IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. VII (Jul.-Aug. 2017), PP 46-51
www.iosrjournals.org

A Novel Steganography Using Mapping Technique for Different Size Images without Cover File Transformation

K.S.Sadasiva rao[1], Dr A.Damodaram[2]
[1] Associate Professor, Dept of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad, India
karrisrini@gmail.com
[2] Professor of CSE, School of Information Technology, Jawaharlal Nehru Technological University, Hyderabad & The Vicechancellor, SVU University, Tirupathi, India
damodarama@rediffmail.com

Abstract: *Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the transmitted information. Steganography is the process of hiding data bits on cover or carrier file. In this paper, instead of embedding the data bits directly on carrier color image, original data bits will be mapped on the carrier file with key vectors. If the size of the source image and cover image is equal (x1 = x2 and y1 = y2) then the corresponding bits are compared in preparing mapping vectors. If the source image (with the size x1, y1) and cover image file (size of x2, y2) sizes are different then the corresponding bits comparison continues till both the images are having the corresponding pixels and for the excess pixels of any image, either in horizontal or in vertical are again compared with the starting pixels of the image and mapping vector prepared for any dissimilar size images. Hence, this paper provides image steganographic process for different size images and also this technique provides higher hiding capacity than the cover image size by reusing the pixel values in comparison and preparing mapping vectors. In this proposed algorithm, original data bits get transmitted without embedding on the carrier or cover image, but there is a logic with which we are transferring the data bits on the carrier file, so any unauthorized user finds this carrier image, it will not give any information as it is plain cover image without any data was stuffed and image quality measuring parameters are also not modified. Hence this technique is a very efficient technique. At least a single bit is not modified in the cover image, so we could not be able to identify steganographic process with any powerful steganalysis techniques, hence it is robust.*

Keywords: *Cryptography, Steganography, Color Image steganography, LSB, mapping vectors, carrier file, different size images, Steganalysis.*

Date of Submission: 16-08-2017 Date of acceptance: 05-09-2017

I. Introduction

The rapid growth in information technology and digital communication has become very significant to protect the information transmission between sender and receiver. Cryptography and Steganography are the two widely used areas to provide security for the data transmitted through widely used internet applications. Cryptography was created as a technique for securing the secrecy of communication and many methods were designed to encrypt and decrypt data in order to uphold the secrecy of the message. Unfortunately, sometimes it is not just enough to keep the content of the message secret but also the existence of the message [3]. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". Steganography is the process of hiding data bits on cover or carrier file. The carrier file may be text file, image file, audio file or video file etc. If that carrier file is an image file, then that technique is called Image steganography[1]. If color image is used as a carrier file to embed data bits, then that type of steganographic technique is called as color image steganography [2]. In Image steganography the information is hidden exclusively in images [5]. Therefore, Steganography introduces a strong way to conceal information and to converse a secret data in an appropriate multimedia carrier file. If color image is used as a carrier file to embed data bits, then that type of steganographic technique is called as color image steganography [2]. The color image is a combination of pixels, each pixel represented with three planes Red, Green and Blue. Each pixel requires 24 bits out of which 8 bits allotted for each Red, Green and Blue planes. Spatial domain and Transform Domain are the two most commonly used Image steganographic Techniques. Generally in spatial domain, RGB planes are used to stuff the data bits at least significant bit positions of the pixel. Hence three bits can be stuffed in each pixel among the three planes [4]. But in the transform domain, the pixel values are converted into the transform co-efficient and then those transformed co-efficient to be used to modify the data. Transform domain techniques have an advantage over spatial domain techniques as they hide information in

areas of the image that are less exposed to compression, cropping and image processing [6]. Hence either spatial domain or transform domain algorithms will replace the cover image bits with the original message bits using least significant bit algorithm or some other variations on those algorithms. There is a trade-off between the amount of secret data that can be embedded, the image distortion and the security of the stego-image [12].

II. State of the Art

Steganography is a process of hiding data in other media to transfer the secured information [1]. Most of the steganographic algorithms are working on gray scale images, but some unauthorized user may suspect some useful information is going in gray scale image, because now a day's nobody is interested in sending gray scale images as general images [7]. Actually many steganographic techniques have been implemented either in color or gray scale images, but in color images all the three planes RGB have been used to stuff the bits. Hence in color image steganography, by using LSB method 3bits/pixel can be replaced with secret data.

