Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Keyless Algorithm for Steganography Using RST

Shaik Abdullah.G
M.E, Computer Science and Engineering,
A.V.C. College of Engineering, Tamil Nadu, India

ABSTRACT - Steganography is one among the foremost powerful tools for information concealing. During this paper, we've got changed least significant bit (LSB) substitution methodology for knowledge concealing. Conventional LSB technique uses the smallest amount important little bit of consecutive pixels for embedding the message which attracts suspicion to transmission of a hidden message. If the suspicion is raised, then the goal of steganography is defeated. Still LSB technique is that the most generally used because it is easy. In our implementation pixels to be substituted with data area unit selected randomly which makes it superior to the standard approach. The strength of the algorithmic rule is additional exaggerated by exploitation keyless steganography. This paper proposes a completely unique technique to cover data in exceedingly twenty four bpp RGB image exploitation modified LSB substitution methodology.

Key Words: - bits per constituent (bpp), least important bit (LSB), pixel, RGB, steganography.

I. INTRODUCTION

Communicating Steganography is mainly used for secure communication. Steganography provides an application to secure its data from being accessed by hackers. The techniques which are used here are simple to implement to provide an ideal cipher, fast, compact, portable and secure communication. This project Steganography is one of the most powerful tools for information hiding. In this paper, we have modified least significant bit (LSB) substitution method for data hiding. Conventional LSB technique uses the least significant bit of consecutive pixels for embedding the message which draws suspicion to transmission of a hidden message. If Communication generally needs privacy and security while the suspicion is raised, then the goal of Steganography is defeated. Still LSB technique is the most widely used as it is simple. In our implementation pixels to be substituted with information are selected randomly which makes it superior to the conventional approach. The robustness of the algorithm is further increased by using keyless Steganography. This paper proposes a novel technique to hide information in a 24 bpp RGB image using modified LSB substitution method. Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

II. EXISTING SYSTEM

Conventional LSB technique uses the least significant bit of consecutive pixels for embedding the message which draws suspicion to transmission of a hidden message. The Internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The important of reducing a chance of the information being detected during the transmission is being an issue now days. Some solution to be discussed is how to passing information in a manner that the very existence of the message is unknown in order to repel attention of the potential attacker. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media. In this research, we clarify what steganography is, the definition, the importance as well as the technique used in implementing steganography. We focus on the Least Significant Bit (LSB) technique in hiding messages in an image. The system enhanced the LSB technique by randomly dispersing the bits of the message in the image and thus making it harder for unauthorized people to extract the original message.

III. PLANNED SYSTEM

The scheme used for selecting and modifying pixels is the focus of the proposed algorithm. In conventional methods selection of pixels is done in an orderly fashion, usually using a key, whereas in the proposed algorithm selection of pixels to be modified is performed randomly. This makes the algorithm securer than conventional algorithms. Another highlight of this algorithm is that the capacity of storing information per pixel is greatly increased without perceivable

changes in the modified image. We can hide the message by substituting the LSB of each pixel with information bits in 24 bpp RGB image. 24 bpp RGB image is a 24 bit depth color image using RGB color model. 24 bit refers to 8 bit for each RGB color channel, i.e. 8 bits for red, 8 bits for green and 8 bits for blue. This implies that we can store three bits of information per pixel at the LSB of RGB. By changing the LSB of RGB values of each pixel, we may get maximum 2X2X2=8 different shades. This change in the pixel bits will be indiscernible to the human eye the above mentioned points highlight the uniqueness of this algorithm and justify its novelty.

A. PLANNED SYSTEM TECHNIQUE

The proposed method offers a significant improvement over the conventional techniques. LSB technique used for steganography of 8 bit format is far more vulnerable to attacks as compared to 24 bit format. The advantage of using a bmp file is that it is capable of hiding a large message. The randomness in pixel selection renders detection of hidden information difficult. In this algorithm storage space is significantly increased by increasing the number of modifiable bits per pixel. The main highlight is that the proposed steganography process requires no key. Mainly no attacker can identify the presence of secret data due to the high quality of stego image. Even if the attacker is suspicious the complete retrieval of hidden message is impossible due to randomness of pixels containing the information.

