IMPROVED LSB BASED IMAGE STEGANOGRAPHY USING RUN LENGTH ENCODING AND RANDOM INSERTION TECHNIQUE FOR COLOR IMAGES

G. G. Rajput and Ramesh Chavan*

Department of Computer Science,
Rani Channamma University, Belagavi, KA, India 591156

ABSTRACT

Image Steganography is a technique for securing the secret message using a cover image in such a manner that the alterations made to the image are perceptually indiscernible. In this paper a novel method for secret message hiding in color images is proposed. The message is encoded by extracting the RGB components of a color image. Run length encoding is performed on the data and insertion of the data in least significiant bits(LSB) of the pixel is guided by linear congruential generator (LCG). A 3R-3G-2B LSB pattern is recommended for insertion of the data making the information more secure without bringing any significant distortions to the original image. The experiments performed on various color images demonstrate the efficacy of the proposed algorithm in terms of PSNR of cover image and that of stego-image.

KEYWORDS

cover, secret message, LSB, LCG, RLE, stego-image.

1. INTRODUCTION

Image Steganography allows for two parties (sender and intended receiver) to communicate secretly and covertly. The general principle underlying the image steganographic method is to embed the secret message in the image without bringing change in the characteristics of the image. Assuming that, an attacker has unlimited computation power and is able and willing to perform a variety of attacks, it should not be possible for the attacker to decode the message (Visual Attacks, Enhanced LSB Attacks, Chi-Square Analysis, and other statistical analyses). The embedding method should be such that, the stego-image(information coded image) should not reveal the existence of secret image/message. One of the approaches to code the secret message in an image is to place the secret message in the noise component of a signal. If it is possible to code the information in such a way that it is indistinguishable from true random noise, an attacker has no chance in detecting the secret communication. However, such an approach is not suitable for noise-free images. The simplest way of hiding information in an image is to replace the least significant bit (LSB) of every element(pixel) with one bit of the secret message. Since flipping the LSB of a byte (or a word) only means the addition or subtraction of a small quantity, the

Natarajan Meghanathan et al. (Eds) : SAI, ICAITA, CSITA, ISPR, Signal - 2018
pp. 75–82, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81007

sender assumes that the difference will lie within the noise range and that it will therefore not be generally noticed. However, the approach is not secure since an attacker can extract the LSBs and simply "decode" the cover, just as if he were the receiver. Instead, an approach of inserting the information bits in LSBs of randomly selected elements will make the information more secure. However, the intended receiver should be aware of the procedure of random selection to retrieve the secret message. The key to this may be sent by the sender through secret channel (eg. personal email) to the intended receiver. On the other side, the key may be embedded in the one of the elements of the image and the information regarding the same may be sent to intended receiver through secret channel. In this paper, we propose to use this approach for hiding the secret message in LSBs of the color image. To make the system more secure, first we perform run length encoding on the secret message, secondly, perform angular rotation of the color image and then use a pre-defined pattern for message insertion in elements of the RGB components of the color image. After the insertion of message, lastly, we perform reverse angular rotation on the imageto obtain a stego-image (image with a secret message).

2. LITERATURE SURVEY

Many techniques have been proposed in the literature for hiding messages in images such that the alterations made are indiscernible in the generated stego-image. The spatial domain techniques manipulate directly the pixel bit values to embed the secret message (eg. LSB, pixel-value differencing). The secret bits are written directly to the cover image pixel bytes making it easy to implement. Consequently, the spatial domain techniques are simple and easy to implement. The transform domain techniques involve image transformation such as cosine transformation, Fourier transform and wavelet transformation. However, there are techniques that share the characteristic of both of the spatial domain and transform domain (eg. pattern block encoding, spread spectrum methods and masking). The fact that, the resulting images should be statistically indistinguishable from untampered images has been studied in the form of PSNR values.

A review on image stegnographic techniques is presented in [4,5].

Aura [6] has introduced a flexible scheme applicable to random access covers, especially to digital images. He developed a secret key steganography system based on pseudorandom permutations. Due to the construction of the scheme, the secret information is distributed over the whole cover in a rather random manner.

A protocol which allows public key steganography has been proposed by Anderson in [7, 8]; it relies on the fact that encrypted information is random enough to "hide in plain sight". If the stego-message is not targeted towards a specific person, but for example is posted in an Internet newsgroup, the problem worsens. Although the protocol also works in this case (only the intended receiver can decrypt the secret message, since only he has the correct private key) all possible receivers have to try to decode every posted object.

Ajit Danti et.al [9] have proposed a 2-3-3 LSB insertion method, where in eight bits of secret data is inserted in LSB of RGB (Red, Green and Blue) pixel values of the cover image in 2,3,3 order, respectively, to embed a color secret image into a cover image.

