International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

An Improvement on the Security of Odd-Even-LSB Based Steganography by Adding Encryption

Ayda Alizadeharasi[1], Maryam Safaei Rizi[2]

[1]M.Sc. Computer Science. Department of Computer Science University of Kerala Kariavattom Thiruvananthapuram 695581, India

[2]M.Sc. Computer Science. Department of Computer Science University of Kerala Kariavattom Thiruvananthapuram 695581, India

Abstract: ***Information can be hide by various methods. Steganography is one of the most common techniques using for hiding secret message inside the cover objects by using Least Significant Bit (LSB). Basically, the secret data refers to a message which is saved as a text file that needs to be hidden.The paper purposed an image based steganography that odd-even Least Significant Bits techniques and cryptography technique will use for enhance the security of simple odd-even LSB which has been introduced by Nain.N et al. (2012). This paper aims to increase the security of odd-even-LSB based steganography by adding encryption algorithm on text message before embedding. The purposed algorithm tested byPSNR and the results shows that the improved algorithm is 2.5 percent more secure than the previous algorithm. Although the algorithm was attacked by cropping, resizing, jpeg compression and adding noise and the result examined.***

Keywords: steganography, security, cryptography, LSB, hiding

1. Introduction

Nowadays a digital communication has become very common part of human life therefore, enhancing the secure transferring of information among users, become one of the important subject to study between the practitioners and researchers. The literature shows that the Steganography and cryptography are two popular methods applied for enhancing the security of communication.

Steganography is the art of hiding information.it is the art of hiding message in the cover message without leaving any trackable sign. In the past, people used hidden tattoos or invisible ink to convey steganography content. Today, computer and network technologies provide easy way to use communication channels for steganography. Watermarking and fingerprinting are two closely related techniques to steganography. These technologies are mainly concerned with the protection of intellectual property. But steganography is concern with the hiding of text in another information like image, text, audio, video (Arvind Kumar et al,2010 and Vikas Tyagi, 2012)[5]-[6].

Cryptography is a technique employed for protecting information by converting them into cipher text (unreadable). The secret key uses for convert the cipher text to the readable meaning full text. cryptography divide into two classifications:

1) Symmetric key: this kind uses single key in both sender and user side.
2) Public key: this kind uses two keys, public key which is known to everyone and private key which known only by receiver side

The aim of this paper is to enhance the odd-even LSB algorithm by using cryptography

2. Review of LSB

In imageprocessing, information can be insert into every bit of cover image but for hiding the information, the busy area of image can be calculated and hide information in less perceptible parts of cover image [1], [2].

Image watermarking methods are based on the pixel value's Least Significant Bit (LSB) modifications [3] which means it embeds the information in the least significant bits of pixel values of the cover image.For example, if the pixel value is 138 which is equivalent to 10001010 in binary and the secret message is 1, the value of the pixel will be change to 10001011 which is 139 in decimal.

3. Proposed Technique

Neeta Nain et.al (2012) *in* their study entitled "Steganography using Odd-even Based Embedding and Compensation Procedure to Restore Histogram" that describe about odd-even based embedding technique [4].

Based on the mentioned paper, the main objective of current study is to enhance the simple odd-even based embedding, because embedding the message data directly in the cover image means it is quite straightforward to detect that embedding message. Therefore, by adding encryption algorithm to the secret message with using symmetric key between sender and receiver side can make quite more secure data transfer.

Firstly, this study applied cryptography for transforming plain text message into cipher text according to Raphael A.J (cryptography and steganography). The figure 1 shows the plain secret message which is going to be change to cipher text by cryptography and the figure 2 shows the cipher text message.

Figure 1: plain secret message

Figure 2: cipher text message

As shown in figure 2 the secret message is in a form of unreadable and for reading, it needs a key for encryption.After receiving cipher text in receiver side, the decryption algorithm will be operating on the cipher message to get to the main secrete message. The figure 3 shows the message after decryption.

Figure 3: decrypted message

The purposed algorithm will first encrypt the secrete message as shown figure 1 and 2 and after hide it into the cover image.by this method if the line rubbers catch the image they cannot decrypt the secrete message without knowing the encryption key. The figure 4 shows the original cover image which can be used any image for the purpose of cover image by users.

Figure 4: Original cover image

Figure 5: Cover image after steganography

Finally, the result of previous steps will appear as figure 5. The figure shows the cover image after steganography. Consequently, after decrypting the embedded image (figure 5) with the secrete key, the secrete message will appear as below:

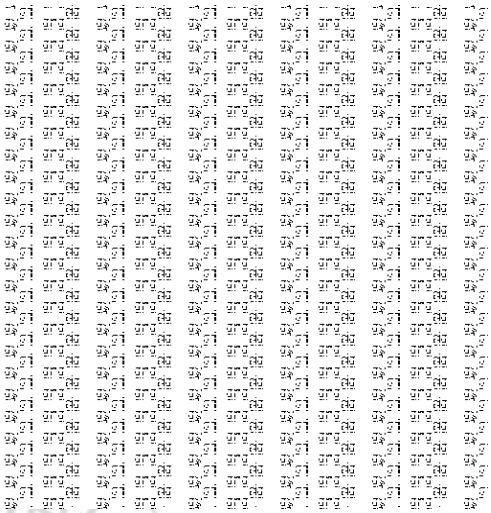

Figure 6: secrete message after encryption

Figure 5 shows the suggested algorithm. It illustrates that, if the secrete message elicit by the line rubbers the image will appear likewise image which is shown in figure 6. It should point out that the massage could be decrepit by agreed key for decryption between the two or more users. That means they need an additional key for decryption.

4. Conclusion

The purposed algorithm tested with PSNR. The tested PSNR shows that the security has been improved 2.5 percent compare to previous algorithm. It should be noted that the run time of this test compare to previous algorithm has taken 3.84 per cent more which indicates the improved odd-even-LSB in this study will takes more time to run. However, the results indicate that this algorithm is high secure than thepreviousalgorithm.

5. References

[1] Lee, G. J., Yoon, E. J. and Yoo, K. Y. (2008), “A new LSB based Digital Watermarking Scheme with Random Mapping Function”, in 2008 IEEE DOI 10.1109/UMC.2008.33
[2] Fazli, S. and Khodaverdi, G (2009), Trade-off between Imperceptibility and Robustness of LSB Watermarking using SSIM Quality Metrics, in 2010 IEEE DOI 10.1109/ICMV.2009.68
[3] Watermarking Systems Engineering Enabling Digital Assets and Other Applications, Mauro Barni (university of siena,Italy),Franco Bartolini (university of Florence,Italy), MARCEL DEKKER, INC
[4] Nain N Singh.j ,Dayma I,Meena R.2012.steganography using Odd-even Based Embedding and Compensation procedure to restore histogram.proceedings of the world congress on Engineering and computer science

2012.Vol I WCECS 2012,October 24-26,2012,San Francisco,USA

[5] Arvind Kumar and Km. Pooja. "Steganography- A Data Hiding Technique". International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010

[6] Vikas Tyagi,Atul Kumar,Roshan Patel,Sachin Tyagi,Saurabh Singh Gangwar."image steganography using significant bit with cryptography".Journal of Global Research in Computer Science Volume 3,No.3,March 2012.