High Security Image Steganography with Multistage Encoding

Ajitkumar M Parmar[1], Prof. Krishna Chauhan[2]
[1]M. Tech. Scholar, [2]Research Guide
[1,2]Department of Electronics and Communication Engineering, Sagar Institute of Research and Technology, Bhopal

Abstract - Image Steganography is the image processing branch to hide secret information behind the image with different techniques so that no one unauthorized can predict about the hidden information. The techniques must be that much efficient which do not reveal in the presence of any information in the image. In this paper a methodology is proposed to hide information securely as well as the stages are multiple which enhances the security of technique. For basic steganography technique LSB method is adopted and to enhance the security the secret information which is in the form of three images are converted into text, i.e. first stage of security than the text is encoded than hide behind the cover image in different layers. Here technique utilizes all the three layers to hide three different images.

Keywords - Image Steganography, LSB, Text Encoding and Information Security etc.

I. INTRODUCTION

Constantly communicated through the Internet are flows of information generated from many diverse applications such as e-commerce transactions, audio and video streaming or online chatting. The security of such data communication, which is required and vital for many applications nowadays, has been a major concern and ongoing topic of study given that the Internet is by design open and public in nature. Many techniques have been proposed for providing a secure transmission of data. Data encryption and information hiding techniques have become popular and generally complement each other. Whereas encryption transforms data into seemingly meaningless bits, called cipher text, through the use of sophisticated and robust algorithm, information hiding [1] is the process of concealing messages in such a way that no one apart from the sender and the intended receiver even knows that there is a hidden message. The word steganography is of Greek origin which means "covered or hidden writing" [2]. The technique has been used in ancient times where secret messages were tattooed on the shaven heads of the messengers. These messengers were sent away after their hair grew up and were later shaved again to recover the messages.

In computer systems as well, steganography is extensively used. Pictures are embedded in video material. Secure shell connections, remote desktop software such as telnet, virtual host always include some amount of delay before sending the information packets over the network. These delays can be used to encode data. Texts are hidden in web pages. Information is concealed within computer files which can be audio files, jpeg images or bit mapped images which are larger in size and contain lot of information in it. For example, every nth color bit is replaced with some message bit and sent over the transport network. This change is so minute that it usually goes unnoticed due to highly redundant code stream.

The general idea of hiding secret information in media has a wider range of applications that go beyond steganography. For example, an image printed on a document could be annotated by metadata that could lead a user to its higher resolution. Due to the high proliferation of digital images and the high degree of redundancy present in digital images, there is an increased interest in the usage of images as the cover object in steganography. The Least-Significant-Bit (LSB) technique is one of the most widely used scheme for image steganography. This technique involves the modification of the LSB planes of the images. In this technique, the message is stored in the LSB of the pixels which could be considered as random noise. Therefore altering them does not significantly affect the quality of the cover image. Variations of the LSB algorithms include one or more LSB bits. The motivation for this study is to provide security to confidential RGB images such as maps or sensitive signed documents. The basic principle of steganography is to hide the secret information in the cover object, which can be a digital medium such as image, audio or video file, to obtain a stego file that has secret information hidden in it.

The different types of steganography techniques are substitution, transform domain, spread spectrum, statistical and distortion techniques and cover generation techniques. Substitution techniques replace the least significant bits of each pixel in the cover file with bits from the secret document. The transform domain technique hides secret information in the transform space (like frequency domain) by modifying the least significant coefficients of the cover file.

II. PROPOSED STEGANOGRAPHY TECHNIQUE

The image steganography should be as secure as possible to make the secret information almost unable to access as well as unpredictable for strangers. The efficiency of the steganography technique should be reflect from the same qualities as discussed before. The block diagram of proposed methodology is explained in the figure below. The whole system is divided into two parts. First part is the embedding of secret messages behind cover image and get stego image. Second part is extraction of secret messages from stego image.

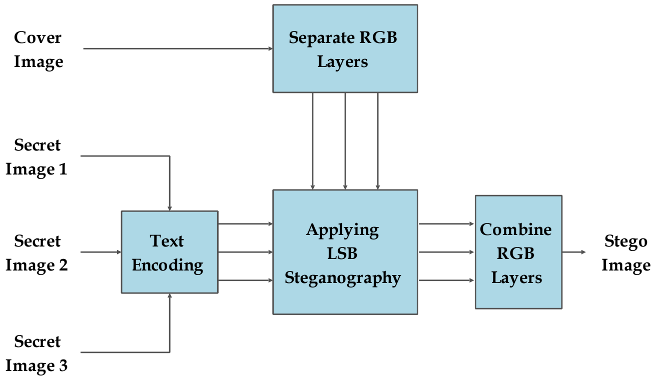


Fig. 2.1 Embedding Process of Secret Messages and get Stego Image

The first process is shown in the Fig. 2.1, here are four inputs one cover image that should be colour image and three secret monochrome images are taken to hide behind cover image. The cover image is separated into red, green and blue layers. The secret images is encoded into text. The text stream of first secret image is hiding behind red layer of the cover image. The text stream of second secret image is hiding behind green layer of the cover image.