IV. THE PLANNED FRAMEWORK

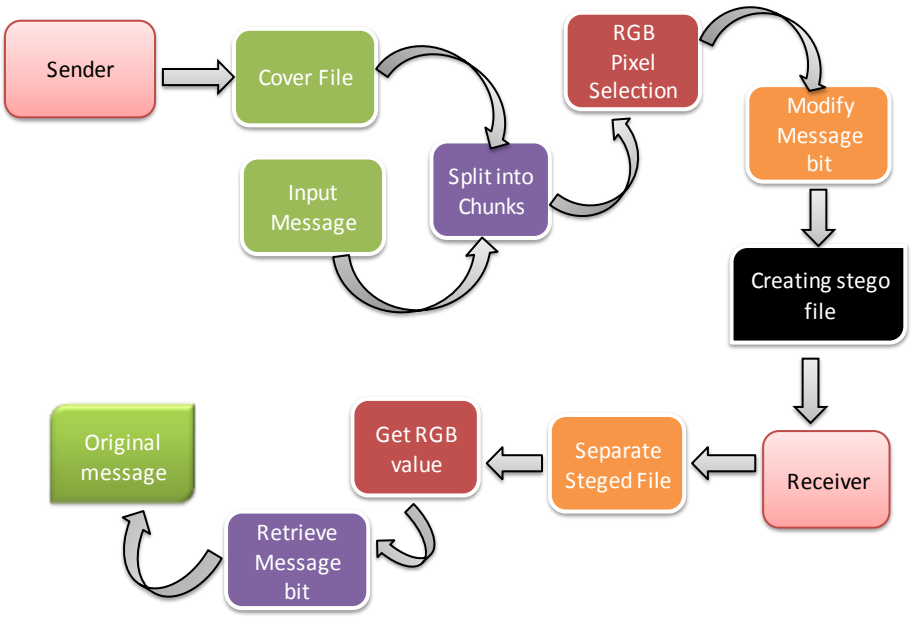

Fig.1: The Planned Framework

V. IMAGE SPLITTING AND PIXEL SELECTION

First get the cover file and message from user and then calculate the image height and width by using code. After that the image has splited into several chunks depends upon message length. Then select one pixel from the all chunks randomly using keyless algorithm. If the chunk size is 256 x 256 ,the method of pixel selection is LSB to LSB -4 of red and LSB-3 to LSB -5 of blue (LSB of red being the most significant bit of next location) LSB to LSB-4 of green and LSB to LSB -2 of blue (LSB of green being the most significant bit of next location) and the bit for selecting from subsequent two blocks is derived from LSB of blue of the current pixel. And here the blue value is 0 to select the next block of the image otherwise the blue value is 1 to select the next to next block of the image.

VI. CREATING STEGED IMAGE

For example: We have used 1024X768 images. ASCII describes a communications system where 7-bit words represent printable symbols and control codes. The message to be embedded is ‘meetatnine’. ASCII of m= 109= 1101101 ASCII of e= 101= 1100101

ORIGINAL PIXEL VALUE: 01110000:10010001:11000110
MODIFIED PIXEL VALUE: 01110001:10010001:11000110

VII. RETRIEVING ORIGINAL MESSAGE

Receiver after getting the steged image from the sender then the receiver perform the reverse process of the creating steged image The first think receiver doing the separating the steged image Then receiver finds the RGB component value And they will got the modified message bit Finally they got the original message.

Table -1: Observation Table

VIII. IMPLEMENTATION RESULT

The scheme used for selecting and modifying pixels is the focus of the proposed algorithm. In conventional methods selection of pixels is done in an orderly fashion, usually using a key, whereas in the proposed algorithm selection of pixels to be modified is performed randomly. This makes the algorithm securer than conventional algorithms. Another highlight of this algorithm is that the capacity of storing information per pixel is greatly increased without perceivable changes in the modified image. The above mentioned points highlight the uniqueness of this algorithm and justify its novelty. By adopting the above stated methodology stego process has been performed. Following are some stego covers and Steged images.

