Moderate Bit Insertion for Hiding Crypto-Data in Digital Image for Steganography

Balkrishan
Assistant Professor, Yadavindra College of
Engineering, Punjabi University, Guru Kashi Campus,
Talwandi Sabo, District, Bathinda (Punjab) India.

Amar Partap Singh
Professor, Sant Longowal Institute of
Engineering and Technology (Deemed-to-be-
University), Longowal-148106,
District: Sangrur (Punjab) India.

ABSTRACT

The simplest method based on least-significant-bit (LSB) substitution embeds important data in the least significant bits of the cover image. The LSB method introduces a small distortion in the cover image. Many data hiding techniques are focused usually to reduce the distortion in the cover image when sensitive data is embedded into the same. However, post processing of stego-image or its transmission may cause serious errors in the information being carried by stego-image. The receiver cannot extract the correct information from the stego-image having any such type of distortion. To overcome these problems, a new method is proposed for crypto data hiding within grey scale image in the spatial domain so that the interceptor will not notice about the existence of the important data. The basic concept of the proposed method is to embed the important crypto data in the 4th moderately-significant-bit of pixel of an image. The first 3 LSB bits of image pixel are used for local pixel adjustment to reduce the effect of degradation in the cover image. Experiments are performed on four different images of same size and the results show that the visual quality of the stego image is acceptable. This method provides a higher security as well as robustness to the attacks including compression, cropping, etc. as compared to LSB substitution method.

General Terms Crypto-data Security

Keywords: Steganography, Moderate-Significant-Bit, Data-Hiding, Crypto-data

1. INTRODUCTION

The popularity of the internet and advancement of computer hardware offers a better communication between sender and receiver for transmission of large amount of data via network. However, it also increases the risk of illegal access and unauthorized tampering with contents of information while transmitting the secret data. To safely transmit the important data through the Internet networks, some mechanisms must be provided to guard important data against illegal interception [1]. In order to keep the attackers away, a variety of techniques have been proposed. One of the most famous methods is data encryption [2, 3], which uses a certain algorithm to transform data into cipher texts. Only the user that has keys can decrypt the secret data from the cipher texts. For any grabber who does not have a key, the cipher texts will look like nothing but streams of meaningless codes. Although data encryption is a good way to prevent attackers and hackers from accessing secret data, it still has some weaknesses [4]. The goal is to make the embedded data invisible to the attackers and hackers under the cover image, i.e., to make the stego image, after processing, as similar as possible to the original cover image [5]. Steganography is an art and science of data hiding and invisible communication. A very simple and efficient method based on Least-significant-bit (LSB) substitution is to hide the important data bit in the pixel of the host image. Though embedding data in LSB position introduces small distortion to the host image yet embedded data is more easily lost when the stego image is used for various purposes at a later stage [6]. Many articles [7, 8] have addressed approaches related to LSB substitution. For storing the stego image into memory and save the memory space and increase the transmission rate, some software discards the LSB i.e image become 7 bits per pixel instead of 8 bits. Storing data in the LSB is, therefore, less safe. In this paper, steganography is combined with cryptography to provide additional layer of security for the important data. Here, we describe the method in which crypto-data is embedded at moderate-significant-bit (4th LSB) position of the host image, an approach seldom seen in the literature [5]. In this method, if any pixel value gets changed on account of embedding crypto-data bit, adjustment at lower bit positions ensures minimum change in pixel value. Thus, the existence of important information in the cover image is difficult to detect.

2. PROPOSED METHOD

The post processing (compression, cropping etc.) of stego image obtained using least significant-bit of cover image may result in loss of embedded secret data. To provide additional layer of security, secret data is enciphered using flexible matrix [9]. A method is proposed here to embed important secret data in the moderate significant bit position of the cover image. One bit of cipher message inserted in the 4th LSB of pixel of cover image. To lower the degradation of image quality, we add post pixel adjustment to increase the visual quality of stego image. Let Z (i, j) be the pixel of cover image. If secret data bit equal to the 4th LSB, then no pixel adjustment is required. If secret data bit is not equal to the 4th LSB, then modify the pixel by complementing Z (i, 1 to 3). The advantages of the proposed method are (a) Attacks on stego-image are very less. (2) The quality of the cover image does not get affected appreciably. The experimental results are given to reveal the advantages of the proposed method. The procedure used for post pixel adjustment of selected pixel is summarized below:

(a) If the embedded crypto-data bit equal to the 4th LSB of pixel of cover image then no pixel adjustment is required and go to next pixel.