In most of the proposed spatial domain or transform domain algorithms will replace the cover image bits with the original message bits using least significant bit algorithm or some other variations on those algorithms. The following are the list of papers observed to know about the related work done :-

1. Anil kumar et al. [8] proposed a work, in which the authors uses hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. This technique makes sure that the message has been encrypted before hiding it into a cover image. If in any case the cipher text got revealed from the stego image, the intermediate person other than receiver can't access it, as it is in encrypted form, which requires to decrypt to get original data.

2. Mekha Jose et al. [9] proposed steganographic algorithm, which allows to hide an image with in a cover image. The proposed algorithm make use of LSB technique. The bits of the secret image are embedded in random pixels of the cover image and these random pixels are generated by RC4 algorithm. Through this method user can embed 3 bits at each pixel, hence the cover image is required to be at least 8 times bigger than the secret image.
3. Odai M. Al-Shatanawi et al. [10] Presented a narrative approach, in which a new algorithm proposed to hide large amount of data in color image. This algorithm based on different size image segmentations (DSIS) and modified least significant bit (MLSB), where the DSIS algorithm has been applied to embed a secret image randomly. The number of bits replaced in each byte is non uniform. This proposed approach is efficient and satisfied high imperceptible with high payload reached to four bits per byte.
4. Xinyi Zhou et al. [11] Proposed a work, proposed a more secure steganography by implementing randomness of the LSB embedding positions and encrypt the message which control embedded positions, so the hidden information cannot be extracted without the corresponding private key.
5. Marghny H. Mohamed et al. [12] Presented a steganographic method, the image is divided into two parts, one for embedding the secret message and applies change to the value of some bits that have the secret bits obtained by the simple LSB substitution technique. The other part is used to indicate which change is applied to each pixel exist in the first part.
6. Pratiksha Sethi et al. [13] presented a narrative approach stated that Steganography hides the continuation of data and Cryptography converts data into cipher text. In the proposed anticipated system, the file we want to protect is firstly compressed to shrink in size and then it was transformed into cipher text by using AES algorithm and then the encrypted data is concealed in the image. Genetic algorithm is used for pixel assortment of image.
7. Anil Kumar et al. [8] presented a steganographic method using RSA and Hash-LSB techniques, where the algorithm designed to provide more security to data and for data hiding method. The proposed technique uses hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of cover image. This technique makes sure that the message has been encrypted before hiding it into a cover image.
8. Hemalatha S et al. [14] proposed a work novel image steganographic technique to hide both image and key in color cover image using Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT). In this proposed work 256 x 256 size color image used as cover image and the secret information is a gray scale image of size 128 x 128. To transfer secret image, first a key is generated and encrypted. Only the resultant key hidden in the cover image by using IWT.

III. Proposed System

In this proposed algorithm, instead of embedding the data bits directly on carrier color image, original data bits will be mapped on the carrier file with the help of key vectors. If the size of the source image and cover image is equal, in both horizontal and vertical order ($x1 = x2$ and $y1 = y2$) then the corresponding bits of the cover image compared with the corresponding bits of the cover image in preparing differential vectors. The values in differential vectors are ranging from -255 to +255 for each Red, Green and Blue planes with the size of (x1, y1) or (x2, y2) as the both images are with the same size. If the source image with the size (x1, y1) and cover image file with the size (x2, y2) are not equal, then the corresponding bits comparison continues till the

source image is having the corresponding pixels in the cover image and for the excess pixels of source image, either in horizontal or in vertical are again compared with the starting pixels of the cover image and mapping vector prepared for any dissimilar size of images. If the column pixels are excess, then pixel comparison continues with starting column of the same row. If the row pixels are excess, then pixels comparison continues with starting row of the same cover image. This process will continue till the end of mapping all the pixels of the source image by comparing with the cover image. These mapping vectors are transmitted to the destination, which are helpful in reconstructing the source image.

The similar way of bits recollection process is going to be implemented at the receiving end. Hence, this paper provides image steganographic process for different size images and also this technique provides higher hiding capacity than the cover image size by reusing (horizontally / vertically) the pixel values in comparison and preparing mapping vectors. In this proposed algorithm, original data bits get transmitted without embedding on the carrier or cover image, but there is a logic with which we are transferring the data bits of comparison with the carrier file. Even if any unauthorized user finds this carrier image, it will not give any information as it is plain cover image without any data was stuffed and image quality measuring parameters are also not modified. Hence this technique is a very efficient technique. At least a single bit is not modified in the cover image, so we could not be able to identify steganographic process with any powerful steganalysis techniques, hence it is robust.

