROCEDURE

Before Encoding				After Encoding				After Decoding	
Cover Image			Data Bit	Difference	Stego Image			Difference	Data Bit
Pixel No.	Bit 5	Bit 6			Pixel No.	Bit 5	Bit 6		
1	0	0	0	0	1	0	0	0	0
2	0	1	0	1	2	1	1	0	0
3	1	0	0	1	3	0	0	0	0
4	1	1	0	0	4	1	1	0	0
5	0	0	1	0	5	1	0	1	1
6	0	1	1	1	6	0	1	1	0
7	1	0	1	1	7	1	0	1	1
8	1	1	1	0	8	0	1	1	1

It is worth mentioning that the data bits before the application of encoding and after the decoding procedure remains the same. More precisely, what we have encoded is been achieved at the deciodong end.

IV. EXPERIMENTAL RESULTS

We have used four test images mostly used by steganographic community for the implementation purposes, as shown in Fig. 3. The specification of these images are: Grey level Lena 512×512×8; Color Lena 512×512×3; Grey level Baboon 512×512×8; and Color Baboon 512×512×3.

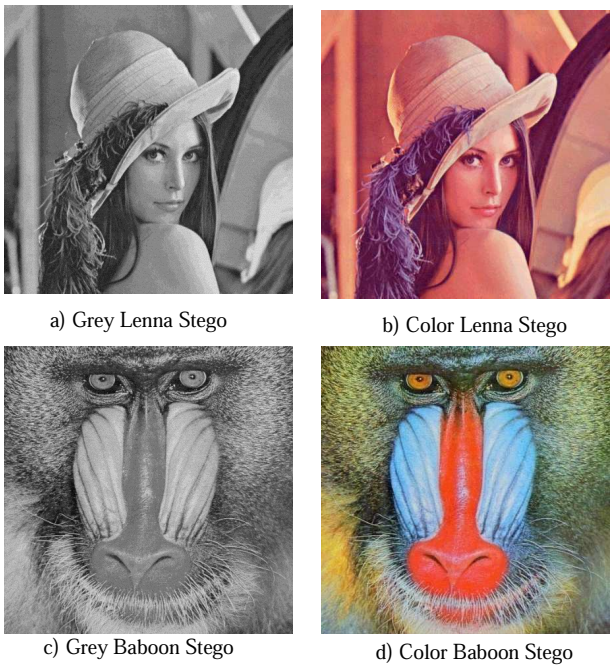


(a) Lena Grey (b) Lena Color

(c) Baboon Grey (d) Baboon Color

Fig. 3. Cover images

A long random bit stream is used as a secret message. MATLAB tool is used for implementation purposes. Fig. 4 shows the resultant stego images after the implementation of the proposed algorithm.



a) Grey Lenna Stego b) Color Lenna Stego

c) Grey Baboon Stego d) Color Baboon Stego

Fig. 4: Stego Images

It can be seen in Fig.4 that Human Visualization System (HVS) can not detect differences between the cover images shown in Fig. 3 and stego images shown in Fig. 4. This shows the effectives of the proposed technique in terms of imperceptibility. The PSNR of all the stego images are given in Table 2 –5.

V. Comparison with the existing techniques

We compared experimental results of the proposed technique with state of the art algortihms and found that our results are better.

The comparison of the results are given in Table II–V. Table II is showing the comparison of proposed technique for Lena gray image.

TABLE II. Comparison of MSB Lena Stego Grey Image

Techniques	PSNR	Payload
[7]	36.28	837332
[15]	48.2	5460
[16]	48.22	5336
[17]	46.6	59900
[18]	48.69	60241
[19]	41.79	50960
[21]	39	24108
[22]	30	1024
[23]	36.6	85507
[24]	38	74600
[25]	48.82	71674
Proposed	51.17977	262144

The results given in Table II show that our technique outperformed for Lena grey image compared to other techniques in terms of payload and PSNR.

Table III is comparing the proposed algorithm with existing method for Lena color image. The result show that the proposed algorithm has high PSNR compared to the method presented in [24].

TABLE III. Comparison of Lena color image

Technique	PSNR	Payload
[24]	39.566	1156000
Proposed	52.3438	786432

The comparison results against the Baboon gray and color images are given in Table IV and V.

The results presented in Table IV and V indicate that the proposed technique performed well in comparison with other techniques in terms of PSNR and Payload capacity.

TABLE IV. Comparison for Baboon gray image

Technique	PSNR	Payload
[7]	33.01	916010
[15]	48.2	5421
[16]	48.2	5208
[17]	47.61	19130
[18]	48.34	21411
[19]	48.36	22696
[21]	39	2905
[22]	29	1024
[23]	32.8	14916
[24]	38	15176
[25]	37.9	56291
Proposed	51.1803	262144

TABLE V. Comparison of MSB Baboon color image

Technique	PSNR	Payload
[24]	39.6	1156000
Proposed	52.6897	786432

VI. Conclusions

In this work an image steganographic technique based on MSB is presented. The technique uses the difference of two pixel's bits of the cover image. Bit No. 5 and 6 of a pixel are targeted for embedding. The difference between bit 5 and 6 is set according to the incoming secret information bit. If the difference between bit 5 and 6 is equal to the incoming secret bit then no change is required in bit 5. If the difference between bit 5 and 6 does not match with the incoming bit then bit 5 is changed to make the difference and incoming bit equal.

