Merge and Split approach incolor image Steganography using Run Length Encoding and LSB Techniques

G. G. Rajput[1], Ramesh Chavan*[2]

1 Department of Computer Science, Karnataka State Akkamahadevi Women's University,
Vijayapura, KA, India.
2 Department of Computer Science, Rani Channamma University, Belagavi, KA, India.

D.O.I-10.51201/12471
https://doi.org/10.51201/12471

Abstract: *The purpose of steganography is to communicate secret messages between the sender and intended recipient in such a way that no one suspects the very existence of the message. The techniques aim to protect the secret information from third parties by embedding them into other information such as text, audio signals, images, and video frames. In this paper we propose a novel approach of hiding secret messages in multiple images (a cover image)using run length encoding and LSB techniques and communicate the message to intended person over the communication channel by transmitting individual images.Experiments are performed on a set of color images and performance of the proposed system is presented.*

Keywords: message, LSB, LCG, stego-image, RGB, RLE, multiple images

Introduction:

In today's growing digital world, Steganography and Cryptography are popular means of protecting the information over communication channel [1]. However, compared to cryptography, in stegnograhy approach the very existence of the secret message is not known to third party[2,3].Today, image steganography can be used in a large amount of data formats such as .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. In image steganography, an image acts as cover object and is used to hide the message, a host object which is to be transmitted. A steganography algorithm is used to carry out the required process of hiding message in cover object resulting in a stego-image. Image steganography technique should have following characteristics [6]:

- Allow for maximum data to be stored inside cover image
- Imperceptibility i.e. the visual quality of stego-image should not reveal the presence of secret information, and
- Robustness – attacker should not be able to discover the message.

Among several approaches of image steganography, the Least-Significant-Bit(LSB) steganographic data embedding isfound to be simple to understand, easy to implement, and it produces stego-image that is same as that of cover image. The result is that its visual infidelity cannot be judged by naked eyes. Steganography methods based on LSB with subtle variations is found in the literature [2,3,4,5].

A secure steganographicapproach has four requirements:

i. Secret text embedded in the image shall be retrieved through a secure key known between sender and intended receiver.

ii. The method adopted shall not reveal the very existence of secret information in the stego-image.
iii. In case, the presence of message is known, it should be impossible for the third party to organize the secret text for information retrieval.
iv. It should be computationally infeasible to detect hidden messages.

The locations in the image to embed the secret message are computed using random number generator techniques. One of the most successful random number generators is the linear congruential Generator (LCG). The method requires four 'magic' numbers.

$X_0 \geq 0$, the seedvalue; a multiplier $a \geq 0$, an increment; $c \geq 0$ and lastly, the modulus; with
$m > X0$, $m > a$, $m > c$.

The desired sequence of random numbers $<X_n>$ is then obtained by using the formula

$$X_{n+1} = (aX_n + c) \bmod m \text{ --(1)}$$

where $0 \leq X_n \leq (m-1)$ and $n \geq 0$. The sequence so generated is called a linear congruential sequence.
In our previouswork[13], secret message hiding in color images has been proposed by encoding the message in the RGB components of the color image. Run length encoding is done on the data and data is inserted in the least significant bits(LSB) of each pixel, the choice of the pixel being guided by linear congruential generator (LCG). A 3R-3G-2B LSB pattern is used for insertion of the data for security without bringing any significant distortions to the original image. In this paper, we aim to improve upon the technique by considering multiple color images for secret message hiding so that it becomes impossible, statistically, for third person to extract the complete message embedded in multiple images.

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[1]. A brief overview of the image steganography methods is presented below.

Parvez and Gutub [9] have proposed RGB color image steganography wherein higher number of bits of secret text is stored in lower color component of the color image. In other words, R channel has low intensity value compared to other channels, the change made in channel R does not affect the quality of cover image and that thestego-image will not show a significant distortion. The low intensity of a channel has less effect on the overall color of the pixel than the higher valuesof other channels. Accordingly they altered more bits of the channel having 'low' value than a channel with a 'high' value. However, the choice of pixels is detectable and that the capacity is unpredictable. In the technique proposed by Gutub et al. [10], the cipher text is hidden inside an RGB image using a pseudorandom number generator (PRNG) thereby allowingrandomness in selection of pixels. Using two seed values tworandom numbers were generated with first random number being used to determine the RGB component where cipher text will be hidden and second random number determines the number of bits that can be hidden in it. Again here, the capacity is unpredictable due to the choice of second random number value. In the method proposed by Kaur et al. [11] variable number of bits are hidden in RGB channels of an image. The LSBs of one channel is used as key and data is stored in remaining two channels. The usage of 4 LSBs in some of the data channelsincreases the hiding capacity. Both security and capacity is enhanced and proposed method is enhancement of limitation of earlier method proposed by them[12, 13, 14]. However, amount of data embedded in a single image is limited. More data can be embedded in multiple images. In this paper we present a method of embedding data in an image which is a merged version of several images. The merged image forms a cover image wherein data is hidden. After embedding data, the resulting stego is split into multiple images and sent to the intended receiver over communication channel. The details of the proposed method are presented below.