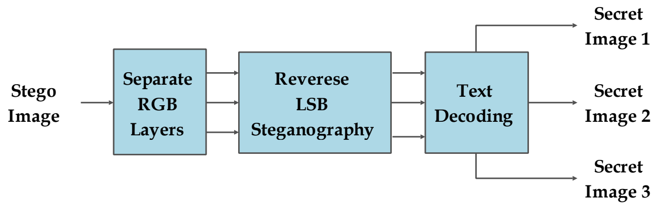


Fig. 2.2 Extraction Process of Secret Messages From Stego Image

The text stream of third secret image is hiding behind blue layer of the cover image. The hiding process is done using LSB steganography method which is best one for same goal. Now combine layers and stego image is generated.

The procedure for extraction of embedded secret messages hidden behind stego image is explained in the Fig. 2.2. The stego image is taken as input to the process that red, green and blue layers. The reverse steganography is performed to get the text and these texts (from red, green and blue layers) are decoded into monochrome images.

The flow chart of the implemented computer algorithm is shown in the Fig. 2.3. The steps are having two steps embedding of secret information and get stego image second is to extract secret information from stego image and calculate the quality of recovered secret information.

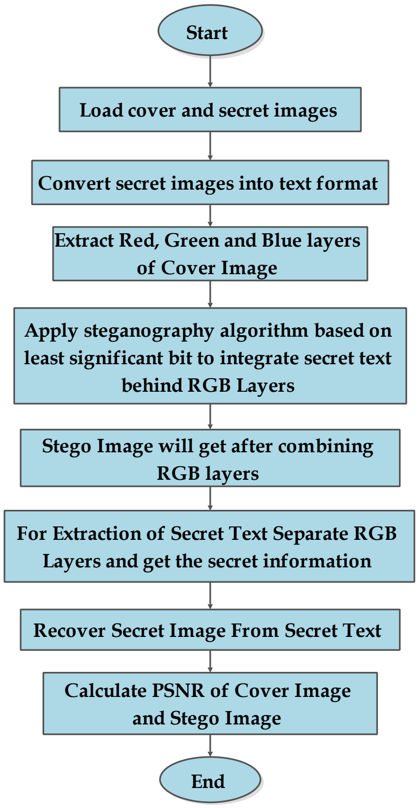
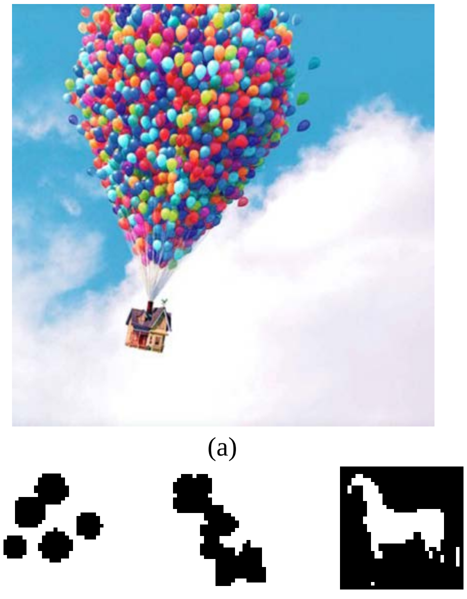

Start
Load cover and secret images
Convert secret images into text format
Extract Red, Green and Blue layers of Cover Image
Apply steganography algorithm based on least significant bit to integrate secret text behind RGB Layers
Stego Image will get after combining RGB layers
For Extraction of Secret Text Separate RGB Layers and get the secret information
Recover Secret Image From Secret Text
Calculate PSNR of Cover Image and Stego Image
End

Fig. 2.3 Flow chart of proposed methodology

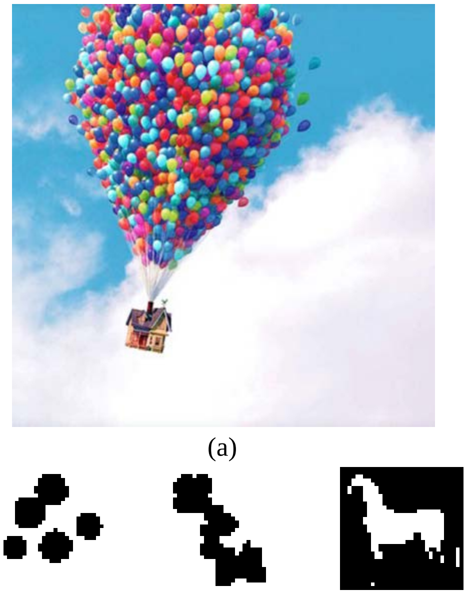
III. SIMULATION RESULTS

The efficient secure image steganography technique is explained in the previous section of paper. In this section the step by step inputs and outputs are shown in the below figures.