(b) If the embedded crypto-data bit is one as well as not equal to the 4th LSB of pixel of cover image, then modify the pixel by Z(i, 1 to 3) = 0.

(c) If the embedded crypto-data bit is zero as well as not equal to the 4th LSB of pixel of cover image, then modify the pixel by Z (i, 1 to 3) = 1.

2.1 Proposed Algorithm

Message Ciphering & Embedding Module

Step-1: Commencing with first character, read secret message character-wise from saved text file.

Step-2: Encrypt each character into eight crypto-bits using Flexible Matrix **[9].**

Step-3: Repeat step 2 for all characters of the saved text file to obtain a series of crypto-bits.

Step-4: Read each pixel of the cover image commencing with first pixel Z(i, j) where i=1 : 256 and j= 1: 256.

Step-5: Convert each pixel into equivalent eight-bit binary number.

Step-6: Embed one cipher-bit of message into the 4th LSB of pixel of cover image.

Step-7: Repeat step 5 to 6 until all the cipher message bits are embedded into the cover image.

Post Pixel Adjustment

(a) If the encrypted embedded data bit equal to the 4th LSB of pixel of cover image then no pixel adjustment is required and go to next pixel.

(b) If the encrypted embedded data bit is one, not equal to the 4th LSB of pixel of cover image then modify the pixel by Z(i, 1 to 3) = 0.

(c) If the encrypted embedded data bit is zero, not equal to the 4th LSB of pixel of cover image then modify the pixel by Z (i, 1 to 3) = 1.

Message Extraction & Decryption Module

Step-1: Read pixel of the stego-image starting from first pixel.

Step-2: Convert each pixel value into equivalent binary number.

Step-3: Extract crypto-bit from 4th LSB of pixel of cover image commencing with first pixel Z(i, j) where i=1 : 256 and j= 1: 256.

Step-4: Go to next pixel and repeat steps from 2 to 3.

Step-5: Repeat steps 2 to 4 until all the crypto-bits of the secret message are extracted.

Step-6: Decrypt every 8 crypto-bits into character using Flexible Matrix.

Step-7: Repeat step-6 for all the remaining crypto-bits to obtain characters.

Step-8: Save all characters in the form of text file.

