International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 527-534
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Secret Data Hiding Using Image Segmentation and Least Significant BIT (LSB) Insertion Steganography

[1]Neethu Natarajan, [2]Teena Jose and [3]Suvanam Sasidhar Babu

[1]Dept. of Computer Science and Engineering,
SNGCE, Kadayiruppu, Ernakulam (Dt.),
Kerala, India.

[2]Dept. of Computer Science,
Bharathiar University, Coimbatore.

[3]Dept. of Computer Science and Engineering,
SNGCE, Kadayiruppu, Ernakulam Dt.,
Kerala India.

Abstract

In this paper secret data hided inimage segments using least significant bit (LSB) steganography is proposed. The color image is divided into four equal parts and the secret data is also divided into four equal parts and those divided data is hided in the image segments using least significant bit steganography. Data hiding is done using color channels in the color image.

Index Terms: Steganography, least significant bit(LSB), color channels, image segmentation.

1. Introduction

Internet has a special role in our daily life because its helps us to connect to the each and every corner of this world. We can communicate through this medium within seconds, and we transfer datas through this medium. Those datas may be confidential or not, but the communication is not secure. Because anyone can monitor our data that pass through the internet so weak security is a big problem in e-communication. So we are using a method known as Steganography, which hides data in a carrier medium. In this work we are using color image as carrier medium. The advantage of using steganography is anyone can view the image which is used as carrier medium but the authorized person can only extract the secret data embedded in the image. We can hide the data in the color image without making any changes to the actual color image. So third party doesn't even know that the secret data is hided in the color image.

This approach is mainly divided into two steps one is embedding and other is extraction [2].The widely used algorithm in steganography is the least significant bit insertion algorithm [2, 6-9]. This algorithm work on color images by using the three color channels. The eight bits are divided into three bits in red color channel, three bits in green color channel and two bits in the blue color channel with many variations of the sequence used [6-9].

This system is very secure than ordinary LSB approach because the bits ordering is used in the method is needed for decoding those datas from the carrier. so third party cannot decode those data without knowing the bits ordering.

This paper is organized as follows: the proposed approach is presented in the next section then the conclusion part followed by relevant references.

2. Proposed System

The proposed system has two main algorithms one is embedding algorithm and other is extracting algorithm.

These two algorithms consists of different steps that shown below:

a) Embedding algorithm

Embedding algorithm is used to embed the secret data into the carrier color image using least significant bit insertion algorithm. The method is used for the purpose is shown in the below figure 2.1.

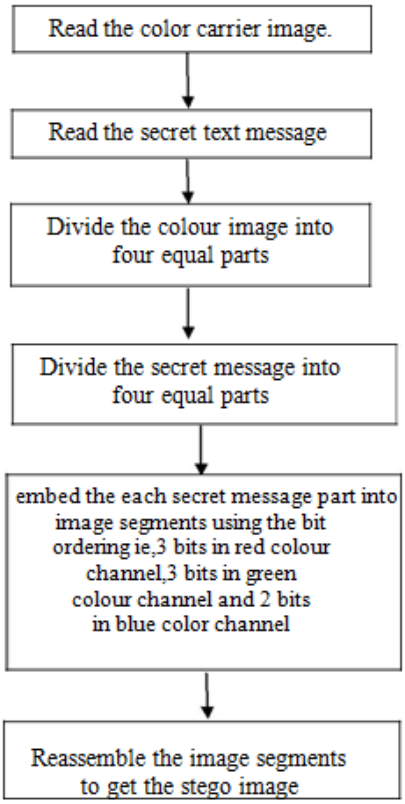

Fig. 2.1: Embedding Algorithm

b) Extraction Algorithm

Extraction algorithm is used to extract the secret data from the stego image using the same algorithm that is used for embedding .The method is used for the purpose is shown in the below figure 2.2.

