Improved Capacity Image Steganography Algorithm using 16-Pixel Differencing with n-bit LSB Substitution for RGB Images

Meenakshi S Arya, Meenu Rani, Charndeep Singh Bedi
Department of Computer Science Engineering, Baba Farid College of Engineering and Technology, Muktsar Road, Bathinda, Punjab, India.

Article Info

Article history:

Received Apr 10, 2016
Revised Oct 15, 2016
Accepted Oct 29, 2016

Keyword:

Pixel differncing
Steganography

ABSTRACT

With the intrusion of internet into the lives of every household and terabytes of data being transmitted over the internet on daily basis, the protection of content being transmitted over the internet has become an extremely serious concern. Various measures and methods are being researched and devised everyday to ensure content protection of digital media. To address this issue of content protection, this paper proposes an RGB image steganography based on sixteen-pixel differencing with n-bit Least Significant Bit (LSB) substitution. The proposed technique provides higher embedding capacity without sacrificing the imperceptibility of the host data. The image is divided into 4×4 non overlapping blocks and in each block the average difference value is calculated. Based on this value the block is classified to fall into one of four levels such as, lower, lower-middle, higher-middle and higher. If block belongs to lower level then 2-bit LSB substitution is used in it. Similarly, for lower-middle, higher-middle and higher level blocks 3, 4, and 5 bit LSB substitution is used. In our proposed method there is no need of pixel value readjustment for minimizing distortion. The experimental results show that stego-images are imperceptible and have huge hiding capacity.

Corresponding Author:

Meenakshi S Arya,
Department of Computer Science Engineering,
Baba Farid College of Engineering and Technology,
Muktsar Road, Bathinda, Punjab-151004, India.
Email: raina.arya@gmail.com

1. INTRODUCTION

In the past few years, the use of internet over the world for data transmission has increased at a phenomenal rate. However this has given rise to new issues such as invisible transmission of data via digital media, copy right protection, and protection of this data from unauthorized attackers etc. Since Internet is a public network, securing the information on internet is very important. Various techniques which have been developed to secure the data include cryptography, watermarking and steganography. In cryptography secret message is converted from one form to another by using encryption key but transmission of confidential information in this way gives clue to an enemy and then encrypted message is decrypted by attackers. Watermarking provides the protection of intellectual property. In watermarking chances of message to be decrypted is more. Out of all these techniques, steganography hide all the clues of secret communication of confidential data. The main goal of steganography is to communicate securely in a completely undetectable manner [1]. Steganography is used in different type of application such as Media database system, Access control system, Confidential communication and secret data storing.

Steganography is a technique for securing information by hiding it in some other medium, such that the existence of information is concealed to everyone except for the intended sender and receiver [2]. Steganography is derived from Greek words ‘stego’ which defines ‘covered part’ and ‘graphia’ which define ‘writing’. Steganography embeds crucial information into cover image without the notice of interceptors. Steganography should be imperceptible and covey as much information as possible. Steganography refers to art and science of hiding secret information in some other media. By hiding the secret message inside an image, there will be the change in statistics, but this change should be very ease of Use less such that the intruder will not suspect it. The important information to be hided is called secret message and the medium in which the information is hided is called the carrier object. The carrier object containing hidden message is called stego object. The algorithm used to embed the confidential information in cover medium at sender side and extracting the hidden message from the stego object at receiver side is called stego system. A block diagram of steganography is illustrated in Figure 1. Types of Steganography [3]