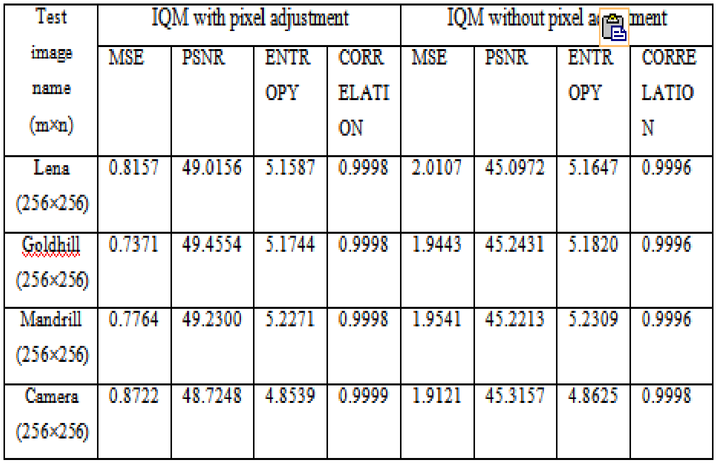
3. RESULTS AND DISCUSSION

Experimental results of the proposed method are presented and discussed in this section. The program was written in MATLAB 7, and executed on a personal computer (PC). Figure 1 shows cover and stego-images with and without pixel adjustment used in Table-1. The images tested in our experiment are all 8-bit images with 256 gray levels shown in Figure 1(a). Simulation results are performed by embedding the cipher message information 500 bytes, inside the different cover images. In the proposed method, the first step to encipher the important data using flexible matrix [9] and encrypted data embedded at 4th LSB position in the given pixel of cover image. Similarly, the results are obtained with and without pixel adjustment using same method shown in Figure 1(b) & (c). In order to evaluate the proposed method for enciphering the information using flexible matrix [9], the effects of distortions are evaluated using Image Quality Measures (IQM) [10]. The effectiveness of the proposed method is evaluated by applying it to four different types of standard test-bench images of the same size (Lena, Mandril, Goldhil and Cameraman) for achieving insertion of 500 bytes of message using 4th LSB position in the pixel of the cover image. Table-1 shows the values of MSE, PSNR, Entropy and Correlation for insertion of 500 bytes of crypto-data at 4th LSB position in the pixel of cover image with and without pixel adjustment. We can compress the stego image upto 30% without loss of embedded data. In the proposed method, visual quality of the cover image does not get affected appreciably after embedding crypto-data into moderate significant bit of the pixel in the cover image.