Chin□Feng Lee et.al [11] scheme performs the logical Exclusive□OR (XOR) operation to smoothen the secret bit stream and to embed the result into a cover medium. Additionally, the

proposed scheme employs generalized difference expansion transform for image recovery after data extraction; consequently, the image fidelity can be preserved.

The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography. Many of the proposed algorithms in the literature are based on LSB insertion methods because of the fact that an altered image with slight variations in its colors, in LSB positions of the color pixels, will be indistinguishable from the original by a human being, just by looking at it. However, a simple LSB implementation is vulnerable to attacks [13]. Hence, extended implementation of LSB method are proposed in the literature [14,15,16].In RGB based steganography, the R, G, and B components(channels) are treated as independent bytes and LSB substitution is applied.

Parvez and Gutub [17] proposed RGNB based technique. The idea in that, for insignificant colors, significantly more bits can be changed per channel. For example, suppose in a pixel with R=55, G=255 and B=255, a change in the R channel will not show a significant distortion. The lower color value of a channel has less effect on the overall color of the pixel than the higher value. Therefore, more bits can be changed in a channel having 'low' value than a channel with a 'high' value. However, the choice of pixels is straight forward and the capacity is unpredictable. In the technique proposed by Gutub et al. [18], the RGB image is used as cover media and the cipher text is hidden inside the image using a pseudorandom number generator (PRNG) thereby including more randomization in selection of pixels. The PRNG produces two new random numbers per iteration, say seed1 and seed2. The seed1 random number is used to determine the RGB component where cipher text will be hidden and seed2 determines the number of bits that can be hidden in it. However, the capacity is unpredictable due to the choice of seed2 value. Kaur et al. [19] proposed a RGB intensity based algorithm in which variable number of bits are hidden in different channels. The LSBs of one of the three channels is used as indicator and data is stored in other two channels. The advantage in this technique is usage of 4 LSBs in some of the data channels, which increases the hiding capacity. Both security and capacity is enhanced.

In this paper, we propose an RGB based LSB insertion in a way that the text message is secured and not vulnerable to attacks. The variation of LSB method is proposed using run length encoding scheme and random selection of pixels. A specific fixed pattern is defined for choice of number of LSBs in each of R, G, and B channels. Moreover, the insertion of secret message is done by performing angular rotation of the cover image and reversing back to its original position after insertion making the scheme more secure.

3. PROPOSED METHOD

Digital images are recorded as a matrix or array of small picture elements, or pixels. Each pixel is represented by a numerical value. In general, the pixel value is related to the brightness or color. In case of color digital images, the commonly used color space is RGB. In RGB cube model, a pixel in a color image possesses three components; Red (R), Green (G), and Blue (B). Each component comprises of 8 bits. These R, G, and B components (channels) can be treated as independent bytes and LSB substitution can be applied. In simplest LSB substitution, it means 3 data bits can be hidden in one pixel. However, it is not wise to implement in this form, since such approach is vulnerable to attacks for secret message retrieval. The method proposed in this paper is described below.

Hiding the Secret Message (Data Hiding):

The cover image is a color image with 24 bits per pixel described in RGB color space. The secret text message is binarized and stored as stream of bits. Run length encoding is performed on the stream of bits [12].Angular transformation is performed on the cover image and the three channels, R, G, and B, respectively, of the cover image are extracted and Run Length Encoded data is inserted in the LSBs of the pixels of the channels in the following pattern: 3 LSBs of R channel, 3 LSBs of Green channel and 2 LSBs of Blue channel- a total of 8 bits are used per color pixel. However, the choice of pixel is based on linear congruential generator (LCG). Given a seed, LCG generates a sequence of pseudo random numbers which are taken as pixel positions in the channels and the sequence is followed to insert the secret data in LSBs positions in pattern specified. The number of pixels used for inserting the data is recorded in the last pixel of the cover image. After the insertion, reverse angular transformation is performed to generate the final stego-image. The algorithm for generating stego-image is presented below. The seed value (stego-key) used for LCG method is sent to the intended receiver through a secure medium.

Step 1. Read the cover medium i.e. color image.

Step 2. Read the secret message(text), perform runlength encoding and then binarize.

Step 3. Compare size of binarized secret data against size of cover image to ensure that the cover image is not distorted after embedding. For example, for true image 24bit of size 20x20 pixels, (8 bits/ pixel) 3200bits of binarised data can be embedded using LSB technique.

Step 4. A sequence of random positions is generated using LCG method with a choice of seed value. These positions represent the pixel positions in the channels of color image.

Step 5. Starting from the first random position of pixel, insertion of data is performed in 3R-3G-2B pattern

Step 6. The number of pixels used for inserting the is written in LSB of the last pixel of the image.

Step 7. Reverse angular transformation is performed to retain original position of the cover.

Step 8. Output the stego image

Secret Message Retrieval

The process of retrieving the secret message from stego-image is presented below.

