ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Hybrid Approach for Embedding Text or Image in Cover Images

Ashwini B. Akkawar, Prof. komal B. Bijwe

P.G Student, Department of Computer Science and Engineering, P. R. Pote (Patil) College of Engineering & Technology , Amravati ,India .

Assistant Professor, Department of Computer Science and Engineering, P. R. Pote (Patil) College of Engineering & Technology, Amravati, India.

ABSTRACT: The recent growth in computational power and technology has propelled the need for highly secured data communication. One of the best techniques for secure communication is Steganography-a covert writing. It is an art of hiding the very existence of communicated message itself.**.** The aim is to design a steganography algorithm which not only hide the message behind the image but also provide more security than others .A new steganography technique for embedding both text or image in cover images by using LSB & Link List method is implemented. This steganography technique is completely a time domain (pixel based) and secret messages are embedded directly into 24-bit color image. Two ways are provided for embedding the secret data inside cover image such as sequential encoding and random encoding for both text & image .For the purpose of security, encryption technique is used with a user-defined key. RGB image format is used to improve the quality of the stego image. At last that RGB image will saved as BMP image file so that no lossy compression can occur and the original message do not destroy and can be extract as it is. Aspect ratio for both text and image after hiding in cover image maintains exactly same. Performance of proposed steganography technique is evaluated by calculating values of MSE(Mean square error), PSNR(Peak signal to noise ratio), ET(Elapse time).

KEYWORDS: Link List method ,LSB, Stego-image, PSNR , MSE ,ET ,BMP.

I. INTRODUCTION

Steganography is the science of invisible communication which hides any private data within an innocent-looking cover object. The word Steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. Steganography is an information hiding technique developed in recent years. It is a procedure that makes use of human perceptive sense of visual or aural redundancy to digital multimedia, and that embeds the secret information in the public media to transfer digital media carrying confidential information to achieve covert communications [1]. Steganography is different from cryptography. The goal of cryptography is to provide secure communications by transforming the data into a form that cannot be understood. Steganography techniques, on the other hand, hide the existence of the message itself, which makes it cumbersome for a third person to find out the message. Unlike steganography, sending encrypted information may draw attention. Accordingly, cryptography is not the good solution for secure communication but only part of the solution. Both techniques can be used together to better protect information [3]. Basic steganography model is shown in Fig.1.1

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

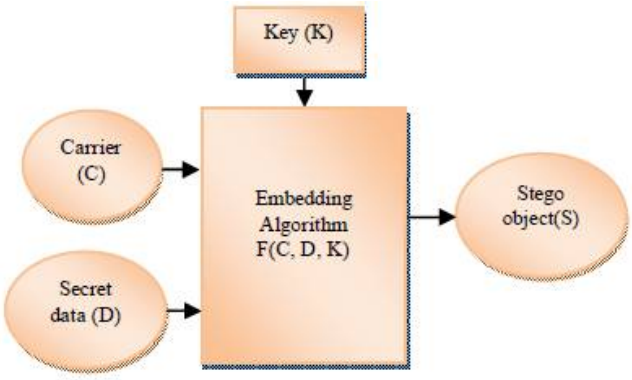

Fig 1.1: Basic steganography model

The basic model consists of Carrier(C), Secret Data(D), Stego Key(K).

1. Carrier is the cover object in which the message is embedded.
2. Secret data can be any type of confidential data that can be plain text, cipher text or other image.
3. Key mainly used to ensure that only recipient having the decoding key will be able to extract the message from a cover-object.
4. By using the embedding algorithm, the secret data is embedded into the cover object in a way that does not change the original image in a human perceptible way.
5. Finally, the stego object which is the output of the process is the cover-object with the secretly embedded data[4].

