MODIFICATION IN LSB METHOD OF IMAGE BASED STEGANOGRAPHY

*InduNehra, Student(M.Tech), RCEW, Jaipur
*Aishwary, Assistant Professor, RCEW Jaipur

ABSTRACT:LSB is well know method for stegnography. There are several changes suggested by different researchers time to time on LSB and stegnography. Most of the methods are by using enryption and in decryption of the message in different ways. This paper proposes the java APIs for encoding and decoding of messages which is to be staged.

Keywords: Stegnography, image based steganography, Efficiency consideration in LSB method, image encoding algorithm, image decoding algorithm.

I. INTRODUCTION

The proposed method is using very compact and effective APIs of java for implementation and understanding of encryption and decryption which is given in javax.crypto package.

Efficiency Considerations

Which working with the concept of LSB, three main issues which needs to be covered for efficiency and security of message which is hidden in the image.

- **Storing length of message: As per most of the references, the length is stored in first 31 pixels and data is stored in next each pixel. This is the general idea. So a malicious user can retrieve the first step of message by first 31 pixels.**

- **Storing message: After the length, the data is being stored in each pixel which can be easily retrieved by any malicious**

The proposed method is the optimization of the steganography method of LSB and they which is LSB and they uses of Java Cryptography APIs of Java. Now the latest version of java we have base64 method for encoding and decoding.

The proposed method is the optimization of the steganography method of LSB and they which is LSB and they uses of Java Cryptography APIs of Java. Now the latest version of java we have base64 method for encoding and decoding.

for encryption and decryption.

A lots of researchers have worked on concept of LSB. Some of them have designed good algorithm. But a very few number of researchers have taken it to implementation level. Our focus of the work was to implement one of the best models, in which the data can be moved in secure and safe way. We tried to study various language specifications. Java has implemented one of the best security model so we used java security for designing t**he tool.**

user. We had idea of hide the message not in continuous pixel, this might be stored in even pixels or odd pixels or any arbitrary order like every 3th pixel. Its dependent on the size of message to be hidden behind the image. Also the pixel number can be retrieved dynamically by size of images and size of messages.

- Encoding messages: The first concen of study was to make message more and more secure. Any malicious user can retrieve the data easily if the structure of storage of message is known. So one more thought was to given on security of data/message.

We found that data should be stored in LSB after encryption so that this will be next layer of security. If working with java, java provides a good set of classes in package javax.crypto for encryption and decryption.

In the modified method following changes can be proposed:

- For better image after embedding of message, we used alternative pixel for storing the message. If each message is being stored in each pixel, the image quality degrades so we stored each bit of message in even or odd number of pixel. Like first bit will be stored in 12^{nd} pixel and then next bit to 14^{th} pixel and so on.

- For security of data, length is stored in some random pixel in the image. As per given in most of the standards, length is being stored in first 32 pixels which can easily be retrieved by any of the person for misuse. So we have used concepts that length is to be stored in any of the arbitrary location which is known only to sender and receiver. Agreed upon protocol will work and embed/decode the message accordingly

- Also for security of data, message can be encrypted by using java cryptography APIs which are available in javax.crypto package. So that the retrieval of exact message will be more tougher. The same is done by reverse at receiver end.

Comparison of Standard LSB method and Proposed Method

Standard LSB Method	**Our LSB Method**
Using sequence pixel of Cover Image.	Using Random pixel of Cover Image.
Message length is stored in first 31 bytes which is common and not safe.	Message length is stored in any arbitrary location.
Store 3 byte information per pixel	Store 1 byte information per pixel which will improve the result
Stego image looks almost same as the cover image.	Stego image looks same as the cover image, Better than Standard LSB.
The location of message in pixels are same	The location can be defined on the basis size of message to be embedded in the image

Image Encoding Algorithm in proposed method

Inputs: Hidden Message, Stego key and Cover Image

Output: Stego Image

Procedure

Step 1 calculate length of message and hide length in any 32-bit.

Step 2 extract the characters of Message.

Step 3 Encrypt message by using javax.crypto APIs.

Step 4 extract characters from stegokey .

Step 5 calculate pixel value from Cover Image.