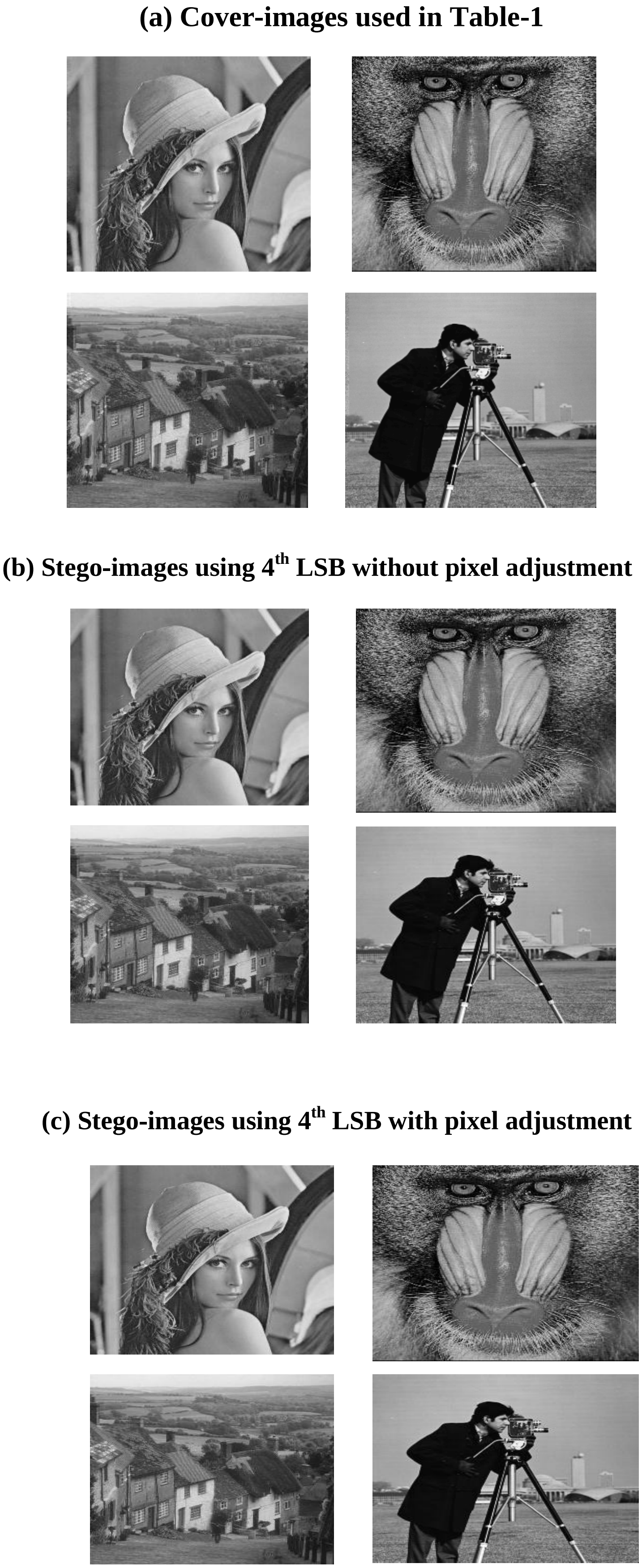
4. CONCLUSION

The major goal of data hiding is to embed skillfully important data in the cover image so that the interceptors will not notice the existence of the data. It is not like the goal of data encryption, which restricts the regular access to the embedded data, and also dissimilar to the goal of watermarking, which stresses on the survival of the embedded data after image operation. In this paper, we propose a new type of crypto-data hiding method with some distortion tolerance in moderate significant bit. Moderate significant bit replacement is seldom used in data hiding, since there will be degradation of image quality. However, the proposed method embeds crypto-data efficiently at the position of moderate significant bit of the cover image with and without local pixel adjustment. Post pixel adjustment lowers the degradation of stego-image that looks similar to the original host image. The data hiding and extraction processes are simple. For data extraction, the original cover image is not required. Furthermore, no other extra information is needed for data extraction process. Experimental results indicate that the proposed method produces good quality stego-images.

Table-1 Results obtained with proposed algorithm for embedding 500 bytes of crypto data at 4^{th} LSB position of the cover image



Test image name (m×n)	IQM with pixel adjustment				IQM without pixel a[illegible]ment			
	MSE	PSNR	ENTROPY	CORRELATION	MSE	PSNR	ENTROPY	CORRELATION
Lena (256×256)	0.8157	49.0156	5.1587	0.9998	2.0107	45.0972	5.1647	0.9996
Goldhill (256×256)	0.7371	49.4554	5.1744	0.9998	1.9443	45.2431	5.1820	0.9996
Mandrill (256×256)	0.7764	49.2300	5.2271	0.9998	1.9541	45.2213	5.2309	0.9996
Camera (256×256)	0.8722	48.7248	4.8539	0.9999	1.9121	45.3157	4.8625	0.9998



(a) Cover-images used in Table-1

(b) Stego-images using 4th LSB without pixel adjustment

(c) Stego-images using 4th LSB with pixel adjustment

Fig.1 Cover and Stego images with and without pixel adjustment used in Table-1

5. REFERENCES

[1] R. Z. Wang, C. F. Lin, and J. C. Lin, “Image hiding by optimal LSB substitution and genetic algorithm,” Pattern Recognition, vol. 34, no. 3, pp. 671–683, 2001.

[2] Y.H. Chu, S. Chang, “Dynamical cryptography based on synchronized chaotic systems,” Electronic Letters, vol. 35 (12), pp. 974–975, 1999.

[3] H. J. Highland, “Data encryption: a non-mathematical approach,” Computer Security 16, pp. 369–386, 1997.

[4] C. C. Chang, J. Y. Hsiao, and C. S. Chan, “Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy,” Pattern Recognition, vol. 36, no. 7, pp. 1583–1595, 2003.

[5] R. Z. Wang, C. F. Lin, and J. C. Lin, “Hiding data in images by optimal moderately-significant-bit replacement,” Electronics Letters, vol. 36, no.25, pp. 2069-2070, 2000.

[6] Balkrishan and Amar Partap Singh, “Secure Data Communication using Moderate Bit Substitution for Data Hiding with Three Layer Security,” IE(I) Journal-ET, vol. 91, pp. 45-50,july 2010.

[7] F. A. P. Petitcolas, R. J. Anderson and M.G. Kuhn, “Information Hiding–A Survey,” Proceedings of IEEE, vol. 87, pp. 1062-1078, July 1999.

[8] D. W. Bender, N.M. Gruhl, A. Lu, Techniques for data hiding, IBM Systems J. 35,pp. 313–336, 1996.

[9] Balkrishan and Amar Partap Singh, “Hiding Encrypted Data using Randomly Chosen Moderate Bit Insertion in Digital Image Steganography,” Journal of Computer Science and Engineering, vol. 1, issue 2, pp. 21-27, June 2010.

[10] Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing,” Pearson Education, 2003.