II. RELATED WORK

[1] proposed image steganography combined with pre-processing of DES encryption. When transmitting the secret information, firstly, encrypt the information intended by DES encryption and then is written in the image through the LSB steganography. Encryption algorithm improves the lowest matching performance between the image and the secret information by changing the statistical characteristics of the secret information to enhance the anti-detection of the image steganography. [2] proposed dual layer of security to the data, in which first layer is to encode data using Least Significant Bit image steganography method and in the second layer encrypt the data using Advance Encryption Standard Algorithm. Steganography does not replace the encryption of data, instead it provides extra security feature to it. [3] proposed method which embbeds data in two cover images using four bit LSB technique. The secret data is hidden in binary form in two cover images due to which double protection has been provided to confidential data which can be any text, audio, video or image. [4] tries to elucidate the basic concepts of steganography, its types and techniques and dual steganography. [5] presented one technique that embedded the text file in a video file in such a way that the video does not lose its functionality using DCT & LSB Modification method. This method applies imperceptible modification. This proposed method strives for high security to an eavesdropper's inability to detect hidden information. [6] proposes Linked List method and Feistel Network for hiding Information inside Video. The two main algorithms used for data encryption and data embedding are Feistel Network and Linked List method respectively.

In [7] several solutions for color image pixels that reveals the secret image without loss and preserves the cover image using quantization. This methodology can be further enhanced for 3D images and can be used for embedding text. [8] uses the concept of neural network that has the ability to develop significance from complicated or loose data; it may be used to extract patterns. [9] proposed improved steganalysis methods, based on the most reliable detectors of thinly-spread LSB steganography presently known, focusing on the case when grayscale Bitmaps are used as cover images**.** In [10] steganography algorithm for embedding a message into a RGB 24-bit color image. It will be done by using the concepts of linked list data structure. It will help us to achieve some important advantages. First, we can create a "stegokey"by the address of message blocks. Second, it makes the detection of message harder.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

III.SCOPE OF RESEARCH

There has been a rapid growth of interest in this subject over the last ten years Steganography can be used anytime you want to hide data. In the business world steganography can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser. Terrorists can also use steganography to keep their communications secret and to coordinate attacks. All of this sounds fairly nefarious, and in fact the obvious uses of steganography are for things like espionage.There are a number of peaceful applications. The simplest and oldest are used in map making, where cartographers sometimes add a tiny fictional street to their maps . A similar trick is to add fictional names to mailing lists as a check against unauthorized resellers. Most of the newer applications use steganography like a watermark, to protect a copyright on information. As it has numerous application in real world ,we must have to enhance the security level of data being transmitted and prevent its unauthorized access.

IV. PROPOSED METHODOLOGY

The RGB image has 24 bits values per pixel represent by (00000000, 00000000 and 00000000) for black and (11111111, 11111111 and 11111111) for white pixels. The RGB image is the most suitable because it contains alot of information that help in hiding the secret information with a bit change in the image resolution which does not affect the image quality and make the message more secure[11].
In this research paper the RGB images are used as a carrier message to hide the secret message by using new proposed method. Two ways are provided for embedding the secret data inside cover image such as sequential encoding and random encoding for both text & image. In Sequential encoding only one key is entered by user and pixel are selected sequentially for embedding cipher text obtained by XORing the secret message with key provided by user. In random encoding two keys are provided by the user ,one is to lock the function on receiver side and other for to carry out encryption. In this case pixels are selected randomly for embedding secret data i.e either text or image using random number generator which automatically implements link list concept.
The proposed algorithm includes four parts in it:-
1. User-defined key – This includes the key entered by user to encrypt the message. The key should be an integer between 0-255. This key will help to provide security to the hidden message because even if third party will get the stego image he/she cannot extract the message without exact key.
2. Encryption - In this part of algorithm the message is encrypted using key by applying the method of encryption that is XOR the message binary values with the key and gets the cipher message.
3. Embedding –Using embedding algorithm given below, the message is embedding into an image of RGB format.
4. Extraction –The message can be extracted if the exact key is known.