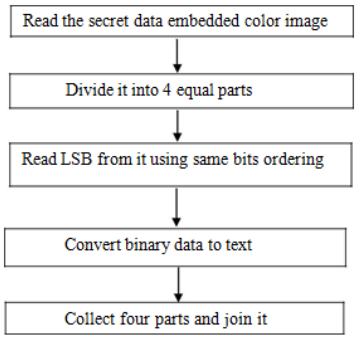

Fig. 2.2: Extraction Algorithm

3. Results

This method is implemented in Intel® core™i3 CPU with 4 GB Memory running with windows 7 operating system using MATLAB. The image used is an RGB color JPEG images with size 512 ×512, resolution 96 × 96 dpi and bit depth 24. Visualization results shown in the below figures, fig.3.1 shows the GUI of the approach

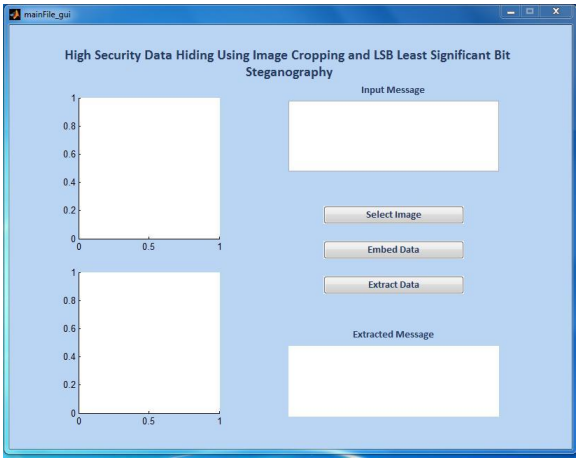

Fig. 3.1: GUI of the Method Proposed

First we read the color image using the button select image then we have to divide the image into four parts that shown in the below figure3.2:

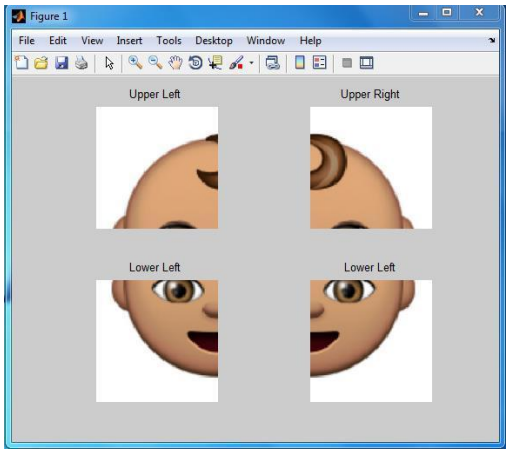

Fig. 3.2: Color Image is Divided into 4 Equal Parts

Then input the message and hided it in the image segments. That process is shown in the below figure.3.3:

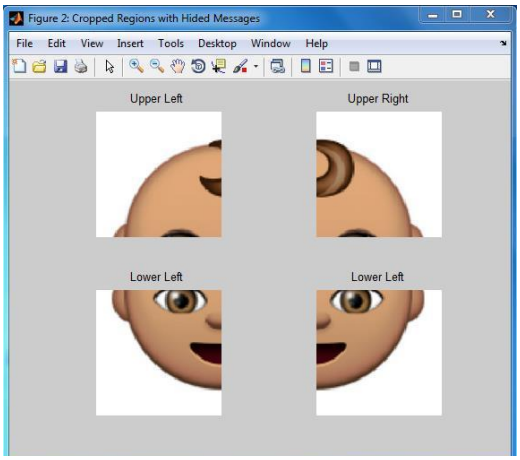

Fig. 3.3: Cropped Regions with Hided Messages

Then reassemble the segments and we get the stego image. The final GUI of our method is shown in fig.3.4:

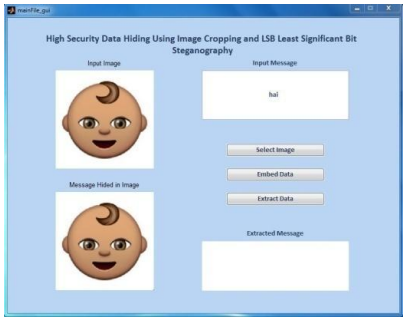

Fig. 3.4: After Reassembling the Stego Segments

Then we can extract the secret data using the extract button shown in the figure4.After extraction the result is shown in fig. 3.5:

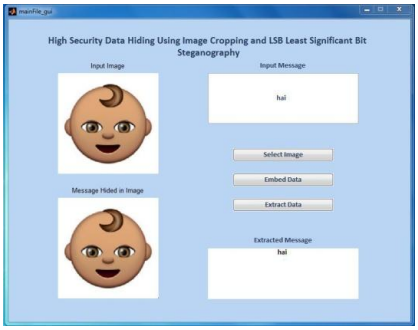

Fig. 3.5: After Extraction GUI of Proposed Method

4. Conclusion

This least significant bit insertion approach is highly secure than other traditional methods because the image is segmented and the secret text message is also segmented and the message is embedded into the color channels segments using a bits ordering. So unauthorized monitors cannot extract the data without knowing the ordering of bits. So the method is secure and more complex than other methods.

References

[1] Al-Afandy K.A., Faragallah O.S., Elmhalawy A., El-Rabaie, E.S.M., El-Banby G.M., High security data hiding using image cropping and LSB least significant bit steganography, 4th IEEE International Colloquium on Information Science and Technology (2016), 400-404.

[2] Jassim F.A., A novel steganography algorithm for hiding text in image using five modulus method, arXiv preprint arXiv 72 (17) (2013), 39-44.

[3] Bandyopadhyay D., Dasgupta K., Mandal J.K., Dutta P., A novel secure image steganography method based on Chaos theory in spatial domain, International Journal of Security, Privacy and Trust Management 3(1) (2014), 11-22.

[4] Jain N., Meshram S., Dubey S., Image Steganography Using LSB and Edge–Detection Technique, International Journal of Soft Computing and Engineering 2(3) (2012), 217-222.

[5] Rakhi, Vijay Prakash Singh, Data Hiding In Skin Tone of Images Using Steganography, International Journal of Electronics and Communication Engineering 2(4) (2014), 105-112.

[6] Goel S., Rana A., Kaur M., Comparison of image steganography techniques, International Journal of Computers and Distributed Systems 3(1) (213), 20-30.

[7] Lwin T., Suwai P., Information Hiding System Using Text and Image Steganography, International Journal of Scientific Engineering and Technology Research 3(4) (2014), 1972-1977.

[8] Vyas K., Pal B.L., A Proposed Method In Image Steganography To Improve Image Quality With LSB Technique, International Journal of Advanced Research in (2014), 5246-5251.

[9] Rawat D., Bhandari V., Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method, International Journal of Computer Applications 67(1) (2013), 22-25.

[10] Thiyagarajan P., Aghila G., Prasanna Venkatesan V., Stego-Image Generator (SIG)-Building Steganography Image Database, Advances in Digital Image Processing and Information Technology Springer Berlin Heidelberg (2011), 257-267.

[11] Doshi R., Jain P., Gupta L., Steganography and Its Applications in Security, International Journal of Modern Engineering Research 2(6) (2012), 4634-4638.

[12] RAJESH, M. "A SYSTEMATIC REVIEW OF CLOUD SECURITY CHALLENGES IN HIGHER EDUCATION." The Online Journal of Distance Education and e-Learning 5.4 (2017): 1.

[13] Rajesh, M., and J. M. Gnanasekar. "Protected Routing in Wireless Sensor Networks: A study on Aimed at Circulation." Computer Engineering and Intelligent Systems 6.8: 24-26.

[14] Rajesh, M., and J. M. Gnanasekar. "Congestion control in heterogeneous WANET using FRCC." Journal of Chemical and Pharmaceutical Sciences ISSN 974 (2015): 2115.

[15] Rajesh, M., and J. M. Gnanasekar. "Hop-by-hop Channel-Alert Routing to Congestion Control in Wireless Sensor Networks." Control Theory and Informatics 5.4 (2015): 1-11.

[16] Rajesh, M., and J. M. Gnanasekar. "Multiple-Client Information Administration via Forceful Database Prototype Design (FDPD)." IJRESTS 1.1 (2015): 1-6.

[17] Rajesh, M. "Control Plan transmit to Congestion Control for AdHoc Networks." Universal Journal of Management & Information Technology (UJMIT) 1 (2016): 8-11.

[18] Rajesh, M., and J. M. Gnanasekar. "Consistently neighbor detection for MANET." Communication and Electronics Systems (ICCES), International Conference on. IEEE, 2016.