Methodology:

In in this paper we present a method for embedding text in multiple images by merging the images to form a single cover-image.A 3-3-2 color component pattern approach is followed to embed the secret image as described in our earlier work [12, 13, 14]. The positions of the pixels are chosen at random using LCG. Hiding the data with this approach has more efficient and more capable to hold more data in cover. After the embedding the data in cover image, the cover image is split back into multiple images. On the receiving end, the extraction process requires that all the images arereceived. The received images are merged into a single image and using the key(seed value), the message is extracted. This method has limitation that is if any one of the cover images is not receivedas input on received end, then extraction process is not possible. The limitation also acts as a security for the data hidden in all image, until all the image are not combined the data cannot be retrieved. This method has a larger capacity to hold data and acts an advantage for this method. Thecombinations of two or more images are studied in multiple ways for embedding the data. The algorithmic steps are shown below.

Algorithm : **stego-image generation**
Input : text data and RGB images
Output : set of stego-images

Step 1. Read multiple images and merge into a single image to generate a cover object and perform angular transformation (90).

Step 2. Read the text data. Apply RLE encodingto obtainbinarized secret data. The size of binarizedtext, in bits,should be less than the number of LSBs available in the cover imagecover image generated.

Step 3. Generate sequence of random positions of pixels for bit insertion using LCG method.

Step 4. Following the pixels locations generated by LCG insert the binarized text in the RGB Components, the pattern of insertion to be followed is 3-3-2.

Step 5. The number of pixels used in embedding the text is written in LSB of the last pixel of the cover image. For more security, this number may be encrypted.

Step 6. App1y reverse angular transformation to retain original position of the merged image, resulting in a what we call stego-image.

Step 7. Perform the splitting of image into individual images and rename them sequentially.

Output are the stego images.

Secret Data decoding is done using the following algorithm

Algorithm **: Text retrieval from stego-image**

Input : Set of stego-images in sequence, generated by above algorithm

Output : Text data

Step 1. Read all the stego images in a sequence and the stego-key (seed value of LCG). Merge all input images to form a single image.

Step 2. Using stego-key determine the pixel locations used for embedding data and in that order retrieve the secret message from the three primary components in the pattern 3-3-2. Note that the size of the embedded text, in terms of number of pixels utilized, is written in the last pixel of the stego image.

Step 3. Reconstruct the text message from the extracted bits and apply RLE decoding for the generating the secret message. Output the text data.

Experimental Results

Standard RGB images are used to implement the proposed method [7]. The Structural Similarity Index (SSIM) quality assessment based luminance, contrast, andstructure, is used to validate the proposed method [14]. The overall index is a multiplicative combination of the three terms[11].

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma} \text{----------------(2)}$$

Where,

$$l(x,y) = \frac{2\mu_x\mu_y + C_2}{\mu_x^2 + \mu_y^2 + C_1} \text{-------------------------------- (3)}$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \text{ ------------------------------ (4)}$$

$$s(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \text{---------------------------------- (5)}$$

where μ_x, μ_y, and σ_{xy} are the local means, standard deviations, and cross-covariance for images *x, y*. For $\alpha = \beta = \gamma = 1$ (the default for Exponents), and C3 = C2/2 (default selection of C3) the index simplifies to:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \text{---------------------------(6)}$$

The mean-squared error (MSE) between two images g(x,y) (cover image) and **ĝ**(x,y) (stego-image), is defined as

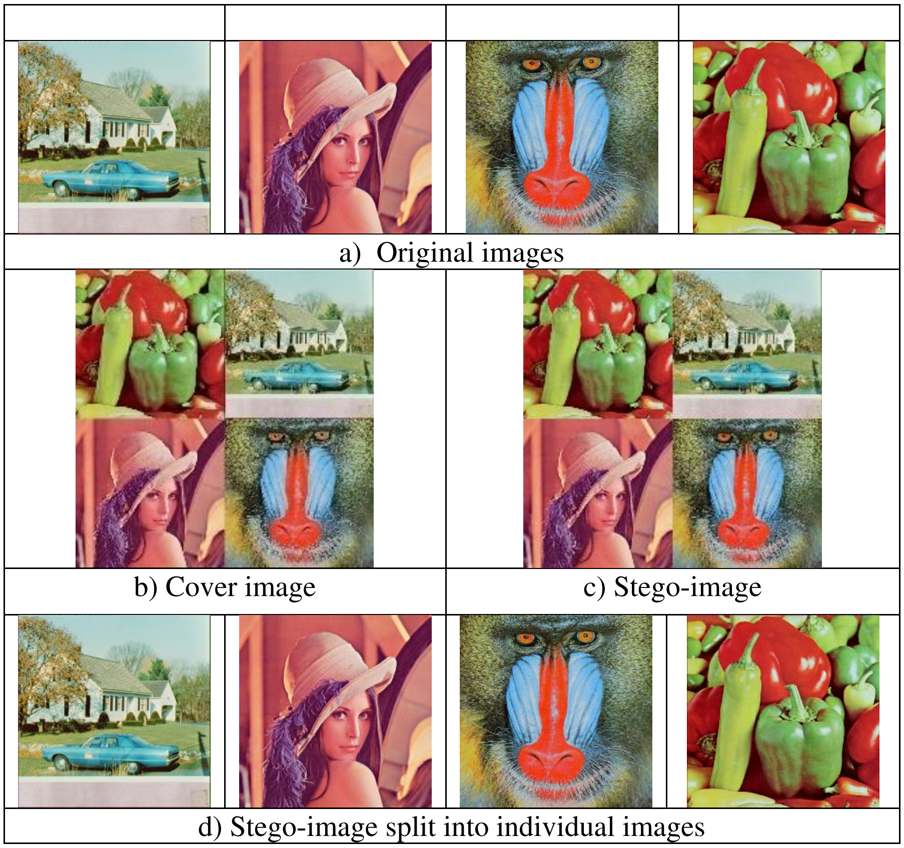
$$E_{MSE} = \frac{1}{MN} \; {}_{n=1}^{M} \sum_{m=1}^{N} [\; \hat{g}(x,y) - \; g(x,y)]^2 \text{-------------------------(7)}$$

