A New Robust Method of Hiding Text Characters for Secure Open Channel Transmission

Harsh Vikram Singh, S. P. Singh and Anand Mohan
Department of Electronics Engineering,
Institute of Technology
Banaras Hindu University
Varanasi-221005, India

Summary
This paper discusses a new method of hiding ASCII characters based on match between bit value of the randomly selected image pixel and the data bits. Bit positions in the higher nibbles of the cover image are used for data hiding at a position indicated using a 2-bit code. Simulation results on *Lena*, *Gibbon and Cat* images [1] for hiding a large set of ASCII text characters indicate that suggested technique achieves *PSNR* up to 44.7 dB as against minimum required 34 dB for acceptable perceptual quality [2]. Also, the bounds of the change in the original pixel value due to data hiding are limited to $\pm$ 3. Therefore besides retaining perceptual quality of the original cover the proposed method offers high robustness as compared to the LSB insertion technique [3, 4], it is less prone to attacks by eaves droppers and hence it can be effectively used for secure open channel transmissions.

Keywords: Steganography, Secure data transmission, Data Hiding.

1. Introduction

The staggering growth in communication technology and usage of public domain channels (i.e. Internet) has greatly facilitated transfer of data. However, such open communication channels have greater vulnerability to security threats causing unauthorized information access. This might lead to disclosure, modification or even deletion of classified/unclassified data files or copyright violation [5]. Therefore preventing unauthorized information access has been a prime consideration for growing use of *steganography* techniques [6] for applications like copyright protection, feature tagging and secret communication [7]. As a result, steganography has become an interesting and challenging field of research striving to achieve greater immunity of hidden data against signal processing operations on the host cover media; e.g. a good steganography technique should offer immunity of hidden data against lossy compression, scaling, interception, modification, or removal etc. and ensure that embedded data remains inviolate and recoverable [8]. However, a trade-off between the quantity of hidden data and its degree of immunity to host signal modification is needed in most cases [9]. Data hiding requires embedding data into digital media like image, audio, or text, however, due to providing high embedding efficiency the still images are preferred as hosts as compared to others. LSB insertion [3, 4] is a popular steganography technique using still images as hosts. In this method the data bit is inserted into the LSBs of the randomly selected host pixels. The *LSB* technique retains host image quality but it has severe limitation of total data loss if the LSBs of the cover pixels are changed either accidentally during transmission or intentionally by attackers. Although, this problem can be minimized by inserting data into higher order bits of the host pixel but at the expense of worsening the perceptual quality of the cover image [10, 11]. Therefore, data hiding in still images needs addressing constrains related to the working of human visual system (*HVS*) and the resulting modifications of the host image [12].

This paper describes a new technique of hiding ASCII characters based on match between bit value of the randomly selected image pixel and the data bits. Higher nibbles of the cover image have been used for hiding 800 ASCII text characters at a position indicated using a 2-bit code. It is illustrated considering *Lena*, *Gibbon and Cat* cover images [1]. The suggested method achieves *PSNR* up to 44.7 dB as against minimum required (34 dB) [2] with limits of the variation in the original pixel value within $\pm$ 3. In addition it offers improved robustness as compared to the LSB insertion technique [3, 4] and thus can be effectively used for secure data transmissions.

2. Proposed Hiding Algorithm

Select the pixels in random manner from the cover image I of size $M \times N$ having pixel $I(i, j)$ at i^{th} row and j^{th} column. Let P_k denote the bit position of the image pixels ($1 \le P_k \le 8$ for 8-bit grayscale) with $P_k = 8$ and $P_k = 1$ representing the *MSB* and *LSB* positions, respectively; and O_{P_k} be the original bit value at P_k. Let D be the data of size l bits to be embedded whose n^{th} bit is D_n.

2.1 Data Hiding

- Scan bit position P_k $(P_k = 5,6,7,8)$ in the randomly selected $I(i, j)$ pixel and match with n^{th} bit of data D_n.

Manuscript received July 5, 2007
Manuscript revised July 25, 2007

- Store position P_k of the pixel obtained in above step as 2-bit code at bit pair positions $(1,2)$, $(2,3)$, $(1,3)$, $(2,4)$, or $(1,3)$ assigning (00), (01), (10) and (11) for P_k = 5, 6, 7, and 8 respectively.
- Skip the pixel $I(i, j)$ for no match and select the next pixel.
- If match is found, repeat two steps given above by incrementing "n" until $n \le l$.

