IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

Digital image steganography using LSB and pseudo-random technique

Naveen Kalia
kalianaveen003@gmail.com
Ramgarhia Institute of Engineering and Technology, Phagwara, Punjab

Manit Kapoor
manit_kapoor@yahoo.co.in
Ramgarhia Institute of Engineering and Technology, Phagwara, Punjab

Dr. Naveen Dhillon
naveendhillon@rediffmail.com
Ramgarhia Institute of Engineering and Technology, Phagwara, Punjab

ABSTRACT

This paper purposed an image based steganography that uses the Least Significant Bits (LSB) techniques and pseudo-random encoding technique on images to enhance the security of the communication. In the L-SB approach, the fundamental thought is to replace the Least Significant Bits (LSB) of the cover picture with the Bits of the messages to be covered up without pulverizing the property of the cover image significantly. The LSB-based method is the most difficult one as it is hard to separate between the cover-object and stego-object if few LSB bits of the cover are replaced. In Pseudo-Random technique, an arbitrary key is utilized as a seed for the Pseudo-Random Number Generator is required in the inserting procedure. Both the systems utilized a stego-key while installing messages inside the cover picture. By utilizing the key, the chance of getting attacked by the attacker is reduced.

Keywords— *Steganography, LSB, Random-key, Image, Secret message, Stego-key, Cover image, Techniques*

1. INTRODUCTION TO STEGANOGRAPHY

Digital steganography is the craftsmanship and investigation of concealing correspondences; a steganographic technique subsequently inserts mystery information out in the open spread media so as not to stir a busybody's doubt. A steganographic technique has two fundamental angles: steganographic limit and indistinctness. Be that as it may, these two attributes are inconsistent with one another. Besides, it is very hard to expand the steganographic limit and all the while keeping up the imperceptibility of a steganographic technique. Moreover, there are still extremely constrained techniques for steganography to be utilized with correspondence conventions, which speak to whimsical however encouraging steganography mediums. Digital picture steganography, as a technique for mystery correspondence, expects to pass on a lot of secret information, generally to the extent of spread photo, between conveying parties. Moreover, it expects to keep away from the doubt of non-imparting gatherings to this sort of correspondence. Consequently, this exploration addresses and proposes a few techniques to improve these major parts of digital photo steganography. Thus, a few attributes and properties of the digital photo have been utilized to expand the steganographic limit and upgrade the stego photo quality (perceptibility). This section gives a general prologue to the examination by first clarifying the exploration foundation. At that point, the principle inspirations of this examination and the exploration issue are characterized and talked about. Next, the examination point is recognized dependent on the setup meaning of the exploration issue and inspirations. Then, the main motivations of this study and the research problem are defined and discussed. Now, the research aim is identified based on the established definition of the research problem and motivations.

1.1 Steganography and Cryptography

Cryptography and steganography have different goals. Cryptography conceals only the meaning or contents of a secret message from an eavesdropper. However, steganography conceals even the existence of this message (Lou and Liu, 2002). Furthermore, steganography gives more privacy and data security than cryptography since it disguises the insignificant presence of secret message instead of just ensuring the message substance. In this way, one of the significant shortcomings of cryptosystems is that despite the fact that the message has been encoded, regardless it exists.

Despite the fact that both cryptographic and steganographic techniques have secret communication, they have diverse definitions as far as system breaking. A cryptographic technique is viewed as broken if an attacker can read the secret message. In any case, a steganographic framework is viewed as broken if an attacker can recognize the presence or read the substance of the hidden message. Moreover, a steganographic system will be considered to have fizzled if an attacker suspects a particular file or steganography method even without decoding the message. Thus, this thought makes steganographic systems more delicate than cryptography systems in terms of system failure. Additionally, steganographic systems must avoid all kinds of suspicion in order to achieve security and not be considered fizzled system. Since includes an additional layer of security to cryptography, joining steganography and encryption gives a definitive in private communication. In this manner, the reason for steganography is to supplement cryptography and to abstain from raising the suspicion of system attackers but not to replace cryptography.

Stepwise explanation of this Encoding process is given below:

Step 1: Select a cover image through which we want to send data using LSB and RGB technique.

Step 2: Now initialize the text you want to send through the image.

Step 3: Before sending the data we need to encrypt text data because of more safety and security options as we will able to send data to safe hands.

Step 4: In this step, we put our data in LSB and send it through our communication sources. In a very normal manner.

Step 5: As we already discussed above this is the improved version of the LSB technique by using RGB. The proposed approach is compatible with the gray level image as well as RGB colour image. For RGB colour image R-value, G value and B value will be considered as an individual pixel. The motivation behind this approach is to improve the quality of stego-image as well as to maximize the data hiding capacity of cover-image. A newly proposed key-pixel cipher is the safeguard of this approach.