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

$$PSNR = -10 \; \log_{10} \frac{e_{MSE}}{S^2} \text{ ------------------------(8)}$$

where S is the maximum pixel value.

Sample stego-images obtained by proposed method are shown Fig. 1. The parameters MSE, PSNR values and SSIM values are tabulated in Table 1. Subjective test was performed with the help of selected viewers to distinguish between cover image and stego-image who did not distinguish with certainly.



a) Original images

b) Cover image

c) Stego-image

d) Stego-image split into individual images

Figure 1. Sample images: cover image and stego-images

	MSE			***PSNR***			***SSIM***
Image	***R***	***B***	***G***	***R***	***B***	***G***	
House	0.03	0.02	0.01	64.0686	64.5999	67.3712	0.9999
Lena	0.03	0.02	0.01	63.9636	64.4165	67.2933	1.0000
Mandril	0.03	0.02	0.01	64.0347	64.4756	67.3451	1.0000
Pepper	0.03	0.02	0.01	64.1266	64.7565	67.4366	1.0000
Merged Image	**0.00**	**0.00**	**0.00**	**75.5468**	**73.5235**	**76.1100**	**1.0000**

Table 1: MSE, PSNR & SSIM values of images

Conclusion:

An efficient color image steganography using RLE and LSBapproachesis presented in this paper. Run-length encoding is performed on the secret message and this run length encoded bits are inserted in the color components of the cover image, obtained by merging multiple images, and then performing angular rotation of the image. The insertion is done in a specific 3-3-2 pattern of the three color components. The image is then rotated back and split into individual images and sequence number is assigned. The specific pattern 3-3-2, the seed value used in generating random pixel positions, angular rotation, and sequence numbers 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] R. Mishra and P. Bhanodiya, "A review on steganography and cryptography," 2015 International Conference on Advances in Computer Engineering and Applications, Ghaziabad, 2015, pp. 119-122.

[2] 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] Chang, Chin-Chen, and Hsien-Wen Tseng. "Data hiding in images by hybrid LSB substitution." Multimedia and Ubiquitous Engineering, 2009. MUE'09. Third International Conference on. [EEE, 2009.

[4] Zayed, Hala H. "A High-Hiding Capacity Technique for Hiding Data in images Based on K-Bit LSB Substitution." The 30th lnternational Conference on Artifical Intelligence. 2005.

[5] Nadeem Akhtar, Pragati Johri, Shabbaaz Khan, "Enbancing the Security and Quality of LSB based Image Steganography", [EEE lnternational Conference on Computational lntelligence and Computer Networks (CICN),27-29 September, 2013, Mathura, lndia

[6] Wang, Ran-Zan, Chi-Fang Lin, and Ja-Chen Lin. "Image hiding by optimal LSB substitution and geneticalgorithm." Pattern recognition 34.3 (2001): 671-683.

[7] Rafael C. Gonzalez, Richard E. Woods, " Digital Image Processing", 3rd edition, 2009.

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

[9] 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.

[10] 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.

[11] Zhou Wang, Alan Conrad Bovik, Hamid Rahim Sheikh, Eero P. Simoncelli , "Image Quality Assessment: From Error Visibility to Structural Similarity", Ieee Transactions On Image Processing, Vol. 13, No. 4, pp.600-612 April 2004.

[12] 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.

[13] 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.
SSRN: https://ssrn.com/abstract=3131654 orhttp://dx.doi.org/10.2139/ssrn.3131654

[14] G. G. Rajput, Ramesh Chavan. "Improved LSB based Image Steganography using Run Length encoding and Random Insertion technique for Colour Images", World Scientific News 112 (2018) 180-192.