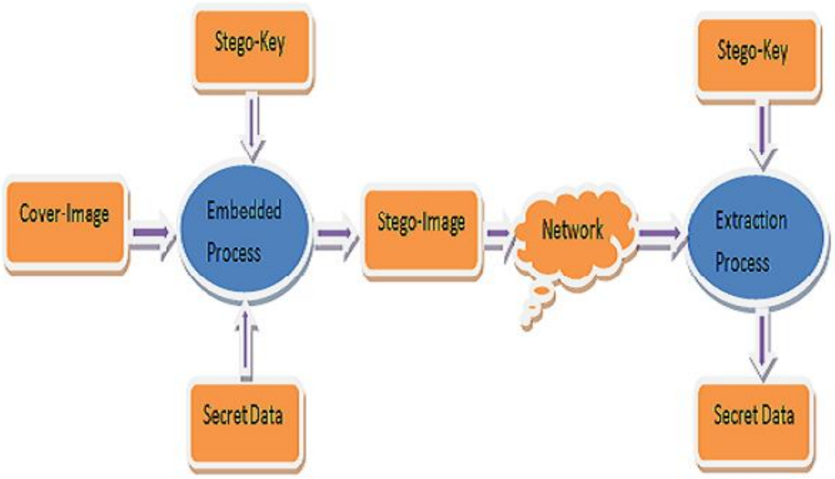


Figure 1. Block Diagram of Steganography

1.1. Linguistic Steganography

The linguistic steganography is one form of steganography in which text is used as cover medium. It can further be classified as Semagrams (Symbols and signs are used for hiding the confidential message) and Open Codes (Hiding the confidential message in a legitimate piece of text in a way that is unclear to average reader

1.2. Technical Steganography

Technical Steganography uses scientific methods to conceal a confidential message, such as the use of invisible ink, microdots etc. It’s further constituents include the Cover (Carrier of the message such as image, audio, video, text or some other digital media) and the Method (Spatial domain and transform domain).

a. Spatial Domain [4]

Spatial domain steganography in which the confidential information is embedded in the pixel intensity values of cover multimedia data. Steganography in spatial domain considered as a simple and low complexity method and usually is done in the luminance component and color component. The spatial methods are most frequently employed because of fine concealment, great capability of hidden information and easy realization.

b. Frequency Domain [5]

The main strength of transform domain techniques is addressing the restrictions of spatial methods, moreover special features to represent an alternative view of a signal. The main drawback with frequency domain refers to high computational requirement [6]. Three techniques in frequency domain are namely DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), and DFT (Discrete Fourier Transform).

1.3. Image Steganography

Embedding the secret data in image is called image steganography. It can hide large amount of information because image file is large in size. Pixel intensities are used to hide the data in image steganography. Imperceptibility, robustness, perceptual transparency and payload capacity are the factors which need to be considered while applying any steganographic algorithm.The basic philosophy in majority of the spatial domain steganography schemes is to embed the secret data directly in the intensity value of pixel of the cover multimedia data.

The paper is organized as follows. Section 2 gives a detailed description of various concepts being used for implementation. Section 3 explains in detail the proposed algorithms for embedding and extraction of the stego data. Section 4 describes the experimental outcomes and results. The conclusion and future scope is presented in section 5.

2. DESCRIPTION OF VARIOUS TECHNIQUES USED

2.1. Pixel Value Differencing (PVD)

Pixel value differencing (PVD) [6] based steganography is one of popular approaches for secret data hiding in the spatial domain. The PVD based methods have been proposed to enhance the embedding capacity without introducing obvious visual artifacts into stago images. In PVD based schemes the number of embedded bits is determined by the difference between the pixel and its neighbor. The large the difference amount is, the more secret bits can be embedded. Suppose two neighboring pixels, xi and x_{i+1}, are used and their difference value is d_i=x_i+1–x_i, where 0≤ |d_i|≤ 255. A large |d_i| means a complex block. Then classify |di| into a set of contiguous ranges, denoted by Rk, where k = 0, 1, ..., K − 1 is the range index. Denote l_k, u_k, and w_k as the lower bound, the upper bound, and the width of Rk, respectively. The value of w_k is designed to be a power of 2. If |d_i | ∈ R_k, the corresponding two pixels are expected to carry log 2 (w_k) bits. That is, their pixel values are changed so that the absolute value of their new difference equals to |d_i|=|y_i+1− y_i|=l_k+b_i , where b_i is the decimal value of the to-be-embedded bits. The embedding operation can be described as.