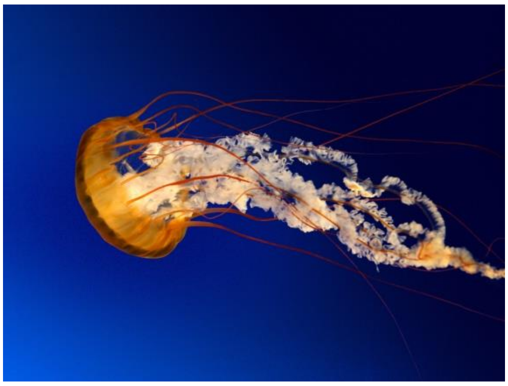

Fig. 1: Cover image

Fig. 2: LSB image

Data is encrypted and used in LSB
Function (ax+b) mod 26

Fig. 3: Improved LSB Image

Stego Image Block Diagram:

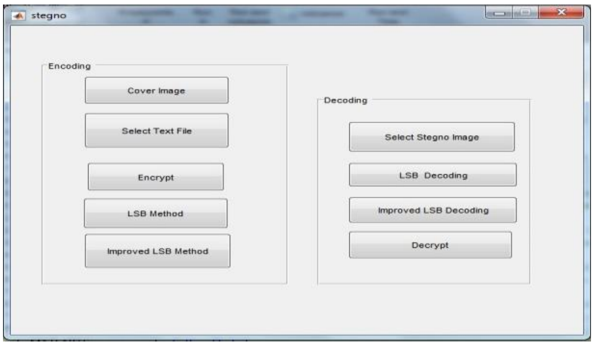

Fig. 4: Block use for initializing Stego image

Step wise explanation of this Decoding process is given below:

Step 6: Now select stegno image to decode the whole process

Step 7: Now select LSB Decoding and we will able to obtain a cover image

Step 8: In this step Improved LSB Decoding and we will able to obtain a cover image.

Step 9: This is the final step through which we are able to decrypt data from the setgno image and got the final data.

Fig. 5: Stego image

Fig. 6: LSB Decode image

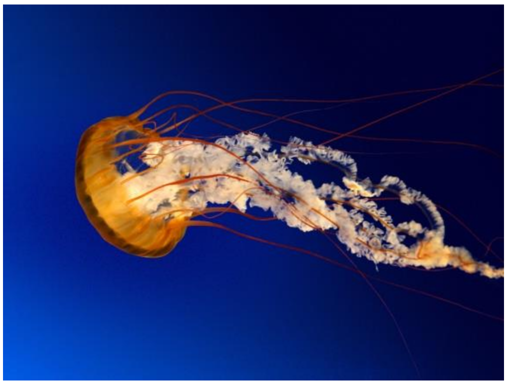

Fig. 7: Cover Image

Finally, here we got decrypted data using symmetric XOR decryption

2. CONCLUSION

- We have developed the system which can embed an image or text into the image.
- Developed an algorithm that can extract the hidden message that can be in the form of image or text from the image.
- We develop the algorithm for encoding and decoding using LSB and random Improved LSB techniques.
- In this paper perform the various test cases for the system using different images and different types of text and image messages.
- Evaluate the performance of the existing system.

3. REFERENCES

[1] Feng, J.B., Lin, I.C., Tsai, C.S., Chu, Y.P., “Reversible watermarking: current status and key issues”, International Journal of Network Security, 2006.
[2] David Salomon, "Data Compression, the complete reference 4th ed.", Springer
[3] Liao, Z., Huang, Y., Li, C., “Research on data hiding capacity”, International Journal of Network Security, 2007.
[4] J. Harmsen and W. Pearlman, “Steganalysis of additive noise modelable information hiding”, in Proc. SPIE Security Watermarking Multimedia Contents, 2003.
[5] T. Sharp, “An implementation of key-based digital signal steganography”, in Proc. Information Hiding Workshop, Springer LNCS, 2001.
[6] R. R. Ahirwal, D. Ahirwal, and Y. K. Jain, “A High Capacitive and Confidentiality Based Image Steganography using Private stego-key”, in Proc. of the International Conference on Information Science and Applications, Chennai, India, 2010.
[7] Shila P. Hivrale, S. D. Sawarkar, Vijay Bhosale, and Seema Koregaonkar, “Statistical Method for Hiding Detection in LSB of Digital Images: An Overview”, Proceedings of world academy of science, engineering and technology, 2008.
[8] H. Zhang, G. Geng, and C. Xiong, “Image Steganography using Pixel-Value Differencing,” Second International Symposium on Electronic Commerce and Security, 2009.
[9] Mehdi Hussain, Mureed Hussain, “Pixel Intensity Based High Capacity Data Embedding Method”, IEEE, 2010.
[10] H.B. Kekre, Archana Athawale, Pallavi N. Halarnkar “Performance Evaluation of Pixel Value Differencing and Kekre’s Modified Algorithm for Information Hiding in Images”, International Conference on Advances in Computing, Communication and Control, 2009.
[11] “Lempel–Ziv–Welch” “wikipedia.org”, available at: http://en.wikipedia.org/wiki/LZW
[12] LZW compression “cvisiontech.com”, available at: http://www.cvisiontech.com/file-formats/pdf/lzw-compression.html