The above algorithm achieves both reduced perceptual distortion of the original image as the higher order pixel nibble is not altered and also avoids the eavesdropper attention to attack the stego-image.

2.2 Data Retrieval

The hidden data extraction is achieved by using the same random selection algorithm to select the pixel $I(i, j)$ of the stego-image. Use the embedding code word to find out the data bit using known pixel number $I(i, j)$ and its corresponding code bit pair positions. The extracted data bits are then arranged in their original order to complete the retrieval process.

3. MSE and PSNR

Imperceptibility takes advantage of human psycho-visual redundancy, which is very difficult to quantify. The (weighted) mean squared error between the cover image and the stego-image (embedding distortion) is used as the measure to assess the relative perceptibility due to the embedded text. Mean square error (*MSE*) and Peak Signal to Noise Ratio (*PSNR*) can be used as metrics to measure the degree of imperceptibility [13]. Mathematically *MSE* can be derived as

$$MSE = \frac{1}{MN}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(f_{i,j} - g_{i,j})^2\right]$$

Where *M* and *N* are the rows and columns respectively of the image. Let $f_{i,j}$ be the pixel value of the cover-image and $g_{i,j}$ denote the pixel value of the stego-image. The *PSNR* can be calculated using *MSE* as

$$PSNR = 10 \log_{10}\left(\frac{L^2}{MSE}\right)$$

Where *L* is the peak signal value of the cover image (for 8-bit images, *L*=255).

4. Simulation Results

The performance of the proposed data hiding algorithm has been evaluated by embedding 800 *ASCII* characters in the *IEEE* standard *Lena*, *Gibbon and Cat* cover images of size 512×512 and using *MATLAB* image processing tool. The simulation results on *Lena*, *Gibbon and Cat* cover images hiding 800 ASCII text characters and for different bit pairs $P_k = (1,2),(1,3),(1,4),(2,3),(2,4)$ and $(3,4)$ are given in figures 2 to 19. Table-1 indicates the calculated minimum and maximum differences between the pixel values before and after data embedding for different bit pair combinations storing the 2-bit code word. It is evident from Table-1 that minimum variation in the original pixel value occurs for bit pair (1, 2). The *PSNR* values are computed by analyzing the difference between original images and corresponding stego-images for all cases of bit pair combinations (Table-1) for *Lena*, *Gibbon and Cat* cover images as given in Table-2. Considering a minimum of 34 dB *PSNR* threshold for stego-image perceptual quality [14] it is obvious from Table-2 that bit pairs (1, 2), (2, 3) or (1, 3) can be used for storing the 2-bit code and also that bit pair (1, 2) can be used for achieving minimal change in perceptual quality.

5. Conclusion

A new robust steganography technique for hiding ASCII text characters based on matching of bit values has been presented which retains perceptual quality of the cover media. Simulation results on IEEE standard *Lena*, *Cat and Gibbon* images hiding 800 text characters indicate that the proposed technique achieves up to 44.7 dB *PSNR* with variation in the original pixel values bounded within ± 3. The enhanced robustness as compared to LSB substitution technique is achieved due to data matching instead of substitution. Therefore the proposed method can be effectively utilized for secure transmission using open channel environment.

Table 1

Bit pairs	Change in pixel value	
	Maximum	Minimum
1,2	3	-3
1,3	5	-5
2,3	6	-6
1,4	9	-9
2,4	10	-10
3,4	12	-12

Table 2

Bit pairs	PSNR (dB)		
	Lena	Gibbon	Cat
1,2	44.709	42.587	42. 842
1,3	41.964	40.813	39.986
2,3	38.754	38.864	36.617
1,4	35.026	34.760	34.034
2,4	33.847	33.135	32.835
3,4	32.750	32.038	31.720