IX. SOME OF THE MODULES WE HAVE DESIGNED AS FOLLOWS

Fig -2: Sender Side

Fig -3: Enter the Secret Message

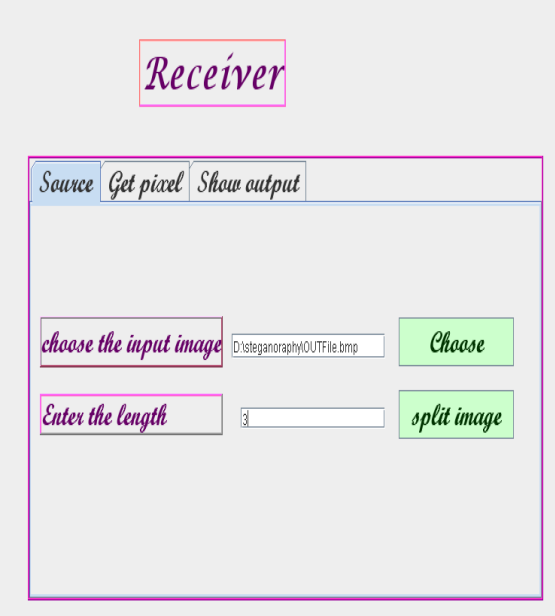

Fig -4: Enter the Message Bit Length

Fig -5: Show Output

X. CONCLUSION

The block based steganography provides robust and effective technique for information hiding. It was shown by experimental results that the proposed method offers a significant improvement over the conventional techniques. LSB technique used for steganography of 8 bit format is far more vulnerable to attacks as compared to 24 bit format. The advantage of using a bmp file is that it is capable of hiding a large message. The randomness in pixel selection renders detection of hidden information difficult. In this algorithm storage space is significantly increased by increasing the number of modifiable bits per pixel. The main highlight is that the proposed steganography process requires no key. Mainly no attacker can identify the presence of secret data due to the high quality of stego image. Even if the attacker is suspicious the complete retrieval of hidden message is impossible due to randomness of pixels containing the information.

REFERENCES

[1] M. M Amin, M. Salleh, S . Ibrahim, M.R.K Atmin, and M.Z.I. Shamsuddin, "Information hiding using steganography," IEEE 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, pp. 21-25, January 2003.

[2] Deshpande Neeta, Kamalapur Snehal and Daisy Jacobs, "Implementation of LSB steganography and its evaluation for various bits," IEEE 1st International Conference on Digital Information Management, India, pp. 173-178, December 2006.

[3] S .K. Moon and R.S. Kawitkar, "Data security using data hiding," IEEE International Conference on Computational Intelligence and Multimedia Applications, India, pp. 247-251, January 2007.

[4] V. Lokeswara Reddy, Dr. A. Subramanyam and Dr.P. Chenna Reddy, "Implementation of LSB steganography and its evaluation for variousfile formats," Int. J. Advanced Networking and Applications, vol. 2, pp.868-872, 2011.

[5] Gandharba Swain and Saroj Kumar Lenka, "A hybrid approach to steganography embedding at darkest and brightest pixels," Proceedingsof the International Conference on Communication and Computational Intelligence ,Kongu Engineering College, Perundurai, Erode, T.N.,India, pp.529-534, December 2010.

[6] William Stallings, "Cryptography and Network Security, Principles Practice" Edition 3rd. Prentice Hall 2003, ISBN 0-13-091429-0.

[7] M. S. Sutaone and M.V. Khandare, "Image based steganography usingLSB insertion technique," IET International Conference on Wireless,Mobile and Multimedia Networks, India, pp. 146-151, January 2008.

[8] Beenish Mehboob and Rashid Aziz Faruqui, "A steganographyImplementation," IEEE-International symposium on Biometrics &Security technologies, ISBAST, Islamabad, April 2008.

[9] A Vadivel, A.K.Majumdar and Shamik Sural, "Performance comparison of distance matrices in Context-based image retrieval applications." IIT Kharagpur research work.

BIOGRAPHIES

Shaik Abdullah.G received the B.Tech Degree Information Technology. Currently Pursuing the M.E (Computer Science and Engineering) in A.V.C. College of Engineering – Mayiladuthurai, Tamil Nadu, India.
His research interest includes Cloud Computing and Network Security.