IV. Proposed System At Sender Side

As almost all the steganographic algorithms either spatial domain or transform domain are using bit replacement algorithms, the steganalysis techniques are used to find any variation in the carrier image comparing with the cover image. These Steganalysis techniques are mostly working on the statistical characteristics of an image. Whenever there is partial or slight change in the carrier image, those changes can be detected by commercial steganalysis tools, even though it is not identified by human necked eye. Most of the LSB based steganographic algorithms will be getting PSNR value is much more than 20 (i.e., if this value is greater than 20, human eye cannot detect the change in the cover image and stego image). Also, the LSB based and the related steganographic techniques are simple, well known and easier to identify it by the steganalyst.

In this proposed paper, the source picture was regenerated at receiver side, even though the picture was not transmitted by the sender. At sender side, the source picture was compared with the cover image and generates the differential vectors for all the three planes (RGB). If we assume the source image with the size(x1, y1) and cover image with the size(x2, y2). The sender side algorithm prepares the differential vectors for the RGB planes with the size of (x1, y1) or (x2, y2) as the sizes of the both of the images are similar. If the source image with the size (x1, y1) and cover image file with the size (x2, y2) are not equal, then the corresponding bits comparison continues till the source image is having the corresponding pixels in the cover image and for the excess pixels of source image, either in horizontal or in vertical are again compared with the starting pixels of the cover image and mapping vector prepared for any dissimilar size of images. If the column pixels are excess, then pixel comparison continues with starting column of the same row. If the row pixels are excess, then pixels comparison continues with starting row of the same cover image. This process will continue till the end of mapping all the pixels of the source image by comparing with the cover image. These mapping vectors are transmitted to the destination, which are helpful in reconstructing the source image. The same cover image was maintained by both the sender and receiver ends with their repositories. As per the pixel representation in color image, all the three planes differential vector values are ranging only between -255 to +255.

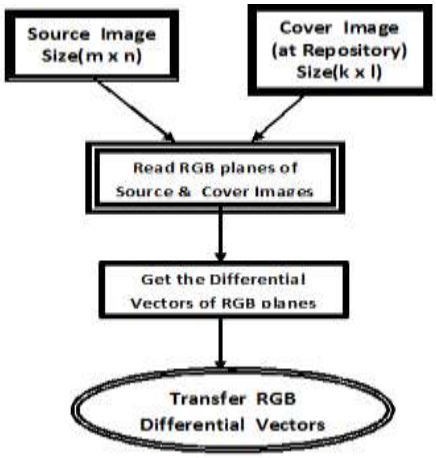

Fig. Proposed system at Sender Side

Algorithm at Sender Side:-

1. Read source image(x1, y1) and cover image(x2, y2) which are color images.
2. Display the cover image and source images.
3. Consider the sender and receiver having same repository of carrier/cover images.
4. Construct the 'differential vectors' by comparing the corresponding pixels of the source image with cover file for all RGB planes.
5. If (x1 = x2) and (y1 = y2) then consider both images are with same size and prepare the same size of differential vectors for all RGB planes.
6. If (x1 > x2) and (y1 > y2) then the size of the source image is bigger horizontally and vertically, then implement re-comparison for all the excess bits and prepare the required size of differential vectors for all RGB planes.
7. If (x1 > x2) and (y1 <y2) then the size of the source image is bigger horizontally, then implement re-comparison for all the excess bits.
8. If (x1 < x2) and (y1 > y2) then the size of the source image is bigger vertically, then implement re-comparison for all the excess bits and prepare the required size of differential vectors for all RGB planes.
9. If (x2 > x1) and (y2 > y1) then the size of the source image is smaller in horizontal and vertically, then implement comparison for all the existing bits only and prepare the required size of differential vectors for all RGB planes.
10. Transfer the differential vectors of RGB planes to the destination end.
11. Stop the process.

V. Proposed System At Receiver Side

At the receiver end, the differential vectors of RGB planes are received. These differential RGB vector values are operated with the corresponding RGB vector values of cover image at receiver side image repository in reconstructing the source image RGB vector values. While constructing the Source image with RGB vector values, problem arises, when the sizes of differential vectors is not matching with the sizes of cover image RGB vectors. In such case a comparison study implemented with the corresponding pixels available and whenever excess pixels are in source image, the comparison study continues with the same row of the cover image or with the starting row bits of the cover image. Finally, the required RGB planes vectors are generated and they were used in reconstructing the source image at destination end.