Usually, the LSB are targeted in steganographic systems, therefore using the MSB makes the system more secure. Furthermore, comparative analysis shows that the proposed technique has greater PSNR that shows the effectiveness of the proposed scheme. Payload capacity of the proposed technique is also comparatively better than the available techniques which can be used to hide more data in a single cover image.

References

[1]. Z. Khan, M. Shah, M. Naeem, T. Mahmood, S.N.A. Khan, N. Amin, D. Shahzad, "Threshold based Steganography: A Novel Technique for Improved Payload and SNR", International Arab Journal of Information Technology, vol. 13, No. 4, pp.380-386, 2016.

[2]. M. Hussain and M. Hussain, "A survey of image steganography techniques," International Journal of Advanced Science and Technology, vol. 54, pp. 113-124, 2013.

[3]. P. Thomas, "Literature survey on modern image steganographic techniques," International Journal of Engineering Research and Technology, vol. 2, 2013.

[4]. M. Juneja, and P.S. Sandhu, “Designing of Robust Steganography Technique Based on LSB Insertion and Encryption”. Proceedings of International Conference on Advances in Recent Technologies in Communication and Computing, pp. 302–305, 2009.

[5]. H. Yang, X. Sun and G. Sun, “A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution”, Radio Engineering, vol. 18, pp. 509-516, 2009.

[6]. S. Channalli and A. Jadhav, “Steganography an Art of Hiding Data”, International Journal on Computer Science and Engineering, vol. 1, 2009.

[7]. C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," IEEE Transactions on Information Forensics and Security, vol. 3, pp. 488-497, 2008.

[8]. K.-H. Jung, K.-J. Ha and K.-Y. Yoo, “Image data hiding method based on multi-pixel differencing and LSB substitution methods”, Proc. 2008 International Conference on Convergence and Hybrid Information Technology, Daejeon, Korea, 2008, pp. 355-358.

[9]. H. Zhang, G. Geng and C. Xiong, “Image Steganography Using Pixel-Value Differencing”, Second International Symposium on Electronic Commerce and Security, 2009.

[10]. W. J. Chen, C. C. Chang and T. H. N. Le, “High Payload Steganography Mechanism Using Hybrid Edge Detector”, Expert Systems with Applications, vol. 37, pp. 3292-3301, 2010.

[11]. Z. Khan, M. Shah, M. Naeem, D. Shahzad, T. Mahmood, “LSB Steganography using Bits Complementation”, International Conference on Chemical Engineering and Advanced Computational Technologies, Pretoria, South Africa, pp. 84-87, 2014.

[12]. M. A. Al-Husainy, “Image Steganography by Mapping Pixels to Letters”, Journal of Computer Science, vol. 5, pp. 33-38, 2009.

[13]. H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, “Labeling Method in Steganography”, World Academy of Science, Engineering and Technology, France, 2007.

[14]. M. Islam, M. Shah, Z. Khan, T. Mahmood, M.J. Khan, “A New Symmetric Key Encryption Algorithm Using Images as Secret Keys” 13th IEEE International Conference on Frontiers of Information Technology, pp. 1-5, 2015.

[15]. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, pp. 354-362, 2006.

[16]. J. Hwang, J. Kim, and J. Choi, "A reversible watermarking based on histogram shifting," in Digital Watermarking, ed: Springer, 2006, pp. 348-361.

[17]. C.-C. Lin and N.-L. Hsueh, "A lossless data hiding scheme based on three-pixel block differences," Pattern Recognition, vol. 41, pp. 1415-1425, 2008.

[18]. Y. Hu, H.-K. Lee, and J. Li, "DE-based reversible data hiding with improved overflow location map," , IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, pp. 250-260, 2009.

[19]. D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, pp. 1613-1626, 2003.

[20]. C. D. Vleeschouwer, J. Delaigle, and B. Macq, "Circular interpretation of histogram for reversible watermarking," Proceedings of the IEEE 4th Workshop on Multimedia Signal Processing, pp. 345-350, 2001.

[21]. M. Goljan, J. J. Fridrich, and R. Du, "Distortion-free data embedding for images," Proceedings of the 4th Information Hiding Workshop, Pittsburgh, PA, pp. 27-41, 2001.

[22]. G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, "Distortionless data hiding based on integer wavelet transform," Electronics Letters, vol. 38, pp. 1646-1648, 2002.

[23]. M. U. Celik, G. Sharma, and E. Saber, "Reversible data hiding," Proceedings of IEEE International Conference on Image Processing, vol. 2, pp. 157-160, 2002.

[24]. Y. Yalman, F. Akar, and I. Erturk, "An image interpolation based reversible data hiding method using R-weighted coding," IEEE 13th International Conference on Computational Science and Engineering, pp. 346-350, 2010.

[25]. L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," IEEE Transactions on Information Forensics and Security, vol. 5, pp. 187-193, 2010.