$$(y_i, y_{i+1}) = \begin{cases} (x_i - r_c, x_{i+1} + r_f) if\ d_i\ is\ odd \\ (x_i - r_f, x_{i+1} + r_c) if\ d_i\ is\ even \end{cases} \qquad (1)$$

2.2. Least Significant Bit (LSB)

The LSB based steganography [7] is one of famous approaches in the spatial domain. LSB based steganography is one of the conventional techniques capable of hiding large secret message in a cover image without introducing many perceptible distortions. It works by replacing the LSBs of randomly selected pixels in the cover image with the secret message bits. The selection of pixels may be determined by a secret key. The embedding operation of LSB steganography may be described by the following equation.

$$y = 2\left\lfloor \frac{x_i}{2} \right\rfloor + m_i \qquad (2)$$

where m_i, x_i, and y_i are the i-th message bit, the i-th selected pixel value before embedding and that after embedding, respectively. Many steganographic tools using the LSB based steganographic technique, such as Steghide, S-tools, Steganos, etc. By changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be identify by the human eye, thus the message is successfully hidden in image as shown in Figure 2. The proposed algorithm is an extension to the algorithm proposed in [8] and the results are found to be better than the ones in the already existing literature.

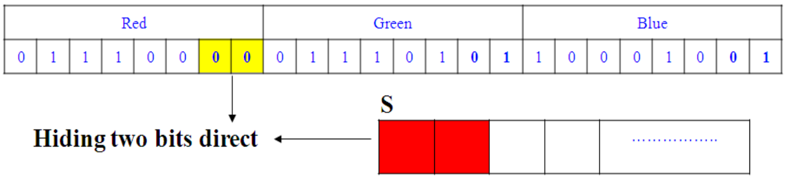


Figure 2. Hiding two bits directly in a Message

3. PROPOSED TECHNIQUE

3 steps of proposed image steganography are depicted in Figure 3:

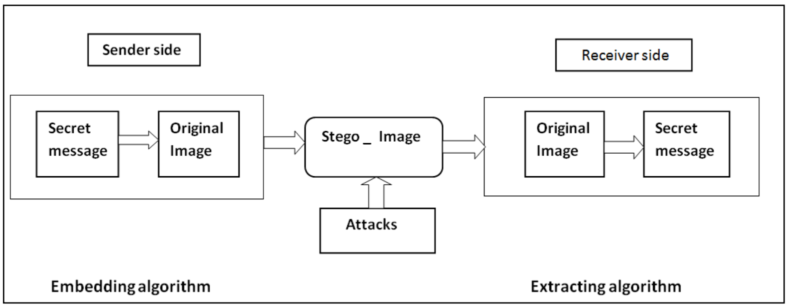


Figure 3. Block Diagram of Proposed Image Steganography

3.1. Embedding Process

Flow Chart of proposed embedding process shown in Figure 4:

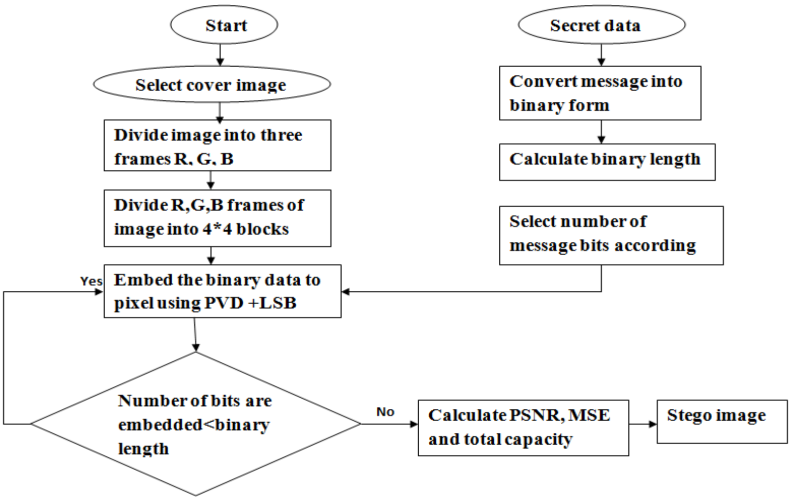

Start
Select cover image
Divide image into three frames R, G, B
Divide R,G,B frames of image into 4*4 blocks
Yes
Embed the binary data to pixel using PVD +LSB
Number of bits are embedded<binary length
No
Calculate PSNR, MSE and total capacity
Stego image
Secret data
Convert message into binary form
Calculate binary length
Select number of message bits according