➢ Sequential Encoding Algorithm

Input: RGB image file, a secret message, and a key.
Output: Stego image
Begin
Step1: Select the “canvas image” in which the secret message will hide which can be either text or image.
Step2: Enter the encryption key to encrypt the message file between 0-255.
Step3: Now convert the secret message into their ASCII integer values if the message is text otherwise obtain the integer value representation of image and convert image to grayscale image in order to reduce amount of data to hide .
Step3 (a): Apply header to the beginning of the message (so that at the extraction time it will easy to find from where our message is starting).
Step 3(b): Ensuring Sufficient "Hiding Space".
Step3 (c): XOR the binary format of secret message with the key entered by user.
Step4: Hide the data points using the RGBBGRRG order.
Step4 (a): Hide the data along the columns moving from left to right through the target image.
Step5: Determine whether or not we have reached the end of the image. Then need to move to the next column

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

and reset our pattern to the top row.
Step6: Step5 will follow until the complete message is hidden into the image.
Step7: Convert the RGB stego file into the bitmap file format.
End

- **Sequential Decoding Algorithm**

Input: Import the image with hidden message and the same key will be entered by user when embed the message
Output: RGB image file and the secret message file.
Extraction algorithm follows all the same steps but in reverse order and in the last step the secret message file and the cover image file will save separately.

- **Random Encoding Algorithm**

Input: RGB image file, a secret message, and a key.
Output: Stego image
Begin
Step1: Select the “canvas image” in which the secret message will hide which can be either text or image.
Step2: Enter the encryption key to encrypt the message file between 0-255.
Step3: Now convert the secret message into their ASCII integer values if the message is text otherwise obtain the integer value representation of image and convert image to grayscale image in order to reduce amount of data to hide .
Step3 (a): Apply header to the beginning of the message (so that at the extraction time it will easy to find from where our message is starting).
Step 3(b): Ensuring Sufficient "Hiding Space".
Step3 (c): XOR the binary format of secret message with the key entered by user.
Step4: Preparing Hiding Canvas and Initialize Random Number Generator to a "Common" State. We need this value shared for the Decoding Steps.
Step5: We will randomly "hide" the message across pixels in the "canvas". That is why the previous step generated a set of Random Numbers to be used during this step. For each "word" of the MSG_ENC_SET Variable we will select the next 3 random numbers and apply the same RGBBGRRG Encoding process within the those random pixel values.
Step6: Step5 will follow until the complete message is hidden into the image.
Step7: Convert the RGB stego file into the bitmap file format.
End

- **Random Decoding Algorithm**

Input: Import the image with hidden message and the same key will be entered by user when embed the message
Output: RGB image file and the secret message file.
Extraction algorithm follows all the same steps but in reverse order and in the last step the secret message file and the cover image file will save separately.

IV. EXPERIMENTAL RESULTS

Work on embedding TEXT using same approach has been done previously .Work on embedding IMAGE using LSB and Link List method in cover image is added here. This algorithm is implemented using MATLAB R2012a (7.14.0.739) and gives satisfactory results. First we see the results for embedding text in cover image for both sequential and random encoding .The hidden text message is “Welcome to Pote college..”

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

- **Results for embedding text in cover image for both sequential and random encoding.**

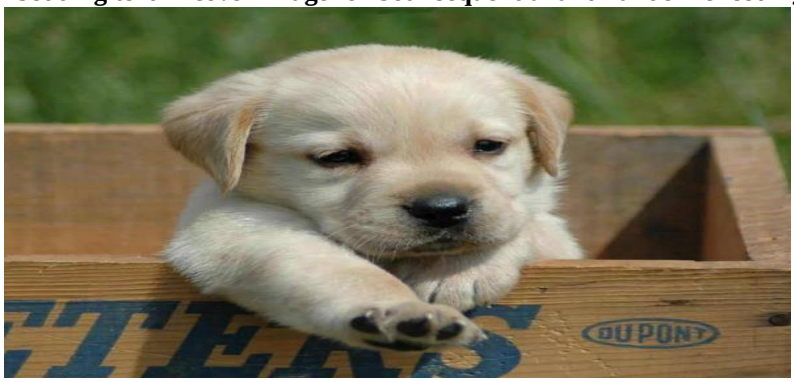

Fig A:Cover Image to hide the text message

Fig A shows the cover image which used to hide the secret text "Welcome to Pote college.." .Cover object can be anything like text ,audio, video.