Step 1. Read the stego image.

Step 2. Using stegokey (seed value),generate the sequence of random numbers representing the position of the pixels used for inserting text in RGB channels. Following the pixel positions, read the data bits in 3-3-2 pattern and store it in the array. The number of pixels to read is known from the data embedded in last pixel of the stego- image.

Step 3. Perform run-length decoding on the extracted bits.

Step 4. Output the secret message.

4. EXPERIMENTAL RESULTS

Windows wallpapers are used to implement the proposed method. The wallpaper images have resolution of 1920x 1200 pixels, 24-bit true color. The quality of the stego-image is measured in terms of parameters, namely, Mean-Squared Error (MSE) and Peak Signal-to-Noise Ratio(PSNR) [20].

The mean-squared error (MSE) between two images g(x,y) (cover image) and $\hat{\mathbf{g}}(x,y)$(stego-image), is defined as

$$E_{MSE} = \frac{1}{MN}\sum_{n=1}^{M}\sum_{m=1}^{N}[\ \hat{g}(x,y) - \ g(x,y)]^2 \text{----------(1)}$$

where mean-squared error depends strongly on the image intensity scaling, PSNR scales MSE according to image range and is given by

$$PSNR = -10\ \log_{10}\frac{e_{MSE}}{S^2} \text{----------(2)}$$

where S is the maximum pixel value.

The Structural Similarity Index (SSIM) quality assessment index is based on the computation of three terms, namely the luminance term, the contrast term and the structural term. The overall index is a multiplicative combination of the three terms.

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma} \text{----------(3)}$$

Where,

$$l(x,y) = \frac{2\mu_x\mu_y+C_2}{\mu_x^2+\mu_y^2+C_1} \text{---------- (4)}$$

$$c(x,y) = \frac{2\sigma_x\sigma_y+C_2}{\sigma_x^2+\sigma_y^2+C_2} \text{---------- (5)}$$

$$s(x,y) = \frac{\sigma_{xy}+C_3}{\sigma_x\sigma_y+C_3} \text{---------- (6)}$$

Where μx, μy, σx,σy, and σxy are the local means, standard deviations, and cross-covariance for images *x, y*. If α = β = γ = 1 (the default for Exponents), and C3 = C2/2 (default selection of C3) the index simplifies to:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \text{----------(7)}$$

The stego-image obtained for sample images are shown Figure 1. The corresponding MSE, PSNR values and SSIM values are tabulated in Table 1. A subjective test was also performed by asking the selected viewers to compare the images before and after information hiding.

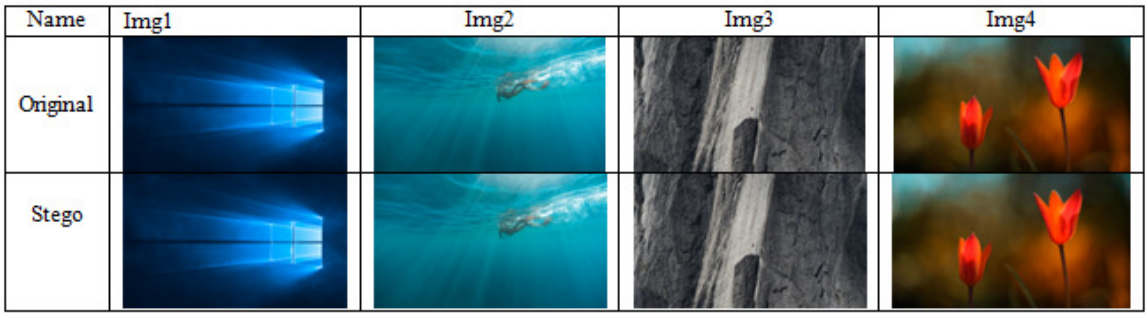

Figure 1. Original image & Stego-Image

Table 2:MSE, PSNR & SSIM of image

	MSE			PSNR			SSIM Value
Image	**R**	**B**	**G**	**R**	**B**	**G**	
Img1	0.00	0.00	0.00	78.9340	76.8051	79.6121	1.0000
Img2	0.00	0.00	0.00	81.4715	76.8606	79.5288	1.0000
Img3	0.0	0.00	0.00	78.5079	76.5043	79.1556	1.0000
Img4	0.00	0.00	0.00	78.8163	76.9480	80.0724	1.0000

5. CONCLUSION

An efficient method based on RGB steganography is presented in this paper. The secret message is embedded in the RGB channels of the cover image in a specific pattern i.e. 3-3-2. The positions of the pixels are chosen at random using LCG. The security of the data is ensured by first performing run-length encoding on the secret message and this run length encoded bits are inserted in the cover image by performing angular rotation of the image. Reverse angular rotation is performed to generate stego-image. The specific pattern 3-3-2, the seed value used in generating random pixel positions and angular rotation forms the stego-key which is send to the intended receiver using a secure medium. The performance of the proposed method is noted in terms of PSNR and it is observed that the alterations made are indiscernible in the generated stego-image. Our proposed algorithm is targeted to achieve increased text embedding capacity into the cover image followed by ensuring high security of the secret message.