Step 6 select LSB bit from pixel and select stego key characters and put into Image pixel.

Step 7 insert characters of message in pixels of Image.

Step 8 repeatestep 6 until characters has been embedded.

Step 9 repeatestep from 2 to 7 messsage length.

Step 10 output in Stego image.

Image Decoding Algorithm in proposed method

Inputs: Stego Image and Stego key

Output: Cover Image and Message

Procedure

Step 1 calculate length of message from given 32-bit pixel.

Step 2 extract pixels from Stego Image.

Step 3 start from 32 pixel and extract stego key characters from first component of the pixels..

Step 4 If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program.

Step 5 If the key is correct, then go to next pixels and extract secret message characters from first component of next pixels. Follow Step 5 till up to terminating symbol, otherwise follow step 6.

Step 6 extract Characters from Stego Image.

Step 7 extract special bit from Characters.

Step 8 obtain message by decrypting using javax.crypto classes and Cover Image.

REFERENCES

- Ali-al, H. Mohammad, A. 2010. Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition, European Journal Of Scientific Research, vol 39(1), pp 231-239.

- Aneesh Jain, IndranilSen Gupta, ―A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images‖, TENCON 2007 - 2007 IEEE Region 10 Conference, vol.2
- Atallah M. Al-Shatnawi, "A New Method in Image ste-ganography with improved image quality", Applied mathe-matical science, Vol. 6, no79, 2012.

- A.Joseph Raphael et al(2012), Cryptography and Steganography – A Survey, Int. J. Comp. Tech. Appl., Vol 2 (3) pp 626-630

- BassamJamilMohd, Saed Abed and Thaier Al- Hayajneh, Computer Engineering Department Hashemite University, Zarqa, Jordan Sahel Alouneh,ComputerEngi-neering Department, German-Jordan University, Amman, Jordan, "FPGA Hardware of the LSB Steganography Meth-od" IEEE 2012.

- CHIN-CHEN CHANG, , H.W .TSENG. ,"A steganographic method for digital images using side match. Pattern Recognition Letters, 2004,vol. 25, p.1431-1437.
- Himanshu Gupta et al(2013), Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method, International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6 pp 212-214

- MamtaJuneja (2013), An Improved LSB based Steganography Technique for RGB Color Images, 2nd International Conference on Latest Computational Technologies (ICLCT'2013) June 17-18

- MasoudNosrati(2013), An introduction to steganography methods, World Applied Programming, Vol (1), No (3) pp 191-195

- Mehdi Kharrazi, Husrev T. Sencar, and NasirMemon,, Image Steganography and: Concepts and Practice", Depart-ment of Electrical and Computer Engineering Department of Computer and Information Science Polytechnic Universi-ty,Brooklyn, NY 11201, USA.
- Mrs. Kavitha, KavitaKadam, AshwiniKoshti, PriyaDunghav, "Steganography Using Least Significant Bit Algo-rithm", International Journal of Engineering Research and applications, vol.2, issue 3, pp. 338-341May-June2012.
- Nagham Hamid, AbidYahya, R. Badlishah Ahmad, Osamah M, "Image Steganography Techniques: An Over-view", International Journal of computer science and securi-ty, vol (6), Issue (3), 2012.

- R. Amirtharajan, R. Akila, P. Deepikachowdavarapu "A Comparative Analysis of Image Steganogra-phy",International Journal of computer Applications,Vol2- No3, May 2010.
- Shamim Ahmed Laskar(2012), High Capacity data hiding using LSB Steganography and Encryption, International Journal of Database Management Systems (IJDMS) Vol.4, No.6,

- SaeedMahmoudpour, SattarMirzakuchaki,"Hardware Architecture for a Message Hiding Algorithm with Novel Randomizers", International Journal of Computer Applica-tions (0975 – 8887) Volume 37– No.7, January 2012.

- Vijay kumarsharma, Vishal Shrivastava, "A Steganog-raphy algorithm for hiding image in image by improved LSB substitution by minimize technique", Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, 15th February 2012.
- Java.oracle.com
- https://www.scribd.com/doc/48764974/Steganography-Data-hiding-using-LSB-algorithm