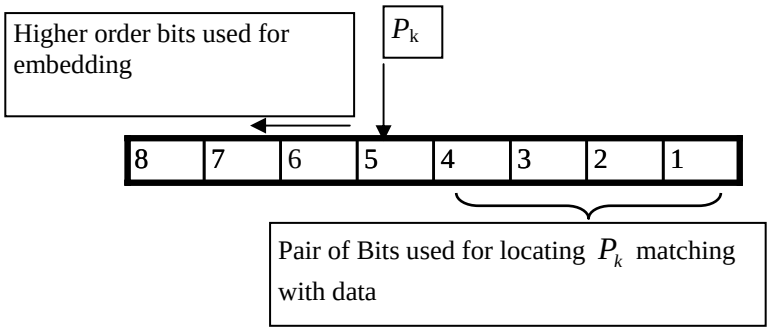


Fig. 1: Representation of image pixel

Fig. 2 Codes in bit pair 1, 2

Fig. 3 Codes in bit pair 1, 3

Fig. 4 Codes in bit pair 2, 3

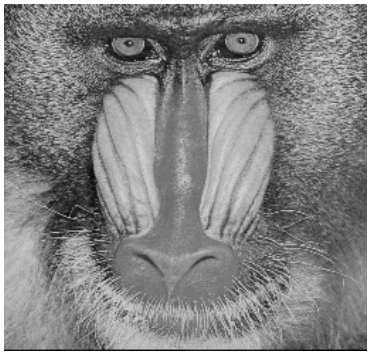


Fig. 8 Codes in bit pair 1, 2

Fig. 5 Codes in bit pair 1, 4

Fig. 6 Codes in bit pair 2, 4

Fig. 7 Codes in bit pair 3, 4

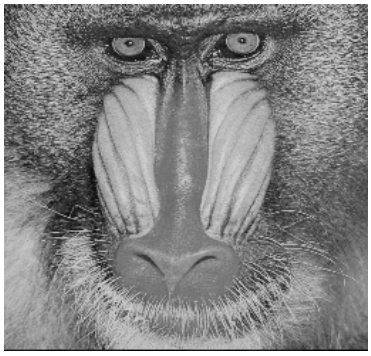


Fig. 9 Codes in bit pair 1, 3

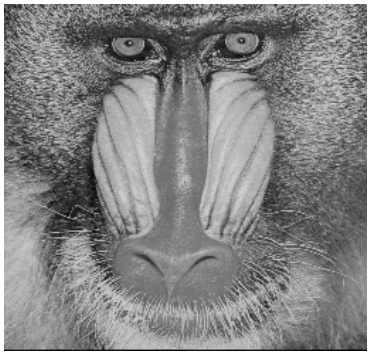


Fig. 10 Codes in bit pair 2, 3

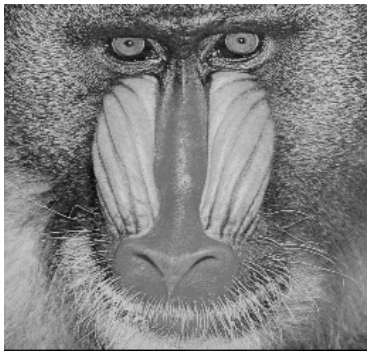


Fig.11 Codes in bit pair 1, 4

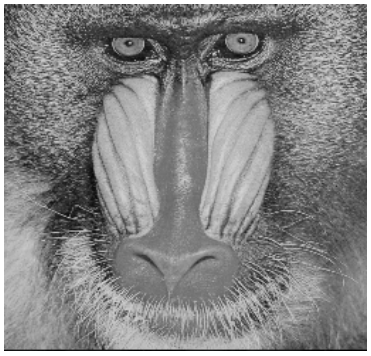


Fig. 12 Codes in bit pair 2 , 4

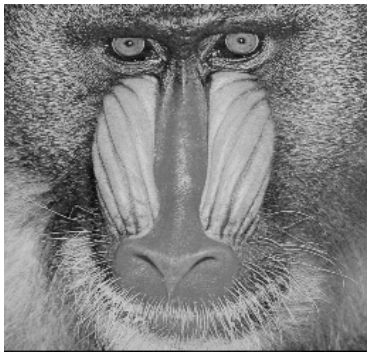


Fig. 13 Codes in bit pair 3, 4

Fig. 14 Codes in bit pair1, 2

Fig. 15 Codes in bit pair 1, 3

Fig. 16 Codes in bit pair 2, 3

Fig. 17 Codes in bit pair 1, 4

Fig. 18 Codes in bit pair 2, 4

Fig. 19 Codes in bit pair 3, 4

References:

[1] The USC-SIPI Image Database, http://www.petitcolas.net/fabien/watermarking/image_database/index.html

[2] D. Artz, "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing*, Vol.5, pp. 75-80, 2001

[3] Ross J. Anderson and Fabien A. P. Petitcolas "On the Limits of Steganography" *IEEE Journal on Selected Areas in Communications*, Vol. 16, pp. 474-481, 1998.