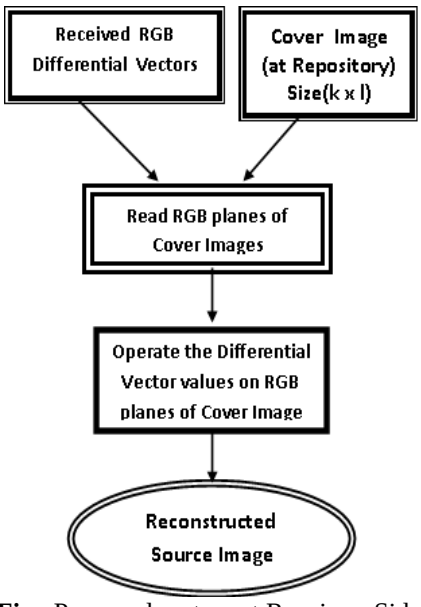

Fig. Proposed system at Receiver Side

Algorithm at Receiver Side:-

1. Read the cover image(x2, y2) which is color image.
2. Display the cover image.
3. Consider the sender and receiver having same repository of carrier/cover images.
4. Read the 'differential vectors' for all RGB planes.

5. If (x1 = x2) and (y1 = y2) then consider both images are with same size and Reconstruct the same size RGB planes vectors for source image.
6. If (x1 > x2) and (y1 > y2) then the size of the source image is bigger horizontally and vertically, hence Reconstruct the required size of RGB planes vectors for source image.
7. If (x1 > x2) and (y1 <y2) then the size of the source image is bigger horizontally hence Reconstruct the required size of RGB planes vectors for source image.
8. If (x1 < x2) and (y1 > y2) then the size of the source image is bigger vertically, hence Reconstruct the required size of RGB planes vectors for source image.
9. If (x2 > x1) and (y2 > y1) then the size of the source image is smaller in horizontal and vertically, hence Reconstruct the required size of RGB planes vectors for source image.
10. Generate source image with the help of RGB planes of the size(x1, y1).
11. Stop the process.