Figure 4. Flow Chart of Proposed Embedding Process

3.2. Embedding Algorithm

a. Read the image file of size m*m. (I_{org}) of m*m
b. Make its frames (Red, Green, Blue). $I_{org} = (I_R, I_G, I_B)$
c. Divide frames into blocks of 4*4 pixel group.
d. Select block from each frame one by one.
e. Calculate average difference value using equation given below.

$$d = \frac{1}{15}\sum_{i=0}^{15}|X_i - X_{min}| \quad (3)$$

f. Number of bits is calculated with d value using given range table.
g. Take message and convert it into binary.
h. msg_bin = dec2bin (msg,8)
i. Apply LSB substitution.
j. Pix(1, n) = msg(n_bits)
k. After substitution, rearrange pixel groups to form stego image.
l. Calculate PSNR, MSE, r.

3.3. Extraction Process

Flowchart of proposed extraction process is illustrated in Figure 5:

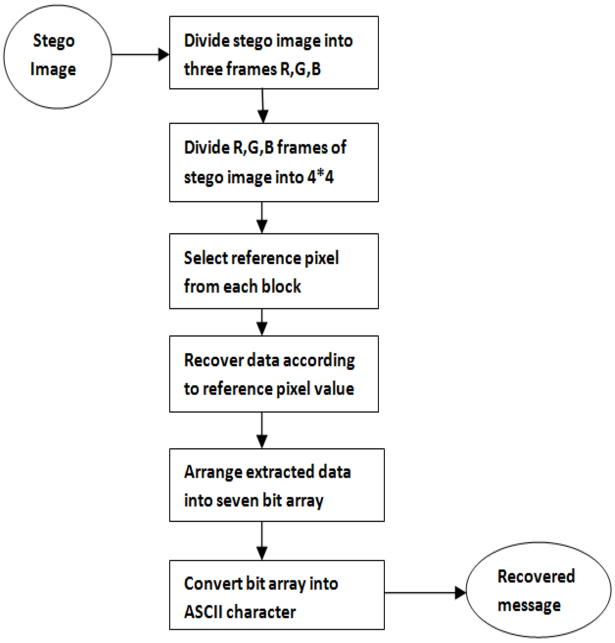

Stego Image
Divide stego image into three frames R,G,B
Divide R,G,B frames of stego image into 4*4
Select reference pixel from each block
Recover data according to reference pixel value
Arrange extracted data into seven bit array
Convert bit array into ASCII character
Recovered message

Figure 5. Flowchart of proposed extraction process

3.3.1. Extraction Algorithm

a. Take a stego image of size m*m.
*(Istego) of m*m*

b. Make its frames (Red, Green, Blue).
Istego = (ISR, ISG, ISB)

c. Divide frames into blocks of 4*4 pixel group.

d. Select block from each frame one by one.

e. Select reference pixel from each block.
ref-pix = [{Rs, Gs, Bs},Frame{pix(4,4)}]

f. Grouping of LSB'S of each pixel according to value of reference pixel.
msg = pix[(Rs, Gs, Bs), n]