REFERENCES

[1] Foley, J., et al., Computer Graphics, Principles and Practice, Reading, MA: Addison Wesley, 1990

[2] N.F. Johnson, S.C. Katzenbeisser, "A survey of steganographic techniques", in: S. Katzenbeisser, F.A.P. Petitcolas (Eds.), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Inc., Norwood, 2000.

[3] N.F. Johnson, S. Jajodia, "Exploring steganography: seeing the unseen", IEEE Computer 31 (2) (1998) 26–34.

[4] A. Cheddad, J. Condell, K. Curran, and P.M. Kevitt, "Digital image steganography: survey and analysis of current methods", Signal Processing, vol. 90, pp.727-752, 2010.

[5] Gandharba Swain, Saroj Kumar Lenka, Classification of Image Steganography Techniques in Spatial Domain: A Study, International Journal of Computer Science & Engineering Technology (IJCSET),5(3), pp 219-233, 2014

[6] Aura, T., "Practical Invisibility in Digital Communication," in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, 1996, pp. 265–278

[7] Anderson, R. J., "Stretching the Limits of Steganography," in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, 1996, pp. 39–48.

[8] Anderson, R. J., and F. A. P. Petitcolas, "On The Limits of Steganography," IEEE Journal of Selected Areas in Communications, vol. 16, no. 4, 1998, pp. 474–481

[9] G.R. Manjula, Ajit Danti," A Novel Based Least Significant Bit (2-3-3) Image Steganography in Spatial Domain", Intenational journal of security, privacy and Trust Management(IJSPTM) Vol.4 No 1 february 2015.

[10] R.Z. Wang, C.F. Lin, J.C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recognition 34 (3) (2001) 671–683.

[11] Chin-Feng Lee, Chi-Yao Weng, Aneesh Sharma, "Steganographic access control in data hiding using run-length encoding and modulo-operations" SECURITY AND COMMUNICATION NETWORKS ; 9:139 –148 Published online 16 June 2011 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.333.

[12] Rafael C. Gonzalez, Richard E. Woods, "Run-Length Encoding"," Digital Image Processing", 3rd edition, Chapter 8, section 8.2.5, pp.553-559, 2011.

[13] C. K. Chan, and L. M. Chang, "Hiding data in images by simple LSB substitution", Pattern Recognition, vol.37, pp.469-474, 2004.

[14] M. A. B. Younes, and A. Jantan, "A new steganography approach for image encryption exchange by using least significant bit insertion", International Journal of Computer Science and Network Security, vol.8, no.6, pp.247-254, 2008.

[15] H. B. Kekre, A. A. Athawale, and P. N. Halarnkar, "Increased capacity of information hiding in LSB's method for text in image", International Journal of Electrical, Computer and System Engineering, vol.2, no.4, pp.246-249, 2008.

[16] G. Swain, and S. K. Lenka, "LSB array based image steganography technique by exploring the four least significant bits", CCIS, Vol. 270, part II, 2012, pp.479-488.

[17] M. T. Parvez, and A. A. Gutub, "RGB intensity based variable-bits imagesteganography", in Proceedings of IEEE Asia-pacific Services Computing Conference, 2008, pp.1322-1327.

[18] A. Gutub, A. Al-Qahtani, and A. Tabakh, "Triple-A secure RGB image steganography based on randomization", in Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, 2009, pp.400-403.

[19] M. Kaur, S. Gupta, P. S. Sandhu, and J. Kaur,"A dynamic RGB intensity based steganography scheme", World Academy of Science, Engineering and Technology, vol.67, pp.833-836, 2010.

[20] Krenn,R.,"Steganograph and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf.

[21] MSE &PSNR, http://in.mathworks.com/help/vision/ref/psnr.html.

[22] SSIM, http://in.mathworks.com/help/images/ref/ssim.html.

[23] G. G Rajput, Ramesh Chavan, "A Novel Approach for Image Steganography Based on LSB Technique", International Conference on Compute and Data Analysis Proceedings ICCDA '17, May 19-23, 2017, Lakeland, FL, USA © 2017 Association for Computing Machinery, ACM ISBN 978-1-4503-5241-3/17/05.

[24] G. G Rajput, Ramesh Chavan "A Novel Approach for Image Steganography Based on Random LSB Insertion in Color Images", Proceedings of the International Conference on Intelligent Computing Systems (ICICS 2017 – Dec 15th – 16th 2017), India, Elsevier's SSRN eLibrary – Journal of Information Systems & eBusiness Network – ISSN: 1556-5068.