Fig B :Stego Image with hidden message using sequential encoding

Fig B: shows the stego image which is obtained after encoding secret text message sequentially by only one using user defined key and sequential encryption algorithm.

Fig C:Stego Image with hidden message using random encoding

Fig C shows the stego image which is obtained after encoding text message randomly by using two user defined key and random encryption algorithm.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

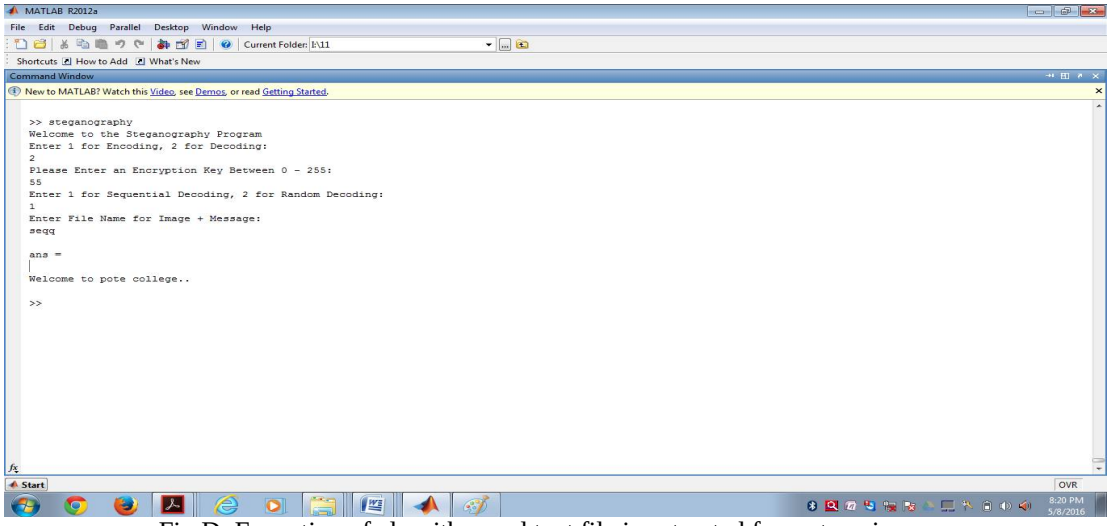

Fig D: Execution of algorithm and text file is extracted from stego image.

Here fig A shows the cover image used to hide the secret text message ,after encoding using sequential algorithm we get fig.B and same message is encoded using random algorithm and we get fig.C all these images look exactly same. Fig D shows the execution of algorithm and text file is extracted from stego image.

Table1: Camparison of results value for three images A,B,C

Images	Dimensions	Size	MSE	PSNR	Elapse Time
Fig A	600*450	29.7KB	-	-	-
Fig B	600*450	791KB	0.00	88.19dB	26.2600Sec
Fig C	600*450	791 KB	0.00	88.55dB	23.5600sec

- **Results for embedding image in cover image for both sequential and random encoding.**

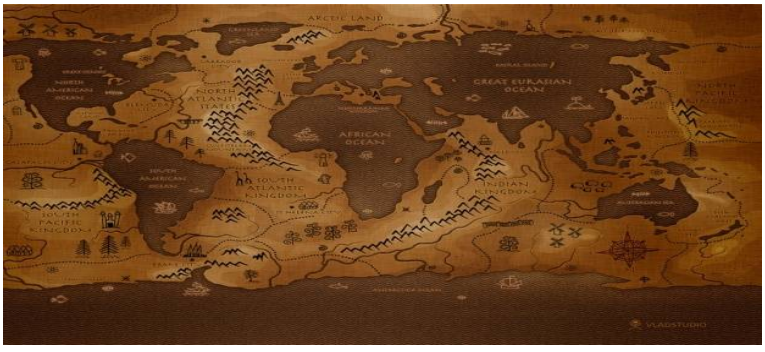

Fig E:Cover Image to hide the image

Fig. E shows the cover image which used to hide the secret image .Cover object can be anything like text ,audio, video.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Fig. F :Stego Image with hidden image using sequential encoding

Fig.F shows the stego image which is obtained after encoding secret image sequentially by only one using user defined key and sequential encryption algorithm.