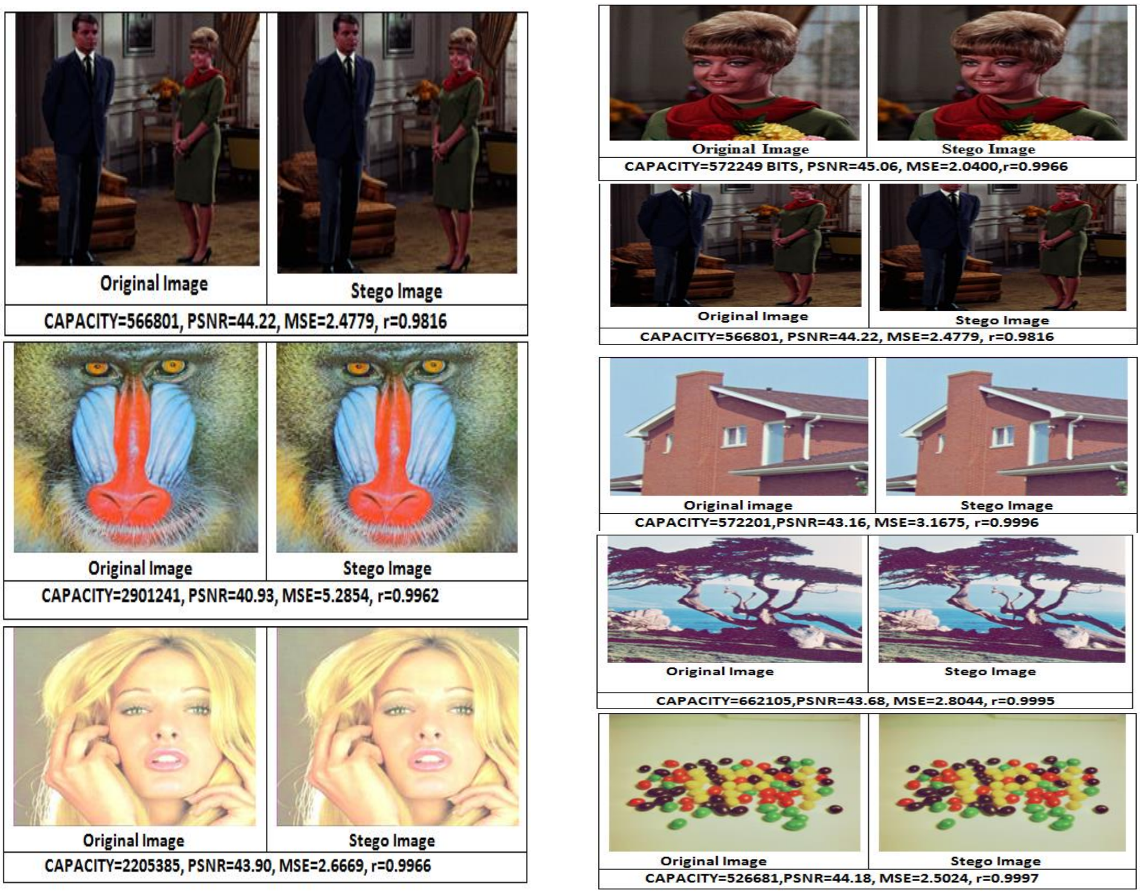
g. Arrange extracted data into eight bit array.

h. Convert binary into ASCII character.
msg_bin = bin2dec (msg,8)

i. Embedded message.

4. EXPERIMENTAL RESULTS

The experimental results were simulated in MATLAB. Various cover images of varying capacities and sizes were taken and the algorithm was implemented to embed the stego information into these cover images. It was observed that the proposed algorithm enabled higher number of bits to be incorporated in the host data without causing any significant perceptible change to the cover image. An improvement in the PSNR, MSE as well as correlation coefficient has been registered in the proposed method. Performance matrices of various images at varying capacity is illustrated in Figure 6.


Original Image
Stego Image
CAPACITY=566801, PSNR=44.22, MSE=2.4779, r=0.9816
Original Image
Stego Image
CAPACITY=2901241, PSNR=40.93, MSE=5.2854, r=0.9962
Original Image
Stego Image
CAPACITY=2205385, PSNR=43.90, MSE=2.6669, r=0.9966
Original Image
Stego Image
CAPACITY=572249 BITS, PSNR=45.06, MSE=2.0400,r=0.9966
Original Image
Stego Image
CAPACITY=566801, PSNR=44.22, MSE=2.4779, r=0.9816
Original image
Stego Image
CAPACITY=572201,PSNR=43.16, MSE=3.1675, r=0.9996
Original Image
Stego Image
CAPACITY=662105,PSNR=43.68, MSE=2.8044, r=0.9995
Original Image
Stego Image
CAPACITY=526681,PSNR=44.18, MSE=2.5024, r=0.9997

(a) (b)

Figure 6. Performance Matrices of Various Images at VARYING CApacity
(a) (256 * 256) (b) (512 * 512)

Comparison of existing algorithm and proposed algorithm at different capacity is shown in Table 1.