[4] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", *Computer*, Vol.31, pp. 26-34, 1998.

[5] W. Bender, D. Gruhl, N. Morimoto and A. Lu "Techniques for Data Hiding", *IBM Systems Journals*, Vol.35, NOS 3-4, pp. 313-336, 1996.

[6] M.M Amin, M. Salleh, S.Ibrahim, M. R. Katmin, and M.Z.I. Shamsuddin "Information hiding using Steganography", *Proc. 4th IEEE Conference on Telecommunication Technology*, Shah Alam, Malaysia, pp. 21-25, 2003.

[7] Cox et al. "*A* Secure, Robust Watermark for Multimedia", *Lecture Notes in Computer Science* Vol. 1, 174, Springer-Verlag, Berlin, pp. 185-206, 1996.

[8] F.A.P. Peticolas, R.J.Anderson and M.G.Kuhn, "Inforamition Hiding- A survey", *Proc. of IEEE*, Vol. 87, Issue: 7, pp. 1062-1078, 1999.

[9] Harsh Vikram Singh, A. K. Singh, S.K. Balasubramanian and Anand Mohan, "Minimizing Security Threats in Multimedia Systems", *Proc. 2nd IEEE International Conf. on Distributed Framework for Multimedia Applications* Penang, Malaysia, pp. 102-107, 2006.

[10] S. Venkatraman, A. Abraham, "Significance of Steganography on Data Security**",** *Proc. Information Technology: Coding and Computing*, (ITCC 2004) Vol. 2, pp. 347 – 351, 2004.

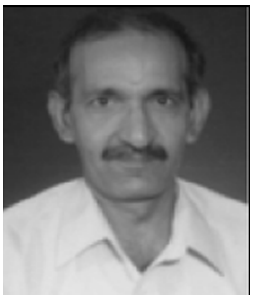
[11] Giuseppe Mastronardi, Marcello Castellano, and Francescomaria Marino "Steganography Effects in Various Formats of Images-A Preliminary Study", *Proc. International workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, 2001.

[12] Neil F. Johnsom, Zoran Duric and Sushil Jajodia "INFORMATION HIDING: Steganography and Watermarking – Attacks and Countermeasures", Kluwer Academic Publications, London, U.K., 2003.

[13] Jessica Fridrich, M. Goljan and R. Du "Detecting LSB Steganography in Color and Gray-Scale Images", *IEEE Multimedia Special Issue on Security*, pp. 22-28, 2001.

[14] R. Chandramouli and N Memon "Analysis of LSB Based Image Steganography Techniques", *Proc. International Conf. of Image Processing*, pp. 1019-1022, 2001.

Harsh Vikram Singh received B.Tech. (Hon) degree in Electronics Engineering from Institute of Engineering and Technology, Purvanchal University, India. Currently, he is Ph. D. student at Institute of Technology, Banaras Hindu University, Varanasi-India He is a recipient of UGC (SRF and JRF) fellowship. His research is focused on Information Security, Steganography, Cryptography, Digital Signal and Image Processing.



S. P. Singh is presently working as a professor in the department of Electronics Engineering in Institute of Technology, Banaras Hindu University, Varanasi-India. He received B.Sc. in science, B.Tech., M.Tech. and Ph.D. in Electronics Engineering from IT-BHU. He has authored or coauthored over 70 research papers in international/national journals/conference proceedings. His areas of current research include bio-electromagnetic, microwave antennas, image processing and network security.

Anand Mohan is presently working as a professor in the department of Electronics Engineering in Institute of Technology, Banaras Hindu University, Varanasi-India. He has 26 years of teaching and 3 years of Industry experience in reputed firm. He completed his B.Sc. (Engg.), M.Tech and Ph.D. in Electronics Engineering from IT-BHU. He has more than 60 research publications in international and national journals and conferences proceedings. He is the chairman of Armament Sensor and Electronics (ASE) panel, Defence Research and Development Organisation (DRDO), India. His research areas include Digital Hardware, Microprocessor Engg. & Instrumentation, information and network security, image processing, steganography and cryptography.