Fig. G: Stego Image with hidden image using random encoding

Here fig.E shows the cover image used to hide the secret image ,after encoding using sequential algorithm we get fig. F and same image is encoded using random algorithm and we get fig.G all these images look exactly same. H and Fig. I shows the secret image needs to hide in cover image and decrypted image from stego image respectively.

Fig H:Secret image needs to hide inside cover image

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Fig I: Image extracted from stego image

Table 2: Camparison of results value for three images E,F,G

From Table 1 and Table 2, We can see that PSNR value for random encoding is more than the sequential encoding

Image	Dimensions	Size	MSE	PSNR	Elapse Time
Fig E	1600*1200	668KB	-	-	-
Fig F	1600*1200	5.49MB	0.01	65.71	17.559 Sec
Fig G	1600*1200	5.49MB	0.01	65.78	18.114 Sec

means it random encoding minimizes the difference between cover image & stego image. The size of stego image remains same for sequential & random encoding for both text & image which means aspect ratio maintains exactly same for both text and image.

V. CONCLUSION

In this paper we have implemented hybrid approach which combines LSB & Link List method for embedding both text & image in cover image. Encoding is performed in two ways such as sequential encoding and random encoding. Both of this encoding technique work successfully using this hybrid approach and hides successfully both text & image in cover images. By using same hybrid approach we can use audio or vedio as cover object and increases the payload capactity of secret data.

REFERENCES

[1] Yang Ren-er, Zheng Zhiwei, Tao Shun, Ding Shilei," Image Steganography Combined with DES Encryption Pre-processing", Sixth International Conference on Measuring Technology and Mechatronics Automation, pp. 323-326, 2014.
[2] Satwinder Singh and Varinder Kaur Attri," Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm", International Journal of Signal Processing, Image Processing and Pattern Recognition) Vol. 8, No. 5 pp. 259-266, 2015.
[3] Ketki Thakre, Nehal Chitaliya," Dual Image Steganography for Communicating High Security Information", International Journal of Soft Computing and Engineering (IJSCE), Volume-4, Issue-3, pp.7-12, July 2014.
[4] Ms. Ketki Thakre Dr.Nehal Chitaliya," Highly Secured Dual Steganographic Technique: A Retrospective" , International Journal of Engineering Research & Technology (IJERT)Vol. 2 Issue 10, pp. 2849-2827, October – 2013.
[5] Poonam V Bodhak , Baisa L Gunjal ,"Improved Protection In Video Steganography Using DCT & LSB" , International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, pp.31-37,April 2012 .
[6] P. Selvigrija , E. Ramya , "Dual Steganography for Hiding Text in Video by Linked List Method" , 2015 IEEE International Conference on Engineering and Technology (ICETECH), 20th March 2015, Coimbatore, TN, India.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

[7] Rohit G Bal1, Dr P Ezhilarasu , "An Efficient Safe and Secured Video Steganography Using Shadow Derivation ", International Journal of Innovative Research in Computerand Communication Engineering (An ISO 3297: 2007 Certified Organization)Vol. 2, Issue 3, pp.3251-3257, March 2014

[8] Richa Khare ,Rachana Mishra ,Indrabhan Arya," Video Steganography by LSB Technique using Neural Network", Sixth International Conference on Computational Intelligence and Communication Networks,pp. 898-902, 2014.

[9] Manu Devi ,Nidhi Sharma," Improved Detection of Least Significant Bit SteganographyAlgorithms in Color and Gray Scale Images", Proceedings of 2014 RAECS UIET Panjab University Chandigarh, 06 – 08 March, 2014.

[10] Masoud Nosrati , Ronak Karimi ,Mehdi Hariri," Embedding Stego-Text in Cover ImagesUsing linked List Concepts and LSB Technique", World Applied Programming, Vol (1), No (4), pp. 264-268 ,October 2011.

[11] Babita, Mrs. Ayushi," Secure Image Steganography Algorithm using RGB Image Format and Encryption Technique", International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4 No. 06,pp.758-762 Jun 2013.