Table 1. Comparison of Existing Algorithm and Proposed Algorithm at Different Capacity

Images	Capacity (bits)	Gandharba Swain's scheme			Proposed scheme			Capacity(bits)
		PSNR	MSE	r	PSNR	MSE	r	
Girl1	569929	43.38	2.9854	0.9991	45.06	2.0400	0.9966	572249
Couple	553882	42.13	3.9785	0.9980	44.22	2.4779	0.9816	566801
House1	571801	42.97	3.2775	0.9992	43.16	3.1675	0.9996	572201
Tree	626638	41.62	4.4748	0.9994	43.68	2.8044	0.9995	662105
Jelly bean 2	520483	44.88	2.1138	0.9994	44.18	2.5024	0.9997	526681
Lena	2297680	40.64	5.6115	0.9984	41.98	4.1460	0.9985	2306809
Baboon	2877658	35.22	19.5127	0.9966	40.93	5.2854	0.9962	2901241
Tiffany	2159377	40.19	6.2199	0.9965	43.90	2.6669	0.9966	2205385
Peppers	2286574	39.52	7.2495	0.9986	41.98	4.1472	0.9986	2292137
Pot	2167504	41.29	4.8308	0.9991	41.58	4.5446	0.9990	2181177

5. CONCLUSION

For the image steganography various methods have been proposed. In this paper we propose an improved approach of image steganography that uses sixteen-pixel differencing with n-bit LSB substitution. The performance metrics are indicative of good results it leads to lower MSE and higher PSNR values. The existing algorithm can further be extended by increasing its robustness to geometric attacks through use of hybrid substitution techniques.

REFERENCES

[1] S. Arun Kumar et al, "Steganography in Images Using LSB Technique", *International Journal of Latest Trends in Engineering and Technology (IJLTET)*, Vol. 5, January 2015, pp. 426-430.

[2] G. Mohit, "A Novel Text Steganography Technique Based on Html Documents", *International Journal of Advanced Science and Technology*, Vol. 35, October 2011, pp. 129-138.

[3] V. Deepankar, "Steganography Techniques", *International Journal of Emerging Research in Management & Technology*, Vol. 3, May 2014, pp. 132-135.

[4] T. Namita et al, "Spatial Domain Image Steganography based on Security and Randomization", *International Journal of Advanced Computer Science and Applications*, Vol. 5, 2014, pp. 156-159.

[5] N. Dhinaharan et al, "*Trends in Computer Science, Engineering and Information Technology*", Proc. of First International Conference on Computer Science, Engineering and Information Technology, September 2011.

[6] L.Weiqi et al, "A More Secure Steganography based on Adaptive Pixel-Value Differencing Scheme proposed that Pixel-Value Differencing (PVD)", *Journal of Multimedia Tools and Applications*, Vol. 52, no.2, January 2010, pp.407-430.

[7] S. Arun Kumar et al, "Steganography in Images Using LSB Technique", *International Journal of Latest Trends in Engineering and Technology (IJLTET),* Vol. 5, January 2015, pp. 426-430.

[8] Gandharba Swain, "Digital Image Steganography using Nine-Pixel Differencing and Modified LSB Substitution", *Indian Journal of Science and Technology*, Vol. 7, September 2014, pp. 1444-1450.

BIOGRAPHY OF AUTHOR

Dr Meenakshi S Arya is currently working as Associate Professor and Head of the Department at Baba Farid College of Engineering and Technology. She completed her Ph.D. in the area of Digital Image Processing in the year 2014. Her resaerch interests are in the field of Digital Inage Processing and Data Mining and Warehousing.