(a)

(b) (c) (d)

Fig. 3.1 Inputs to the system (a) Cover Image, (b) Secret Image 1, (c) Secret Image 2, (d) Secret Image 3

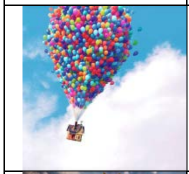
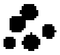
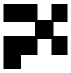
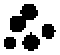
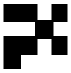
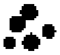
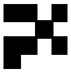
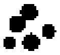
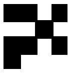

(a)

(b) (c) (d)

Fig. 3.2 outputs to the system (a) Stego Image, (b) Recovered Secret Image 1, (c) Recovered Secret Image 2, (d) Recovered Secret Image 3

The proposed methodology is implemented on simulation tool and the user interface is shown in the figure 3.1. In Fig. 3.1 cover image with three secret images are shown. In Fig. 3.2 the stego image with recovered secret images and the similarity with the original secret image is also shown below images in terms of peak signal to noise ratio(PSNR), root mean square error(RMSE) and mean square error (MSE).

Table 1: PSNR Comparison of Cover and Stego Image

Stego Image	Secret Image1	Secret Image2	Secret Image3	PSNR(dB)
				81.21 dB
				81.16 dB
				81.26 dB
				81.43 dB

IV. CONCLUSION AND FUTURE SCOPE

The results of the proposed methodology are shown in the previous section and from the algorithm it can be clear that the whole process of steganography is separated in to multiple stages and the different stage has different format of information which significantly increases the security of the algorithm and no one strange can extract the secret information until the proper knowing of algorithm. The other factor is the traces of hidden information on stego image. From the results it is unable to identify visually the difference between stego and cover image.

The future technology other than LSB with the multiple stages make system more better in terms of security as well as efficiency.

REFERENCES

[1] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn," Information hiding survey", IEEE, 87(7):1062-1078, 1999.

[2] G. J. Simmons, "The Prisoner's problem and the subliminal channel in Advances in Cryptology", Proc. crypto '83:55–67, 1983.

[3] Udit Budddia and Deepak Kundur, "Digital video steganalysis exploiting collusion Sensitivity", IEEE, 1(4):502-516, 2006.

[4] Furuta, T,.Noda, H., Niimi, M., Kawaguchi E,"Bit-plane decomposition steganography using wavelet compressed

video", Joint Conference of the Fourth International Conference, 2(5): 970 - 974, 2003.

[5] V.Karthekayani and kammalakan, "Conversion grayscale image to color image with and without texture synthesis", International journal of computer science and network security, 7(4):11-16, 2007.

[6] Eiji Kawaguchi and Richard O. Eason, "Principle and applications of BPCS-Steganography", Proc. SPIE ,3528: 464-473 , 1999.

[7] Nameer N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm" Jordan Journal of Science publications, 3 (4): 223-232, 2007.

[8] K B Raja, C R Chowdary K R Venugopal, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Images", IEEE, 170-176, 2005.

[9] Naofumi," Technique of lossless steganography", IEICE Transactions on Communications, 90(11):1-4, 2007.

[10] Nan jiang and wan jiang, "Random oracle model of information modeling" , World academy of science, 18:1307-6884, 2006.

[11] Vishal,Wilson and bryon, "Linear,color separablehuman visual system model for vector diffusioning system", Journal of Electronic Imaging, 1:277-292, 1992.

[12] Ying Wang; Moulin, P,"Statistical Signal Processing" , IEEE, 56(11) : 339 –342, 2003.

[13] Mastronardi, G.; Castellano, M. Marino, "Intelligent Data Acquisition and Advanced Computing Systems" IEEE,11:116 – 119, 2003.

[14] M. Shirali-Shahreza and M.H. Shirali-Shahreza, "An Improved Version of Persian/Arabic Text Steganography Using "La" Word'" Proceedings of the 6th National Conference on Telecommunication Technologies 2008 (NCTT 2008), Putrajaya, Malaysia, August 26–28, 2008.

[15] Porter, Thomas; Tom Duff, "Compositing Digital Images", Computer Graphics 18 (3): 253–259, 1984.

[16] Alvy Ray Smith, "Alpha and the History of Digital Compositing", Microsoft Tech Memo, 7:08-15, 2005.