VI. Results

Fig 1: Difference in Red planes of pixels

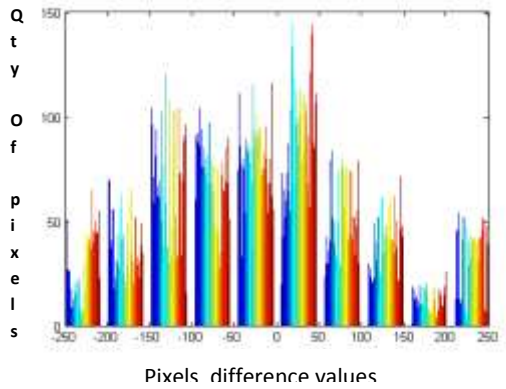

Fig 2 : Difference in Green planes of pixels

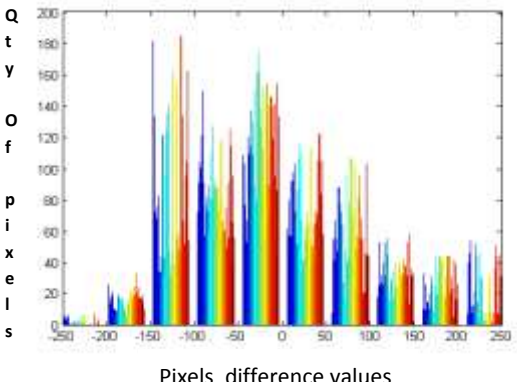

Fig 3 : Difference in Blue planes of pixels

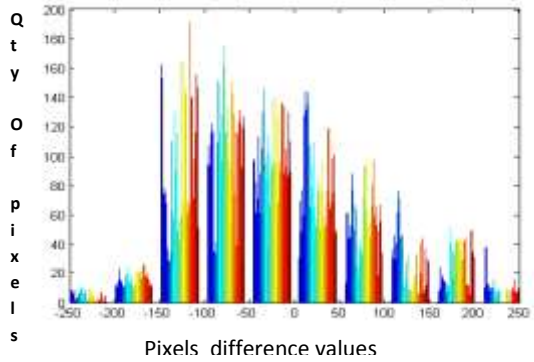

Fig 4 : The source Image need to send

Fig 5 : The Cover Image sent through channel

Fig 6 : The Source image re-constructed at Receiver end

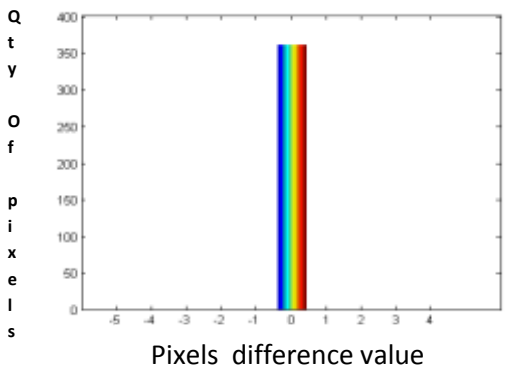

Fig 7 : The Histogram showing the difference between the source image at sender side and reconstructed image at receiver side.

VII. Conclusion

In all the referenced articles [1–15] improved spatial domain or transform domain techniques were used either image bits are directly replaced with original data bits or transformed coefficients are evaluated and replaced on the image. In such case, a powerful commercial steganalysis technique can identify the stegnographic process. Where as in this proposed technique neither the data bits were directly replaced on any image nor the stego file was transmitted on the channel. Only the constructed differential vectors files were transmitted on the channel. Even though any hacker identified the cover file he cannot detect any information it as there is no information about the source file. Hence this technique is more robust and efficient.

References

[1]. Niels Provos and Peter Honeyman, Hide and Seek: An Introduction to Steganography, IEEE Security & Privacy, 2003.
[2]. Niel F Johnson, Sushil Jajodia, Exploring Steganography: Seeing The Unseen, IEEE, 1998.
[3]. Tahir Ali, Amt Doegar, "A Novel Approach of LSB Based Steganography Using Parity Checker", IJARCSSE, Vol.5, Issue 1, January 2015, pp. 314-321.
[4]. Wien Hong And Tung-Shou Chen, A Novel Data Embedding Method Using Adaptive Pixel Pair Matching, IEEE Transactions On Information Forensics And Security, Volume 7, No. 1, February 2012.
[5]. T. Morkel, J.H.P. Eloff, M.S. Oliver, "An Overview of image steganography", Pretoria, South Africa, Information and Computer Security Architecture (ICSA) Research Group, pp 1-11, June 2005.
[6]. Mehdi hussain and Mureed hussian, "A survey of image steganography technique", International Journalof Advanced science and technology, vol.54, May 2013, pp.113-123.
[7]. Neha Gupta, Nidhi Sharma, "Hiding Image in Audio using DWT and LSB", IJCA, Vol. 81, No. 2, November 2013, pp.11-14.
[8]. Anil kumar, Rohini Sharma, "A Secure Image Steganography Base on RSA Algorithm and Hash-LSB Technique", IJARCSSE, Vol. 3, Issue 7, July 2013, pp. 363-372.
[9]. Mekha Jose, "Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality", IJSR, Vol. 3, Issue. 9, Sept. 2014, pp. 2281-2284.
[10]. Odai M. Al-Shatanawi, Nameer N. El. Emam, "A NEW IMAGE STEGANOGRAPHY ALGORITHM BASED ON MLSB METHOD WITH RANDOM PIXELS SELECTION", IJNSA, Vol. 7, No. 2, Mar 2015, pp. 37 – 53.
[11]. Xinyi Zhou, Wei Gong, Wenlong Fu, LianJing Jin, "An Improved Method for LSB Based Color Image Steganography Combined with Cryptography", IEEE, ICIS 2016, Japan, June 2016.
[12]. Marghny H. Mohamed, Loay M. Mohamed, "High Capacity Image Steganography Technique based on LSB Substitution Method", An Internation journal of Applied Mathematics & Information Sciences, Vol. 10, No. 1, Jan 2016, pp. 259 – 266.
[13]. Pratiksha Sethi, V. Kapoor, "A Proposed Novel Architecture for Information Hiding in Image Steganography by using Genetic Algorithm and Cryptography", ELSEVIER – ScienceDirect, Procedia Computer Science 87 (2016), pp. 61 - 66.
[14]. Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, " A SECURE COLOR IMAGE STEGANOGRAPHY IN TRANSFORM DOMAIN", IJCIS, Vol. 3, No. 1, Mar 2013, pp. 17 – 24.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

K S Sadasiva Rao. "A Novel Steganography Using Mapping Technique for Different Size Images without Cover File Transformation." IOSR Journal of Computer Engineering (IOSR-JCE) , vol. 19, no. 4, 2017, pp. 46–51.